aws

GuardDuty Amazon-Benutzerhandbuch

Amazon GuardDuty

Amazon GuardDuty: GuardDuty Amazon-Benutzerhandbuch

Table of Contents

Was ist Amazon GuardDuty?

Amazon GuardDuty ist ein Service zur Bedrohungserkennung, der kontinuierlich AWS Datenquellen und Protokolle in Ihrer AWS Umgebung überwacht, analysiert und verarbeitet. GuardDuty verwendet Threat-Intelligence-Feeds wie Listen bösartiger IP-Adressen und Domains, Datei-Hashes und Modelle für maschinelles Lernen (ML), um verdächtige und potenziell bösartige Aktivitäten in Ihrer AWS Umgebung zu identifizieren. Die folgende Liste bietet einen Überblick über potenzielle Bedrohungsszenarien, anhand derer Sie Folgendes erkennen GuardDuty können:

- Kompromittierte und exfiltrierte Anmeldeinformationen AWS .
- Exfiltration und Zerstörung von Daten, die zu einem Ransomware-Ereignis führen können. Ungewöhnliche Muster von Anmeldeereignissen in den unterstützten Engine-Versionen von Amazon Aurora und RDS Amazon-Datenbanken, die auf ein ungewöhnliches Verhalten hinweisen.
- Unautorisierte Cryptomining-Aktivitäten in Ihren Amazon Elastic Compute Cloud (AmazonEC2) -Instances und Container-Workloads.
- Vorhandensein von Malware in Ihren EC2 Amazon-Instances und Container-Workloads sowie neu hochgeladene Dateien in Ihren Amazon Simple Storage Service (Amazon S3) -Buckets.
- Ereignisse auf Betriebssystemebene, Netzwerk- und Dateiereignisse, die auf unberechtigtes Verhalten in Ihren Amazon Elastic Kubernetes Service (AmazonEKS) -Clustern, Amazon Elastic Container Service (AmazonECS) AWS Fargate (Fargate) -Aufgaben sowie EC2 Amazon-Instances und Container-Workloads hinweisen.

Was ist Amazon GuardDuty

Inhalt

Eigenschaften von GuardDuty

Im Folgenden finden Sie einige der wichtigsten Methoden, mit denen Amazon GuardDuty Sie bei der Überwachung, Erkennung und Verwaltung potenzieller Bedrohungen in Ihrer AWS Umgebung unterstützen kann.

Überwacht kontinuierlich bestimmte Datenquellen und Ereignisprotokolle

- Fundamentale Bedrohungserkennung — Wenn Sie GuardDuty in an aktivieren AWS-Konto, GuardDuty werden automatisch die grundlegenden Datenquellen aufgenommen, die mit diesem Konto verknüpft sind. Zu diesen Datenquellen gehören AWS CloudTrail Verwaltungsereignisse, VPC Flow-Logs (von EC2 Amazon-Instances) und DNS Logs. Sie müssen nichts anderes aktivieren, um mit der Analyse und Verarbeitung dieser Datenquellen zu beginnen und die zugehörigen Sicherheitsergebnisse zu generieren. GuardDuty Weitere Informationen finden Sie unter GuardDuty grundlegende Datenquellen.
- Auf den Anwendungsfall ausgerichtete GuardDuty Schutzpläne — Für einen besseren Einblick in die Sicherheit Ihrer AWS Umgebung bei der Erkennung von Bedrohungen GuardDuty bieten wir spezielle Schutzpläne, die Sie aktivieren können. Schutzpläne helfen Ihnen bei der Überwachung von Protokollen und Ereignissen anderer AWS Dienste. Zu diesen Quellen gehören EKS Auditprotokolle, RDS Anmeldeaktivitäten, Amazon S3 S3-Datenereignisse in CloudTrail, EBS Volumen, Runtime Monitoring in Amazon EKSEC2, Amazon und Amazon ECS -Fargate sowie Lambda-Netzwerkaktivitätsprotokolle. GuardDutyfasst diese Protokoll- und Ereignisquellen unter dem Begriff Funktionen zusammen. Sie können jederzeit einen oder mehrere spezielle Schutzpläne in AWS-Region einem unterstützten Paket aktivieren. GuardDuty beginnt mit der Überwachung, Verarbeitung und Analyse der Aktivitäten auf der Grundlage des von Ihnen aktivierten Schutzplans. Weitere Informationen zu den einzelnen Schutzplänen und ihrer Funktionsweise finden Sie im entsprechenden Schutzplandokument.

Schutzplan	Beschreibung
S3-Schutz	Identifiziert potenzielle Sicherheitsrisiken wie Datenexfi ltrations- und Zerstörungsversuche in Ihren Amazon S3 S3-Buckets.
EKSSchutz	EKSAudit Log Monitoring analysiert Kubernetes-Auditpr otokolle aus Ihren EKS Amazon-Clustern auf potenziell verdächtige und böswillige Aktivitäten.

Schutzplan	Beschreibung
Laufzeit-Überwachung	Überwacht und analysiert Ereignisse auf Betriebss ystemebene auf AmazonEKS, Amazon und Amazon ECS (einschließlich AWS Fargate)EC2, um potenzielle Laufzeitb edrohungen zu erkennen.
Malware-Schutz für EC2	Erkennt das potenzielle Vorhandensein von Malware, indem es die EBS Amazon-Volumes scannt, die Ihren EC2 Amazon-Instances zugeordnet sind. Es besteht die Möglichkeit, diese Funktion bei Bedarf zu nutzen.
Malware-Schutz für S3	Erkennt das potenzielle Vorhandensein von Malware in den neu hochgeladenen Objekten in Ihren Amazon S3 S3-Bucket s.
RDSSchutz	Analysiert und erstellt ein Profil Ihrer RDS Anmeldeak tivitäten im Hinblick auf potenzielle Zugriffsbedrohungen auf die unterstützten Amazon Aurora- und RDS Amazon-Da tenbanken.
Lambda Protection	Überwacht Lambda-Netzwerkaktivitätsprotokolle, beginnend mit VPC Flussprotokollen, um Bedrohungen für Ihre AWS Lambda Funktionen zu erkennen. Zu diesen potenziellen Bedrohungen gehören beispielsweise Cryptomining und die Kommunikation mit bösartigen Servern.

Aktivieren Sie den Malware-Schutz für S3 unabhängig

GuardDuty bietet die Flexibilität, Malware Protection for S3 unabhängig zu verwenden, ohne den GuardDuty Amazon-Service zu aktivieren. Weitere Informationen zu den ersten Schritten nur mit Malware Protection for S3 finden Sie unterGuardDuty Malware-Schutz für S3. Um alle anderen Schutzpläne nutzen zu können, müssen Sie den GuardDuty Dienst aktivieren.

Verwaltung einer Umgebung mit mehreren Konten

Sie können eine AWS Umgebung mit mehreren Konten verwalten, indem Sie entweder die AWS Organizations (empfohlene) oder die herkömmliche Einladungsmethode verwenden. Weitere Informationen finden Sie unter Verwalten mehrerer Konten.

Generiert Sicherheitsergebnisse für erkannte Bedrohungen

Wenn potenzielle Sicherheitsbedrohungen im Zusammenhang mit Ihren AWS Ressourcen GuardDuty erkannt werden, werden Sicherheitsergebnisse generiert, die Informationen über die potenziell gefährdete Ressource liefern. Generieren Sie nach GuardDuty der Aktivierung in Ihrem Konto, Beispielergebnisse um die zugehörigen Erkenntnisdetails Dateien anzuzeigen. Eine vollständige Liste der Sicherheitsergebnisse finden Sie unterErkenntnistypen.

Mit GuardDuty können Sie auch ein Testerskript verwenden, das spezifische GuardDuty Sicherheitserkenntnisse generiert, um zu verstehen, wie die GuardDuty Ergebnisse überprüft und darauf reagiert werden. Weitere Informationen finden Sie unter GuardDuty Testergebnisse in speziellen Konten.

Bewertung und Verwaltung von Sicherheitsergebnissen

GuardDuty konsolidiert Ihre Sicherheitsfeststellungen für alle Konten und zeigt die Ergebnisse im Übersichts-Dashboard auf der GuardDuty Konsole an. Sie können die Ergebnisse auch über AWS Security Hub API AWS Command Line Interface, oder AWS SDK abrufen. Mit einem ganzheitlichen Überblick über Ihren aktuellen Sicherheitsstatus können Sie Trends und potenzielle Probleme erkennen und die erforderlichen Abhilfemaßnahmen ergreifen. Weitere Informationen finden Sie unter Verwaltung der GuardDuty Ergebnisse.

Integrieren Sie es in verwandte AWS Sicherheitsdienste

Um Sie bei der Analyse und Untersuchung der Sicherheitstrends in Ihrer AWS Umgebung weiter zu unterstützen, sollten Sie die folgenden AWS sicherheitsbezogenen Services in Kombination mit in Betracht ziehen. GuardDuty

- AWS Security Hub— Dieser Service bietet Ihnen einen umfassenden Überblick über den Sicherheitsstatus Ihrer AWS Ressourcen und hilft Ihnen, Ihre AWS Umgebung anhand der Sicherheitsstandards und bewährten Verfahren der Branche zu überprüfen. Dies geschieht unter anderem dadurch, dass Ihre Sicherheitsergebnisse aus mehreren AWS Diensten (einschließlich Amazon Macie) und unterstützten AWS Partner Network (APN) -Produkten verarbeitet, aggregiert, organisiert und priorisiert werden. Security Hub hilft Ihnen dabei, Ihre Sicherheitstrends zu analysieren und die Sicherheitsprobleme mit der höchsten Priorität in Ihrer AWS Umgebung zu identifizieren.

Informationen zur gemeinsamen Verwendung von Security Hub GuardDuty und Security Hub finden Sie unterIntegration GuardDuty mit AWS Security Hub. Weitere Informationen zu Security Hub finden Sie im AWS Security Hub Benutzerhandbuch.

- Amazon Detective — Dieser Service hilft Ihnen dabei, Sicherheitslücken oder verdächtige Aktivitäten zu analysieren, zu untersuchen und schnell die Ursache zu identifizieren. Detective sammelt automatisch Protokolldaten von Ihren AWS Ressourcen. Es verwendet dann Machine Learning, statistische Analysen und die Diagrammtheorie, um Visualisierungen zu erstellen, mit denen Sie effektive Sicherheitsuntersuchungen schneller und effizienter durchführen können. Die vorgefertigten Datenaggregationen, Zusammenfassungen und Kontexte von Detective helfen Ihnen bei der Analyse und Bestimmung der Art und des Ausmaßes potenzieller Sicherheitsprobleme.

  Hinweise zur gemeinsamen Verwendung von GuardDuty und Detective finden Sie unterIntegration GuardDuty mit Amazon Detective. Weitere Informationen zu Detective finden Sie im Amazon Detective User Guide.
- Amazon EventBridge — Dieser Service hilft Ihnen, Benachrichtigungen zu erhalten und nahezu in Echtzeit auf GuardDuty Sicherheitslücken zu reagieren. GuardDutyerzeugt ein Ereignis, wenn sich die Ergebnisse ändern. Sie können wählen, von wie oft Sie die Benachrichtigungen erhalten möchten EventBridge. Weitere Informationen finden Sie unter Was ist Amazon EventBridge im EventBridge Amazon-Benutzerhandbuch.

PCIDSSEinhaltung der Vorschriften

GuardDuty unterstützt die Verarbeitung, Speicherung und Übertragung von Kreditkartendaten durch einen Händler oder Dienstleister und wurde als konform mit dem Payment Card Industry (PCI) Data Security Standard (DSS) validiert. Weitere Informationen zum AWS PCI Compliance-Paket PCIDSS, einschließlich der Beantragung einer Kopie, finden Sie unter PCIDSSStufe 1.

Weitere Informationen finden Sie im AWS Sicherheitsblog unter Neuer Drittanbietertest vergleicht Amazon GuardDuty mit Systemen zur Erkennung von Netzwerkeindringlingen.

Preisgestaltung in GuardDuty

Kostenloses AWS-Kontingent hilft Ihnen dabei, die einzelnen Dienste bis zu den angegebenen Limits kostenlos zu erkunden und auszuprobieren AWS -Services . Es gibt drei Kategorien: 12 Monate kostenlose, immer kostenlose und kurzfristige kostenlose Testversionen. Amazon GuardDuty gehört

zur Kategorie der kurzfristigen kostenlosen Testversionen und bietet eine kostenlose 30-Tage-Testversion an. Wenn Sie die Nutzung GuardDuty nach Ablauf dieser kostenlosen Testversion fortsetzen, fallen je nachdem, wie Sie diesen Service nutzen, Kosten an.

Malware-Scan auf Abruf (unter Malware-Schutz fürEC2) und Malware-Schutz für S3 fallen nicht in die Kategorie der kostenlosen GuardDuty 30-Tage-Testversion. Malware Protection for S3 fällt in die Kategorie der kostenlosen 12-monatigen Tests, Kostenloses AWS-Kontingent wohingegen der On-Demand-Malware-Scan einem pay-as-you-use Kostenmodell folgt. Es gibt weder eine kostenlose 30-Tage-Testversion noch ein 12-monatiges kostenloses Kontingent mit Malware-Scan auf Abruf. Weitere Informationen finden Sie unter GuardDuty Preise.

Verwenden Sie die kostenlose GuardDuty 30-Tage-Testversion

Wenn Sie es GuardDuty zum ersten Mal in einer verwenden AWS-Region, werden Sie AWS-Konto automatisch für eine kostenlose 30-Tage-Testversion in dieser Region registriert. Einige der Schutzpläne werden ebenfalls automatisch aktiviert und sind in der kostenlosen 30-Tage-Testversion enthalten. Da es GuardDuty sich um einen regionalen Dienst handelt, erhalten Sie für Ihr Konto bei der ersten Aktivierung in einer anderen Region eine kostenlose 30-Tage-Testversion GuardDuty und einige unterstützte Schutzpläne in dieser Region.

Wenn Sie mit mehreren Konten in einer GuardDuty Organisation arbeiten, erhält jedes Konto eine eigene kostenlose 30-Tage-Testversion GuardDuty und Schutzpläne.

Die folgende Tabelle zeigt, welche Schutzpläne automatisch aktiviert werden, wenn Sie sie GuardDuty zum ersten Mal aktivieren.

Schutzplan	In der kostenlosen GuardDuty 30-Tage-Testversion enthalten	Hat eine eigene kostenlose 30-Tage-Testversion [1]	
EKSSchutz	Ja	Ja	
Lambda Protection	Ja	Ja	
Malware-Schutz für EC2 – GuardDuty-hat einen Malware-Scan initiiert	Ja	Ja	

Schutzplan	In der kostenlosen GuardDuty 30-Tage-Testversion enthalten	Hat eine eigene kostenlose 30-Tage-Testversion [1]	
Malware-Schutz für EC2 – Malware-Scan auf Abruf	Nein	Nein	
GuardDuty Malware-Schutz für S3	Nein	Nein	
RDSSchutz	Ja	Ja	
Laufzeit-Überwachung	Nein	Ja	
S3-Schutz	Ja	Ja	

[1] Für jeden Schutzplan gibt es eine eigene kostenlose Testversion. Wenn Sie beispielsweise einen Schutzplan aktivieren, nachdem die kostenlose GuardDuty 30-Tage-Testversion für Ihr Konto abgelaufen ist und ein neuer Schutzplan veröffentlicht wird, können Sie diesen Schutzplan mit einer eigenen kostenlosen Testversion aktivieren. Weitere Informationen zu kostenlosen Testversionen für Schutzpläne finden Sie in dem Dokument, das zu den einzelnen Schutzplänen gehört.

Geschätzte Nutzungskosten während der kostenlosen Testversion anzeigen — Während der kostenlosen 30-Tage-Testversion GuardDuty und möglicherweise eines Schutzplans werden die GuardDuty geschätzten Nutzungskosten für Ihr Konto angezeigt. Wenn Sie ein delegiertes GuardDuty Administratorkonto haben, können Sie die geschätzten Gesamtkosten für die Nutzung und die Aufschlüsselung auf Kontoebene für alle Mitgliedskonten, die aktiviert wurden, einsehen. GuardDuty Weitere Informationen finden Sie unter Schätzung der Kosten GuardDuty .

Nutzungskosten nach Ablauf der kostenlosen Testphase — Wenn Sie nach Ablauf der kostenlosen Testphase einen der Schutzpläne weiterhin nutzen GuardDuty , fallen für Sie die entsprechenden Nutzungskosten an. Um Ihre Rechnung einzusehen, navigieren Sie in der https://console.aws.amazon.com/billing/Konsole zum Cost Explorer. Weitere Informationen zur AWS Kontoabrechnung finden Sie im AWS Billing Benutzerhandbuch.

Nutzung des Malware-Schutzes für S3 mit einem kostenlosen Nutzungskontingent für 12 Monate

Malware Protection for S3 verwendet ein kostenloses Kontingent für Ihr Abonnement AWS-Konten , das entweder neu ist, über ein laufendes kostenloses Kontingent oder ein abgelaufenes 12-monatiges kostenloses Kontingent verfügt. Weitere Informationen finden Sie unter Preise für Malware Protection for S3.

Zugreifen GuardDuty

Sie können es GuardDuty auf eine der folgenden Arten verwenden:

GuardDuty Konsole

https://console.aws.amazon.com/guardduty/

Die Konsole ist eine browserbasierte Oberfläche für den Zugriff und die Verwendung GuardDuty. Die GuardDuty Konsole bietet Zugriff auf Ihr GuardDuty Konto, Ihre Daten und Ressourcen.

AWS Befehlszeilentools

Mit AWS Befehlszeilentools können Sie Befehle an der Befehlszeile Ihres Systems ausgeben, um GuardDuty Aufgaben und AWS Aufgaben auszuführen. Die Befehlszeilen-Tools können auch beim Erstellen von Skripts für Aufgaben hilfreich sein.

Informationen zur Installation und Verwendung AWS CLI finden Sie im AWS Command Line Interface Benutzerhandbuch. Die verfügbaren AWS CLI Befehle für GuardDuty finden Sie in der CLIBefehlsreferenz.

GuardDuty HTTPS API

Sie können AWS programmgesteuert mit dem darauf zugreifen GuardDuty GuardDuty HTTPSAPI, sodass Sie HTTPS Anfragen direkt an den Dienst richten können. Weitere Informationen finden Sie in der GuardDuty API Referenz.

AWS SDKs

AWS bietet Softwareentwicklungskits (SDKs), die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen bestehen (Java, Python, Ruby,. NET, iOS, Android und mehr). SDKsSie bieten eine bequeme Möglichkeit, programmatischen Zugriff auf zu GuardDuty erstellen. Informationen zu den AWS SDKs, einschließlich deren Download und Installation, finden Sie unter Tools für Amazon Web Services.

Konzepte und Terminologie

Wenn Sie mit Amazon beginnen GuardDuty, können Sie davon profitieren, mehr über die wichtigsten Konzepte zu erfahren.

Account

Ein Standardkonto von Amazon Web Services (AWS), das Ihre AWS Ressourcen enthält. Sie können sich AWS mit Ihrem Konto anmelden und es aktivieren GuardDuty.

Sie können auch andere Konten einladen, Ihr AWS Konto zu aktivieren GuardDuty und mit diesem verknüpft zu werden GuardDuty. Wenn Ihre Einladungen akzeptiert werden, wird Ihr Konto als GuardDuty Administratorkonto festgelegt und die hinzugefügten Konten werden zu Ihren Mitgliedskonten. Sie können dann die GuardDuty Ergebnisse dieser Konten in ihrem Namen einsehen und verwalten.

Benutzer des Administratorkontos können die GuardDuty Ergebnisse für ihr eigenes Konto und alle ihre Mitgliedskonten konfigurieren GuardDuty , einsehen und verwalten. Sie können bis zu 10.000 Mitgliedskonten anlegen GuardDuty.

Benutzer von Mitgliedskonten können die GuardDuty Ergebnisse in ihrem Konto konfigurieren GuardDuty sowie einsehen und verwalten (entweder über die GuardDuty Verwaltungskonsole oder GuardDuty API). Benutzer von Mitgliedskonten können keine Ergebnisse in den Konten anderer Mitglieder anzeigen oder verwalten.

Ein Konto AWS-Konto kann nicht gleichzeitig ein GuardDuty Administratorkonto und ein Mitgliedskonto sein. An AWS-Konto kann nur eine Mitgliedschaftseinladung annehmen. Das Annehmen einer Mitgliedschaftseinladung ist optional.

Weitere Informationen finden Sie unter Verwaltung mehrerer Konten bei Amazon GuardDuty.

Detektor

Amazon GuardDuty ist ein regionaler Service. Wenn Sie eine bestimmte Option aktivieren GuardDuty AWS-Region, AWS-Konto wird Ihnen eine Melder-ID zugewiesen. Diese 32-stellige alphanumerische ID ist einzigartig für Ihr Konto in dieser Region. Wenn Sie beispielsweise GuardDuty für dasselbe Konto in einer anderen Region aktivieren, wird Ihr Konto mit einer anderen Melder-ID verknüpft. Das Format von a detectorId ist`12abc34d567e8fa901bc2d34e56789f0`.

Alle GuardDuty Ergebnisse, Konten und Aktionen im Zusammenhang mit der Verwaltung von Ergebnissen und dem GuardDuty Service verwenden die Detector-ID, um einen API Vorgang auszuführen.

Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite Einstellungen oder führen Sie den aus ListDetectorsAPI.

> **Note**
>
> In Umgebungen mit mehreren Konten werden alle Erkenntnisse für Mitgliedskonten zum Detektor des Administratorkontos weitergeleitet.

Einige GuardDuty Funktionen werden über den Detektor konfiguriert, z. B. die Konfiguration der Häufigkeit von Benachrichtigungen über CloudWatch Ereignisse und die Aktivierung oder Deaktivierung optionaler Schutzpläne für GuardDuty die Verarbeitung.

Verwenden Sie den Malware-Schutz für S3 innerhalb GuardDuty

Wenn Sie Malware Protection for S3 in einem Konto aktivieren, auf dem diese Option aktiviert GuardDuty ist, werden die Aktionen von Malware Protection for S3 wie das Aktivieren, Bearbeiten und Deaktivieren einer geschützten Ressource nicht mit der Detektor-ID verknüpft.

Wenn Sie die Bedrohungserkennungsoption Malware Protection for S3 nicht aktivieren GuardDuty und auswählen, wird keine Detektor-ID für Ihr Konto erstellt.

Grundlegende Datenquellen

Der Ursprung oder Speicherort eines Datensatzes. Um eine nicht autorisierte oder unerwartete Aktivität in Ihrer AWS Umgebung zu erkennen. GuardDuty analysiert und verarbeitet Daten aus AWS CloudTrail Ereignisprotokollen, AWS CloudTrail Verwaltungsereignissen, AWS CloudTrail Datenereignissen für S3, VPC Ablaufprotokollen, DNS Protokollen, siheGuardDuty grundlegende Datenquellen.

Merkmal

Ein für Ihren GuardDuty Schutzplan konfiguriertes Feature-Objekt hilft dabei, unbefugte oder unerwartete Aktivitäten in Ihrer AWS Umgebung zu erkennen. Jeder GuardDuty Schutzplan konfiguriert das entsprechende Featureobjekt für die Analyse und Verarbeitung von Daten. Zu den Featureobjekten gehören EKS Audit-Logs, RDS Login-Aktivitätsüberwachung, Lambda-

Netzwerkaktivitätsprotokolle und EBS Volumes. Weitere Informationen finden Sie unter Funktionen Aktivierung in GuardDuty.

Erkenntnis

Ein von GuardDuty erkanntes potenzielles Sicherheitsrisiko. Weitere Informationen finden Sie unter Die GuardDuty Ergebnisse von Amazon verstehen.

Die Ergebnisse werden in der GuardDuty Konsole angezeigt und enthalten eine detaillierte Beschreibung des Sicherheitsproblems. Sie können Ihre generierten Ergebnisse auch abrufen, indem Sie die ListFindingsAPIOperationen GetFindingsund aufrufen.

Sie können Ihre GuardDuty Ergebnisse auch über Amazon CloudWatch Events einsehen. GuardDuty sendet Ergebnisse CloudWatch per HTTPS Protokoll an Amazon. Weitere Informationen finden Sie unter Erstellen von benutzerdefinierten Antworten auf GuardDuty Erkenntnisse mit Amazon CloudWatch Events.

IAMRolle

Dies ist die IAM Rolle mit den erforderlichen Berechtigungen, um das S3-Objekt zu scannen. Wenn das Markieren gescannter Objekte aktiviert ist, helfen die IAM PassRole Berechtigungen dabei, dem gescannten Objekt Tags GuardDuty hinzuzufügen.

Ressource des Malware-Schutzplans

Nachdem Sie den Malware-Schutz für S3 für einen Bucket aktiviert haben, GuardDuty wird die Ressource „Malware-Schutz für den EC2 Plan“ erstellt. Diese Ressource ist mit der Paket-ID von Malware EC2 Protection for verknüpft, einer eindeutigen Kennung für Ihren geschützten Bucket. Verwenden Sie die Ressource des Malware-Schutzplans, um API Operationen an einer geschützten Ressource durchzuführen.

Geschützter Bucket (geschützte Ressource)

Ein Amazon S3 S3-Bucket gilt als geschützt, wenn Sie Malware Protection for S3 für diesen Bucket aktivieren und sein Schutzstatus auf Aktiv geändert wird.

GuardDuty unterstützt nur einen S3-Bucket als geschützte Ressource.

Schutzstatus

Der Status, der mit der Ressource Ihres Malware-Schutzplans verknüpft ist. Nachdem Sie Malware Protection for S3 für Ihren Bucket aktiviert haben, gibt dieser Status an, ob Ihr Bucket korrekt eingerichtet ist oder nicht.

S3-Objektpräfix

In einem Amazon Simple Storage Service (Amazon S3) -Bucket können Sie Präfixe verwenden, um Ihren Speicher zu organisieren. Ein Präfix ist eine logische Gruppierung der Objekte in einem S3-Bucket. Weitere Informationen finden Sie unter Objekte organisieren und auflisten im Amazon S3 S3-Benutzerhandbuch.

Scan-Optionen

Wenn GuardDuty Malware Protection for aktiviert EC2 ist, können Sie angeben, welche EC2 Amazon-Instances und Amazon Elastic Block Store (EBS) -Volumes gescannt oder übersprungen werden sollen. Mit dieser Funktion können Sie die vorhandenen Tags, die Ihren EC2 Instances und Ihrem EBS Volume zugeordnet sind, entweder zu einer Liste mit Einschluss-Tags oder einer Ausschluss-Tag-Liste hinzufügen. Die Ressourcen, die mit den Tags verknüpft sind, die Sie zu einer Liste mit Einschlusstags hinzufügen, werden auf Malware gescannt, und die Ressourcen, die zu einer Ausschlusstag-Liste hinzugefügt wurden, werden nicht gescannt. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.

Aufbewahrung von Schnappschüssen

Wenn GuardDuty Malware Protection for aktiviert EC2 ist, besteht die Möglichkeit, die Snapshots Ihrer EBS Volumes in Ihrem AWS Konto aufzubewahren. GuardDuty generiert die EBS Replikat-Volumes auf der Grundlage der Snapshots Ihrer Volumes. EBS Sie können die Snapshots Ihrer EBS Volumes nur dann behalten, wenn der Malware-Schutz für den EC2 Scan Malware in den Replikat-Volumes erkennt. EBS Wenn in den EBS Replikat-Volumes keine Malware erkannt wird, GuardDuty werden die Snapshots Ihrer EBS Volumes unabhängig von der Aufbewahrungseinstellung für Snapshots automatisch gelöscht. Weitere Informationen finden Sie unter Snapshot-Beibehaltung.

Regel zur Unterdrückung

Unterdrückungsregeln ermöglichen die Einrichtung sehr spezifischer Kombinationen von Attributen, um Ergebnisse zu unterdrücken. Sie können beispielsweise mithilfe des GuardDuty Filters eine Regel definieren, um nur die Instanzen automatisch zu archivieren`Recon:EC2/Portscan`, die in einem bestimmtenVPC, einem bestimmten AMI Tag oder mit einem bestimmten EC2 Tag ausgeführt werden. Diese Regel würde dazu führen, dass Port-Scan-Ergebnisse von den Instances automatisch archiviert werden, die die Kriterien erfüllen. Es ermöglicht jedoch weiterhin Warnmeldungen, wenn Instanzen GuardDuty entdeckt werden, die andere bösartige Aktivitäten wie das Mining von Kryptowährungen ausführen.

Die im GuardDuty Administratorkonto definierten Unterdrückungsregeln gelten für die Mitgliedskonten GuardDuty . GuardDuty Mitgliedskonten können die Unterdrückungsregeln nicht ändern.

Bei Unterdrückungsregeln werden GuardDuty trotzdem alle Ergebnisse generiert. Die Unterdrückungsregeln sorgen für eine Unterdrückung von Ergebnissen, während gleichzeitig ein vollständiger und unveränderlicher Verlauf aller Aktivitäten aufgezeichnet wird.

Gewöhnlich werden Unterdrückungsregeln verwendet, um Ergebnisse zu verbergen, die Sie als falsch positive Ergebnisse für Ihre Umgebung ermittelt haben, und um das Rauschen durch Ergebnisse mit niedrigem Wert zu reduzieren, sodass Sie sich auf größere Bedrohungen konzentrieren können. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Liste vertrauenswürdiger IPs

Eine Liste vertrauenswürdiger IP-Adressen für die hochsichere Kommunikation mit Ihrer AWS Umgebung. GuardDuty generiert keine Ergebnisse auf der Grundlage vertrauenswürdiger IP-Listen. Weitere Informationen finden Sie unter Arbeiten mit vertrauenswürdigen IP- und Bedrohungslisten.

Liste der bedrohlichen IP-Adressen

Eine Liste bekannter böswilliger IP-Adressen. Generiert nicht nur Ergebnisse aufgrund einer potenziell verdächtigen Aktivität, GuardDuty sondern generiert auch Ergebnisse auf der Grundlage dieser Bedrohungslisten. Weitere Informationen finden Sie unter Arbeiten mit vertrauenswürdigen IP- und Bedrohungslisten.

Erste Schritte mit GuardDuty

Dieses Tutorial bietet eine praktische Einführung in. GuardDuty Die Mindestanforderungen für die Aktivierung GuardDuty als eigenständiges Konto oder als GuardDuty Administrator mit AWS Organizations werden in Schritt 1 behandelt. Die Schritte 2 bis 5 behandeln die Verwendung zusätzlicher Funktionen, die von empfohlen werden GuardDuty , um das Beste aus Ihren Ergebnissen herauszuholen.

Themen

Bevor Sie beginnen

GuardDuty ist ein Dienst zur Bedrohungserkennung, der GuardDuty grundlegende Datenquellen beispielsweise AWS CloudTrail Ereignisprotokolle, AWS CloudTrail Verwaltungsereignisse, Amazon VPC Flow Logs und DNS Protokolle überwacht. GuardDuty analysiert auch Funktionen, die mit seinen Schutztypen verknüpft sind, nur wenn Sie sie separat aktivieren. Zu den Funktionen gehören Kubernetes-Auditprotokolle, RDS Anmeldeaktivitäten, S3-Protokolle, EBS Volumes, Laufzeitüberwachung und Lambda-Netzwerkaktivitätsprotokolle. Durch die Verwendung dieser Datenquellen und Funktionen (falls aktiviert) werden Sicherheitsergebnisse für Ihr Konto GuardDuty generiert.

Nach der Aktivierung beginnt GuardDuty es mit der Überwachung Ihrer Umgebung. Sie können GuardDuty die Option für jedes Konto in jeder Region jederzeit deaktivieren. Dadurch werden die grundlegenden Datenquellen und alle Funktionen, die separat aktiviert wurden, nicht mehr GuardDuty verarbeitet.

Sie müssen keine der GuardDuty grundlegende Datenquellen explizit aktivieren. Amazon GuardDuty bezieht unabhängige Datenströme direkt von diesen Diensten. Für ein neues GuardDuty Konto sind alle verfügbaren Schutzarten, die in einem unterstützt werden, AWS-Region standardmäßig

aktiviert und in der 30-tägigen kostenlosen Testphase enthalten. Sie können einen oder alle von ihnen deaktivieren. Wenn Sie bereits GuardDuty Kunde sind, können Sie wählen, ob Sie einige oder alle Schutzpläne aktivieren möchten, die in Ihrem AWS-Region Paket verfügbar sind. Weitere Informationen finden Sie unter Funktionen für die einzelnen Schutztypen in GuardDuty.

Beachten Sie bei der Aktivierung GuardDuty die folgenden Punkte:

- GuardDuty ist ein regionaler Dienst, was bedeutet, dass alle Konfigurationsverfahren, die Sie auf dieser Seite ausführen, in jeder Region, mit der Sie überwachen möchten, wiederholt werden müssen GuardDuty.

  Wir empfehlen dringend, die Aktivierung GuardDuty in allen unterstützten AWS Regionen durchzuführen. Auf diese Weise können GuardDuty auch in Regionen, die Sie nicht aktiv nutzen, Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten generiert werden. Dies ermöglicht auch GuardDuty die Überwachung von AWS CloudTrail Ereignissen für globale AWS Dienste wieIAM. Wenn diese Option nicht in allen unterstützten Regionen aktiviert GuardDuty ist, ist ihre Fähigkeit zur Erkennung von Aktivitäten, die globale Dienste betreffen, eingeschränkt. Eine vollständige Liste der Regionen, in denen GuardDuty es verfügbar ist, finden Sie unterRegionen und Endpunkte.
- Jeder Benutzer mit Administratorrechten in einem AWS Konto kann diese Option aktivieren GuardDuty. Gemäß der bewährten Sicherheitsmethode der geringsten Rechte wird jedoch empfohlen, eine IAM Rolle, einen Benutzer oder eine Gruppe zu erstellen, die GuardDuty speziell verwaltet werden soll. Informationen zu den für die Aktivierung erforderlichen Berechtigungen GuardDuty finden Sie unterErforderliche Berechtigungen zum Aktivieren von GuardDuty.
- Wenn Sie die GuardDuty Option zum ersten Mal in einer beliebigen AWS-Region Region aktivieren, werden standardmäßig auch alle verfügbaren Schutztypen aktiviert, die in dieser Region unterstützt werden, einschließlich Malware-Schutz fürEC2. GuardDuty erstellt eine dienstverknüpfte Rolle für Ihr Konto mit dem Namen. `AWSServiceRoleForAmazonGuardDuty` Diese Rolle umfasst die Berechtigungen und Vertrauensrichtlinien, die es ermöglichen, Ereignisse direkt aus GuardDuty dem zu verarbeiten und zu analysieren, GuardDuty grundlegende Datenquellen um daraus Sicherheitsresultate zu generieren. Malware Protection for EC2 erstellt eine weitere dienstbezogene Rolle für Ihr Konto mit dem Namen. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Diese Rolle umfasst die Berechtigungen und Vertrauensrichtlinien, die es Malware Protection for ermöglichen, Scans ohne Agenten EC2 durchzuführen, um Malware in Ihrem Konto zu erkennen. GuardDuty Sie ermöglicht es GuardDuty , einen EBS Volume-Snapshot in Ihrem Konto zu erstellen und diesen Snapshot mit dem GuardDuty Dienstkonto zu teilen. Weitere Informationen finden Sie unter Dienstbezogene

Rollenberechtigungen für GuardDuty. Weitere Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden serviceverknüpfter Rollen.

- Wenn Sie Ihr Konto GuardDuty zum ersten Mal in einer Region aktivieren, wird Ihr AWS Konto automatisch für eine GuardDuty kostenlose 30-Tage-Testversion für diese Region registriert.

Erste Schritte: Amazon GuardDuty für eigenständige Umgebungen oder Umgebungen mit mehreren Konten aktivieren

Schritt 1: Amazon aktivieren GuardDuty

Der erste Schritt zur Verwendung GuardDuty besteht darin, es in Ihrem Konto zu aktivieren. Nach der Aktivierung GuardDuty wird sofort mit der Überwachung auf Sicherheitsbedrohungen in der aktuellen Region begonnen.

Wenn Sie die GuardDuty Ergebnisse für andere Konten innerhalb Ihrer Organisation als GuardDuty Administrator verwalten möchten, müssen Sie Mitgliedskonten hinzufügen und diese ebenfalls aktivieren GuardDuty .

> **Note**
>
> Wenn Sie den GuardDuty Malware-Schutz für S3 ohne Aktivierung aktivieren möchten GuardDuty, finden Sie die entsprechenden Schritte unterGuardDuty Malware-Schutz für S3.

Standalone account environment

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/
2. Wählen Sie die Option Amazon GuardDuty — Alle Funktionen.
3. Wählen Sie Erste Schritte.
4. Sehen Sie sich auf der GuardDuty Seite Willkommen bei die Servicebedingungen an. Wählen Sie „Aktivieren GuardDuty“.

Multi-account environment

> **Important**
>
> Voraussetzung für diesen Prozess ist, dass Sie derselben Organisation angehören wie alle Konten, die Sie verwalten möchten, und Zugriff auf das AWS Organizations Verwaltungskonto haben, um einen Administrator GuardDuty innerhalb Ihrer Organisation delegieren zu können. Für die Delegierung eines Administrators sind möglicherweise zusätzliche Berechtigungen erforderlich. Weitere Informationen finden Sie unter Für die Benennung eines delegierten GuardDuty Administratorkontos sind Berechtigungen erforderlich.

Um ein GuardDuty delegiertes Administratorkonto zu bestimmen

1. Öffnen Sie die AWS Organizations Konsole unter https://console.aws.amazon.com/organizations/und verwenden Sie das Verwaltungskonto.
2. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Ist in Ihrem Konto GuardDuty bereits aktiviert?

   - Falls GuardDuty es noch nicht aktiviert ist, können Sie Erste Schritte auswählen und dann auf der Seite Willkommen GuardDuty bei einen GuardDuty delegierten Administrator benennen.
   - Wenn diese Option aktiviert GuardDuty ist, können Sie auf der Seite Einstellungen einen GuardDuty delegierten Administrator benennen.
3. Geben Sie die zwölfstellige AWS Konto-ID des Kontos ein, das Sie als delegierten Administrator für die Organisation festlegen möchten, und wählen Sie GuardDuty Delegieren aus.

   > **Note**
   >
   > Falls dies noch nicht aktiviert GuardDuty ist, wird durch die Benennung eines delegierten Administrators die Aktivierung GuardDuty für dieses Konto in Ihrer aktuellen Region aktiviert.

So fügen Sie Mitgliedskonten hinzu

Dieses Verfahren umfasst das Hinzufügen von Mitgliederkonten zu einem GuardDuty delegierten Administratorkonto durch. AWS Organizations Es besteht auch die Möglichkeit, Mitglieder auf Einladung hinzuzufügen. Weitere Informationen zu beiden Methoden zum Zuordnen von Mitgliedern finden Sie GuardDuty unter. Verwaltung mehrerer Konten bei Amazon GuardDuty

1. Melden Sie sich im delegierten Administratorkonto an
2. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
3. Wählen Sie im Navigationsbereich Settings (Einstellungen) und dann Accounts (Konten) aus.

   In der Kontentabelle werden alle Konten in der Organisation angezeigt.
4. Wählen Sie die Konten aus, die Sie als Mitglieder hinzufügen möchten, indem Sie das Kontrollkästchen neben der Konto-ID aktivieren. Wählen Sie dann im Menü Aktion die Option Mitglied hinzufügen.

> **Tip**
>
> Sie können das Hinzufügen neuer Konten als Mitglieder mit dem Feature Automatisch aktivieren automatisieren. Dies gilt jedoch nur für Konten, die Ihrer Organisation beitreten, nachdem das Feature aktiviert wurde.

Schritt 2: Beispiel-Erkenntnisse generieren und die grundlegenden Abläufe erkunden

Wenn ein Sicherheitsproblem GuardDuty entdeckt wird, wird ein Befund generiert. Ein GuardDuty Befund ist ein Datensatz, der Details zu diesem speziellen Sicherheitsproblem enthält. Die Einzelheiten der Erkenntnis können Ihnen bei der Untersuchung des Problems helfen.

GuardDuty unterstützt die Generierung von Stichprobenergebnissen mit Platzhalterwerten, anhand derer Sie die GuardDuty Funktionalität testen und sich mit den Ergebnissen vertraut machen können, bevor Sie auf ein echtes Sicherheitsproblem reagieren müssen, das von entdeckt wurde. GuardDuty Folgen Sie der nachstehenden Anleitung, um Beispielergebnisse für jeden Befundtyp zu generieren GuardDuty, der unter verfügbar ist. Weitere Möglichkeiten zur Generierung von Stichprobenergebnissen, einschließlich der Generierung eines simulierten Sicherheitsereignisses in Ihrem Konto, finden Sie unter. Beispielergebnisse

So erstellen und untersuchen Sie Beispiel-Erkenntnisse

1. Wählen Sie im Navigationsbereich Settings (Einstellungen).
2. Klicken Sie auf der Seite Settings unter Sample findings auf Generate sample findings.
3. Wählen Sie im Navigationsbereich Zusammenfassung aus, um die in Ihrer AWS Umgebung generierten Erkenntnisse zu den Ergebnissen anzuzeigen. Weitere Informationen zu den Komponenten des Übersichts-Dashboards finden Sie unter Übersichts-Dashboard.
4. Wählen Sie im Navigationsbereich Findings aus. Die Beispielergebnisse werden auf der Seite Aktuelle Ergebnisse mit dem Präfix [SAMPLE] angezeigt.
5. Wählen Sie eine Erkenntnis aus der Liste aus, um Details zur Erkenntnis anzuzeigen.

    - Sie können die verschiedenen Informationsfelder überprüfen, die im Bereich mit den Erkenntnisdetails verfügbar sind. Verschiedene Arten von Erkenntnissen können unterschiedliche Felder haben. Weitere Informationen zu den verfügbaren Feldern für alle Erkenntnistypen finden Sie unter Erkenntnisdetails. In der Detailansicht können Sie die folgenden Aktionen durchführen:

        - Wählen Sie oben im Bereich die Ergebnis-ID aus, um die vollständigen JSON Details zum Ergebnis zu öffnen. Die vollständige JSON Datei kann auch von diesem Panel heruntergeladen werden. Das JSON enthält einige zusätzliche Informationen, die nicht in der Konsolenansicht enthalten sind, und ist das Format, das von anderen Tools und Diensten aufgenommen werden kann.
        - Sehen Sie sich den Abschnitt Betroffene Ressource an. In einem echten Fall helfen Ihnen die Informationen hier dabei, eine Ressource in Ihrem Konto zu identifizieren, die untersucht werden sollte, und sie enthalten Links zu den entsprechenden AWS Management Console oder umsetzbaren Ressourcen.
        - Wählen Sie das + oder - beim Lupensymbol, um einen inklusiven oder exklusiven Filter für dieses Detail zu erstellen. Weitere Informationen zu Filtern finden Sie unter Filtern von Ergebnissen.
6. Archivieren Sie all Ihre Beispiel-Erkenntnisse

    a. Wählen Sie alle Erkenntnisse aus, indem Sie das Kontrollkästchen oben in der Liste aktivieren.

    b. Deaktivieren Sie alle Erkenntnisse, die Sie behalten möchten.

    c. Wählen Sie das Menü Aktionen und dann Archivieren, um die Beispiel-Erkenntnisse auszublenden.

> **Note**
>
> Um die archivierten Erkenntnisse anzuzeigen, wählen Sie Aktuell und dann Archiviert, um zur Erkenntnisansicht zu wechseln.

Schritt 3: Konfigurieren Sie den Export von GuardDuty Ergebnissen in einen Amazon S3 S3-Bucket

GuardDuty empfiehlt, Einstellungen für den Export von Ergebnissen zu konfigurieren, da Sie so Ihre Ergebnisse in einen S3-Bucket exportieren können, um sie nach Ablauf der Aufbewahrungsfrist von GuardDuty 90 Tagen auf unbestimmte Zeit zu speichern. Auf diese Weise können Sie Aufzeichnungen über die Ergebnisse führen oder Probleme in Ihrer AWS Umgebung im Laufe der Zeit verfolgen. Der hier beschriebene Prozess führt Sie durch die Einrichtung eines neuen S3-Buckets und die Erstellung eines neuen KMS Schlüssels zur Verschlüsselung der Ergebnisse von der Konsole aus. Weitere Informationen dazu, wie Sie Ihren eigenen vorhandenen Bucket oder einen Bucket in einem anderen Konto verwenden können, finden Sie unter Exportieren von Erkenntnissen.

So konfigurieren Sie die Option zum Export von Erkenntnissen an S3

1. Um die Ergebnisse zu verschlüsseln, benötigen Sie einen KMS Schlüssel mit einer Richtlinie, die die Verwendung dieses Schlüssels für die Verschlüsselung ermöglicht GuardDuty . Die folgenden Schritte helfen Ihnen dabei, einen neuen KMS Schlüssel zu erstellen. Wenn Sie einen KMS Schlüssel von einem anderen Konto verwenden, müssen Sie die Schlüsselrichtlinie anwenden, indem Sie sich bei dem Konto anmelden AWS-Konto , dem der Schlüssel gehört. Die Region Ihres KMS Schlüssels und Ihres S3-Buckets müssen identisch sein. Sie können jedoch dasselbe Bucket und Schlüsselpaar für jede Region verwenden, aus der Sie Erkenntnisse exportieren möchten.

   a. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms.

   b. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.

   c. Klicken Sie im Navigationsbereich auf Kundenverwaltete Schlüssel.

   d. Klicken Sie auf Create key.

   e. Wählen Sie unter Schlüsseltyp die Option Symmetrisch und dann Weiter.

> **Note**
>
> Eine ausführliche Anleitung zur Erstellung Ihres KMS Schlüssels finden Sie unter Schlüssel erstellen im AWS Key Management Service Entwicklerhandbuch.

f. Geben Sie einen Alias für Ihren Schlüssel ein und wählen Sie dann Weiter aus.

g. Wählen Sie Weiter und dann erneut Weiter, um die standardmäßigen Verwaltungs- und Nutzungsberechtigungen zu akzeptieren.

h. Nachdem Sie die Konfiguration überprüft haben, wählen Sie Fertigstellen, um den Schlüssel zu erstellen.

i. Wählen Sie auf der Seite Vom Kunden verwaltete Schlüssel Ihren Schlüsselalias aus.

j. Wählen Sie im Abschnitt Schlüsselrichtlinie die Option Zur Richtlinienansicht wechseln aus.

k. Wählen Sie Bearbeiten und fügen Sie Ihrem KMS Schlüssel die folgende Schlüsselrichtlinie hinzu, um GuardDuty Zugriff auf Ihren Schlüssel zu gewähren. Diese Anweisung erlaubt es GuardDuty , nur den Schlüssel zu verwenden, zu dem Sie diese Richtlinie hinzufügen. Stellen Sie beim Bearbeiten der Schlüsselrichtlinie sicher, dass die JSON Syntax gültig ist. Wenn Sie die Anweisung vor der finalen Anweisung hinzufügen, müssen Sie nach der schließenden Klammer ein Komma hinzufügen.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"
        }
    }
}
```

Ersetzen *Region1* mit der Region Ihres KMS Schlüssels. Ersetzen *444455556666* mit dem AWS-Konto , dem der KMS Schlüssel gehört. Ersetzen *KMSKeyId* mit der Schlüssel-ID des KMS Schlüssels, den Sie für die Verschlüsselung ausgewählt haben. Um all diese Werte — Region, und Schlüssel-ID — zu identifizieren AWS-Konto, sehen Sie sich die Werte ARNIhres KMS Schlüssels an. Informationen zum Auffinden des Schlüssels ARN finden Sie unter Schlüssel-ID finden und ARN.

Ersetzen Sie auf ähnliche Weise *111122223333* mit dem AWS-Konto des GuardDuty Kontos. Ersetzen *Region2* mit der Region des GuardDuty Kontos. Ersetzen *SourceDetectorID* mit der Melder-ID des GuardDuty Kontos für *Region2*.

Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite „Einstellungen“ oder führen Sie den aus ListDetectorsAPI.

l. Wählen Sie Save (Speichern) aus.

2. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
3. Wählen Sie im Navigationsbereich Settings (Einstellungen).
4. Wählen Sie unter Exportoptionen für Erkenntnisse die Option Jetzt konfigurieren.
5. Wählen Sie Neuer Bucket. Geben Sie einen eindeutigen Namen für Ihren S3-Bucket ein.
6. (Optional) Sie können Ihre neuen Exporteinstellungen testen, indem Sie Beispiel-Erkenntnisse generieren. Wählen Sie im Navigationsbereich Settings (Einstellungen).
7. Wählen Sie unter dem Abschnitt Beispiel-Erkenntnisse die Option Beispiel-Erkenntnisse erstellen. Die neuen Ergebnisse der Stichprobe werden als Einträge im S3-Bucket angezeigt, der GuardDuty in bis zu fünf Minuten erstellt wurde.

Schritt 4: Richten Sie die GuardDuty Suche nach Warnmeldungen ein SNS

GuardDuty ist in Amazon integriert EventBridge, wodurch Befunddaten zur Verarbeitung an andere Anwendungen und Dienste gesendet werden können. Mit EventBridge Hilfe von GuardDuty Ergebnissen können Sie automatische Antworten auf Ihre Ergebnisse einleiten, indem Sie Findereignisse mit Zielen wie AWS Lambda Funktionen, Amazon EC2 Systems Manager Manager-Automatisierung, Amazon Simple Notification Service (SNS) und mehr verknüpfen.

In diesem Beispiel erstellen Sie ein SNS Thema, das das Ziel einer EventBridge Regel sein soll. Anschließend erstellen Sie EventBridge eine Regel, die Ergebnisdaten erfasst GuardDuty. Die resultierende Regel leitet die Erkenntnisdetails an eine E-Mail-Adresse weiter. Weitere Informationen dazu, wie Sie Erkenntnisse an Slack oder Amazon Chime senden und auch die Arten der Benachrichtigungen zu Erkenntnissen ändern können, finden Sie unter Einrichten eines Amazon-SNS-Themas und eines Endpunkts.

Um ein SNS Thema für Ihre Ergebniswarnungen zu erstellen

1. Öffnen Sie die SNS Amazon-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Themen aus.
3. Wählen Sie Create Topic (Thema erstellen) aus.
4. Wählen Sie für Typ die Option Standard.
5. Geben Sie unter Name **`GuardDuty`** ein.
6. Wählen Sie Create Topic (Thema erstellen) aus. Die Themendetails für Ihr neues Thema werden geöffnet.
7. Wählen Sie im Abschnitt Subscriptions (Abonnements) die Option Create subscription (Abonnement erstellen) aus.
8. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.
9. Geben Sie als Endpunkt die E-Mail-Adresse ein, an die Benachrichtigungen gesendet werden sollen.
10. Wählen Sie Create subscription (Abonnement erstellen) aus.

    Sie müssen Ihre E-Mail-Adresse bestätigen, nachdem Sie das Abonnement erstellt haben.
11. Um nach einer Abonnementnachricht zu suchen, gehen Sie zu Ihrem E-Mail-Posteingang und wählen Sie in der Abonnementnachricht die Option Abonnement bestätigen.

> **Note**
>
> Um den Status der E-Mail-Bestätigung zu überprüfen, rufen Sie die SNS Konsole auf und wählen Sie Abonnements.

Um eine EventBridge Regel zu erstellen, um GuardDuty Ergebnisse zu erfassen und zu formatieren

1. Öffnen Sie die EventBridge Konsole unter https://console.aws.amazon.com/events/.

2. Wählen Sie im Navigationsbereich Rules aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie einen Namen und eine Beschreibung für die Regel ein.

   Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.
5. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus.
6. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
7. Wählen Sie Weiter.
8. Wählen Sie unter Event source (Ereignisquelle) AWS events (Ereignisse) aus.
9. Wählen Sie für Ereignismuster die Option Ereignismusterformular.
10. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
11. Wählen Sie unter AWS -Service die Option GuardDuty aus.
12. Wählen Sie als Ereignistyp die Option GuardDutyFinding aus.
13. Wählen Sie Weiter.
14. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.
15. Wählen Sie unter Ziel auswählen SNSdas Thema und für Thema den Namen des SNS Themas aus, das Sie zuvor erstellt haben.
16. Wählen Sie im Abschnitt Zusätzliche Einstellungen unter Zieleingabe konfigurieren die Option Eingabe-Transformer.

    Durch das Hinzufügen eines Eingangstransformators werden die JSON gesendeten Suchdaten GuardDuty in eine für Menschen lesbare Nachricht formatiert.
17. Wählen Sie Configure input transformer (Eingabetransformator konfigurieren).
18. Fügen Sie im Abschnitt Ziel-Eingabe-Transformer für Eingabepfad den folgenden Code ein:

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
```

```
}
```

19. Um die E-Mail zu formatieren, fügen Sie in das Feld Vorlage den folgenden Code ein und achten Sie darauf, den roten Text durch die Werte zu ersetzen, die Ihrer Region entsprechen:

```
"You have a severity severity GuardDuty finding type Finding_Type in
 the Region_Name Region."
"Finding Description:"
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. Wählen Sie Bestätigen aus.
21. Wählen Sie Weiter.
22. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein. Weitere Informationen finden Sie unter EventBridge Amazon-Tags im EventBridge Amazon-Benutzerhandbuch.
23. Wählen Sie Weiter.
24. Überprüfen Sie die Details der Regel und wählen Sie dann Create rule (Regel erstellen) aus.
25. (Optional) Testen Sie Ihre neue Regel, indem Sie anhand des in Schritt 2 beschriebenen Prozesses Beispiel-Erkenntnisse generieren. Sie erhalten für jede generierte Beispiel-Erkenntnis eine E-Mail.

Nächste Schritte

Wenn Sie die Nutzung fortsetzen GuardDuty, werden Sie verstehen, welche Arten von Ergebnissen für Ihre Umgebung relevant sind. Wenn Sie eine neue Erkenntnis erhalten, können Sie Informationen, einschließlich Empfehlungen zur Problembehebung, zu dieser Erkenntnis finden, indem Sie in der Beschreibung der Erkenntnis im Bereich mit den Erkenntnisdetails die Option Weitere Informationen auswählen oder indem Sie unter nach dem Namen der Erkenntnis in Erkenntnistypen suchen.

Die folgenden Funktionen helfen Ihnen bei der Feinabstimmung, GuardDuty sodass die relevantesten Ergebnisse für Ihre AWS Umgebung bereitgestellt werden können:

- Um Ergebnisse auf einfache Weise nach bestimmten Kriterien wie Instanz-ID, Konto-ID, S3-Bucket-Name und mehr zu sortieren, können Sie darin Filter erstellen und speichern GuardDuty. Weitere Informationen finden Sie unter Filtern von Ergebnissen.

- Wenn Sie Erkenntnisse zu erwartetem Verhalten in Ihrer Umgebung erhalten, können Sie die Erkenntnisse anhand der Kriterien, die Sie mit Unterdrückungsregeln definieren, automatisch archivieren.
- Um zu verhindern, dass Ergebnisse aus einer Untergruppe vertrauenswürdiger Daten generiert werdenIPs, oder um zu verhindern, dass die GuardDuty Überwachung IPs außerhalb des normalen Überwachungsbereichs liegt, können Sie Listen vertrauenswürdiger IP-Adressen und Bedrohungen einrichten.

GuardDuty grundlegende Datenquellen

GuardDuty verwendet die grundlegenden Datenquellen, um die Kommunikation mit bekannten bösartigen Domänen und IP-Adressen zu erkennen und potenziell anomales Verhalten und nicht autorisierte Aktivitäten zu identifizieren. Bei der Übertragung von diesen Quellen zu GuardDuty werden alle Protokolldaten verschlüsselt. GuardDutyextrahiert verschiedene Felder aus diesen Protokollquellen für die Profilerstellung und die Erkennung von Anomalien und verwirft diese Protokolle anschließend.

GuardDuty Bei der ersten Aktivierung in einer Region gibt es eine kostenlose 30-Tage-Testversion, die die Bedrohungserkennung für alle grundlegenden Datenquellen umfasst. Während dieser kostenlosen Testversion können Sie die geschätzte monatliche Nutzung, aufgeschlüsselt nach jeder grundlegenden Datenquelle, überwachen. Als delegiertes GuardDuty Administratorkonto können Sie sich die geschätzten monatlichen Nutzungskosten anzeigen lassen, aufgeschlüsselt nach jedem Mitgliedskonto, das zu Ihrer Organisation gehört und aktiviert wurde. GuardDuty Nach Ablauf der 30-Tage-Testversion können Sie Informationen AWS Billing zu den Nutzungskosten abrufen.

Für den GuardDuty Zugriff auf Ereignisse und Protokolle aus diesen grundlegenden Datenquellen fallen keine zusätzlichen Kosten an.

Nachdem Sie Ihre aktiviert GuardDuty haben AWS-Konto, beginnt sie automatisch mit der Überwachung der in den folgenden Abschnitten erläuterten Protokollquellen. Sie müssen nichts anderes aktivieren, um mit der Analyse und Verarbeitung dieser Datenquellen zu beginnen, um entsprechende Sicherheitsergebnisse zu generieren. GuardDuty

Themen

AWS CloudTrail Management-Ereignisse

AWS CloudTrail bietet Ihnen eine Historie der AWS API Anrufe für Ihr Konto, einschließlich der API Anrufe, die AWS Management Console, die AWS SDKs, die Befehlszeilentools und bestimmte AWS Dienste verwendet haben. CloudTrail hilft Ihnen auch dabei, zu ermitteln, welche Benutzer und Konten AWS APIs für unterstützende Dienste aufgerufen wurden CloudTrail, von welcher

Quell-IP-Adresse aus die Anrufe aufgerufen wurden, und zu welcher Uhrzeit die Anrufe aufgerufen wurden. Weitere Informationen finden Sie unter Was ist AWS CloudTrail im AWS CloudTrail - Benutzerhandbuch.

GuardDuty überwacht CloudTrail Verwaltungsereignisse, auch bekannt als Ereignisse auf der Kontrollebene. Diese Ereignisse bieten Einblick in Verwaltungsvorgänge, die mit Ressourcen in Ihrem AWS Konto ausgeführt werden.

Im Folgenden finden Sie Beispiele für CloudTrail Verwaltungsereignisse, die GuardDuty überwacht werden:

- Konfiguration der Sicherheit (IAM`AttachRolePolicy`APIBetrieb)
- Konfiguration von Regeln für das Routing von Daten (Amazon EC2 `CreateSubnet` API Operations)
- Einrichtung der Protokollierung (AWS CloudTrail `CreateTrail`APIOperationen)

Wenn Sie diese GuardDuty Option aktivieren, werden CloudTrail Verwaltungsereignisse direkt CloudTrail über einen unabhängigen und duplizierten Ereignisstrom verarbeitet und Ihre CloudTrail Ereignisprotokolle analysiert.

GuardDuty verwaltet Ihre CloudTrail Ereignisse nicht und wirkt sich auch nicht auf Ihre vorhandenen CloudTrail Konfigurationen aus. Ebenso haben Ihre CloudTrail Konfigurationen keinen Einfluss darauf, wie GuardDuty die Ereignisprotokolle genutzt und verarbeitet werden. Verwenden Sie die CloudTrail Servicekonsole oderAPI, um den Zugriff auf Ihre CloudTrail Ereignisse und deren Aufbewahrung zu verwalten. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Wie GuardDuty geht man mit AWS CloudTrail globalen Ereignissen um

Bei den meisten AWS Diensten werden CloudTrail Ereignisse dort aufgezeichnet, AWS-Region wo sie erstellt wurden. Bei globalen Diensten wie AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3) CloudFront, Amazon und Amazon Route 53 (Route 53) werden Ereignisse nur in der Region generiert, in der sie auftreten, aber sie haben globale Bedeutung.

Wenn GuardDuty CloudTrail globale Service-Ereignisse mit Sicherheitswert wie Netzwerkkonfigurationen oder Benutzerberechtigungen verarbeitet werden, repliziert es diese Ereignisse und verarbeitet sie in jeder Region, in der Sie sie aktiviert haben. GuardDuty Dieses

Verhalten hilft dabei, Benutzer- und Rollenprofile in jeder Region zu GuardDuty verwalten, was für die Erkennung ungewöhnlicher Ereignisse von entscheidender Bedeutung ist.

Wir empfehlen dringend, dass Sie alle aktivieren GuardDuty AWS-Regionen , die für Sie aktiviert sind. AWS-Konto Auf diese Weise GuardDuty können Sie Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten gewinnen, auch in den Regionen, die Sie möglicherweise nicht aktiv nutzen.

VPC-Flow-Protokolle

Die VPC Flow Logs-Funktion von Amazon VPC erfasst Informationen über den IP-Verkehr zu und von Netzwerkschnittstellen, die mit den Amazon Elastic Compute Cloud (AmazonEC2) -Instances in Ihrer AWS Umgebung verbunden sind.

Wenn Sie es aktivieren GuardDuty, beginnt es sofort mit der Analyse Ihrer VPC Flow-Logs von EC2 Amazon-Instances in Ihrem Konto. Es verarbeitet VPC Flow-Log-Ereignisse direkt aus der VPC Flow Logs-Funktion über einen unabhängigen und doppelten Stream von Flow-Logs. Dieser Prozess wirkt sich nicht auf ggf. vorhandene Flow-Protokollkonfigurationen aus.

Lambda Protection

Lambda Protection ist eine optionale Erweiterung für Amazon GuardDuty. Derzeit umfasst Lambda Network Activity Monitoring VPC Amazon-Flow-Protokolle von allen Lambda-Funktionen für Ihr Konto, auch von den Protokollen, die kein Netzwerk verwenden. VPC Um Ihre Lambda-Funktion vor potenziellen Sicherheitsbedrohungen zu schützen, müssen Sie Lambda Protection in Ihrem GuardDuty Konto konfigurieren. Weitere Informationen finden Sie unter Lambda Protection.

GuardDuty Überwachung der Laufzeit

Wenn Sie den Security Agent (entweder manuell oder über GuardDuty) in EKS Runtime Monitoring oder Runtime Monitoring für EC2 Instances verwalten und derzeit auf einer EC2 Amazon-Instance bereitgestellt GuardDuty ist und diese Gesammelte Laufzeit-Ereignistypen von dieser Instance erhält, fallen GuardDuty Ihnen keine Gebühren AWS-Konto für die Analyse der VPC Flow-Logs dieser EC2 Amazon-Instance an. Dadurch werden doppelte Nutzungskosten für das Konto GuardDuty vermieden.

GuardDuty verwaltet Ihre Flow-Logs nicht und macht sie auch nicht in Ihrem Konto zugänglich. Um den Zugriff auf und die Aufbewahrung Ihrer Flow-Logs zu verwalten, müssen Sie die VPC Flow-Logs-Funktion konfigurieren.

Route53 Resolver-Abfrageprotokolle DNS

Wenn Sie AWS DNS Resolver für Ihre EC2 Amazon-Instances verwenden (Standardeinstellung), GuardDuty können Sie über die internen Resolver auf Ihre Anfrage- und DNS Antwort-Route53-Resolver-Abfrageprotokolle zugreifen und diese verarbeiten. AWS DNS Wenn Sie einen anderen DNS Resolver wie Open DNS oder Google verwenden oder Ihre eigenen DNS Resolver einrichtenDNS, können Sie GuardDuty nicht auf Daten aus dieser Datenquelle zugreifen und diese verarbeiten.

Wenn Sie es aktivieren GuardDuty, beginnt es sofort mit der Analyse Ihrer Route53 DNS Resolver-Abfrageprotokolle aus einem unabhängigen Datenstrom. Dieser Datenstrom ist von den Daten getrennt, die über das Feature Route-53-Resolver-Abfrageprotokollierung bereitgestellt werden. Die Konfiguration dieser Funktion hat keinen Einfluss auf die Analyse. GuardDuty

> **Note**
>
> GuardDuty unterstützt keine DNS Überwachungsprotokolle für EC2 Amazon-Instances, auf denen gestartet wurde, AWS Outposts da die Amazon Route 53 Resolver Abfrageprotokollierungsfunktion in dieser Umgebung nicht verfügbar ist.

Funktionen Aktivierung in GuardDuty

Wenn Sie Amazon GuardDuty zum ersten Mal aktivieren oder darin einen Schutztyp aktivieren GuardDuty, GuardDuty beginnt die Verarbeitung des entsprechenden Schutzes Grundlegende Datenquellen in Ihrer AWS Umgebung. GuardDuty verwendet diese Datenquellen, um eine Reihe von Ereignissen zu verarbeiten, z. B. VPC Ablaufprotokolle, DNS Protokolle sowie AWS CloudTrail Ereignis- und Verwaltungsprotokolle. Anschließend analysiert es diese Ereignisse, um potenzielle Sicherheitsbedrohungen zu identifizieren, und generiert Erkenntnisse in Ihrem Konto.

GuardDuty Kann neben Protokolldatenquellen auch zusätzliche Daten von anderen AWS Diensten in Ihrer AWS Umgebung verwenden, um potenzielle Sicherheitsbedrohungen zu überwachen und zu analysieren.

Feature-Aktivierung

Wenn Sie zusätzliche GuardDuty Schutzmaßnahmen hinzufügen, z. B. S3-Schutz, Laufzeitüberwachung oder EKS Schutz, können Sie die GuardDuty Funktion entsprechend dem Schutztyp konfigurieren. In der Vergangenheit wurden GuardDuty Schutzmaßnahmen `dataSources` in der genannt. APIs Nach März 2023 werden neue GuardDuty Schutztypen nun jedoch als `features` und nicht `dataSources` konfiguriert. GuardDuty unterstützt weiterhin die Konfiguration von Schutztypen, die vor März 2023 eingeführt wurdenAPI, wie `dataSources` über, aber neue Schutztypen sind nur als verfügbar`features`.

Wenn Sie GuardDuty Konfiguration und Schutztypen über die Konsole verwalten, sind Sie von dieser Änderung nicht direkt betroffen und müssen keine Maßnahmen ergreifen. Die Aktivierung von Funktionen wirkt sich auf das Verhalten derjenigen ausAPIs, die zur Aktivierung aufgerufen werden, GuardDuty oder auf die darin enthaltenen Schutztypen. GuardDuty Weitere Informationen finden Sie unter GuardDuty APIÄnderungen.

GuardDuty APIÄnderungen im März 2023

Die GuardDuty APIs konfigurierten Schutzfunktionen, die nicht zur Liste von gehörenGuardDuty grundlegende Datenquellen. Ein Feature-Objekt enthält Feature-Details, wie Feature-Namen und Status, und kann zusätzliche Konfigurationen für einige Feature enthalten. Diese Migration wirkt sich auf Folgendes APIs in der GuardDuty APIAmazon-Referenz aus:

- CreateDetector

- GetDetector
- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

Funktion-Aktivierung im Vergleich zu Datenquellen

In der Vergangenheit wurden alle GuardDuty Features durch ein `dataSources` Objekt in der weitergegebenAPI. Ab März 2023 GuardDuty bevorzugt `features` das Objekt anstelle des `dataSources` Objekts in derAPI. Alle früheren Datenquellen verfügen über entsprechende Feature, aber neuere Feature verfügen möglicherweise nicht über entsprechende Datenquellen.

Die folgende Liste zeigt den Vergleich zwischen `dataSources` und `features` Objekt, wenn es durch ein übergeben wirdAPI:

- Das `dataSources`-Objekt enthält Objekte für jeden Schutztyp und seinen Status. Das `features` Objekt ist eine Liste verfügbarer Funktionen, die jedem darin enthaltenen Schutztyp entsprechen GuardDuty.

  Ab März 2023 ist die Aktivierung von Funktionen die einzige Möglichkeit, neue GuardDuty Funktionen in Ihrer AWS Umgebung zu konfigurieren.
- Das `dataSources` Schema in der API Anfrage oder Antwort ist überall dort, AWS-Region wo es verfügbar GuardDuty ist, dasselbe. Möglicherweise sind nicht alle Feature von in jeder Region verfügbar. Daher können sich die Namen der verfügbaren Feature je nach Region unterscheiden.

Verstehen, wie die Aktivierung von Features funktioniert

Sie geben GuardDuty APIs weiterhin ein `dataSources` Objekt zurück, sofern zutreffend, und sie geben auch ein `features` Objekt zurück, das dieselben Informationen in einem anderen Format enthält. GuardDuty Funktionen, die vor März 2023 eingeführt wurden, werden über `dataSources` Objekt und `features` Objekt verfügbar sein. GuardDuty Funktionen, die seit März 2023 eingeführt wurden, werden nur über das `features` Objekt verfügbar sein. Sie können in derselben API Anfrage

keinen Detektor erstellen oder aktualisieren oder beschreiben, dass Sie beides `dataSources` und die `features` Objektnotation AWS Organizations verwenden. Um GuardDuty Schutztypen zu aktivieren, müssen Sie Ihre vorhandenen Datenquellen auf das `features` Objekt migrieren, indem Sie dieselben verwendenAPIs, die jetzt auch das `features` Objekt enthalten.

> **Note**
>
> GuardDuty fügt nach dieser Änderung keine neue Datenquelle hinzu.

GuardDuty hat die Verwendung von Datenquellen eingestellt. Es unterstützt jedoch weiterhin die GuardDuty grundlegende Datenquellen. Die GuardDuty bewährten Methoden empfehlen, die Aktivierung von Funktionen für alle Schutzarten zu verwenden, die bereits für Ihr Konto aktiviert sind. Die bewährten Methoden erfordern außerdem die Aktivierung von Features, wenn Sie einen neuen Schutztyp für Ihr Konto aktivieren.

Änderungen bei der Aktivierung von Features einbeziehen

- Wenn Sie GuardDuty Konfigurationen über APIsSDKs, oder eine AWS CloudFormation Vorlage verwalten und potenzielle neue GuardDuty Funktionen aktivieren möchten, müssen Sie Ihren Code und Ihre Vorlage entsprechend ändern. Weitere Informationen finden Sie APIs in der aktualisierten Version der GuardDuty APIAmazon-Referenz.
- Für GuardDuty Funktionen, die vor diesem Upgrade konfiguriert wurden, können Sie weiterhin die AWS CloudFormation Vorlage APIsSDKs, oder verwenden. Wir empfehlen jedoch, zur Verwendung von `feature`-Objekt zu wechseln.

  Alle Datenquellen haben ein äquivalentes Feature-Objekt. Weitere Informationen finden Sie unter Zuordnung von `dataSources` zu `features`.
- Derzeit ist `additionalConfiguration` im `features`-Objekt nur für bestimmte Schutzarten verfügbar.
  - Für solche Schutztypen gilt: Wenn Ihre Funktion auf eingestellt `AdditionalConfiguration` `status` ist, die Konfiguration Ihrer Funktion `ENABLED` jedoch nicht aktiviert `status` ist`ENABLED`, GuardDuty werden in diesem Fall keine Maßnahmen ergriffen.
  - Folgendes APIs ist davon betroffen:
    - UpdateDetector
    - UpdateMemberDetectors

- UpdateOrganizationConfiguration

Zuordnung von **`dataSources`** zu **`features`**

Die folgende Tabelle zeigt die Zuordnung der Schutztypen, `dataSources` und `features`.

GuardDuty Art des Schutzes	Name der Datenquelle *	Feature name
VPC-Flow-Protokolle	`flowLogs` (schreibgeschützt; kann nicht geändert werden)	`FLOW_LOGS` (schreibgeschützt; kann nicht geändert werden)
Route53 Resolver-Abfrageprotokolle DNS	`dnsLogs` (schreibgeschützt; kann nicht geändert werden)	`DNS_LOGS` (schreibgeschützt; kann nicht geändert werden)
CloudTrail Ereignisse	`cloudTrail` (schreibgeschützt; kann nicht geändert werden)	`CLOUD_TRAIL` (schreibgeschützt; kann nicht geändert werden)
S3	`s3Logs`	`S3_DATA_EVENTS`
EKSÜberwachung des Auditprotokolls	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Malware-Schutz für EC2	`malwareProtection.scanEc2InstanceWithFindings.ebsVolumes`	`EBS_MALWARE_PROTECTION`
RDSAnmeldeereignisse	GuardDuty bietet nur Unterstützung für die Aktivierung von Funktionen für diese Schutztypen.	`RDS_LOGIN_EVENTS`
EKSÜberwachung der Laufzeit		`EKS_RUNTIME_MONITORING`

GuardDuty Art des Schutzes	Name der Datenquelle *	Feature name
Laufzeit-Überwachung		`RUNTIME_MONITORING`

GuardDuty Sicherheitsagent für EKS Amazon-Cluster		`EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`
		
		`RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`

GuardDuty Sicherheitsagent für ECS Amazon-Fargate-Cluster		`RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT`

GuardDuty Art des Schutzes	Name der Datenquelle *	Feature name
GuardDuty Sicherheitsagent für EC2 Amazon-Instances		`RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT`
Lambda Protection		`LAMBDA_NETWORK_LOGS`

* GetUsageStatistics verwendet seine eigenen `dataSource`-Namen. Weitere Informationen finden Sie unter Schätzung der Kosten GuardDuty oder GetUsageStatistics.

GuardDuty S3-Schutz

S3 Protection unterstützt Amazon bei der GuardDuty Überwachung von AWS CloudTrail Datenereignissen für Amazon Simple Storage Service (Amazon S3), die API Operationen auf Objektebene beinhalten, um potenzielle Sicherheitsrisiken für Daten in Ihren Amazon S3-Buckets zu identifizieren.

GuardDuty überwacht sowohl AWS CloudTrail Verwaltungsereignisse als auch AWS CloudTrail S3-Datenereignisse, um potenzielle Bedrohungen in Ihren Amazon S3 S3-Ressourcen zu identifizieren. Beide Datenquellen überwachen verschiedene Arten von Aktivitäten. Beispiele für CloudTrail Verwaltungsereignisse für S3 sind Operationen, die Amazon S3 S3-Buckets auflisten oder konfigurieren, wie `ListBucketsDeleteBuckets`, und`PutBucketReplication`. Zu den Beispielen für CloudTrail Datenereignisse für S3 gehören API Operationen auf Objektebene wie, `GetObjectListObjects`, `DeleteObject` und. `PutObject`

Wenn Sie Amazon GuardDuty für eine aktivieren AWS-Konto, GuardDuty beginnt die Überwachung von CloudTrail Verwaltungsereignissen. Sie müssen die Anmeldung bei S3-Datenereignissen nicht explizit aktivieren oder konfigurieren AWS CloudTrail , um S3 Protection verwenden zu können. Sie können die S3-Schutzfunktion (die CloudTrail Datenereignisse für S3 überwacht) für jedes Konto an jedem AWS-Region Ort aktivieren, an dem diese Funktion bei Amazon verfügbar ist GuardDuty, jederzeit. Wer AWS-Konto bereits aktiviert ist GuardDuty, kann S3 Protection mit einer 30-tägigen kostenlosen Testphase zum ersten Mal aktivieren. Für Geräte AWS-Konto , die GuardDuty zum ersten Mal aktiviert werden, ist S3 Protection bereits aktiviert und in dieser kostenlosen 30-Tage-Testversion enthalten. Weitere Informationen finden Sie unter Schätzung der Kosten GuardDuty .

Wir empfehlen Ihnen, S3 Protection in GuardDuty zu aktivieren. Wenn diese Funktion nicht aktiviert ist, GuardDuty können Sie Ihre Amazon S3 S3-Buckets nicht vollständig überwachen oder Ergebnisse für verdächtigen Zugriff auf die in Ihren S3-Buckets gespeicherten Daten generieren.

Wie GuardDuty verwendet S3-Datenereignisse

Wenn Sie S3-Datenereignisse (S3 Protection) aktivieren, GuardDuty beginnt es mit der Analyse von S3-Datenereignissen aus all Ihren S3-Buckets und überwacht sie auf böswillige und verdächtige Aktivitäten. Weitere Informationen finden Sie unter AWS CloudTrail Datenereignisse für S3.

Wenn ein nicht authentifizierter Benutzer auf ein S3-Objekt zugreift, bedeutet dies, dass das S3-Objekt öffentlich zugänglich ist. Verarbeitet solche Anfragen daher GuardDuty nicht. GuardDuty

verarbeitet die an die S3-Objekte gestellten Anfragen unter Verwendung gültiger IAM (AWS Identity and Access Management) oder AWS STS (AWS Security Token Service) Anmeldeinformationen.

> **Hinweis**
>
> Nach der Aktivierung von S3 Protection GuardDuty überwacht Amazon die Datenereignisse aus den Amazon S3 S3-Buckets, die sich in derselben Region befinden, in der Sie den Schutz aktiviert haben. GuardDuty

Wenn auf der Grundlage der Überwachung von S3-Datenereignissen eine potenzielle Bedrohung GuardDuty erkannt wird, generiert es eine Sicherheitsfeststellung. Informationen zu den Arten von Ergebnissen, die für Amazon S3 S3-Buckets generiert werden GuardDuty können, finden Sie unterGuardDuty S3-Suchttypen.

Wenn Sie den S3-Schutz deaktivieren, wird die S3-Datenereignisüberwachung der in Ihren S3-Buckets gespeicherten Daten GuardDuty beendet.

Feature in S3 Protection

AWS CloudTrail Datenereignisse für S3

Datenereignisse, auch bekannt als Vorgänge auf der Datenebene, bieten Einblicke in die Ressourcen-Vorgänge, die für oder innerhalb einer Ressource ausgeführt wurden. Datenereignisse sind oft Aktivitäten mit hohem Volume.

Im Folgenden finden Sie Beispiele für CloudTrail Datenereignisse für S3, die überwacht GuardDuty werden können:

- `GetObject`APIOperationen
- `PutObject`APIOperationen
- `ListObjects`APIOperationen
- `DeleteObject`APIOperationen

GuardDuty Bei der ersten Aktivierung ist S3 Protection standardmäßig aktiviert und auch in der 30-tägigen kostenlosen Testphase enthalten. Dieses Feature ist jedoch optional und Sie können sie jederzeit für jedes Konto oder jede Region aktivieren oder deaktivieren. Weitere Informationen zur Konfiguration von Amazon S3 als Feature finden Sie unter S3-Schutz.

S3 Protection für ein einzelnes Konto konfigurieren

Für Konten, die mit verknüpft sind AWS Organizations, kann dieser Vorgang über die Konsoleneinstellungen automatisiert werden. Weitere Informationen finden Sie unter Konfigurieren von S3 Protection in Umgebungen mit mehreren Konten.

So aktivieren oder deaktivieren Sie S3 Protection

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für ein einzelnes Konto zu konfigurieren.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich S3 Protection.
3. Auf der Seite S3 Protection finden Sie den aktuellen Status von S3 Protection für Ihr Konto. Wählen Sie Aktivieren oder Deaktivieren, um S3 Protection zu einem beliebigen Zeitpunkt zu aktivieren oder zu deaktivieren.
4. Wählen Sie Bestätigen, um Ihre Auswahl zu bestätigen.

API/CLI

1. Führen Sie updateDetector unter Verwendung Ihrer gültige Detektor-ID für die aktuelle Region aus und übergeben Sie das `features`-Objekt `name` als `S3_DATA_EVENTS` auf `ENABLED` oder `DISABLED` gesetzt, um S3 Protection zu aktivieren oder zu deaktivieren.

   > **Note**
   >
   > Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite Einstellungen oder führen Sie den aus ListDetectorsAPI.

2. Alternativ können Sie verwenden AWS Command Line Interface. Um S3 Protection zu aktivieren, führen Sie den folgenden Befehl aus und stellen Sie sicher, dass Sie Ihre eigene gültige Detektor-ID verwenden.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

Um S3 Protection zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED` im Beispiel.

Konfigurieren von S3 Protection in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, den S3-Schutz für die Mitgliedskonten in seiner AWS Organisation zu konfigurieren (zu aktivieren oder zu deaktivieren). Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Das delegierte GuardDuty Administratorkonto kann wählen, ob S3 Protection automatisch für alle Konten, nur für neue Konten oder für keine Konten in der Organisation aktiviert werden soll. Weitere Informationen finden Sie unter Verwalten von Konten mit AWS Organizations.

Konfiguration von S3 Protection für das delegierte Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für das delegierte GuardDuty Administratorkonto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen des Verwaltungskontos verwenden.
2. Wählen Sie im Navigationsbereich S3 Protection.
3. Wählen Sie auf der Seite S3 Protection die Option Bearbeiten.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.

- Wählen Sie Save (Speichern) aus.

Verwendung von Konten manuell konfigurieren

- Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.
- Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Save (Speichern) aus.

API/CLI

Verwenden Sie für die Ausführung updateDetectordie Detektor-ID des delegierten GuardDuty Administratorkontos für die aktuelle Region und übergeben Sie das `features` Objekt `name` als `S3_DATA_EVENTS` und `status` als. `ENABLED`

Alternativ können Sie S3 Protection konfigurieren, indem Sie AWS Command Line Interface Führen Sie den folgenden Befehl aus und stellen Sie sicher, dass Sie ihn ersetzen *`12abc34d567e8fa901bc2d34e56789f0`* mit der Melder-ID des delegierten GuardDuty Administratorkontos für die aktuelle Region.

Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite Einstellungen oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

Automatisches Aktivieren von S3 Protection für alle Mitgliedskonten in der Organisation

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit Ihrem Administratorkonto an.
2. Führen Sie eine der folgenden Aktionen aus:

Verwenden der Seite S3 Protection

1. Wählen Sie im Navigationsbereich S3 Protection.
2. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch S3 Protection sowohl für bestehende als auch für neue Konten in der Organisation.
3. Wählen Sie Save (Speichern) aus.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwenden der Seite Konten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten die Option Für alle Konten aktivieren unter S3 Protection.
4. Wählen Sie Save (Speichern) aus.

Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Selektive Aktivierung oder Deaktivierung von S3 Protection in Mitgliedskonten.

API/CLI

- Um S3 Protection für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen Konto auf *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. Stellen Sie sicher, dass Sie das Produkt ersetzen *`12abc34d567e8fa901bc2d34e56789f0`* mit dem `detector-id` des delegierten GuardDuty Administratorkontos und *`111122223333`*. Um den S3-Schutz zu deaktivieren, `ENABLED` ersetzen Sie ihn durch`DISABLED`.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie S3 Protection für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für alle vorhandenen aktiven Mitgliedskonten in Ihrer Organisation zu aktivieren.

Console

1. Melden Sie sich bei an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich S3 Protection.
3. Auf der Seite S3 Protection können Sie den aktuellen Status der Konfiguration anzeigen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Bestätigen aus.

API/CLI

- Um S3 Protection für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPIVorgang mit Ihren eigenen Konten auf *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. Stellen Sie sicher, dass Sie das Produkt ersetzen *`12abc34d567e8fa901bc2d34e56789f0`* mit dem `detector-id` des delegierten GuardDuty Administratorkontos und *`111122223333`*. Um den S3-Schutz zu deaktivieren, `ENABLED` ersetzen Sie ihn durch`DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Automatisches Aktivieren von S3 Protection für neue Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für neue Konten, die Ihrer Organisation beitreten, zu aktivieren.

Console

Das delegierte GuardDuty Administratorkonto kann über die Konsole entweder über die Seite S3-Schutz oder Konten neue Mitgliedskonten in einer Organisation aktivieren.

So richten Sie Automatisches Aktivieren von S3 Protection für neue Mitgliedskonten ein

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verwendung der Seite S3 Protection:
     1. Wählen Sie im Navigationsbereich S3 Protection.
     2. Wählen Sie auf der Seite S3 Protection die Option Bearbeiten.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass S3 Protection jedes mal automatisch für das Konto aktiviert wird, wenn ein neues Konto Ihrer Organisation beitritt. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Konfiguration ändern.
     5. Wählen Sie Save (Speichern) aus.
   - Verwenden der Seite Konten:
     1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
     2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren.
     3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter S3 Protection die Option Für neue Konten aktivieren.
     4. Wählen Sie Save (Speichern) aus.

API/CLI

- Um S3 Protection für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den UpdateOrganizationConfigurationAPIVorgang mit Ihrem eigenen Konto auf *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. Informationen zur Deaktivierung finden Sie unter Selektive Aktivierung oder Deaktivierung von S3 Protection in Mitgliedskonten. Legen Sie die Einstellungen so fest, dass der Schutzplan in dieser Region für neue Konten (`NEW`), die der Organisation beitreten, für alle Konten (`ALL`) oder für keines der Konten (`NONE`) in der Organisation automatisch aktiviert oder deaktiviert wird. Weitere Informationen finden Sie unter autoEnableOrganization Mitglieder. Je nach Ihren Einstellungen müssen Sie möglicherweise `NEW` durch `ALL` oder `NONE` ersetzen.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Selektive Aktivierung oder Deaktivierung von S3 Protection in Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um S3 Protection für bestimmte Mitgliedskonten zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Auf der Seite Konten finden Sie in der Spalte S3 Protection den Status Ihres Mitgliedskontos.
3. So können Sie S3 Protection selektiv aktivieren und deaktivieren

   Wählen Sie das Konto aus, für das Sie S3 Protection konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen. Wählen Sie im Dropdown-Menü Schutzpläne bearbeiten die Option S3Pro aus und wählen Sie dann die entsprechende Option aus.

API/CLI

Um S3 Protection für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihrer eigenen Melder-ID aus. Das folgende Beispiel

zeigt, wie Sie S3 Protection für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `true` durch `false`.

Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

> **Note**
>
> Wenn Sie Skripts verwenden, um neue Konten zu integrieren und den S3-Schutz in Ihren neuen Konten deaktivieren möchten, können Sie den createDetectorAPIVorgang mit dem optionalen `dataSources` Objekt ändern, wie in diesem Thema beschrieben.

Automatisches Deaktivieren von S3 Protection für neue Konten GuardDuty

> **Important**
>
> Standardmäßig ist S3 Protection für AWS-Konten diesen Beitritt GuardDuty zum ersten Mal automatisch aktiviert.

Wenn Sie ein GuardDuty Administratorkonto haben, das S3-Schutz zum ersten Mal GuardDuty für ein neues Konto aktiviert, und nicht möchten, dass S3 Protection standardmäßig aktiviert

wird, können Sie ihn deaktivieren, indem Sie den createDetectorAPIVorgang mit dem optionalen `features` Objekt ändern. Im folgenden Beispiel wird der verwendet AWS CLI , um einen neuen GuardDuty Detektor bei deaktiviertem S3-Schutz zu aktivieren.

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",
"Status" : "DISABLED"}]'
```

GuardDuty EKSSchutz

EKSAudit Log Monitoring hilft Ihnen dabei, potenziell verdächtige Aktivitäten in EKS Clustern innerhalb von Amazon Elastic Kubernetes Service (AmazonEKS) zu erkennen. EKSAudit Log Monitoring verwendet EKS Auditprotokolle, um chronologische Aktivitäten von Benutzern, Anwendungen, die Kubernetes verwenden, und der Kontrollebene API zu erfassen. Weitere Informationen finden Sie unter EKSÜberwachung des Auditprotokolls.

> **Note**
>
> EKSRuntime Monitoring wird als Teil von Runtime Monitoring verwaltet. Weitere Informationen finden Sie unter GuardDuty Überwachung der Laufzeit.

Funktionen im Bereich EKS Schutz

EKSÜberwachung des Auditprotokolls

EKSAudit-Logs erfassen sequentielle Aktionen innerhalb Ihres EKS Amazon-Clusters, einschließlich Aktivitäten von Benutzern, Anwendungen, die Kubernetes verwendenAPI, und der Kontrollebene. Die Prüfungs-Protokollierung ist eine Komponente aller Kubernetes-Cluster.

Weitere Informationen finden Sie unter Prüfung in der Kubernetes-Dokumentation.

Amazon EKS ermöglicht die Erfassung von EKS Auditprotokollen als CloudWatch Amazon-Logs über die Protokollierungsfunktion der EKS Kontrollebene. GuardDuty verwaltet Ihre Protokollierung auf der EKS Amazon-Kontrollebene nicht und macht auch keine EKS Auditprotokolle in Ihrem Konto zugänglich, wenn Sie sie nicht für Amazon aktiviert habenEKS. Um den Zugriff auf Ihre EKS Audit-Logs und deren Aufbewahrung zu verwalten, müssen Sie die Amazon EKS Control Plane Logging-Funktion konfigurieren. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von Control Plane-Protokollen im EKSAmazon-Benutzerhandbuch.

Informationen zur Konfiguration von EKS Audit Log Monitoring finden Sie unterEKSÜberwachung des Auditprotokolls.

EKSÜberwachung des Auditprotokolls

EKSMit Audit Log Monitoring können Sie potenziell verdächtige Aktivitäten in Ihren EKS Clustern innerhalb von Amazon Elastic Kubernetes Service erkennen. Wenn Sie EKS Audit Log Monitoring aktivieren, beginnt GuardDuty sofort mit der Überwachung EKSÜberwachung des Auditprotokolls Ihrer EKS Amazon-Cluster und deren Analyse auf potenziell bösartige und verdächtige Aktivitäten. Es verarbeitet Kubernetes-Audit-Log-Ereignisse direkt aus der Protokollierungsfunktion der Amazon EKS Control Plane über einen unabhängigen und duplizierten Stream von Audit-Logs. Dieser Prozess erfordert keine zusätzliche Einrichtung und wirkt sich auch nicht auf Ihre bestehenden Protokollierungskonfigurationen der EKS Amazon-Steuerebene aus.

Wenn Sie EKS Audit Log Monitoring deaktivieren, wird die Überwachung und Analyse der EKS Audit-Logs für Ihre EKS Amazon-Ressourcen GuardDuty sofort beendet.

EKSAudit Log Monitoring ist möglicherweise nicht überall verfügbar AWS-Regionen , wo GuardDuty es verfügbar ist. Weitere Informationen finden Sie unter Verfügbarkeit regionsspezifischer Feature.

Wie wirkt sich eine 30-tägige kostenlose Testphase auf Konten aus GuardDuty

- Wenn Sie EKS Audit Log Monitoring GuardDuty zum ersten Mal aktivieren, ist es bereits in der 30-tägigen kostenlosen Testphase enthalten.
- Die bestehenden GuardDuty Konten, für die die kostenlose 30-Tage-Testversion bereits abgeschlossen ist, können EKS Audit Log Monitoring mit einer 30-tägigen kostenlosen Testphase zum ersten Mal aktivieren.

Konfiguration von EKS Audit Log Monitoring für ein eigenständiges Konto

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für ein eigenständiges Konto zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich EKS Schutz aus.
3. Auf der Registerkarte Konfiguration können Sie den aktuellen Konfigurationsstatus von EKS Audit Log Monitoring einsehen. Wählen Sie im Abschnitt EKSAudit Log Monitoring die Option Aktivieren aus, um die Funktion EKS Audit Log Monitoring zu aktivieren, oder Deaktivieren, um sie zu deaktivieren.

4. Wählen Sie Save (Speichern) aus.

API/CLI

- Führen Sie den updateDetectorAPIVorgang mit der regionalen Detektor-ID des delegierten GuardDuty Administratorkontos aus und übergeben Sie den `features` Objektnamen als `EKS_AUDIT_LOGS` und den Status als `ENABLED` oder`DISABLED`.

  Alternativ können Sie EKS Audit Log Monitoring auch aktivieren oder deaktivieren, indem Sie den AWS CLI Befehl a ausführen. Der folgende Beispielcode aktiviert GuardDuty EKS Audit Log Monitoring. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
  ```

Konfiguration der EKS Auditprotokollüberwachung in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, die EKS Audit Log Monitoring; -Funktion für die Mitgliedskonten in ihrer Organisation zu aktivieren oder zu deaktivieren. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Dieses delegierte GuardDuty Administratorkonto kann wählen, ob die EKS Auditprotokollüberwachung für alle neuen Konten automatisch aktiviert werden soll, wenn sie der Organisation beitreten. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten bei Amazon. GuardDuty

Konfiguration von EKS Audit Log Monitoring für ein delegiertes Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Audit Log Monitoring für das delegierte GuardDuty Administratorkonto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen des Verwaltungskontos verwenden.
2. Wählen Sie im Navigationsbereich EKS Schutz aus.
3. Auf der Registerkarte Konfiguration können Sie den aktuellen Konfigurationsstatus von EKS Audit Log Monitoring im entsprechenden Abschnitt einsehen. Um die Konfiguration für das delegierte GuardDuty Administratorkonto zu aktualisieren, wählen Sie im Bereich EKSAudit Log Monitoring die Option Bearbeiten aus.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Save (Speichern) aus.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
   - Wählen Sie Save (Speichern) aus.

API/CLI

Führen Sie den updateDetectorAPIVorgang mit Ihrer eigenen regionalen Melder-ID aus und übergeben Sie das `features` Objekt `name` als `EKS_AUDIT_LOGS` und `status` als `ENABLED` oder`DISABLED`.

Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite „Einstellungen“ oder führen Sie den aus ListDetectorsAPI.

Sie können die EKS Auditprotokollüberwachung aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie ein gültiges delegiertes GuardDuty Administratorkonto verwenden *detector ID*.

> **Note**
>
> Der folgende Beispielcode aktiviert EKS Audit Log Monitoring. Stellen Sie sicher, dass Sie es ersetzen *12abc34d567e8fa901bc2d34e56789f0* mit dem `detector-id` des delegierten GuardDuty Administratorkontos und *555555555555* mit dem AWS-Konto des delegierten GuardDuty Administratorkontos.

Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite Einstellungen oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

Um EKS Audit Log Monitoring zu deaktivieren, `ENABLED` ersetzen Sie es durch`DISABLED`.

Automatische Aktivierung der EKS Auditprotokollüberwachung für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die EKS Auditprotokollüberwachung für bestehende Mitgliedskonten in Ihrer Organisation zu aktivieren.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   Verwenden Sie die EKSSchutzseite

   1. Wählen Sie im Navigationsbereich EKSSchutz aus.

2. Auf der Registerkarte Konfiguration können Sie den aktuellen Status der EKS Auditprotokollüberwachung für aktive Mitgliedskonten in Ihrer Organisation einsehen.

   Um die EKS Audit Log Monitoring-Konfiguration zu aktualisieren, wählen Sie Bearbeiten.

3. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch die Überwachung des EKS Auditprotokolls sowohl für die vorhandenen als auch für die neuen Konten in der Organisation.
4. Wählen Sie Save (Speichern) aus.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwenden der Seite Konten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter EKSAudit Log Monitoring die Option Für alle Konten aktivieren aus.
4. Wählen Sie Save (Speichern) aus.

Wenn Sie die Option „Für alle Konten aktivieren“ nicht verwenden können und die Konfiguration der EKS Auditprotokollüberwachung für bestimmte Konten in Ihrer Organisation anpassen möchten, finden Sie weitere Informationen unterAktiviere oder deaktiviere selektiv die EKS Audit-Log-Überwachung für Mitgliedskonten.

API/CLI

- Um die EKS Audit-Log-Überwachung selektiv für Ihre Mitgliedskonten zu aktivieren oder zu deaktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen aus *`detector ID`*.

- Das folgende Beispiel zeigt, wie Sie die EKS Auditprotokollüberwachung für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie die EKS Auditprotokollüberwachung für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die EKS Auditprotokollüberwachung für alle vorhandenen aktiven Mitgliedskonten in der Organisation zu aktivieren.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich EKSSchutz aus.
3. Auf der Seite EKSSchutz können Sie den aktuellen Status der GuardDuty-initiierten Malware-Scan-Konfiguration einsehen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.

4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Save (Speichern) aus.

API/CLI

- Um die EKS Audit-Log-Überwachung für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen aus *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie die EKS Auditprotokollüberwachung für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Automatische Aktivierung der EKS Auditprotokollüberwachung für neue Mitgliedskonten

Die neu hinzugefügten Mitgliedskonten müssen aktiviert werden, GuardDuty bevor der GuardDuty konfigurationsinitiierte Malware-Scan ausgewählt werden kann. Die auf Einladung verwalteten Mitgliedskonten können den GuardDuty -initiierten Malware-Scan für ihre Konten manuell konfigurieren. Weitere Informationen finden Sie unter Step 3 - Accept an invitation.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die EKS Auditprotokollüberwachung für neue Konten zu aktivieren, die Ihrer Organisation beitreten.

Console

Das delegierte GuardDuty Administratorkonto kann die EKS Auditprotokollüberwachung für neue Mitgliedskonten in einer Organisation entweder über die Seite EKSAuditprotokollüberwachung oder Konten aktivieren.

So aktivieren Sie die EKS Auditprotokollüberwachung für neue Mitgliedskonten automatisch

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verwenden Sie die EKSSchutzseite:
     1. Wählen Sie im Navigationsbereich EKSSchutz aus.
     2. Wählen Sie auf der Seite EKSSchutz unter EKSAudit Log Monitoring die Option Bearbeiten aus.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass bei jedem Beitritt eines neuen Kontos zu Ihrer Organisation die EKS Audit-Log-Überwachung automatisch für das Konto aktiviert wird. Nur das vom Unternehmen delegierte GuardDuty Administratorkonto kann diese Konfiguration ändern.
     5. Wählen Sie Save (Speichern) aus.
   - Verwenden der Seite Konten:
     1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
     2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren.
     3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter EKSAudit Log Monitoring die Option Für neue Konten aktivieren aus.
     4. Wählen Sie Save (Speichern) aus.

API/CLI

- Um die EKS Audit-Log-Überwachung für Ihre neuen Konten selektiv zu aktivieren oder zu deaktivieren, führen Sie den UpdateOrganizationConfigurationAPIVorgang mit Ihrem eigenen aus *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie die EKS Auditprotokollüberwachung für die neuen Mitglieder aktivieren können, die Ihrer Organisation beitreten. Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

Aktiviere oder deaktiviere selektiv die EKS Audit-Log-Überwachung für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die EKS Auditprotokollüberwachung für ausgewählte Mitgliedskonten in Ihrer Organisation zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Auf der Seite Konten finden Sie in der Spalte EKSAudit Log Monitoring den Status Ihres Mitgliedskontos.
3. Um die EKS Audit-Log-Überwachung zu aktivieren oder zu deaktivieren

   Wählen Sie ein Konto aus, das Sie für die EKS Auditprotokollüberwachung konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen. Wählen Sie in der Dropdownliste Schutzpläne bearbeiten die Option EKSAudit Log Monitoring und dann die entsprechende Option aus.

API/CLI

Um die EKS Auditprotokollüberwachung für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen Konto auf *detector ID*.

Das folgende Beispiel zeigt, wie Sie die EKS Auditprotokollüberwachung für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`. Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

GuardDuty Überwachung der Laufzeit

Runtime Monitoring beobachtet und analysiert Ereignisse auf Betriebssystemebene, Netzwerk- und Dateiereignisse, um Ihnen zu helfen, potenzielle Bedrohungen in bestimmten AWS Workloads in Ihrer Umgebung zu erkennen.

Unterstützte AWS Ressourcen in Runtime Monitoring — GuardDuty hatte Runtime Monitoring ursprünglich nur zur Unterstützung von Amazon Elastic Kubernetes Service (AmazonEKS) - Ressourcen veröffentlicht. Jetzt können Sie die Runtime Monitoring-Funktion verwenden, um Bedrohungen auch für Ihre AWS Fargate Amazon Elastic Container Service- (AmazonECS) - und Amazon Elastic Compute Cloud (AmazonEC2) -Ressourcen zu erkennen.

GuardDuty unterstützt keine EKS Amazon-Cluster, die auf AWS Fargate laufen.

In diesem Dokument und anderen Abschnitten, die sich auf Runtime Monitoring beziehen, GuardDuty verwendet die Terminologie des Ressourcentyps, um sich auf EC2 Ressourcen von AmazonEKS, FargateECS, Amazon und Amazon zu beziehen.

Runtime Monitoring verwendet einen GuardDuty Security Agent, der Einblick in das Laufzeitverhalten wie Dateizugriff, Prozessausführung, Befehlszeilenargumente und Netzwerkverbindungen bietet. Für jeden Ressourcentyp, den Sie auf potenzielle Bedrohungen überwachen möchten, können Sie den Security Agent für diesen spezifischen Ressourcentyp entweder automatisch oder manuell verwalten (mit Ausnahme von Fargate (ECSnur Amazon)). Wenn Sie den Security Agent automatisch verwalten, erlauben Sie, GuardDuty den Security Agent in Ihrem Namen zu installieren und zu aktualisieren. Wenn Sie den Security Agent für Ihre Ressourcen jedoch manuell verwalten, sind Sie dafür verantwortlich, den Security Agent bei Bedarf zu installieren und zu aktualisieren.

Mit dieser erweiterten Funktion GuardDuty können Sie potenzielle Bedrohungen identifizieren und darauf reagieren, die möglicherweise auf Anwendungen und Daten abzielen, die in Ihren individuellen Workloads und Instanzen ausgeführt werden. Beispielsweise kann eine Bedrohung potenziell damit beginnen, dass ein einzelner Container kompromittiert wird, auf dem eine anfällige Webanwendung ausgeführt wird. Diese Webanwendung verfügt möglicherweise über Zugriffsberechtigungen für die zugrunde liegenden Container und Workloads. In diesem Szenario könnten falsch konfigurierte Anmeldeinformationen möglicherweise zu einem umfassenderen Zugriff auf das Konto und die darin gespeicherten Daten führen.

Durch die Analyse der Laufzeitereignisse der einzelnen Container und Workloads GuardDuty kann in einer Anfangsphase potenziell eine Kompromittierung eines Containers und der zugehörigen

AWS Anmeldeinformationen erkannt und Versuche, Berechtigungen zu erweitern, verdächtige API Anfragen und böswillige Zugriffe auf die Daten in Ihrer Umgebung erkannt werden.

Inhalt

Funktionsweise

Um Runtime Monitoring verwenden zu können, müssen Sie Runtime Monitoring aktivieren und anschließend den GuardDuty Security Agent verwalten. In der folgenden Liste wird dieser zweistufige Prozess erklärt:

1. Aktivieren Sie Runtime Monitoring für Ihr Konto, damit es die Runtime-Ereignisse akzeptieren GuardDuty kann, die es von Ihren EC2 Amazon-Instances, ECS Amazon-Clustern und EKS Amazon-Workloads empfängt.
2. Verwalten Sie den GuardDuty Agenten für die einzelnen Ressourcen, für die Sie das Laufzeitverhalten überwachen möchten. Je nach Ressourcentyp können Sie wählen, ob Sie den GuardDuty Security Agent entweder manuell installieren oder ihn in Ihrem Namen verwalten lassen GuardDuty möchten. Dies wird als automatische Agentenkonfiguration bezeichnet.

   GuardDuty verwendet Instanzidentitätsrollen, die den Security Agent für jeden Ressourcentyp authentifizieren, um die zugehörigen Runtime-Ereignisse an den VPC Endpunkt zu senden.

> **Note**
>
> GuardDuty macht Ihnen die Runtime-Ereignisse nicht zugänglich.

Wenn Sie den Security Agent (entweder manuell oder über GuardDuty) in EKS Runtime Monitoring oder Runtime Monitoring für EC2 Instances verwalten und derzeit auf einer EC2 Amazon-Instance bereitgestellt GuardDuty ist und diese Gesammelte Laufzeit-Ereignistypen von dieser Instance erhält, fallen GuardDuty Ihnen keine Gebühren AWS-Konto für die Analyse der VPC Flow-Logs dieser EC2 Amazon-Instance an. Dies trägt dazu bei, doppelte Nutzungskosten für das Konto zu GuardDuty vermeiden.

In den folgenden Themen wird erklärt, wie die Aktivierung von Runtime Monitoring und die Verwaltung des GuardDuty Security Agents für jeden Ressourcentyp unterschiedlich funktionieren.

Inhalt

So funktioniert Runtime Monitoring mit EC2 Amazon-Instances

Ihre EC2 Amazon-Instances können mehrere Arten von Anwendungen und Workloads in Ihrer AWS Umgebung ausführen. Wenn Sie Runtime Monitoring aktivieren und den GuardDuty Security Agent verwalten, GuardDuty hilft er Ihnen, Bedrohungen in Ihren bestehenden EC2 Amazon-Instances und potenziell neuen zu erkennen. Diese Funktion unterstützt auch von Amazon ECS verwaltete EC2 Amazon-Instances.

Durch die Aktivierung von Runtime Monitoring können Runtime-Ereignisse von aktuell laufenden und neuen Prozessen innerhalb von EC2 Amazon-Instances verarbeitet werden. GuardDuty GuardDuty erfordert einen Security Agent, um Runtime-Ereignisse von Ihrer EC2 Instance an zu senden GuardDuty.

Bei EC2 Amazon-Instances arbeitet der GuardDuty Security Agent auf Instance-Ebene. Sie können entscheiden, ob Sie alle oder nur ausgewählte EC2 Amazon-Instances in Ihrem Konto überwachen

möchten. Wenn Sie ausgewählte Instances verwalten möchten, ist der Security Agent nur für diese Instances erforderlich.

GuardDuty kann auch Laufzeitereignisse von neuen Aufgaben und bestehenden Aufgaben, die in EC2 Amazon-Instances innerhalb von ECS Amazon-Clustern ausgeführt werden, verarbeiten.

Um den GuardDuty Security Agent zu installieren, bietet Runtime Monitoring die folgenden zwei Optionen:

- Verwenden Sie die automatische Agentenkonfiguration (empfohlen), oder
- Den Security Agent manuell verwalten

Verwenden Sie die automatische Agentenkonfiguration über GuardDuty (empfohlen)

Verwenden Sie die automatische Agentenkonfiguration, die es GuardDuty ermöglicht, den Security Agent in Ihrem Namen auf Ihren EC2 Amazon-Instances zu installieren. GuardDuty verwaltet auch die Updates für den Security Agent.

GuardDuty Installiert den Security Agent standardmäßig auf allen Instanzen in Ihrem Konto. Wenn Sie den Security Agent nur für ausgewählte EC2 Instances installieren und verwalten möchten GuardDuty , fügen Sie Ihren EC2 Instances nach Bedarf Inklusions- oder Ausschluss-Tags hinzu.

Manchmal möchten Sie möglicherweise nicht die Laufzeitereignisse für alle EC2 Amazon-Instances überwachen, die zu Ihrem Konto gehören. In Fällen, in denen Sie die Runtime-Ereignisse für eine begrenzte Anzahl von Instances überwachen möchten, fügen Sie diesen ausgewählten Instances ein Inklusion-Tag wie`GuardDutyManaged`: `true` hinzu. Beginnend mit der Verfügbarkeit der automatisierten Agentenkonfiguration für Amazon EC2 gilt: Wenn Ihre EC2 Instance über ein Inclusion-Tag (`GuardDutyManaged`:`true`) verfügt, GuardDuty berücksichtigt das Tag und verwaltet den Security Agent für die ausgewählten Instances, auch wenn Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

Wenn es jedoch eine begrenzte Anzahl von EC2 Instances gibt, für die Sie Laufzeitereignisse nicht überwachen möchten, fügen Sie diesen ausgewählten Instances ein Ausschluss-Tag (`GuardDutyManaged`:`false`) hinzu. GuardDuty berücksichtigt das Ausschluss-Tag, indem der Security Agent für diese EC2 Ressourcen weder installiert noch verwaltet wird.

Auswirkung

Wenn Sie die automatische Agentenkonfiguration in einer AWS-Konto oder einer Organisation verwenden, GuardDuty erlauben Sie, die folgenden Schritte in Ihrem Namen durchzuführen:

- GuardDuty erstellt eine SSM Zuordnung für all Ihre EC2 Amazon-Instances, die SSM verwaltet werden und in der https://console.aws.amazon.com/systems-manager/Konsole unter Fleet Manager angezeigt werden.
- Verwendung von Inclusion-Tags bei deaktivierter automatisierter Agentenkonfiguration — Wenn Sie nach der Aktivierung von Runtime Monitoring die automatische Agentenkonfiguration nicht aktivieren, sondern Ihrer EC2 Amazon-Instance ein Inklusion-Tag hinzufügen, bedeutet dies, dass Sie die Verwaltung des Security Agents in Ihrem Namen gestatten GuardDuty . SSMDie Assoziation installiert dann den Security Agent in jeder Instance, die über das Inclusion-Tag (`GuardDutyManaged:true`) verfügt.
- Wenn Sie die automatische Agentenkonfiguration aktivieren — Die SSM Assoziation installiert dann den Security Agent auf allen EC2 Instanzen, die zu Ihrem Konto gehören.
- Ausschluss-Tags mit automatisierter Agentenkonfiguration verwenden — Bevor Sie die automatische Agentenkonfiguration aktivieren und Ihrer EC2 Amazon-Instance ein Ausschluss-Tag hinzufügen, bedeutet dies, dass Sie die Installation und Verwaltung des Security Agents für diese ausgewählte Instance verhindern. GuardDuty

  Wenn Sie nun die automatische Agentenkonfiguration aktivieren, installiert und verwaltet die SSM Assoziation den Security Agent in allen Instances mit Ausnahme der EC2 Instances, die mit dem Ausschluss-Tag gekennzeichnet sind.
- GuardDuty erstellt VPC Endpoints in allenVPCs, auch gemeinsam genutztenVPCs, sofern mindestens eine EC2 Linux-Instance vorhanden ist, VPC die sich nicht im Instanzstatus „Beendet“ oder „Herunterfahren“ befindet. Dazu gehören die Versionen „Central“ und „Spoke“. VPC VPCs GuardDuty unterstützt nicht die Erstellung eines VPC Endpunkts nur für zentralisierte BenutzerVPC. Weitere Informationen zur VPC Funktionsweise der zentralisierten Lösung finden Sie unter VPCSchnittstellenendpunkte im AWS Whitepaper Aufbau einer skalierbaren und sicheren VPC AWS Multi-Netzwerk-Infrastruktur.

  Informationen zu den verschiedenen Instance-Status finden Sie unter Instance-Lebenszyklus im EC2Amazon-Benutzerhandbuch.

  GuardDuty unterstützt auchWird gemeinsam VPC mit automatisierten Security Agents verwendet. Wenn alle Voraussetzungen für Ihre Organisation erfüllt sind und AWS-Konto das Shared VPC zum Empfangen von Laufzeitereignissen verwendet GuardDuty wird.

> **Note**
>
> Für die Nutzung des VPC Endpunkts fallen keine zusätzlichen Kosten an.

Den Security Agent manuell verwalten

Es gibt zwei Möglichkeiten, den Security Agent für Amazon EC2 manuell zu verwalten:

- Verwenden Sie GuardDuty verwaltete Dokumente in AWS Systems Manager , um den Security Agent auf Ihren bereits SSM verwalteten EC2 Amazon-Instances zu installieren.

  Wenn Sie eine neue EC2 Amazon-Instance starten, stellen Sie sicher, dass sie SSM aktiviert ist.
- Verwenden Sie RPM Paketmanager (RPM) -Skripts, um den Security Agent auf Ihren EC2 Amazon-Instances zu installieren, unabhängig davon, ob diese SSM verwaltet werden oder nicht.

Nächster Schritt

Erste Schritte mit der Runtime Monitoring-Konfiguration zur Überwachung Ihrer EC2 Amazon-Instances finden Sie unterVoraussetzungen für die Unterstützung Amazon EC2 Amazon-Instances.

So funktioniert Runtime Monitoring mit Fargate (ECSnur Amazon)

Wenn Sie Runtime Monitoring aktivieren, ist GuardDuty es bereit, die Laufzeitereignisse einer Aufgabe zu verarbeiten. Diese Aufgaben werden innerhalb der ECS Amazon-Cluster ausgeführt, die wiederum auf den AWS Fargate (Fargate) Instances ausgeführt werden. GuardDuty Um diese Runtime-Ereignisse empfangen zu können, müssen Sie den vollständig verwalteten, dedizierten Security Agent verwenden.

Runtime Monitoring unterstützt die Verwaltung des Security Agents für Ihre ECS Amazon-Cluster (AWS Fargate) nur über GuardDuty. Die manuelle Verwaltung des Security Agents auf ECS Amazon-Clustern wird nicht unterstützt.

Sie können zulassen GuardDuty , dass der GuardDuty Security Agent in Ihrem Namen verwaltet wird, indem Sie die automatische Agentenkonfiguration für ein AWS Konto oder eine Organisation verwenden. GuardDuty beginnt mit der Bereitstellung des Security Agents für die neuen Fargate-Aufgaben, die in Ihren ECS Amazon-Clustern gestartet werden. In der folgenden Liste wird angegeben, was zu erwarten ist, wenn Sie den GuardDuty Security Agent aktivieren.

Auswirkungen der Aktivierung des GuardDuty Security Agents

GuardDuty erstellt einen virtuellen privaten Cloud-Endpunkt (VPC)

Wenn Sie den GuardDuty Security Agent bereitstellen, GuardDuty erstellt er einen VPC Endpunkt, über den der Security Agent die Runtime-Ereignisse übermittelt GuardDuty.

> **Hinweise**
>
> - Arbeiten VPC mit zentralisiertem und automatisiertem Agenten — Wenn Sie die GuardDuty automatische Agentenkonfiguration für einen Ressourcentyp verwenden, GuardDuty wird in Ihrem Namen ein VPC Endpunkt für alle VPCs Dazu gehören der zentralisierte Modus VPC und der Spoke-ModusVPCs. GuardDuty unterstützt nicht die Erstellung eines VPC Endpunkts nur für zentralisierte BenutzerVPC. Weitere Informationen zur VPC Funktionsweise der zentralisierten Lösung finden Sie unter VPCSchnittstellenendpunkte im AWS Whitepaper Aufbau einer skalierbaren und sicheren VPC AWS Multi-Netzwerk-Infrastruktur.
> - Für die Nutzung des Endpunkts fallen keine zusätzlichen Kosten anVPC.

GuardDuty fügt einen Sidecar-Container hinzu

Bei einer neuen Fargate-Aufgabe oder einem neuen Fargate-Dienst, der gestartet wird, hängt sich ein GuardDuty Container (Sidecar) an jeden Container innerhalb der Amazon Fargate-Aufgabe an. ECS Der GuardDuty Security Agent wird innerhalb des angehängten Containers ausgeführt. GuardDuty Auf diese Weise GuardDuty können die Laufzeitereignisse jedes Containers erfasst werden, der im Rahmen dieser Tasks ausgeführt wird.

Wenn Sie eine Fargate-Aufgabe starten und der GuardDuty Container (Sidecar) nicht in einem fehlerfreien Zustand gestartet werden kann, ist Runtime Monitoring so konzipiert, dass die Ausführung der Aufgaben nicht verhindert wird.

Standardmäßig ist eine Fargate-Aufgabe unveränderlich. GuardDuty stellt den Sidecar nicht bereit, wenn sich eine Aufgabe bereits im laufenden Zustand befindet. Wenn Sie einen Container in einer bereits laufenden Aufgabe überwachen möchten, können Sie die Aufgabe beenden und erneut starten.

So funktioniert Runtime Monitoring mit EKS Amazon-Clustern

Runtime Monitoring verwendet ein EKSAdd-on `aws-guardduty-agent`, das auch als GuardDuty Security Agent bezeichnet wird. Nachdem der GuardDuty Security Agent auf Ihren EKS Clustern installiert wurde, GuardDuty kann er Runtime-Ereignisse für diese EKS Cluster empfangen.

GuardDuty unterstützt EKS Amazon-Cluster, die nur auf EC2 Amazon-Instances ausgeführt werden. GuardDuty unterstützt keine EKS Amazon-Cluster, die auf AWS Fargate laufen.

Sie können die Laufzeitereignisse Ihrer EKS Amazon-Cluster entweder auf Konto- oder Clusterebene überwachen. Sie können den GuardDuty Security Agent nur für die EKS Amazon-Cluster verwalten, die Sie im Hinblick auf die Erkennung von Bedrohungen überwachen möchten. Sie können den GuardDuty Security Agent entweder manuell verwalten oder indem GuardDuty Sie die automatische Agentenkonfiguration verwenden, indem Sie die automatische Agentenkonfiguration verwenden.

Wenn Sie den Ansatz der automatisierten Agentenkonfiguration verwenden, GuardDuty um die Bereitstellung des Security Agents in Ihrem Namen zu verwalten, wird automatisch ein Amazon Virtual Private Cloud (AmazonVPC) -Endpunkt erstellt. Der Security Agent übermittelt die Runtime-Ereignisse über diesen VPC Amazon-Endpunkt an. GuardDuty

Hinweise

- Für die Nutzung des VPC Endpunkts fallen keine zusätzlichen Kosten an.
- Arbeiten VPC mit zentralisiertem und automatisiertem Agenten — Wenn Sie die GuardDuty automatische Agentenkonfiguration für einen Ressourcentyp verwenden, GuardDuty wird in Ihrem Namen ein VPC Endpunkt für alle erstelltVPCs. Dazu gehören der zentralisierte Modus VPC und der Spoke-ModusVPCs. GuardDuty unterstützt nicht die Erstellung eines VPC Endpunkts nur für zentralisierte BenutzerVPC. Weitere Informationen zur VPC Funktionsweise der zentralisierten Lösung finden Sie unter VPCSchnittstellenendpunkte im AWS Whitepaper Aufbau einer skalierbaren und sicheren VPC AWS Multi-Netzwerk-Infrastruktur.

Nach der Konfiguration von Runtime Monitoring

Beurteilen Sie die Runtime-Abdeckung

Nachdem Sie Runtime Monitoring aktiviert und den GuardDuty Security Agent installiert haben, empfehlen wir Ihnen, den Abdeckungsstatus der Ressource, auf der Sie den Security Agent installiert haben, kontinuierlich zu überprüfen. Der Schutzstatus kann entweder fehlerfrei oder fehlerfrei sein. Der Deckungsstatus Fehlerfrei gibt an, dass GuardDuty die Laufzeitereignisse von der entsprechenden Ressource empfangen werden, wenn eine Aktivität auf Betriebssystemebene stattfindet.

Wenn der Abdeckungsstatus für die Ressource Fehlerfrei GuardDuty lautet, kann sie die Laufzeitereignisse empfangen und sie zur Erkennung von Bedrohungen analysieren. Wenn eine potenzielle Sicherheitsbedrohung in den Aufgaben oder Anwendungen GuardDuty erkannt wird, die in Ihren Container-Workloads und -Instances ausgeführt werden, GuardDuty generiert das Programm einen oder mehrere Runtime Monitoring-Findetypen.

Sie können Amazon EventBridge (EventBridge) auch so konfigurieren, dass Sie eine Benachrichtigung erhalten, wenn sich der Versicherungsstatus von Ungesund auf Gesund usw. ändert. Weitere Informationen finden Sie unter Bewertung der Laufzeitabdeckung Ihrer Ressourcen.

Einrichtung CPU und Speicherüberwachung für den GuardDuty Security Agent

Nachdem Sie festgestellt haben, dass der Schutzstatus als Fehlerfrei angezeigt wird, können Sie die Leistung des Security Agents für Ihren Ressourcentyp bewerten. GuardDuty Unterstützt für EKS Amazon-Cluster mit dem Security Agent Version v1.5 oder höher die Konfiguration der Parameter des (Add-on-) Security Agents. Weitere Informationen finden Sie unter Einrichtung CPU und Speicherüberwachung.

GuardDuty erkennt potenzielle Bedrohungen

Sobald GuardDuty die Laufzeitereignisse für Ihre Ressource empfangen werden, beginnt es mit der Analyse dieser Ereignisse. Wenn eine potenzielle Sicherheitsbedrohung in einer Ihrer EC2 Amazon-Instances, ECS Amazon-Clustern oder EKS Amazon-Clustern GuardDuty erkannt wird, generiert es eine oder mehrereRuntime Monitoring: Typen finden. Sie können auf die Ergebnisdetails zugreifen, um die betroffenen Ressourcen einzusehen.

Wie funktioniert die kostenlose 30-Tage-Testversion in Runtime Monitoring

Die 30-tägige kostenlose Testphase funktioniert für neue GuardDuty Konten anders als für bestehende Konten, für die EKS Runtime Monitoring bereits aktiviert wurde, bevor die Runtime Monitoring-Funktion auf EC2 Amazon-Instances und AWS Fargate (ECSnur Amazon) ausgedehnt wurde.

Ich verwende die GuardDuty Testphase oder habe EKS Runtime Monitoring noch nie aktiviert

In der folgenden Liste wird erklärt, wie die kostenlose 30-Tage-Testphase funktioniert, wenn Sie entweder die GuardDuty 30-Tage-Testphase verwenden oder EKS Runtime Monitoring noch nie aktiviert haben:

- Wenn Sie Runtime Monitoring und Runtime Monitoring GuardDuty zum ersten Mal aktivieren, sind EKS Runtime Monitoring und Runtime Monitoring standardmäßig nicht aktiviert.

  Wenn Sie Runtime Monitoring für Ihr Konto oder Ihre Organisation aktivieren, stellen Sie sicher, dass Sie auch den GuardDuty Security Agent für die Ressource konfigurieren, die Sie auf Bedrohungserkennung überwachen möchten. Wenn Sie beispielsweise Runtime Monitoring für Ihre EC2 Amazon-Instances verwenden möchten, müssen Sie nach der Aktivierung von Runtime Monitoring auch den Security Agent für Amazon konfigurierenEC2. Sie können wählen, ob Sie dies manuell oder automatisch über tun möchten GuardDuty.
- Der Runtime Monitoring-Schutzplan ist auf Kontoebene aktiviert. Die kostenlose 30-Tage-Testphase gilt auf Ressourcenebene. Nachdem der GuardDuty Security Agent für einen bestimmten Ressourcentyp bereitgestellt wurde, beginnt die kostenlose 30-Tage-Testversion, sobald GuardDuty das erste Runtime-Ereignis im Zusammenhang mit diesem Ressourcentyp eintrifft. Sie haben den GuardDuty Agenten beispielsweise auf Ressourcenebene bereitgestellt (für EC2 Amazon-Instance, ECS Amazon-Cluster und EKS Amazon-Cluster). Wenn das GuardDuty erste Runtime-Event für eine EC2 Amazon-Instance eingeht, startet die kostenlose 30-Tage-Testversion EC2 nur für Amazon.
- Wenn Sie nur EKS Runtime Monitoring aktivieren möchten — Wenn Sie Runtime Monitoring GuardDuty zum ersten Mal aktivieren, ist EKS Runtime Monitoring standardmäßig nicht aktiviert (nach der Veröffentlichung von Runtime Monitoring). Sie müssen EKS Runtime Monitoring aktivieren. Um ihn optimal zu nutzen, stellen Sie sicher, dass Sie den GuardDuty Security Agent

entweder manuell verwalten oder die automatische Agentenkonfiguration aktivieren, sodass der Agent in Ihrem Namen GuardDuty verwaltet wird. Ihre 30-tägige kostenlose Testphase für EKS Runtime Monitoring beginnt, wenn GuardDuty das erste Runtime-Ereignis für die EKS Amazon-Ressource eingeht.

Ich habe EKS Runtime Monitoring vor dem Start von Runtime Monitoring aktiviert

- Für ein vorhandenes GuardDuty Konto, für das der EKS Runtime Monitoring-Schutzplan aktiviert ist und das die GuardDuty Konsolenerfahrung verwendet, um diesen Schutzplan zu verwenden — Mit der Ankündigung von Runtime Monitoring wurde das Erlebnis der EKS Runtime Monitoring-Konsole nun in Runtime Monitoring konsolidiert. Ihre bestehende Konfiguration für EKS Runtime Monitoring bleibt unverändert. Sie können die API CLI /-Unterstützung weiterhin verwenden, um Operationen im Zusammenhang mit EKS Runtime Monitoring auszuführen.
- Um EKS Runtime Monitoring als Teil von Runtime Monitoring verwenden zu können, müssen Sie Runtime Monitoring für Ihr Konto oder Ihre Organisation konfigurieren. Informationen zur Beibehaltung derselben Konfiguration für Runtime Monitoring finden Sie unterMigration von EKS Runtime Monitoring zu Runtime Monitoring. Dies hat jedoch keine Auswirkungen auf Ihre kostenlose 30-Tage-Testversion für EKS Amazon-Ressourcen.
- Der Runtime Monitoring-Schutzplan ist auf Kontoebene pro Region aktiviert. Nachdem der GuardDuty Security Agent auf einem der angegebenen Ressourcentypen (EC2Amazon-Instance und ECS Amazon-Cluster) bereitgestellt wurde, beginnt die kostenlose 30-Tage-Testversion, sobald das erste Runtime-Ereignis im Zusammenhang mit der Ressource GuardDuty empfangen wird. Für jeden Ressourcentyp ist eine kostenlose 30-Tage-Testversion verfügbar.

  Wenn Sie beispielsweise Runtime Monitoring aktiviert haben, entscheiden Sie sich dafür, den GuardDuty Agenten nur auf einer EC2 Amazon-Instance bereitzustellen. Die kostenlose 30-Tage-Testversion für diese Ressource beginnt erst, wenn das erste Runtime-Ereignis für eine EC2 Amazon-Instance GuardDuty empfangen wird. Später, wenn Sie den GuardDuty Agenten für Fargate (ECSnur Amazon) bereitstellen, beginnt die kostenlose 30-Tage-Testversion für diese Ressource erst, wenn das erste Runtime-Ereignis für den ECS Amazon-Cluster GuardDuty empfangen wird. Da Sie EKS Runtime Monitoring bereits für Ihr Konto aktiviert haben, wird die kostenlose 30-Tage-Testversion für eine EKS Amazon-Ressource GuardDuty nicht zurückgesetzt.

Die wichtigsten Konzepte — Ansätze zur Verwaltung von GuardDuty Security Agents

Beachten Sie die wichtigsten Konzepte, die Ihnen bei der Verwaltung des Security Agents auf Ihren EKS Amazon-Clustern und ECS Amazon-Clustern helfen.

Inhalt

Fargate-Ressource (ECSnur Amazon) — Methoden zur Verwaltung von GuardDuty Sicherheitsagenten

Runtime Monitoring bietet Ihnen die Möglichkeit, potenzielle Sicherheitsbedrohungen entweder auf allen ECS Amazon-Clustern (Kontoebene) oder auf ausgewählten Clustern (Cluster-Ebene) in Ihrem Konto zu erkennen. Wenn Sie die automatische Agentenkonfiguration für jede auszuführende Amazon ECS Fargate-Aufgabe aktivieren, GuardDuty wird für jeden Container-Workload innerhalb dieser Aufgabe ein Sidecar-Container hinzugefügt. Der GuardDuty Security Agent wird in diesem Sidecar-Container bereitgestellt. Auf diese Weise GuardDuty erhalten Sie Einblick in das Laufzeitverhalten der Container in den ECS Amazon-Aufgaben.

Runtime Monitoring unterstützt die Verwaltung des Security Agents für Ihre ECS Amazon-Cluster (AWS Fargate) nur über GuardDuty. Die manuelle Verwaltung des Security Agents auf ECS Amazon-Clustern wird nicht unterstützt.

Bevor Sie Ihre Konten konfigurieren, sollten Sie abwägen, wie Sie den GuardDuty Security Agent verwalten und möglicherweise das Laufzeitverhalten der Container überwachen möchten, die zu den ECS Amazon-Aufgaben gehören. Ziehen Sie die folgenden Ansätze in Betracht.

Themen

GuardDuty Sicherheitsagenten für alle ECS Amazon-Cluster verwalten

Dieser Ansatz hilft Ihnen dabei, potenzielle Sicherheitsbedrohungen auf Kontoebene zu erkennen. Verwenden Sie diesen Ansatz, wenn Sie potenzielle Sicherheitsbedrohungen für alle ECS Amazon-Cluster erkennen möchten GuardDuty , die zu Ihrem Konto gehören.

Den GuardDuty Sicherheitsagenten für die meisten ECS Amazon-Cluster verwalten, einige ECS Amazon-Cluster jedoch ausschließen

Verwenden Sie diesen Ansatz, wenn GuardDuty Sie potenzielle Sicherheitsbedrohungen für die meisten ECS Amazon-Cluster in Ihrer AWS Umgebung erkennen, einige Cluster jedoch ausschließen möchten. Dieser Ansatz hilft Ihnen, das Laufzeitverhalten der Container innerhalb Ihrer ECS Amazon-Aufgaben auf Cluster-Ebene zu überwachen. Die Anzahl der ECS Amazon-Cluster, die zu Ihrem Konto gehören, beträgt beispielsweise 1000. Sie möchten jedoch nur 930 ECS Amazon-Cluster überwachen.

Bei diesem Ansatz müssen Sie den ECS Amazon-Clustern, die Sie nicht überwachen möchten, ein vordefiniertes GuardDuty Tag hinzufügen. Weitere Informationen finden Sie unter Verwaltung eines automatisierten Sicherheitsagenten für Fargate (ECSnur Amazon).

GuardDuty Sicherheitsagenten für ausgewählte ECS Amazon-Cluster verwalten

Verwenden Sie diesen Ansatz, wenn GuardDuty Sie potenzielle Sicherheitsbedrohungen für einige ECS Amazon-Cluster erkennen möchten. Dieser Ansatz hilft Ihnen, das Laufzeitverhalten der Container innerhalb Ihrer ECS Amazon-Aufgaben auf Cluster-Ebene zu überwachen. Die Anzahl der ECS Amazon-Cluster, die zu Ihrem Konto gehören, beträgt beispielsweise 1000. Sie möchten jedoch nur 230 Cluster überwachen.

Bei diesem Ansatz müssen Sie den ECS Amazon-Clustern, die Sie überwachen möchten, ein vordefiniertes GuardDuty Tag hinzufügen. Weitere Informationen finden Sie unter Verwaltung eines automatisierten Sicherheitsagenten für Fargate (ECSnur Amazon).

EKSAmazon-Cluster — Ansätze zur Verwaltung von GuardDuty Sicherheitsagenten

GuardDuty Um die Runtime-Ereignisse aus Ihren EKS Clustern auf Konto- oder Cluster-Ebene verarbeiten zu können, müssen Sie den GuardDuty Security Agent für die entsprechenden Cluster verwalten.

Methoden zur Verwaltung des GuardDuty Security Agents

Vor dem 13. September 2023 konnten Sie den Security Agent so konfigurieren, GuardDuty dass er auf Kontoebene verwaltet wird. Dieses Verhalten deutete darauf hin, dass der Security Agent standardmäßig auf allen EKS Clustern verwaltet GuardDuty wird, die zu einem gehören AWS-Konto. GuardDuty Bietet jetzt eine detaillierte Funktion, die Sie bei der Auswahl der EKS Cluster unterstützt, auf denen Sie den Security Agent verwalten GuardDuty möchten.

Wenn Sie möchtenDen GuardDuty Security Agent manuell verwalten, können Sie immer noch die EKS Cluster auswählen, die Sie überwachen möchten. Um den Agenten jedoch manuell verwalten zu können, ist die Erstellung eines VPC Amazon-Endpunkts für Sie AWS-Konto eine Grundvoraussetzung.

> **Note**
>
> Unabhängig davon, welchen Ansatz Sie zur Verwaltung des GuardDuty Security Agents verwenden, ist EKS Runtime Monitoring immer auf Kontoebene aktiviert.

Themen

- Verwalten Sie den Security Agent über GuardDuty
- Den GuardDuty Security Agent manuell verwalten

Verwalten Sie den Security Agent über GuardDuty

GuardDuty verteilt und verwaltet den Security Agent in Ihrem Namen. Sie können die EKS Cluster in Ihrem Konto jederzeit überwachen, indem Sie eine der folgenden Methoden verwenden.

Themen

- Überwachen Sie alle EKS Cluster
- Überwachen Sie alle EKS Cluster und schließen Sie ausgewählte EKS Cluster aus
- Überwachen Sie ausgewählte Cluster EKS

Überwachen Sie alle EKS Cluster

- Wann sollten Sie diesen Ansatz verwenden — Verwenden Sie diesen Ansatz GuardDuty , wenn Sie den Security Agent für alle EKS Cluster in Ihrem Konto bereitstellen und verwalten möchten.

Standardmäßig GuardDuty wird der Security Agent auch auf einem potenziell neuen EKS Cluster installiert, der in Ihrem Konto erstellt wurde.

- Auswirkungen dieses Ansatzes:
  - GuardDuty erstellt einen Amazon Virtual Private Cloud (AmazonVPC) -Endpunkt, über den der GuardDuty Security Agent die Runtime-Ereignisse übermittelt GuardDuty. Es fallen keine zusätzlichen Kosten für die Erstellung des VPC Amazon-Endpunkts an, wenn Sie den Security Agent über verwalten GuardDuty.
  - Es ist erforderlich, dass Ihr Worker-Knoten über einen gültigen Netzwerkpfad zu einem aktiven `guardduty-data` VPC Endpunkt verfügt. GuardDuty verteilt den Security Agent auf Ihren EKS Clustern. Amazon Elastic Kubernetes Service (AmazonEKS) koordiniert die Bereitstellung des Security Agents auf den Knoten innerhalb der EKS Cluster.
  - GuardDuty Wählt auf der Grundlage der IP-Verfügbarkeit das Subnetz aus, um einen Endpunkt zu erstellen. VPC Wenn Sie erweiterte Netzwerktopologien verwenden, müssen Sie überprüfen, ob die Konnektivität möglich ist.
- Überlegung — Wenn Sie diese Option verwenden, erstellt EKS Runtime Monitoring derzeit kein geteiltes. VPC

Überwachen Sie alle EKS Cluster und schließen Sie ausgewählte EKS Cluster aus

- Wann Sie diesen Ansatz verwenden sollten — Verwenden Sie diesen Ansatz, wenn Sie den Security Agent für alle EKS Cluster in Ihrem Konto verwalten, aber ausgewählte EKS Cluster ausschließen möchten GuardDuty . Bei dieser Methode wird ein Tag-basierter Ansatz verwendet, bei dem Sie die EKS Cluster taggen können, für die Sie keine Runtime-Ereignisse erhalten möchten. Das vordefinierte Tag muss `GuardDutyManaged-false` als Schlüssel-Wert-Paar haben.
- Auswirkungen dieses Ansatzes:
  - Bei diesem Ansatz müssen Sie die automatische GuardDuty Agentenverwaltung erst aktivieren, nachdem Sie den EKS Clustern, die Sie von der Überwachung ausschließen möchten, Tags hinzugefügt haben.

    Daher gilt auch für diesen Ansatz die Auswirkung von Verwalten Sie den Security Agent über GuardDuty. Wenn Sie Tags hinzufügen, bevor Sie die automatische GuardDuty Agentenverwaltung aktivieren, GuardDuty wird der Security Agent für die EKS Cluster, die von der Überwachung ausgeschlossen sind, weder bereitgestellt noch verwaltet.
- Überlegungen:

- Sie müssen das Tag-Schlüssel-Wert-Paar wie folgt hinzufügen`GuardDutyManaged: false` für die ausgewählten EKS Cluster, bevor Sie die automatische Agentenkonfiguration aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern installiert, bis Sie das Tag verwenden.
- Sie müssen verhindern, dass die Tags geändert werden, es sei denn, es handelt sich um vertrauenswürdige Identitäten.

> **Important**
>
> Verwalten Sie die Berechtigungen für die Änderung des `GuardDutyManaged` Tag-Werts für Ihren EKS Cluster mithilfe von Dienststeuerungsrichtlinien oder IAM -richtlinien. Weitere Informationen finden Sie unter Dienststeuerungsrichtlinien (SCPs) im AWS Organizations Benutzerhandbuch oder Steuern des Zugriffs auf AWS Ressourcen im IAMBenutzerhandbuch.

- Bei einem potenziell neuen EKS Cluster, den Sie nicht überwachen möchten, stellen Sie sicher, dass Sie bei der Erstellung dieses EKS Clusters das `GuardDutyManaged false` Schlüssel-Wert-Paar hinzufügen.
- Bei diesem Ansatz werden auch dieselben Überlegungen berücksichtigt, wie für Überwachen Sie alle EKS Cluster angegeben.

Überwachen Sie ausgewählte Cluster EKS

- Wann sollten Sie diesen Ansatz verwenden — Verwenden Sie diesen Ansatz, wenn Sie die Updates für den Security Agent nur für ausgewählte EKS Cluster in Ihrem Konto verteilen und verwalten möchten GuardDuty . Bei dieser Methode wird ein Tag-basierter Ansatz verwendet, bei dem Sie den EKS Cluster taggen können, für den Sie die Runtime-Ereignisse empfangen möchten.
- Auswirkungen dieses Ansatzes:
  - Mithilfe von Inklusion-Tags GuardDuty wird der Security Agent automatisch nur für die ausgewählten EKS Cluster bereitgestellt und verwaltet, die mit `GuardDutyManaged - true` als Schlüssel-Wert-Paar gekennzeichnet sind.
  - Dieser Ansatz hat auch die gleichen Auswirkungen, wie für Überwachen Sie alle EKS Cluster angegeben.
- Überlegungen:

- Wenn der Wert des `GuardDutyManaged` Tags nicht auf festgelegt ist`true`, funktioniert das Inklusion-Tag nicht wie erwartet, und dies kann sich auf die Überwachung Ihres EKS Clusters auswirken.
- Um sicherzustellen, dass Ihre ausgewählten EKS Cluster überwacht werden, müssen Sie verhindern, dass die Tags geändert werden, es sei denn, es handelt sich um vertrauenswürdige Identitäten.

> **Important**
>
> Verwalten Sie die Berechtigungen zum Ändern des Werts des `GuardDutyManaged` Tags für Ihren EKS Cluster mithilfe von Dienststeuerungsrichtlinien oder IAM -richtlinien. Weitere Informationen finden Sie unter Dienststeuerungsrichtlinien (SCPs) im AWS Organizations Benutzerhandbuch oder Steuern des Zugriffs auf AWS Ressourcen im IAMBenutzerhandbuch.

- Bei einem potenziell neuen EKS Cluster, den Sie nicht überwachen möchten, stellen Sie sicher, dass Sie bei der Erstellung dieses EKS Clusters das `GuardDutyManaged` `false` Schlüssel-Wert-Paar hinzufügen.
- Bei diesem Ansatz werden auch dieselben Überlegungen berücksichtigt, wie für Überwachen Sie alle EKS Cluster angegeben.

[1] Weitere Informationen zum Taggen von ausgewählten EKS Clustern finden Sie unter Taggen Ihrer EKS Amazon-Ressourcen im EKSAmazon-Benutzerhandbuch.

Den GuardDuty Security Agent manuell verwalten

- Wann sollten Sie diesen Ansatz verwenden — Verwenden Sie diesen Ansatz, wenn Sie den GuardDuty Security Agent auf all Ihren EKS Clustern manuell verteilen und verwalten möchten. Stellen Sie sicher, dass EKS Runtime Monitoring für Ihre Konten aktiviert ist. Der GuardDuty Security Agent funktioniert möglicherweise nicht wie erwartet, wenn Sie EKS Runtime Monitoring nicht aktivieren.
- Auswirkungen dieses Ansatzes — Sie müssen die Bereitstellung der GuardDuty Security Agent-Software in Ihren EKS Clustern für alle Konten und für alle Standorte, AWS-Regionen an denen diese Funktion verfügbar ist, koordinieren.

- Überlegungen – Sie müssen einen sicheren Datenfluss unterstützen und gleichzeitig Sicherheitslücken im Auge behalten und diese schließen, da ständig neue Cluster und Workloads bereitgestellt werden.

GuardDuty Runtime Monitoring aktivieren

Bevor Sie Runtime Monitoring in Ihrem Konto aktivieren, stellen Sie sicher, dass der Ressourcentyp, für den Sie die Laufzeitereignisse überwachen möchten, die Plattformanforderungen unterstützt. Weitere Informationen finden Sie unter Voraussetzungen.

Wenn Sie EKS Runtime Monitoring vor dem Start von Runtime Monitoring verwendet haben, können Sie mit dem APIs die bestehende Konfiguration für EKS Runtime Monitoring überprüfen und aktualisieren. Sie können Ihre bestehende Konfiguration auch von EKS Runtime Monitoring zu Runtime Monitoring migrieren. Weitere Informationen finden Sie unter Migration von EKS Runtime Monitoring zu Runtime Monitoring.

> **Note**
>
> Derzeit enthält diese Dokumentation Schritte zur Aktivierung von Runtime Monitoring für Ihre Konten und Ihr Unternehmen nur über die Konsole. Sie können Runtime Monitoring auch mithilfe von APIAktionen oder AWS CLI für GuardDuty aktivieren.

Sie können Runtime Monitoring mithilfe der Schritte in den folgenden Themen konfigurieren.

Inhalt

Voraussetzungen für die Aktivierung von Runtime Monitoring

Um Runtime Monitoring zu aktivieren und den GuardDuty Security Agent zu verwalten, müssen Sie die Voraussetzungen für jeden Ressourcentyp erfüllen, den Sie auf Bedrohungserkennung überwachen möchten.

Inhalt

Voraussetzungen für die Unterstützung Amazon EC2 Amazon-Instances

EC2Instanzen SSM verwalten

Die EC2 Amazon-Instances, für die Sie Laufzeitereignisse überwachen GuardDuty möchten, müssen AWS Systems Manager (SSM) verwaltet werden. Dies gilt unabhängig davon, ob GuardDuty Sie den Security Agent automatisch oder manuell verwalten (außerMethode 2 — Mithilfe von Linux-Paketmanagern).

Informationen zur Verwaltung Ihrer EC2 Amazon-Instances mit AWS Systems Manager finden Sie unter Systems Manager für EC2 Amazon-Instances einrichten im AWS Systems Manager Benutzerhandbuch.

Validierung der architektonischen Anforderungen

Die Architektur Ihrer Betriebssystemverteilung kann sich auf das Verhalten des GuardDuty Security Agents auswirken. Sie müssen die folgenden Anforderungen erfüllen, bevor Sie Runtime Monitoring für EC2 Amazon-Instances verwenden können:

- Die folgende Tabelle zeigt die Betriebssystemdistribution, für die verifiziert wurde, dass sie den GuardDuty Security Agent für EC2 Amazon-Instances unterstützt.

Betriebssystem-Verteilung	Kernel-Version	Kernel-Unterstützung	CPUArchitektur	
			x64 () AMD64	Graviton () ARM64
• AL2und AL2023 • Ubuntu 20.04 und Ubuntu 22.04	5.4, 5.10, 5.15, 6.1, 6.5, 6.8	eBPF, Tracepoints, Kprobe	Unterstützt	Unterstützt

  - Debian 11 und
    Debian 12

- Zusätzliche Anforderungen — Nur wenn Sie Amazon ECS /Amazon haben EC2

  Für Amazon ECS /Amazon empfehlen wirEC2, die neueste Version zu verwenden, die für Amazon ECS optimiert ist AMIs (vom 29. September 2023 oder später), oder die ECS Amazon-Agent-Version v1.77.0 zu verwenden.

Überprüfung der Servicesteuerungsrichtlinie Ihres Unternehmens

Wenn Sie eine Dienststeuerungsrichtlinie (SCP) zur Verwaltung von Berechtigungen in Ihrer Organisation eingerichtet haben, stellen Sie sicher, dass die Berechtigungsgrenzen nicht `guardduty:SendSecurityTelemetry` einschränkend sind. Sie ist erforderlich GuardDuty , um Runtime Monitoring für verschiedene Ressourcentypen zu unterstützen.

Wenn Sie ein Mitgliedskonto sind, stellen Sie eine Verbindung mit dem zugehörigen delegierten Administrator her. Informationen zur Verwaltung SCPs für Ihre Organisation finden Sie unter Richtlinien zur Servicesteuerung (SCPs).

Bei Verwendung der automatisierten Agentenkonfiguration

Dazu Verwenden Sie die automatische Agentenkonfiguration (empfohlen) AWS-Konto müssen Sie die folgenden Voraussetzungen erfüllen:

- Wenn Sie Inclusion-Tags mit automatisierter Agentenkonfiguration verwenden, GuardDuty um eine SSM Zuordnung für eine neue Instanz zu erstellen, stellen Sie sicher, dass die neue Instanz SSM verwaltet wird und in der https://console.aws.amazon.com/systems-manager/Konsole unter Fleet Manager angezeigt wird.
- Wenn Sie Ausschluss-Tags mit automatisierter Agentenkonfiguration verwenden:
  - Fügen Sie das `false` Tag`GuardDutyManaged`: hinzu, bevor Sie den GuardDuty automatisierten Agenten für Ihr Konto konfigurieren.

    Stellen Sie sicher, dass Sie Ihren EC2 Amazon-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon aktiviert habenEC2, wird jede EC2 Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

- Damit die Ausnahmetags funktionieren, aktualisieren Sie die Instance-Konfiguration, sodass das Instance-Identitätsdokument im Instance-Metadatenservice (IMDS) verfügbar ist. Das Verfahren Laufzeitüberwachung aktivieren für diesen Schritt ist bereits Teil Ihres Accounts.

CPUund Speicherlimit für den GuardDuty Agenten

CPULimit

Das maximale CPU Limit für den GuardDuty Security Agent, der EC2 Amazon-Instances zugeordnet ist, liegt bei 10 Prozent der gesamten CPU V-Cores. Wenn Ihre EC2 Instance beispielsweise über 4 CPU V-Cores verfügt, kann der Security Agent maximal 40 Prozent der insgesamt verfügbaren 400 Prozent verwenden.

Speicherlimit

Aus dem Speicher, der Ihrer EC2 Amazon-Instance zugeordnet ist, steht ein begrenzter Speicher zur Verfügung, den der GuardDuty Security Agent verwenden kann.

Die folgende Tabelle zeigt das Speicherlimit.

Speicher der EC2 Amazon-Instanz	Maximaler Arbeitsspeicher für den GuardDuty Agenten
Weniger als 8 GB	128 MB
Weniger als 32 GB	256 MB
Mehr als oder gleich 32 GB	1 GB

Nächster Schritt

Der nächste Schritt besteht darin, Runtime Monitoring zu konfigurieren und auch den Security Agent (automatisch oder manuell) zu verwalten.

Voraussetzungen für Support AWS Fargate (ECSnur Amazon)

Validierung der architektonischen Anforderungen

Die von Ihnen verwendete Plattform kann sich darauf auswirken, wie der GuardDuty Security Agent den Empfang der Runtime-Ereignisse von Ihren ECS Amazon-Clustern unterstützt GuardDuty . Sie müssen bestätigen, dass Sie eine der verifizierten Plattformen verwenden.

Erste Überlegungen:

- Die AWS Fargate (Fargate) Plattform für Ihre ECS Amazon-Cluster muss Linux sein. Die entsprechende Plattformversion muss mindestens`1.4.0`, oder sein`LATEST`. Weitere Informationen zu den Plattformversionen finden Sie unter Linux-Plattformversionen im Amazon Elastic Container Service Developer Guide.
- Die Windows-Plattformversionen werden noch nicht unterstützt.

Verifizierte Plattformen

Die Verteilung und CPU Architektur des Betriebssystems wirken sich auf die Unterstützung durch den GuardDuty Security Agent aus. Die folgende Tabelle zeigt die verifizierte Konfiguration für die Installation des GuardDuty Security Agents und die Konfiguration von Runtime Monitoring.

Betriebssystem-Verteilung	Kernel-Unterstützung	CPUArchitektur	
		x64 () AMD64	Graviton () ARM64
Linux	eBPF, Tracepoints, Kprobe	Unterstützt	Unterstützt

Geben Sie ECR Berechtigungen und Subnetzdetails an

Bevor Sie Runtime Monitoring aktivieren, müssen Sie die folgenden Details angeben:

Stellen Sie eine Rolle zur Aufgabenausführung mit Berechtigungen bereit

Für die Rolle zur Aufgabenausführung benötigen Sie bestimmte Amazon Elastic Container Registry (AmazonECR) -Berechtigungen. Sie können entweder die von A mazonECSTask ExecutionRolePolicy verwaltete Richtlinie verwenden oder Ihrer `TaskExecutionRole` Richtlinie die folgenden Berechtigungen hinzufügen:

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Um die ECR Amazon-Berechtigungen weiter einzuschränken, können Sie das ECR Amazon-Repository hinzufügenURI, das den GuardDuty Security Agent für hostet AWS Fargate (ECSnur Amazon). Weitere Informationen finden Sie unter Repository für GuardDuty Agenten auf AWS Fargate (ECSnur Amazon).

Geben Sie die Subnetzdetails in der Aufgabendefinition an

Sie können entweder die öffentlichen Subnetze als Eingabe in Ihrer Aufgabendefinition angeben oder einen ECR VPC Amazon-Endpunkt erstellen.

- Option zur Aufgabendefinition verwenden — Wenn Sie CreateServiceund UpdateServiceAPIsin der Amazon Elastic Container Service API Reference ausführen, müssen Sie die Subnetzinformationen übergeben. Weitere Informationen finden Sie unter ECSAmazon-Aufgabendefinitionen im Amazon Elastic Container Service Developer Guide.
- Verwenden der ECR VPC Amazon-Endpunktoption — Netzwerkpfad zu Amazon ECR angeben — Stellen Sie sicher, dass das ECR Amazon-RepositoryURI, das den GuardDuty Security Agent hostet, über das Netzwerk zugänglich ist. Wenn Ihre Fargate-Aufgaben in einem privaten Subnetz ausgeführt werden, benötigt Fargate den Netzwerkpfad, um den Container herunterzuladen. GuardDuty

  Informationen darüber, wie Fargate den GuardDuty Container herunterladen kann, finden Sie unter Using Amazon ECR Images with Amazon ECS im Amazon Elastic Container Registry-Benutzerhandbuch.

Validierung der Service-Control-Richtlinie Ihres Unternehmens

Dieser Schritt ist erforderlich, um Runtime Monitoring GuardDuty zu unterstützen und die Abdeckung verschiedener Ressourcentypen zu bewerten.

Wenn Sie eine Dienststeuerungsrichtlinie (SCP) zur Verwaltung von Berechtigungen in Ihrer Organisation eingerichtet haben, stellen Sie sicher, dass in Ihrer Richtlinie `TaskExecutionRole` und `guardduty:SendSecurityTelemetry` in der zugehörigen Richtlinie keine Einschränkungen durch die Berechtigungsgrenzen bestehen.

Die folgende Richtlinie ist ein Beispiel für die Zulassung der `guardduty:SendSecurityTelemetry` Richtlinie:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
    "Effect": "Allow",
            "Action": [
                ...,
                ...,
                "guardduty:SendSecurityTelemetry"
            ],
            "Resource": "*"
        }
    ]
}
```

1. Gehen Sie wie folgt vor, um zu überprüfen, ob die Grenze der Berechtigungen keine Einschränkungen darstellt: `guardduty:SendSecurityTelemetry`
    1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM Konsole unter. https://console.aws.amazon.com/iam/
    2. Wählen Sie im Navigationsbereich unter Zugriffsverwaltung die Option Rollen aus.
    3. Wählen Sie den Rollennamen für die Detailseite aus.
    4. Erweitern Sie den Abschnitt Grenze der Berechtigungen. Stellen Sie sicher, dass `guardduty:SendSecurityTelemetry` das nicht verweigert oder eingeschränkt ist.
2. Gehen Sie wie folgt vor, um zu überprüfen, ob die für Ihre **`TaskExecutionRole`** Richtlinie geltenden Zugriffsrechte nicht einschränkend sind`guardduty:SendSecurityTelemetry`:
    1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM Konsole unter https://console.aws.amazon.com/iam/.
    2. Wählen Sie im Navigationsbereich unter Zugriffsverwaltung die Option Richtlinien aus.
    3. Wählen Sie den Richtliniennamen für die Detailseite aus.
    4. Sehen Sie sich auf der Registerkarte Angehängte Entitäten den Abschnitt Als Rechtegrenze angehängt an. Stellen Sie sicher, dass `guardduty:SendSecurityTelemetry` das nicht verweigert oder eingeschränkt ist.

Informationen zu Richtlinien und Berechtigungen finden Sie im IAMBenutzerhandbuch unter Grenzen von Berechtigungen.

Wenn Sie ein Mitgliedskonto sind, stellen Sie eine Verbindung mit dem zugehörigen delegierten Administrator her. Informationen zur Verwaltung SCPs für Ihre Organisation finden Sie unter Richtlinien zur Servicesteuerung (SCPs).

CPUund Speicherlimits

In der Fargate-Aufgabendefinition müssen Sie den Wert CPU und den Speicherwert auf Aufgabenebene angeben. Die folgende Tabelle zeigt die gültigen Kombinationen von Werten auf Taskebene CPU und Speicher sowie die entsprechende maximale Speicherbegrenzung des GuardDuty Security Agents für den Container. GuardDuty

CPUWert	Speicherwert	GuardDuty Maximales Speicherlimit für Agenten
256 (2,5 VCPU)	512 MiB, 1 GB, 2 GB	128 MB
512 (1,5 V) CPU	1 GB, 2 GB, 3 GB, 4 GB	
1024 (1 VCPU)	2 GB, 3 GB, 4 GB	
	5 GB, 6 GB, 7 GB, 8 GB	
2048 (2 VCPU)	Zwischen 4 GB und 16 GB in 1-GB-Schritten	
4096 (4 V) CPU	Zwischen 8 GB und 20 GB in Schritten von 1 GB	
8192 (8 V) CPU	Zwischen 16 GB und 28 GB in Schritten von 4 GB	256 MB
	Zwischen 32 GB und 60 GB in Schritten von 4 GB	512 MB
16384 (16 V) CPU	Zwischen 32 GB und 120 GB in 8-GB-Schritten	1 GB

Nachdem Sie Runtime Monitoring aktiviert und festgestellt haben, dass der Abdeckungsstatus Ihres Clusters fehlerfrei ist, können Sie die Container Insight-Metriken einrichten und anzeigen. Weitere Informationen finden Sie unter Überwachung auf ECS Amazon-Cluster einrichten.

Der nächste Schritt besteht darin, Runtime Monitoring und auch den Security Agent zu konfigurieren.

Voraussetzungen für die Unterstützung Amazon EKS Amazon-Clustern

Validierung der architektonischen Anforderungen

Die von Ihnen verwendete Plattform kann sich darauf auswirken, wie der GuardDuty Security Agent GuardDuty den Empfang von Runtime-Ereignissen von Ihren EKS Clustern unterstützt. Sie müssen bestätigen, dass Sie eine der verifizierten Plattformen verwenden. Wenn Sie den GuardDuty Agenten manuell verwalten, stellen Sie sicher, dass die Kubernetes-Version die GuardDuty Agentenversion unterstützt, die derzeit verwendet wird.

Verifizierte Plattformen

Die Betriebssystemverteilung, die Kernelversion und die CPU Architektur wirken sich auf die vom GuardDuty Security Agent bereitgestellte Unterstützung aus. Die folgende Tabelle zeigt die verifizierte Konfiguration für die Installation des GuardDuty Security Agents und die Konfiguration von EKS Runtime Monitoring.

Betriebssystem-Verteilung	Kernel-Version	Kernel-Unterstützung	CPUArchitektur		Unterstützte Kubernetes-Version
			x64 () AMD64	Graviton () ARM64 (Graviton2 und höher) [1]	
Ubuntu AL2 AL2203 [3]	5.4, 5.10, 5.15, 6.1 [2]	e) BPF Tracepoints, Kprobe	Unterstützt	Unterstützt	v1.21 - v1.30
Bottlerocket					v1.23 - v1.30

1.

Runtime Monitoring for Amazon EKS Clusters unterstützt Graviton-Instances der ersten Generation wie A1-Instance-Typen nicht.

2. Derzeit können mit der Kernel-Version keine `6.1` Generierungen GuardDuty durchgeführt werden, Runtime Monitoring: Typen finden die sich auf Folgendes beziehen. DNSEreignisse

3. Runtime Monitoring unterstützt AL2 023 mit der Veröffentlichung des GuardDuty Security Agents v1.6.0 und höher. Weitere Informationen finden Sie unter GuardDuty Sicherheitsagent für EKS Amazon-Cluster.

Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty

Die folgende Tabelle zeigt die Kubernetes-Versionen für Ihre EKS Cluster, die vom Security Agent unterstützt werden. GuardDuty

Kubernetes-Version	Version des Amazon EKS Add-Ons GuardDuty für den Sicherheitsagenten
1,28 — 1,30	v1.4.1 und neuer
1.27	v1.3.0, v1.3.1
1,26	v1.2.0
1,21 - 1,25	Alle Versionen

Für einige Versionen des GuardDuty Security Agents wird der Standardsupport auslaufen. Informationen zu den Release-Versionen der Agenten finden Sie unterGuardDuty Sicherheitsagent für EKS Amazon-Cluster.

CPUund Speichergrenzen

Die folgende Tabelle zeigt die Speicherlimits CPU und die Speicherlimits für das EKS Amazon-Add-on für GuardDuty (`aws-guardduty-agent`).

Parameter	Minimale Grenze	Maximale Grenze
CPU	200m	1000m
Arbeitsspeicher	256 Mi	1024Mi

Wenn Sie die EKS Amazon-Zusatzversion 1.5.0 oder höher verwenden, GuardDuty bietet es die Möglichkeit, das Add-On-Schema für Ihre CPU und Speicherwerte zu konfigurieren. Informationen zum konfigurierbaren Bereich finden Sie unterKonfigurierbare Parameter und Werte.

Nachdem Sie EKS Runtime Monitoring aktiviert und den Abdeckungsstatus Ihrer EKS Cluster bewertet haben, können Sie die Container-Insight-Metriken einrichten und anzeigen. Weitere Informationen finden Sie unter Einrichtung CPU und Speicherüberwachung.

Nächster Schritt

Der nächste Schritt besteht darin, Runtime Monitoring zu konfigurieren und den Security Agent entweder manuell oder automatisch zu verwalten GuardDuty.

Verwendung von Infrastructure as Code (IaC) mit GuardDuty automatisierten Security Agents

Verwenden Sie diesen Abschnitt nur, wenn die folgende Liste auf Ihren Anwendungsfall zutrifft:

- Sie verwenden Infrastructure-as-Code-Tools (IaC) wie Terraform, um Ihre AWS Ressourcen zu verwalten, AWS Cloud Development Kit (AWS CDK) und
- Sie müssen die GuardDuty automatische Agentenkonfiguration für einen oder mehrere Ressourcentypen aktivieren — Amazon EKSEC2, Amazon oder Amazon ECS -Fargate.

Übersicht über die Abhängigkeit von IaC-Ressourcen

Wenn Sie die GuardDuty automatische Agentenkonfiguration für einen Ressourcentyp aktivieren, GuardDuty werden automatisch ein VPC Endpunkt und eine diesem VPC Endpunkt zugeordnete Sicherheitsgruppe erstellt und der Security Agent für diesen Ressourcentyp installiert. Standardmäßig GuardDuty werden der VPC Endpunkt und die zugehörige Sicherheitsgruppe erst gelöscht, nachdem Sie Runtime Monitoring deaktiviert haben. Weitere Informationen finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Wenn Sie ein IaC-Tool verwenden, verwaltet es ein Abhängigkeitsdiagramm der Ressourcen. Zum Zeitpunkt des Löschens von Ressourcen mithilfe des IaC-Tools werden nur Ressourcen gelöscht, die als Teil des Abhängigkeitsdiagramms von Ressourcen nachverfolgt werden können. IaC-Tools wissen möglicherweise nichts über die Ressourcen, die außerhalb ihrer angegebenen Konfiguration erstellt wurden. Sie erstellen beispielsweise VPC mit einem IaC-Tool ein und fügen diesem dann VPC mithilfe einer AWS Konsole oder einer Operation eine API Sicherheitsgruppe hinzu. Im Diagramm zur Ressourcenabhängigkeit hängt die VPC Ressource, die Sie erstellen, von der zugehörigen Sicherheitsgruppe ab. Wenn Sie diese VPC Ressource mithilfe des IaC-Tools löschen, wird eine Fehlermeldung angezeigt. Sie können diesen Fehler umgehen, indem Sie die zugehörige Sicherheitsgruppe manuell löschen oder die IaC-Konfiguration so aktualisieren, dass sie diese hinzugefügte Ressource enthält.

Häufiges Problem — Löschen von Ressourcen in IaC

Wenn Sie die GuardDuty automatische Agentenkonfiguration verwenden, möchten Sie möglicherweise eine Ressource (Amazon EKSEC2, Amazon oder ECS Amazon-Fargate) löschen, die Sie mithilfe eines IaC-Tools erstellt haben. Diese Ressource ist jedoch von einem VPC Endpunkt abhängig, der erstellt wurde. GuardDuty Dadurch wird verhindert, dass das IaC-Tool die Ressource selbst löscht, und Sie müssen Runtime Monitoring deaktivieren, wodurch der VPC Endpunkt automatisch gelöscht wird.

Wenn Sie beispielsweise versuchen, den in Ihrem Namen GuardDuty erstellten VPC Endpunkt zu löschen, erhalten Sie eine Fehlermeldung, die den folgenden Beispielen ähnelt.

Example

Fehlerbeispiel bei der Verwendung von CDK

```
The following resource(s) failed to delete:
 [mycdkvpcapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpcapplicationprivatesubnet1Subne
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has
 dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request
 ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPL
 HandlerErrorCode: InvalidRequest)
```

Example

Fehlerbeispiel bei der Verwendung von Terraform

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
 19m50s elapsed]
```

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
 20m0s elapsed]

Error: deleting EC2 Subnet (subnet-APKAEIBAERJR2EXAMPLE): DependencyViolation: The
 subnet 'subnet-APKAEIBAERJR2EXAMPLE' has dependencies and cannot be deleted.
       status code: 400, request id: e071c3c5-7442-4489-838c-0dfc6EXAMPLE
```

Lösung - Vermeiden Sie das Problem beim Löschen von Ressourcen

In diesem Abschnitt können Sie den VPC Endpunkt und die Sicherheitsgruppe unabhängig von verwalten GuardDuty.

Um die vollständige Kontrolle über die mit dem IaC-Tool konfigurierten Ressourcen zu erlangen, führen Sie die folgenden Schritte in der angegebenen Reihenfolge aus:

1. Erstellen Sie eineVPC. Um Zugriffsberechtigungen zuzulassen, ordnen Sie dieser VPC Sicherheitsgruppe einen GuardDuty VPC Endpunkt zu.
2. Aktivieren Sie die GuardDuty automatische Agentenkonfiguration für Ihren Ressourcentyp

Nachdem Sie die vorherigen Schritte abgeschlossen haben, GuardDuty wird kein eigener VPC Endpunkt erstellt, sondern der Endpunkt, den Sie mit dem IaC-Tool erstellt haben, wiederverwendet.

Informationen zur Erstellung Ihrer eigenen VPC finden Sie unter VPCNur in den Amazon VPC Transit Gateways erstellen. Informationen zum Erstellen eines VPC Endpunkts finden Sie im folgenden Abschnitt für Ihren Ressourcentyp:

- Informationen zu Amazon EC2 finden Sie unterManuelles Erstellen eines VPC Amazon-Endpunkts.
- Informationen zu Amazon EKS finden Sie unterVoraussetzungen für die Installation des GuardDuty Security Agents.

Runtime Monitoring für ein eigenständiges Konto aktivieren

Gehen Sie wie folgt vor, um Runtime Monitoring in Ihrem Konto zu aktivieren.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.

3. Wählen Sie auf der Registerkarte Konfiguration die Option Aktivieren aus, um Runtime Monitoring für Ihr Konto zu aktivieren.
4. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer EC2 Amazon-Instance, einem ECS Amazon-Cluster oder einem EKS Amazon-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

   Um den GuardDuty Security Agent zu aktivieren

   - Verwaltung eines automatisierten Sicherheitsagenten für EC2 Amazon-Instance
   - Manuelles Verwalten des Security Agents für EC2 Amazon-Instance
   - Verwaltung eines automatisierten Sicherheitsagenten für Fargate (ECSnur Amazon)
   - Automatisches Verwalten des Security Agents für EKS Amazon-Cluster
   - Manuelles Verwalten des Security Agents für EKS Amazon-Cluster

Runtime Monitoring für Umgebungen mit mehreren Konten aktivieren

In Umgebungen mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto die Laufzeitüberwachung für die Mitgliedskonten aktivieren oder deaktivieren und die automatische Agentenkonfiguration für die Ressourcentypen verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten.

Für ein delegiertes Administratorkonto GuardDuty

Um Runtime Monitoring für ein delegiertes GuardDuty Administratorkonto zu aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Runtime Monitoring-Konfiguration die Option Bearbeiten aus.

4. Verwendung von Für alle Konten aktivieren

   Wenn Sie Runtime Monitoring für alle Konten aktivieren möchten, die zur Organisation gehören, einschließlich des delegierten GuardDuty Administratorkontos, wählen Sie Für alle Konten aktivieren.

5. Verwendung von Konten manuell konfigurieren

   Wenn Sie Runtime Monitoring für jedes Mitgliedskonto einzeln aktivieren möchten, wählen Sie Konten manuell konfigurieren.

   - Wählen Sie im Abschnitt Delegierter Administrator (dieses Konto) die Option Aktivieren.

6. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer EC2 Amazon-Instance, einem ECS Amazon-Cluster oder einem EKS Amazon-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

   Um den GuardDuty Security Agent zu aktivieren

   - Verwaltung eines automatisierten Sicherheitsagenten für EC2 Amazon-Instance
   - Manuelles Verwalten des Security Agents für EC2 Amazon-Instance
   - Verwaltung eines automatisierten Sicherheitsagenten für Fargate (ECSnur Amazon)
   - Automatisches Verwalten des Security Agents für EKS Amazon-Cluster
   - Manuelles Verwalten des Security Agents für EKS Amazon-Cluster

Für alle Mitgliedskonten

Um Runtime Monitoring für alle Mitgliedskonten in der Organisation zu aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit dem delegierten GuardDuty Administratorkonto an.

2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Seite Runtime Monitoring auf der Registerkarte Konfiguration im Abschnitt Runtime Monitoring-Konfiguration die Option Bearbeiten aus.
4. Wählen Sie Für alle Konten aktivieren.

5. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer EC2 Amazon-Instance, einem ECS Amazon-Cluster oder einem EKS Amazon-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

   Um den GuardDuty Security Agent zu aktivieren

   - Verwaltung eines automatisierten Sicherheitsagenten für EC2 Amazon-Instance
   - Manuelles Verwalten des Security Agents für EC2 Amazon-Instance
   - Verwaltung eines automatisierten Sicherheitsagenten für Fargate (ECSnur Amazon)
   - Automatisches Verwalten des Security Agents für EKS Amazon-Cluster
   - Manuelles Verwalten des Security Agents für EKS Amazon-Cluster

Für alle bestehenden aktiven Mitgliedskonten

Um Runtime Monitoring für bestehende Mitgliedskonten in der Organisation zu aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit dem delegierten GuardDuty Administratorkonto für die Organisation an.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Auf der Runtime Monitoring-Seite können Sie auf der Registerkarte Konfiguration den aktuellen Status der Runtime Monitoring-Konfiguration einsehen.
4. Wählen Sie im Bereich Runtime Monitoring im Abschnitt Aktive Mitgliedskonten die Option Aktionen aus.
5. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
6. Wählen Sie Bestätigen aus.
7. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer EC2 Amazon-Instance, einem ECS Amazon-Cluster oder einem EKS Amazon-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

Um den GuardDuty Security Agent zu aktivieren

- Verwaltung eines automatisierten Sicherheitsagenten für EC2 Amazon-Instance
- Manuelles Verwalten des Security Agents für EC2 Amazon-Instance
- Verwaltung eines automatisierten Sicherheitsagenten für Fargate (ECSnur Amazon)
- Automatisches Verwalten des Security Agents für EKS Amazon-Cluster
- Manuelles Verwalten des Security Agents für EKS Amazon-Cluster

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Automatische Aktivierung der Laufzeitüberwachung nur für neue Mitgliedskonten

Um Runtime Monitoring für neue Mitgliedskonten in Ihrer Organisation zu aktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit dem designierten delegierten GuardDuty Administratorkonto der Organisation an.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus
3. Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Runtime Monitoring-Konfiguration die Option Bearbeiten aus.
4. Wählen Sie Konten manuell konfigurieren.
5. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren.
6. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer EC2 Amazon-Instance, einem ECS Amazon-Cluster oder einem EKS Amazon-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

   Um den GuardDuty Security Agent zu aktivieren

   - Verwaltung eines automatisierten Sicherheitsagenten für EC2 Amazon-Instance
   - Manuelles Verwalten des Security Agents für EC2 Amazon-Instance

- Verwaltung eines automatisierten Sicherheitsagenten für Fargate (ECSnur Amazon)
- Automatisches Verwalten des Security Agents für EKS Amazon-Cluster
- Manuelles Verwalten des Security Agents für EKS Amazon-Cluster

Nur für ausgewählte aktive Mitgliedskonten

Um die Laufzeitüberwachung für einzelne aktive Mitgliedskonten zu aktivieren

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Überprüfen Sie auf der Seite Konten die Werte in den Spalten Runtime Monitoring und Agent automatisch verwalten. Diese Werte geben an, ob Runtime Monitoring und GuardDuty Agentenverwaltung für das entsprechende Konto aktiviert oder nicht aktiviert sind.
4. Wählen Sie in der Tabelle Konten das Konto aus, für das Sie Runtime Monitoring aktivieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
5. Wählen Sie Bestätigen aus.
6. Wählen Sie Schutzpläne bearbeiten aus. Wählen Sie die geeignete Aktion aus.
7. Wählen Sie Bestätigen aus.
8. GuardDuty Um Runtime-Ereignisse von einem oder mehreren Ressourcentypen — einer EC2 Amazon-Instance, einem ECS Amazon-Cluster oder einem EKS Amazon-Cluster — zu empfangen, verwenden Sie die folgenden Optionen, um den Security Agent für diese Ressourcen zu verwalten:

   Um den GuardDuty Security Agent zu aktivieren

   - Verwaltung eines automatisierten Sicherheitsagenten für EC2 Amazon-Instance
   - Manuelles Verwalten des Security Agents für EC2 Amazon-Instance
   - Verwaltung eines automatisierten Sicherheitsagenten für Fargate (ECSnur Amazon)
   - Automatisches Verwalten des Security Agents für EKS Amazon-Cluster
   - Manuelles Verwalten des Security Agents für EKS Amazon-Cluster

GuardDuty Security Agents verwalten

Sie können den GuardDuty Security Agent für die Ressource verwalten, die Sie überwachen möchten. Wenn Sie mehr als einen Ressourcentyp überwachen möchten, stellen Sie sicher, dass Sie den GuardDuty Agenten für diese Ressource verwalten.

> **Important**
>
> Wenn Sie mit einem GuardDuty Security Agent für eine EC2 Amazon-Instance arbeiten, können Sie den Agenten auf dem zugrunde liegenden Host innerhalb eines EKS Amazon-Clusters installieren und verwenden. Wenn Sie bereits einen Security Agent auf diesem EKS Cluster installiert haben, könnten auf demselben Host zwei Security Agents gleichzeitig ausgeführt werden. Informationen zur GuardDuty Funktionsweise in diesem Szenario finden Sie unterUmgang mit Dual-Security-Agenten.

Die folgenden Themen helfen Ihnen bei den nächsten Schritten zur Verwaltung des Security Agents.

Inhalt

Wird gemeinsam VPC mit automatisierten Security Agents verwendet

Wenn Sie GuardDuty sich dafür entscheiden, den Security Agent automatisch zu verwalten, unterstützt Runtime Monitoring die Verwendung eines gemeinsam genutzten AWS-Konten Systems VPC für diejenigen, die derselben Organisation angehören AWS Organizations. GuardDuty Kann in Ihrem Namen die VPC Amazon-Endpunktrichtlinie auf der Grundlage der VPC für Ihre Organisation geteilten Daten festlegen.

Vor dieser Version wurde die Verwendung von Shared VPCs nur GuardDuty unterstützt, wenn Sie den GuardDuty Security Agent manuell verwalten wollten.

Inhalt

Funktionsweise

Wenn das Eigentümerkonto des geteilten Objekts Runtime Monitoring und automatische Agentenkonfiguration für eine der Ressourcen (Amazon EKS oder AWS Fargate (ECSnur Amazon)) VPC aktiviert, kommen alle gemeinsam genutzten VPCs Ressourcen für die automatische Installation des gemeinsamen VPC Amazon-Endpunkts und der zugehörigen Sicherheitsgruppe im gemeinsamen VPC Besitzerkonto in Frage. GuardDuty ruft die Organisations-ID ab, die dem geteilten Amazon VPC zugeordnet ist.

Jetzt können diejenigen, AWS-Konten die derselben Organisation angehören wie das gemeinsame VPC Amazon-Besitzerkonto, auch denselben VPC Amazon-Endpunkt verwenden. GuardDuty erstellt das geteilte KontoVPC, wenn entweder das gemeinsame VPC Eigentümerkonto oder das teilnehmende Konto einen VPC Amazon-Endpunkt benötigt. Beispiele für die Notwendigkeit eines VPC Amazon-Endpunkts sind die Aktivierung GuardDuty, Runtime Monitoring, EKS Runtime Monitoring oder das Starten einer neuen Amazon ECS -Fargate-Aufgabe. Wenn diese Konten Runtime Monitoring und automatische Agentenkonfiguration für einen beliebigen Ressourcentyp aktivieren, GuardDuty wird ein VPC Amazon-Endpunkt erstellt und die Endpunktrichtlinie mit derselben Organisations-ID wie die des gemeinsamen VPC Eigentümerkontos festgelegt. GuardDuty fügt ein `GuardDutyManaged` Tag hinzu und setzt es `true` für den VPC Amazon-Endpunkt, der GuardDuty erstellt, auf. Wenn das gemeinsame VPC Amazon-Besitzerkonto weder Runtime Monitoring noch automatische Agentenkonfiguration für eine der Ressourcen aktiviert hat, GuardDuty wird die VPC Amazon-Endpunktrichtlinie nicht festgelegt. Informationen zur Konfiguration von Runtime Monitoring und zur automatischen Verwaltung des Security Agents im gemeinsamen VPC Eigentümerkonto finden Sie unter GuardDuty Runtime Monitoring aktivieren.

Jedes Konto, das dieselbe VPC Amazon-Endpunktrichtlinie verwendet, wird als AWS Teilnehmerkonto des zugehörigen gemeinsamen Amazon bezeichnetVPC.

Das folgende Beispiel zeigt die standardmäßige VPC Endpunktrichtlinie des gemeinsamen VPC Eigentümerkontos und des Teilnehmerkontos. Es `aws:PrincipalOrgID` wird die Organisations-ID angezeigt, die der gemeinsam genutzten VPC Ressource zugeordnet ist. Die Verwendung dieser

Richtlinie ist auf die Teilnehmerkonten beschränkt, die in der Organisation des Eigentümerkontos vorhanden sind.

Example

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "*",
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

Voraussetzungen für die Nutzung von Shared VPC

Voraussetzungen für die Ersteinrichtung

Führen Sie die folgenden Schritte in der Datei aus AWS-Konto , in der Sie der Eigentümer der geteilten Datei sein möchtenVPC:

1. Organisation erstellen — Erstellen Sie eine Organisation, indem Sie die Schritte unter Organisation erstellen und verwalten im AWS Organizations Benutzerhandbuch befolgen.

   Informationen zum Hinzufügen oder Entfernen von Mitgliedskonten finden Sie unter Verwaltung AWS-Konten in Ihrer Organisation.
2. Eine gemeinsam genutzte VPC Ressource erstellen — Sie können eine gemeinsam genutzte VPC Ressource über das Besitzerkonto erstellen. Weitere Informationen finden Sie unter Teilen Ihres VPC Kontos mit anderen Konten im VPCAmazon-Benutzerhandbuch.

Spezifische Voraussetzungen für GuardDuty Runtime Monitoring

Die folgende Liste enthält die spezifischen Voraussetzungen für GuardDuty:

- Das Besitzerkonto des geteilten VPC und das teilnehmende Konto können von unterschiedlichen Organisationen in stammen GuardDuty. Sie müssen jedoch derselben Organisation in angehören AWS Organizations. Dies ist erforderlich GuardDuty , um einen VPC Amazon-Endpunkt und eine Sicherheitsgruppe für den gemeinsam genutzten Endpunkt zu erstellenVPC. Informationen darüber, wie geteilte VPCs Arbeit funktioniert, finden Sie im VPCAmazon-Benutzerhandbuch unter Teilen Sie Ihr Konto VPC mit anderen Konten.
- Aktivieren Sie Runtime Monitoring oder EKS Runtime Monitoring sowie die GuardDuty automatische Agentenkonfiguration für alle Ressourcen im gemeinsamen VPC Besitzerkonto und im Teilnehmerkonto. Weitere Informationen finden Sie unter Laufzeitüberwachung aktivieren.

  Wenn Sie diese Konfigurationen bereits abgeschlossen haben, fahren Sie mit dem nächsten Schritt fort.
- Wenn Sie entweder mit einer Amazon EKS - oder einer Amazon-Aufgabe ECS (AWS Fargate nur) arbeiten, stellen Sie sicher, dass Sie die gemeinsam genutzte VPC Ressource auswählen, die dem Besitzerkonto zugeordnet ist, und wählen Sie deren Subnetze aus.

Häufig gestellte Fragen () FAQs

Die folgende Liste enthält die Schritte zur Fehlerbehebung bei den häufig gestellten Fragen bei der Verwendung einer gemeinsam genutzten VPC Ressource mit aktivierter GuardDuty automatisierter Agentenkonfiguration in Runtime Monitoring:

Ich verwende bereits Runtime Monitoring (oder EKS Runtime Monitoring). Wie aktiviere ich SharedVPC?

Informationen zu den Voraussetzungen für die Erstellung einer geteilten Datei VPC finden Sie unterVoraussetzungen.

Wenn sowohl das Konto des gemeinsamen VPC Besitzers als auch das Teilnehmerkonto die Voraussetzungen erfüllen, GuardDuty wird versucht, die VPC Amazon-Endpunktrichtlinie automatisch festzulegen.

Wenn Sie vor dieser Version ein Problem mit der Abdeckung AWS-Konto hatten, weil die geteilte Version VPC nicht unterstützt wurde, befolgen Sie die Voraussetzungen. Wenn Ihr Ressourcentyp

(Amazon EKS oder Amazon ECS (AWS Fargate nur) Task) die Anforderung eines gemeinsamen VPC Endpunkts aufruft, GuardDuty wird versucht, die neue VPC Endpunktrichtlinie festzulegen.

Als gemeinsames VPC Eigentümerkonto möchte ich, dass die Richtlinie für gemeinsame VPC Endgeräte auf eine Untergruppe von Teilnehmerkonten in meiner Organisation beschränkt wird. Wie kann ich das tun?

Wenn dem Endpunkt ein`GuardDutyManaged`: `true` -Tag zugeordnet ist, entfernen Sie es. Dadurch wird verhindert GuardDuty , dass versucht wird, die VPC Endpunktrichtlinie des gemeinsam genutzten VPC Geräts zu ändern oder zu überschreiben.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC Endgeräte mithilfe von Endpunktrichtlinien.

Warum ändert sich der gemeinsam genutzte VPC Endpunkt von **`aws:PrincipalAccount`** zu**`aws:PrincipalOrgId`**? Wie kann ich das verhindern?

Wenn GuardDuty erkannt VPC wird, dass das von mehreren Konten derselben Organisation gemeinsam genutzt wird AWS Organizations, GuardDuty versucht, die Richtlinie so zu ändern, dass die Organisations-ID angegeben wird.

Um dies zu verhindern, entfernen Sie das `true` Tag`GuardDutyManaged`: vom gemeinsamen VPC Endpunkt. Dadurch wird verhindert GuardDuty , dass versucht wird, die VPC Endpunktrichtlinie des gemeinsam genutzten VPC Geräts zu ändern oder zu überschreiben.

Was passiert, wenn das gemeinsame VPC Besitzerkonto oder eines der Teilnehmerkonten GuardDuty oder Runtime Monitoring (oder EKS Runtime Monitoring) deaktiviert wird?

Wenn das gemeinsame VPC Besitzerkonto deaktiviert GuardDuty oder Runtime Monitoring (oder EKS Runtime Monitoring) deaktiviert wird, wird GuardDuty geprüft, ob ein Ressourcentyp, der zum Teilnehmerkonto gehört, den gemeinsamen VPC Endpunkt verwendet hat oder ob ein Teilnehmerkonto jemals die GuardDuty Agentenverwaltung für einen beliebigen Ressourcentyp aktiviert hat. Falls ja, GuardDuty werden der VPC Endpunkt und die Sicherheitsgruppe nicht gelöscht.

Wenn das gemeinsame VPC Teilnehmerkonto Runtime Monitoring (GuardDuty oder EKS Runtime Monitoring) deaktiviert, hat das keine Auswirkungen auf das gemeinsame VPC Besitzerkonto und das Besitzerkonto löscht weder die gemeinsam genutzte VPC Ressource noch die Sicherheitsgruppe.

Wie kann ich die gemeinsam genutzte VPC Ressource löschen? Welche Auswirkungen wird es haben?

Als gemeinsames VPC Besitzerkonto können Sie die gemeinsam genutzte VPC Ressource auch dann löschen, wenn sie von Ihrem Konto oder einem der teilnehmenden Konten in Runtime Monitoring verwendet wird. Informationen zum Löschen der gemeinsam genutzten Datei VPC und zu ihren Auswirkungen finden Sie unterTo delete a VPC endpoint.

Umgang mit auf einem Host installierten Dual-Security-Agents

EC2Amazon-Instances können mehrere Arten von Workloads unterstützen. Wenn Sie einen automatisierten Security Agent auf einer EC2 Amazon-Instance konfigurieren, hat dieselbe EC2 Instance möglicherweise einen anderen Security Agent aktiviertEKS.

Übersicht

Stellen Sie sich ein Szenario vor, in dem Sie Runtime Monitoring aktiviert haben. Jetzt aktivieren Sie den automatisierten Agenten für Amazon EKS über GuardDuty. Sie haben auch den automatisierten Agenten für Amazon aktiviertEC2. Es kann vorkommen, dass derselbe zugrunde liegende Host mit zwei Security Agents installiert wird — einer für Amazon EKS und der andere für AmazonEC2. Dies kann dazu führen, dass zwei Security Agents auf demselben Host laufen, Laufzeitereignisse sammeln und an GuardDuty diese senden und möglicherweise doppelte Ergebnisse generieren.

Auswirkung

- Wenn mehr als ein Security Agent auf demselben Host ausgeführt wird, kann es sein, dass Ihr Konto doppelt so viel Speicherplatz benötigt. CPU Informationen zu den Speicherlimits CPU und den Speicherlimits für die einzelnen Ressourcentypen finden Sie unter Voraussetzungen für diese Ressource.
- GuardDuty hat die Runtime Monitoring-Funktion so konzipiert, dass Ihr Konto nur für einen Stream von Runtime-Ereignissen belastet wird, selbst wenn sich zwei Security Agents überschneiden, die Runtime-Ereignisse von demselben zugrundeliegenden Host sammeln.

Wie GuardDuty geht man mit mehreren Agenten um

GuardDuty erkennt, wenn zwei Security Agents auf demselben Host laufen, und bestimmt nur einen davon als Security Agent, der aktiv Runtime-Ereignisse sammelt. Der zweite Agent verbraucht nur minimale Systemressourcen, um jegliche Beeinträchtigung der Leistung Ihrer Anwendungen zu verhindern.

GuardDuty berücksichtigt die folgenden Szenarien:

- Wenn eine EC2 Instance sowohl in den Zuständigkeitsbereich von Amazon EKS als auch von Amazon EC2 Security Agents fällt, hat der EKS Sicherheitsagent Vorrang. Dies gilt nur, wenn Sie den Security Agent v1.1.0 oder höher für Amazon EC2 verwenden. Ältere Agentenversionen werden weiterhin ausgeführt und sammeln Runtime-Ereignisse, da ältere Agentenversionen von der Priorisierung nicht betroffen sind.
- Wenn sowohl Amazon EKS als auch Amazon Security Agents GuardDuty verwaltet EC2 haben und Ihre EC2 Amazon-Instance ebenfalls SSM verwaltet wird, werden beide Security Agents auf Host-Ebene installiert. Sobald die Agenten installiert sind, wird GuardDuty entschieden, welcher Security Agent weiter ausgeführt wird. Wenn beide Security Agents ausgeführt werden, sammelt letztendlich nur einer von ihnen Runtime-Ereignisse.
- Wenn die Security Agents, die beiden zugeordnet sind EC2 und gleichzeitig EKS ausgeführt werden, GuardDuty kann es nur während der Überschneidungszeit zu doppelten Ergebnissen kommen.

  Dies kann passieren, wenn:

  - Security Agents für beide EC2 und EKS werden GuardDuty (automatisch) konfiguriert, oder
  - Ihre EKS Amazon-Ressource hat einen automatisierten Sicherheitsagenten.
- Wenn der EKS Security Agent bereits läuft und Sie den EC2 Security Agent manuell auf demselben zugrunde liegenden Host installieren und alle Voraussetzungen erfüllen, wird GuardDuty möglicherweise kein zweiter Security Agent installiert.

Verwaltung eines automatisierten Sicherheitsagenten für EC2 Amazon-Instance

> **Note**
>
> Bevor Sie fortfahren, stellen Sie sicher, dass Sie alle Anweisungen befolgenVoraussetzungen für die Unterstützung Amazon EC2 Amazon-Instances.

Migration vom EC2 manuellen Amazon-Agenten zum automatisierten Agenten

Dieser Abschnitt gilt für den AWS-Konto Fall, dass Sie den Security Agent zuvor manuell verwaltet haben und jetzt die GuardDuty automatische Agent-Konfiguration verwenden möchten. Falls dies nicht auf Sie zutrifft, fahren Sie mit der Konfiguration des Security Agents für Ihr Konto fort.

Wenn Sie den GuardDuty Automated Agent aktivieren, GuardDuty verwaltet er den Security Agent in Ihrem Namen. Informationen darüber, welche GuardDuty Schritte erforderlich sind, finden Sie unterVerwenden Sie die automatische Agentenkonfiguration (empfohlen).

Bereinigen von -Ressourcen

SSMZuordnung löschen

- Löschen Sie SSM alle Verknüpfungen, die Sie möglicherweise erstellt haben, als Sie den Security Agent for Amazon EC2 manuell verwaltet haben. Weitere Informationen finden Sie unter Verknüpfungen löschen.
- Auf diese Weise GuardDuty können Sie die Verwaltung von SSM Aktionen übernehmen, unabhängig davon, ob Sie automatisierte Agenten auf Konto- oder Instanzebene verwenden (mithilfe von Inklusions- oder Ausschluss-Tags). Weitere Informationen darüber, welche SSM Aktionen ausgeführt werden können, GuardDuty finden Sie unterDienstbezogene Rollenberechtigungen für GuardDuty.
- Wenn Sie eine SSM Zuordnung löschen, die zuvor für die manuelle Verwaltung des Security Agents erstellt wurde, kann es zu einer kurzen Überschneidung kommen, wenn eine SSM Verknüpfung für die automatische Verwaltung des Security Agents GuardDuty erstellt wird. In diesem Zeitraum kann es aufgrund der SSM Terminplanung zu Konflikten kommen. Weitere Informationen finden Sie unter Amazon EC2 SSM Scheduling.

Inklusions- und Ausschluss-Tags für Ihre EC2 Amazon-Instances verwalten

- Inklusions-Tags — Wenn Sie die GuardDuty automatische Agentenkonfiguration nicht aktivieren, sondern eine Ihrer EC2 Amazon-Instances mit einem Inklusion-Tag (`GuardDutyManaged:true`) kennzeichnen, wird eine SSM Verknüpfung GuardDuty erstellt, die den Security Agent auf den ausgewählten EC2 Instances installiert und verwaltet. Dies ist ein erwartetes Verhalten, das Ihnen hilft, den Security Agent nur auf ausgewählten EC2 Instances zu verwalten. Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring mit EC2 Amazon-Instances.

  Um zu GuardDuty verhindern, dass der Security Agent installiert und verwaltet wird, entfernen Sie das Inclusion-Tag von diesen EC2 Instanzen. Weitere Informationen finden Sie unter Hinzufügen und Löschen von Tags im EC2Amazon-Benutzerhandbuch.
- Ausschluss-Tags — Wenn Sie die GuardDuty automatische Agentenkonfiguration für alle EC2 Instances in Ihrem Konto aktivieren möchten, stellen Sie sicher, dass keine EC2 Instance mit einem Ausschluss-Tag (`GuardDutyManaged:false`) gekennzeichnet ist.

Den GuardDuty Agenten für ein eigenständiges Konto konfigurieren

Configure for all instances

Um Runtime Monitoring für alle Instanzen in Ihrem eigenständigen Konto zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte Konfiguration die Option Bearbeiten aus.
4. Wählen Sie in EC2diesem Abschnitt die Option Aktivieren aus.
5. Wählen Sie Save (Speichern) aus.
6. Sie können überprüfen, ob die SSM Verknüpfung, die GuardDuty erstellt wird, den Security Agent auf allen EC2 Ressourcen installiert und verwaltet, die zu Ihrem Konto gehören.

   a. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

   b. Öffnen Sie die Registerkarte Ziele für die SSM Assoziation (`GuardDutyRuntimeMonitoring-do-not-delete`). Beachten Sie, dass der Tag-Schlüssel als angezeigt wird InstanceIds.

Using inclusion tag in selected instances

Um den GuardDuty Security Agent für ausgewählte EC2 Amazon-Instances zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Sie können überprüfen, ob die SSM Verknüpfung, die GuardDuty erstellt wird, den Security Agent nur auf den EC2 Ressourcen installiert und verwaltet, die mit den Inklusion-Tags gekennzeichnet sind.

   Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

- Öffnen Sie die Registerkarte Ziele für die SSM Verknüpfung, die erstellt wird (`GuardDutyRuntimeMonitoring-do-not-delete`). Der Tag-Schlüssel wird als Tag: angezeigtGuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren EC2 Amazon-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon aktiviert habenEC2, wird jede EC2 Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

Um den GuardDuty Security Agent für ausgewählte EC2 Amazon-Instances zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen nicht erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Gehen Sie wie folgt vor, damit die Ausschluss-Tags in den Instanz-Metadaten verfügbar sind:
   a. Sehen Sie sich auf dem Tab „Details“ Ihrer Instance den Status für Tags zulassen in den Instanz-Metadaten an.

      Wenn es derzeit Deaktiviert ist, gehen Sie wie folgt vor, um den Status auf Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.
   b. Wählen Sie die Instanz aus, für die Sie Tags zulassen möchten.
   c. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.
   d. Wähle „Tags in Instanz-Metadaten zulassen“.
   e. Wählen Sie unter Zugriff auf Tags in Instanzmetadaten die Option Zulassen aus.
   f. Wählen Sie Save (Speichern) aus.

4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, wie auf der Registerkarte Für alle Instanzen konfigurieren angegeben.

Sie können jetzt die Laufzeit beurteilen. Deckung für EC2 Amazon-Instance

Konfiguration des GuardDuty Agenten in einer Umgebung mit mehreren Konten

Für ein delegiertes Administratorkonto GuardDuty

Configure for all instances

Wenn Sie für Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben, wählen Sie eine der folgenden Optionen für das delegierte GuardDuty Administratorkonto:

- Option 1

  Wählen Sie im EC2Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus.
- Option 2
  - Wählen Sie im EC2Abschnitt Automatisierte Agentenkonfiguration die Option Konten manuell konfigurieren aus.
  - Wählen Sie unter Delegierter Administrator (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Save (Speichern) aus.

Wenn Sie Konten manuell für Runtime Monitoring konfigurieren ausgewählt haben, führen Sie die folgenden Schritte aus:

- Wählen Sie im EC2Abschnitt Automatisierte Agentenkonfiguration die Option Konten manuell konfigurieren aus.
- Wählen Sie unter Delegierter Administrator (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Save (Speichern) aus.

Unabhängig davon, welche Option Sie wählen, um die automatische Agentenkonfiguration für das delegierte GuardDuty Administratorkonto zu aktivieren, können Sie sicherstellen, dass die SSM Verknüpfung, die GuardDuty erstellt wird, den Security Agent auf allen EC2 Ressourcen installiert und verwaltet, die zu diesem Konto gehören.

1. Öffnen Sie die AWS Systems Manager Konsole unter. https://console.aws.amazon.com/systems-manager/
2. Öffnen Sie die Registerkarte Ziele für die SSM Assoziation (`GuardDutyRuntimeMonitoring-do-not-delete`). Beachten Sie, dass der Tag-Schlüssel als angezeigt wird InstanceIds.

Using inclusion tag in selected instances

So konfigurieren Sie den GuardDuty Agenten für ausgewählte EC2 Amazon-Instances

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

   Wenn Sie dieses Tag hinzufügen GuardDuty , können Sie den Security Agent für diese ausgewählten EC2 Instanzen installieren und verwalten. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren.
3. Sie können sicherstellen, dass die SSM Verknüpfung, die GuardDuty erstellt wird, den Security Agent nur auf den EC2 Ressourcen installiert und verwaltet, die mit den Inklusion-Tags gekennzeichnet sind.

   Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

   - Öffnen Sie die Registerkarte Ziele für die SSM Verknüpfung, die erstellt wird (`GuardDutyRuntimeMonitoring-do-not-delete`). Der Tag-Schlüssel wird als Tag: angezeigtGuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren EC2 Amazon-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für

Amazon aktiviert habenEC2, wird jede EC2 Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

So konfigurieren Sie den GuardDuty Agenten für ausgewählte EC2 Amazon-Instances

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen nicht erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Gehen Sie wie folgt vor, damit die Ausschluss-Tags in den Instanz-Metadaten verfügbar sind:
   a. Sehen Sie sich auf dem Tab „Details“ Ihrer Instance den Status für Tags zulassen in den Instanz-Metadaten an.

      Wenn es derzeit Deaktiviert ist, gehen Sie wie folgt vor, um den Status auf Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.
   b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.
   c. Wähle „Tags in Instanz-Metadaten zulassen“.
4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, wie auf der Registerkarte Für alle Instanzen konfigurieren angegeben.

Sie können jetzt die Laufzeit beurteilenDeckung für EC2 Amazon-Instance.

Automatische Aktivierung für alle Mitgliedskonten

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Configure for all instances

Bei den folgenden Schritten wird davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben:

1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration für Amazon die Option Für alle Konten aktivieren ausEC2.
2. Sie können überprüfen, ob die SSM Verknüpfung, die GuardDuty erstellt (`GuardDutyRuntimeMonitoring-do-not-delete`), den Security Agent auf allen EC2 Ressourcen installiert und verwaltet, die zu diesem Konto gehören.

   a. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

   b. Öffnen Sie die Registerkarte Ziele für die SSM Assoziation. Beachten Sie, dass der Tag-Schlüssel als angezeigt wird InstanceIds.

Using inclusion tag in selected instances

So konfigurieren Sie den GuardDuty Agenten für ausgewählte EC2 Amazon-Instances

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den EC2 Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

   Wenn Sie dieses Tag hinzufügen GuardDuty , können Sie den Security Agent für diese ausgewählten EC2 Instanzen installieren und verwalten. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren.
3. Sie können überprüfen, ob die SSM Verknüpfung, die GuardDuty erstellt wird, den Security Agent auf allen EC2 Ressourcen installiert und verwaltet, die zu Ihrem Konto gehören.

   a. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

   b. Öffnen Sie die Registerkarte Ziele für die SSM Assoziation (`GuardDutyRuntimeMonitoring-do-not-delete`). Beachten Sie, dass der Tag-Schlüssel als angezeigt wird InstanceIds.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren EC2 Amazon-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon aktiviert habenEC2, wird jede EC2 Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

Um den GuardDuty Security Agent für ausgewählte EC2 Amazon-Instances zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen nicht erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Gehen Sie wie folgt vor, damit die Ausschluss-Tags in den Instanz-Metadaten verfügbar sind:
   a. Sehen Sie sich auf dem Tab „Details“ Ihrer Instance den Status für Tags zulassen in den Instanz-Metadaten an.

      Wenn es derzeit Deaktiviert ist, gehen Sie wie folgt vor, um den Status auf Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.
   b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.
   c. Wähle „Tags in Instanz-Metadaten zulassen“.
4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, wie auf der Registerkarte Für alle Instanzen konfigurieren angegeben.

Sie können jetzt die Laufzeit beurteilenDeckung für EC2 Amazon-Instance.

Automatische Aktivierung nur für neue Mitgliedskonten

Das delegierte GuardDuty Administratorkonto kann die automatische Agentenkonfiguration für EC2 Amazon-Ressourcen so einrichten, dass sie automatisch für die neuen Mitgliedskonten aktiviert wird, wenn sie der Organisation beitreten.

Configure for all instances

Bei den folgenden Schritten wird davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Automatisch für neue Mitgliedskonten aktivieren ausgewählt haben:

1. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
2. Wählen Sie auf der Seite Runtime Monitoring die Option Bearbeiten aus.
3. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass jedes Mal, wenn ein neues Konto Ihrer Organisation beitritt, die automatische Agentenkonfiguration für Amazon automatisch für das Konto aktiviert EC2 wird. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Auswahl ändern.
4. Wählen Sie Save (Speichern) aus.

Wenn der Organisation ein neues Mitgliedskonto beitritt, wird diese Konfiguration automatisch für dieses Konto aktiviert. GuardDuty Um den Sicherheitsagenten für die EC2 Amazon-Instances zu verwalten, die zu diesem neuen Mitgliedskonto gehören, müssen Sie sicherstellen, dass alle Voraussetzungen erfüllt Zum EC2 Beispiel sind.

Wenn eine SSM Zuordnung erstellt wird (`GuardDutyRuntimeMonitoring-do-not-delete`), können Sie überprüfen, ob die SSM Assoziation den Security Agent auf allen EC2 Instances installiert und verwaltet, die zu dem neuen Mitgliedskonto gehören.

- Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
- Öffnen Sie die Registerkarte Ziele für die SSM Assoziation. Beachten Sie, dass der Tag-Schlüssel als angezeigt wird InstanceIds.

Using inclusion tag in selected instances

Um den GuardDuty Security Agent für ausgewählte Instances in Ihrem Konto zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

Durch Hinzufügen dieses Tags GuardDuty kann der Security Agent für diese ausgewählten Instanzen installiert und verwaltet werden. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren.

3. Sie können sicherstellen, dass die SSM Verknüpfung, die GuardDuty erstellt wird, den Security Agent nur auf den EC2 Ressourcen installiert und verwaltet, die mit den Inklusion-Tags gekennzeichnet sind.

   a. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

   b. Öffnen Sie die Registerkarte Ziele für die SSM Verknüpfung, die erstellt wird. Der Tag-Schlüssel wird als Tag: angezeigtGuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren EC2 Amazon-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon aktiviert habenEC2, wird jede EC2 Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

So konfigurieren Sie den GuardDuty Security Agent für bestimmte Instances in Ihrem eigenständigen Konto

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie nicht überwachen und potenzielle Bedrohungen nicht erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Gehen Sie wie folgt vor, damit die Ausschluss-Tags in den Instanz-Metadaten verfügbar sind:

   a. Sehen Sie sich auf dem Tab „Details“ Ihrer Instance den Status für Tags zulassen in den Instanz-Metadaten an.

Wenn es derzeit Deaktiviert ist, gehen Sie wie folgt vor, um den Status auf Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.

b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.

c. Wähle „Tags in Instanz-Metadaten zulassen“.

4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, wie auf der Registerkarte Für alle Instanzen konfigurieren angegeben.

Sie können jetzt die Laufzeit beurteilenDeckung für EC2 Amazon-Instance.

Nur ausgewählte Mitgliedskonten

Configure for all instances

1. Wählen Sie auf der Seite Konten ein oder mehrere Konten aus, für die Sie die Runtime Monitoring-Automated Agent-Konfiguration (Amazon) aktivieren möchten. EC2 Stellen Sie sicher, dass Runtime Monitoring für die Konten, die Sie in diesem Schritt auswählen, bereits aktiviert ist.
2. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um Runtime Monitoring-Automated Agent Configuration (Amazon) zu aktivieren. EC2
3. Wählen Sie Bestätigen aus.

Using inclusion tag in selected instances

Um den GuardDuty Security Agent für ausgewählte Instances zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den Instances, die Sie überwachen und potenzielle Bedrohungen erkennen GuardDuty möchten, das `true` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.

   Wenn Sie dieses Tag hinzufügen GuardDuty , können Sie den Security Agent für Ihre markierten EC2 Amazon-Instances verwalten. Sie müssen die automatische Agentenkonfiguration nicht explizit aktivieren (Runtime Monitoring — Automated Agent configuration (EC2)).

Using exclusion tag in selected instances

> **Note**
>
> Stellen Sie sicher, dass Sie Ihren EC2 Amazon-Instances das Ausschluss-Tag hinzufügen, bevor Sie sie starten. Sobald Sie die automatische Agentenkonfiguration für Amazon aktiviert habenEC2, wird jede EC2 Instance, die ohne Ausschluss-Tag gestartet wird, von der GuardDuty automatisierten Agentenkonfiguration abgedeckt.

Um den GuardDuty Security Agent für ausgewählte Instances zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Fügen Sie den EC2 Instances, die Sie nicht überwachen oder potenzielle Bedrohungen nicht erkennen GuardDuty möchten, das `false` Tag`GuardDutyManaged`: hinzu. Informationen zum Hinzufügen dieses Tags finden Sie unter So fügen Sie einer einzelnen Ressource ein Tag hinzu.
3. Gehen Sie wie folgt vor, damit die Ausschluss-Tags in den Instanz-Metadaten verfügbar sind:

   a. Sehen Sie sich auf dem Tab „Details“ Ihrer Instance den Status für Tags zulassen in den Instanz-Metadaten an.

      Wenn es derzeit Deaktiviert ist, gehen Sie wie folgt vor, um den Status auf Aktiviert zu ändern. Andernfalls überspringen Sie diesen Schritt.

   b. Wählen Sie im Menü Aktionen die Option Instanzeinstellungen aus.

   c. Wähle „Tags in Instanz-Metadaten zulassen“.
4. Nachdem Sie das Ausschluss-Tag hinzugefügt haben, führen Sie dieselben Schritte aus, wie auf der Registerkarte Für alle Instanzen konfigurieren angegeben.

Sie können jetzt beurteilenDeckung für EC2 Amazon-Instance.

Manuelles Verwalten des Security Agents für EC2 Amazon-Instance

Nachdem Sie Runtime Monitoring aktiviert haben, müssen Sie den GuardDuty Security Agent manuell installieren. Durch die Installation des Agenten GuardDuty werden die Runtime-Ereignisse von den EC2 Amazon-Instances empfangen.

Um den GuardDuty Security Agent zu verwalten, müssen Sie einen VPC Amazon-Endpunkt erstellen und dann die Schritte zur manuellen Installation des Security Agents befolgen.

Manuelles Erstellen eines VPC Amazon-Endpunkts

Bevor Sie den GuardDuty Security Agent installieren können, müssen Sie einen Amazon Virtual Private Cloud (AmazonVPC) -Endpunkt erstellen. Dies hilft beim GuardDuty Empfang der Runtime-Ereignisse Ihrer EC2 Amazon-Instances.

> **Note**
>
> Für die Nutzung des VPC Endpunkts fallen keine zusätzlichen Kosten an.

Um einen VPC Amazon-Endpunkt zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich unter VPCPrivate Cloud die Option Endpoints aus.
3. Klicken Sie auf Endpunkt erstellen.
4. Wählen Sie auf der Seite Endpunkt erstellen für Servicekategorie die Option Andere Endpunkt-Services.
5. Geben Sie unter Servicename **`com.amazonaws.`*`us-east-1`*`.guardduty-data`** ein.

   Stellen Sie sicher, dass Sie es ersetzen *`us-east-1`* mit deinem AWS-Region. Dies muss dieselbe Region sein wie die EC2 Amazon-Instance, die zu Ihrer AWS Konto-ID gehört.
6. Wählen Sie Service verifizieren.
7. Nachdem der Servicename erfolgreich verifiziert wurde, wählen Sie den VPCOrt aus, an dem sich Ihre Instance befindet. Fügen Sie die folgende Richtlinie hinzu, um die Nutzung von VPC Amazon-Endgeräten nur auf das angegebene Konto zu beschränken. Unter Angabe der unter dieser Richtlinie angegebenen Organisations-`Condition` können Sie die folgende Richtlinie aktualisieren, um den Zugriff auf Ihren Endpunkt einzuschränken. Informationen zur Bereitstellung des VPC Amazon-Endpunktsupports für ein bestimmtes Konto IDs in Ihrer Organisation finden Sie unterOrganization condition to restrict access to your endpoint.

   ```
   {
    "Version": "2012-10-17",
    "Statement": [
   ```

```
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

Die `aws:PrincipalAccount` Konto-ID muss mit dem Konto übereinstimmen, das den VPC Endpunkt VPC und enthält. Die folgende Liste zeigt, wie Sie den VPC Endpunkt mit einem anderen AWS Konto teilen könnenIDs:

- Um mehrere Konten für den Zugriff auf den VPC Endpunkt anzugeben, `"aws:PrincipalAccount: "111122223333"` ersetzen Sie ihn durch den folgenden Block:

  ```
  "aws:PrincipalAccount": [
            "666666666666",
            "555555555555"
       ]
  ```

  Achten Sie darauf, das AWS Konto IDs durch das Konto IDs der Konten zu ersetzen, die auf den VPC Endpunkt zugreifen müssen.

- Um allen Mitgliedern einer Organisation den Zugriff auf den VPC Endpunkt zu ermöglichen, `"aws:PrincipalAccount: "111122223333"` ersetzen Sie ihn durch die folgende Zeile:

  ```
  "aws:PrincipalOrgID": "o-abcdef0123"
  ```

Achten Sie darauf, die Organisation zu ersetzen *o-abcdef0123* mit Ihrer Organisations-ID.

- Um den Zugriff auf eine Ressource anhand einer Organisations-ID einzuschränken, fügen Sie Ihre `ResourceOrgID` zur Richtlinie hinzu. Weitere Informationen finden Sie `aws:ResourceOrgID`im IAMBenutzerhandbuch.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Wählen Sie unter Zusätzliche Einstellungen die Option DNSNamen aktivieren aus.
9. Wählen Sie unter Subnetze die Subnetze aus, in denen sich Ihre Instance befindet.
10. Wählen Sie unter Sicherheitsgruppen eine Sicherheitsgruppe aus, für die der eingehende Port 443 von Ihrer VPC (oder Ihrer EC2 Amazon-Instance) aktiviert ist. Wenn Sie noch keine Sicherheitsgruppe haben, für die ein eingehender Port 443 aktiviert ist, finden Sie weitere Informationen unter Erstellen einer Sicherheitsgruppe im EC2Amazon-Benutzerhandbuch.

    Wenn bei der Beschränkung der eingehenden Zugriffsberechtigungen für Sie VPC (oder Instance) ein Problem auftritt, stellen Sie den Support für den eingehenden Port 443 von einer beliebigen IP-Adresse aus bereit. `(0.0.0.0/0)`

Manuelles Installieren des Security Agents

GuardDuty bietet die folgenden zwei Methoden zur Installation des GuardDuty Security Agents auf Ihren EC2 Amazon-Instances:

- Methode 1 — Mithilfe AWS Systems Manager — Für diese Methode muss Ihre EC2 Amazon-Instance AWS Systems Manager verwaltet werden.
- Methode 2 — Mithilfe von Linux-Paketmanagern — Sie können diese Methode unabhängig davon verwenden, ob Ihre EC2 Amazon-Instances AWS Systems Manager verwaltet werden oder nicht.

Methode 1 — Indem Sie AWS Systems Manager

Um diese Methode zu verwenden, stellen Sie sicher, dass Ihre EC2 Amazon-Instances AWS Systems Manager verwaltet werden, und installieren Sie dann den Agenten.

AWS Systems Manager verwaltete EC2 Amazon-Instanz

Gehen Sie wie folgt vor, um Ihre EC2 Amazon-Instances zu AWS Systems Manager verwalten.

- AWS Systems Managerhilft Ihnen bei der Verwaltung Ihrer AWS Anwendungen und Ressourcen end-to-end und ermöglicht sichere Abläufe in großem Maßstab.

  Informationen zur Verwaltung Ihrer EC2 Amazon-Instances mit AWS Systems Manager finden Sie unter Systems Manager für EC2 Amazon-Instances einrichten im AWS Systems Manager Benutzerhandbuch.

- Die folgende Tabelle zeigt die neuen GuardDuty verwalteten AWS Systems Manager Dokumente:

Dokumentname	Dokumenttyp	Zweck
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distributor	Um den GuardDuty Security Agent zu verpacken.
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Befehl	Um das Installations- und Deinstallationsskript auszuführen, um den Security Agent zu installieren. GuardDuty

Weitere Informationen zu AWS Systems Manager finden Sie in den Amazon EC2 Systems Manager Manager-Dokumenten im AWS Systems Manager Benutzerhandbuch.

> **Für Debian-Server**
>
> Die von bereitgestellten Amazon Machine Images (AMIs) für Debian Server AWS erfordern die Installation des AWS Systems Manager Agenten (SSMAgenten). Sie müssen einen zusätzlichen Schritt ausführen, um den SSM Agenten zu installieren, damit Ihre Amazon EC2 Debian Server-Instances SSM verwaltet werden. Informationen zu den Schritten, die Sie ergreifen müssen, finden Sie unter SSMAgenten manuell auf Debian-Server-Instances installieren im AWS Systems Manager Benutzerhandbuch.

Um den GuardDuty Agenten für die EC2 Amazon-Instance zu installieren, verwenden Sie AWS Systems Manager

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich Dokumente
3. Wählen Sie unter Owned by Amazon die Option aus`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
4. Wählen Sie Run Command (Befehl ausführen) aus.
5. Geben Sie die folgenden Run-Command-Parameter ein

   - Aktion: Wählen Sie Installieren.
   - Installationstyp: Wählen Sie Installieren oder Deinstallieren.
   - Name: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
   - Version: Wenn dieses Feld leer bleibt, erhalten Sie die neueste Version des GuardDuty Security Agents. Weitere Informationen zu den Release-Versionen finden Sie unterGuardDuty Sicherheitsagent für EC2 Amazon-Instances.
6. Wählen Sie die EC2 Amazon-Zielinstanz aus. Sie können eine oder mehrere EC2 Amazon-Instances auswählen. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Befehle von der Konsole aus AWS Systems Manager ausführen
7. Überprüfen Sie, ob die GuardDuty Agenteninstallation fehlerfrei ist. Weitere Informationen finden Sie unter Der Installationsstatus des GuardDuty Security Agents wird überprüft.

Methode 2 — Mithilfe von Linux-Paketmanagern

Mit dieser Methode können Sie den GuardDuty Security Agent installieren, indem Sie RPM Skripte oder Debian-Skripte ausführen. Je nach Betriebssystem können Sie eine bevorzugte Methode wählen:

- Verwenden Sie RPM Skripts, um den Security Agent auf Betriebssystem-Distributionen AL2 oder AL2 023 zu installieren.
- Verwenden Sie Debian-Skripte, um den Security Agent auf den Betriebssystem-Distributionen Ubuntu oder Debian zu installieren. Hinweise zu den unterstützten Ubuntu- und Debian-Betriebssystem-Distributionen finden Sie unter. Validierung der architektonischen Anforderungen

RPM installation

> **Important**
>
> Wir empfehlen, die RPM Signatur des GuardDuty Security Agents zu überprüfen, bevor Sie ihn auf Ihrem Computer installieren.

1. Überprüfen Sie die GuardDuty Security Agent-Signatur RPM

   a. Bereiten Sie die Vorlage vor

   Bereiten Sie die Befehle mit dem entsprechenden öffentlichen Schlüssel, der Signatur von x86_64RPM, der Signatur von arm64 RPM und dem entsprechenden Zugriffslink zu den in Amazon S3 S3-Buckets gehosteten RPM Skripten vor. Ersetzen Sie den Wert von AWS-Region, die AWS Konto-ID und die GuardDuty Agentenversion, um auf die Skripts zuzugreifen. RPM

   - Öffentlicher Schlüssel:

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/
     publickey.pem
     ```

   - GuardDuty RPMSignatur des Sicherheitsagenten:

     Signatur von x86_64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/
     amazon-guardduty-agent-1.3.0.x86_64.sig
     ```

     Signatur von arm64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/
     amazon-guardduty-agent-1.3.0.arm64.sig
     ```

   - Greifen Sie auf Links zu den RPM Skripten im Amazon S3 S3-Bucket zu:

     Zugangslink für x86_64 RPM

     ```
     s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/
     amazon-guardduty-agent-1.3.0.x86_64.rpm
     ```

Zugangslink für arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.rpm
```

AWS-Region	Name der Region	AWS Konto-ID
eu-west-1	Europa (Irland)	694911143906
us-east-1	USA Ost (Nord-Virginia)	593207742271
us-west-2	USA West (Oregon)	733349766148
eu-west-3	Europa (Paris)	665651866788
us-east-2	USA Ost (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986
ap-northeast-2	Asien-Pazifik (Seoul)	914738172881
eu-north-1	Europa (Stockholm)	591436053604
ap-east-1	Asien-Pazifik (Hongkong)	258348409381
me-south-1	Naher Osten (Bahrain)	536382113932
eu-west-2	Europa (London)	892757235363
ap-northeast-1	Asien-Pazifik (Tokio)	533107202818
ap-southeast-1	Asien-Pazifik (Singapur)	174946120834
ap-south-1	Asien-Pazifik (Mumbai)	251508486986
ap-southeast-3	Asien-Pazifik (Jakarta)	510637619217
sa-east-1	Südamerika (São Paulo)	758426053663

ap-northeast-3	Asien-Pazifik (Osaka)	273192626886
eu-south-1	Europa (Milan)	266869475730
af-south-1	Afrika (Kapstadt)	197869348890
ap-southeast-2	Asien-Pazifik (Sydney)	005257825471
me-central-1	Naher Osten () UAE	000014521398
us-west-1	USA West (Nordkali fornien)	684579721401
ca-central-1	Kanada (Zentral)	354763396469
ca-west-1	Kanada West (Calgary)	339712888787
ap-south-2	Asien-Pazifik (Hyderabad)	950823858135
eu-south-2	Europa (Spain)	919611009337
eu-central-2	Europa (Zürich)	529164026651
ap-southeast-4	Asien-Pazifik (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882

b. Laden Sie die Vorlage herunter

Stellen Sie im folgenden Befehl zum Herunterladen des entsprechenden öffentlichen Schlüssels, der Signatur von x86_64RPM, der Signatur von arm64 RPM und des entsprechenden Zugriffs-Links zu den in Amazon S3 S3-Buckets gehosteten RPM Skripten sicher, dass Sie die Konto-ID durch die entsprechende AWS-Konto ID und die Region durch Ihre aktuelle Region ersetzen.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/
x86_64/amazon-guardduty-agent-1.3.0.x86_64.rpm ./amazon-guardduty-
agent-1.3.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/
x86_64/amazon-guardduty-agent-1.3.0.x86_64.sig ./amazon-guardduty-
agent-1.3.0.x86_64.sig
```

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/
publickey.pem ./publickey.pem
```

c. Importieren Sie den öffentlichen Schlüssel

Verwenden Sie den folgenden Befehl, um den öffentlichen Schlüssel in die Datenbank zu importieren:

```
gpg --import publickey.pem
```

gpg zeigt, dass der Import erfolgreich war

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. Verifiziere die Signatur

Verwenden Sie den folgenden Befehl, um die Signatur zu überprüfen

```
gpg --verify amazon-guardduty-agent-1.3.0.x86_64.sig amazon-guardduty-
agent-1.3.0.x86_64.rpm
```

Wenn die Überprüfung erfolgreich ist, wird eine Meldung ähnlich dem folgenden Ergebnis angezeigt. Sie können nun mit der Installation des GuardDuty Security Agents fortfahren mitRPM.

Beispielausgabe:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Wenn die Überprüfung fehlschlägt, bedeutet dies, dass die Signatur möglicherweise manipuliert RPM wurde. Sie müssen den öffentlichen Schlüssel aus der Datenbank entfernen und den Überprüfungsprozess erneut versuchen.

Beispiel:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Verwenden Sie den folgenden Befehl, um den öffentlichen Schlüssel aus der Datenbank zu entfernen:

```
gpg --delete-keys AwsGuardDuty
```

Versuchen Sie nun erneut, den Überprüfungsprozess durchzuführen.

2. Stellen Sie SSHvon Linux oder macOS aus eine Connect.
3. Installieren Sie den GuardDuty Security Agent mit dem folgenden Befehl:

```
sudo rpm -ivh amazon-guardduty-agent-1.3.0.x86_64.rpm
```

4. Überprüfen Sie, ob die GuardDuty Agent-Installation fehlerfrei ist. Weitere Informationen zu den Schritten finden Sie unterDer Installationsstatus des GuardDuty Security Agents wird überprüft.

Debian installation

> **Important**
>
> Wir empfehlen, die Debian-Signatur des GuardDuty Security Agents zu überprüfen, bevor Sie ihn auf Ihrem Computer installieren.

1. Überprüfen Sie die GuardDuty Debian-Signatur des Security Agents

   a. Bereiten Sie Vorlagen für den entsprechenden öffentlichen Schlüssel, die Signatur des amd64-Debian-Pakets, die Signatur des arm64-Debian-Pakets und den entsprechenden Zugangslink zu den Debian-Skripten vor, die in Amazon S3 S3-Buckets gehostet werden

   Ersetzen Sie in den folgenden Vorlagen den Wert von, die AWS Konto-ID und die AWS-Region GuardDuty Agentenversion, um auf die Debian-Paketskripte zuzugreifen.

- Öffentlicher Schlüssel:

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
publickey.pem
```

- GuardDuty Debian-Signatur des Sicherheitsagenten:

  Signatur von amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/
amazon-guardduty-agent-1.3.0.amd64.sig
```

  Signatur von arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.sig
```

- Zugriffs-Links zu den Debian-Skripten im Amazon S3 S3-Bucket:

  Zugangslink für amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/
amazon-guardduty-agent-1.3.0.amd64.deb
```

  Zugangslink für arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/
amazon-guardduty-agent-1.3.0.arm64.deb
```

AWS-Region	Name der Region	AWS Konto-ID
eu-west-1	Europa (Irland)	694911143906
us-east-1	USA Ost (Nord-Virginia)	593207742271
us-west-2	USA West (Oregon)	733349766148
eu-west-3	Europa (Paris)	665651866788

us-east-2	USA Ost (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986
ap-northeast-2	Asien-Pazifik (Seoul)	914738172881
eu-north-1	Europa (Stockholm)	591436053604
ap-east-1	Asien-Pazifik (Hongkong)	258348409381
me-south-1	Naher Osten (Bahrain)	536382113932
eu-west-2	Europa (London)	892757235363
ap-northeast-1	Asien-Pazifik (Tokio)	533107202818
ap-southeast-1	Asien-Pazifik (Singapur)	174946120834
ap-south-1	Asien-Pazifik (Mumbai)	251508486986
ap-southeast-3	Asien-Pazifik (Jakarta)	510637619217
sa-east-1	Südamerika (São Paulo)	758426053663
ap-northeast-3	Asien-Pazifik (Osaka)	273192626886
eu-south-1	Europa (Milan)	266869475730
af-south-1	Afrika (Kapstadt)	197869348890
ap-southeast-2	Asien-Pazifik (Sydney)	005257825471
me-central-1	Naher Osten () UAE	000014521398
us-west-1	USA West (Nordkali fornien)	684579721401
ca-central-1	Kanada (Zentral)	354763396469
ca-west-1	Kanada West (Calgary)	339712888787
ap-south-2	Asien-Pazifik (Hyderabad)	950823858135

eu-south-2	Europa (Spain)	919611009337
eu-central-2	Europa (Zürich)	529164026651
ap-southeast-4	Asien-Pazifik (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882

b. Laden Sie den entsprechenden öffentlichen Schlüssel, die Signatur von amd64, die Signatur von arm64 und den entsprechenden Zugangslink zu den Debian-Skripten herunter, die in Amazon S3 S3-Buckets gehostet werden

   Ersetzen Sie in den folgenden Befehlen die Konto-ID durch die entsprechende AWS-Konto ID und die Region durch Ihre aktuelle Region.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
amd64/amazon-guardduty-agent-1.3.0.amd64.deb ./amazon-guardduty-
agent-1.3.0.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
amd64/amazon-guardduty-agent-1.3.0.amd64.sig ./amazon-guardduty-
agent-1.3.0.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/
publickey.pem ./publickey.pem
```

c. Importieren Sie den öffentlichen Schlüssel in die Datenbank

```
gpg --import publickey.pem
```

   gpg zeigt, dass der Import erfolgreich war

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

d. Verifiziere die Signatur

```
gpg --verify amazon-guardduty-agent-1.3.0.amd64.sig amazon-guardduty-
agent-1.3.0.amd64.deb
```

   Nach einer erfolgreichen Überprüfung wird eine Meldung angezeigt, die dem folgenden Ergebnis ähnelt:

Beispielausgabe:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Sie können nun mit der Installation des GuardDuty Security Agents unter Verwendung von Debian fortfahren.

Wenn die Überprüfung jedoch fehlschlägt, bedeutet dies, dass die Signatur im Debian-Paket möglicherweise manipuliert wurde.

Beispiel:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Verwenden Sie den folgenden Befehl, um den öffentlichen Schlüssel aus der Datenbank zu entfernen:

```
gpg --delete-keys AwsGuardDuty
```

Versuchen Sie nun erneut, den Überprüfungsprozess durchzuführen.

2. Stellen Sie SSHvon Linux oder macOS aus eine Connect.
3. Installieren Sie den GuardDuty Security Agent mit dem folgenden Befehl:

```
sudo dpkg -i amazon-guardduty-agent-1.3.0.amd64.deb
```

4. Überprüfen Sie, ob die GuardDuty Agent-Installation fehlerfrei ist. Weitere Informationen zu den Schritten finden Sie unterDer Installationsstatus des GuardDuty Security Agents wird überprüft.

Fehler: Nicht genügend Arbeitsspeicher

Wenn bei der EC2 manuellen Installation oder Aktualisierung des GuardDuty Security Agents for Amazon ein `out-of-memory` Fehler auftritt, finden Sie weitere Informationen unterBehebung eines Fehlers wegen unzureichenden Speichers.

Der Installationsstatus des GuardDuty Security Agents wird überprüft

Um zu überprüfen, ob der GuardDuty Security Agent fehlerfrei ist

1. Stellen Sie SSHvon Linux oder macOS aus eine Connect.
2. Führen Sie den folgenden Befehl aus, um den Status des GuardDuty Security Agents zu überprüfen:

```
sudo systemctl status amazon-guardduty-agent
```

Wenn Sie die Installationsprotokolle des Security Agents einsehen möchten, finden Sie sie unter/`var/log/amzn-guardduty-agent/`.

Um die Protokolle einzusehen, tun Sie dies`sudo journalctl -u amazon-guardduty-agent`.

Manuelles Aktualisieren des GuardDuty Security Agents

Sie können den GuardDuty Security Agent mit dem Befehl Ausführen aktualisieren. Sie können dieselben Schritte ausführen, mit denen Sie den GuardDuty Security Agent installiert haben.

Den Security Agent manuell deinstallieren

In diesem Abschnitt finden Sie Methoden zur Deinstallation des GuardDuty Security Agents von Ihren EC2 Amazon-Ressourcen. Wenn Sie außerdem planen, Runtime Monitoring zu deaktivieren, finden Sie weitere Informationen unterAuswirkungen der Deaktivierung.

Methode 1 — Mit dem Befehl Run

So deinstallieren Sie den GuardDuty Security Agent mit dem Befehl Run

1. Sie können den GuardDuty Security Agent deinstallieren, indem Sie die im AWS Systems Manager Benutzerhandbuch AWS Systems Manager unter Befehl ausführen angegebenen Schritte ausführen ausführen. Verwenden Sie die Aktion Deinstallieren in den Parametern, um den GuardDuty Security Agent zu deinstallieren.

Stellen Sie im Abschnitt Ziele sicher, dass sich die Auswirkungen nur auf die EC2 Amazon-Instances auswirken, von denen Sie den Security Agent deinstallieren möchten.

Verwenden Sie das folgende GuardDuty Dokument und den folgenden Vertriebspartner:

- Name des Dokuments: `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
- Vertriebspartner: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`

2. Nachdem Sie alle Details angegeben haben und Ausführen wählen, wird der Security Agent, den er auf den EC2 Ziel-Amazon-Instances bereitgestellt hat, entfernt.

   Um die VPC Amazon-Endpunktkonfiguration zu entfernen, müssen Sie sowohl Runtime Monitoring als auch Amazon EKS Runtime Monitoring deaktivieren.

Methode 2 — Mithilfe von Linux-Paketmanagern

1. Stellen Sie SSHvon Linux oder macOS aus eine Connect.
2. Befehl zur Deinstallation

   Mit dem folgenden Befehl wird der GuardDuty Security Agent von der EC2 Amazon-Instance deinstalliert, zu der Sie eine Verbindung herstellen:

   - FürRPM:

     ```
     sudo rpm -e amazon-guardduty-agent
     ```

   - Für Debian:

     ```
     sudo dpkg --purge amazon-guardduty-agent
     ```

   Nachdem Sie den Befehl ausgeführt haben, können Sie auch die mit dem Befehl verknüpften Protokolle überprüfen.

Löschen Sie den VPC Amazon-Endpunkt

Wenn Sie Runtime Monitoring deaktivieren oder den GuardDuty Security Agent für Ihr Konto deinstallieren möchten, können Sie auch den manuell erstellten VPC Amazon-Endpunkt löschen (Manuelles Erstellen eines VPC Amazon-Endpunkts).

So löschen Sie den VPC Amazon-Endpunkt mithilfe der Konsole

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Endpunkte aus.
3. Wählen Sie den Endpunkt aus, der zum Zeitpunkt der Aktivierung von Runtime Monitoring manuell erstellt wurde.
4. Wählen Sie Aktionen, VPCEndpunkte löschen aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein.
6. Wählen Sie Löschen.

Um den VPC Amazon-Endpunkt zu löschen, verwenden Sie AWS CLI

- delete-vpc-endpoints (AWS Command Line Interface)
- Remove-EC2VpcEndpointCmdlet (Tools für Windows) PowerShell

Verwaltung eines automatisierten Sicherheitsagenten für Fargate (ECSnur Amazon)

Runtime Monitoring unterstützt die Verwaltung des Security Agents für Ihre ECS Amazon-Cluster (AWS Fargate) nur über GuardDuty. Die manuelle Verwaltung des Security Agents auf ECS Amazon-Clustern wird nicht unterstützt.

Gehen Sie wie GuardDuty in den folgenden Abschnitten beschrieben vor, um den Security Agent für Ihre ECS -Fargate-Ressourcen verwalten zu können.

Inhalt

- Den GuardDuty Agenten für ein eigenständiges Konto konfigurieren
- GuardDuty Agent für eine Umgebung mit mehreren Konten konfigurieren

Den GuardDuty Agenten für ein eigenständiges Konto konfigurieren

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Gehen Sie auf der Registerkarte Konfiguration wie folgt vor:

a. Um die automatische Agentenkonfiguration für alle ECS Amazon-Cluster zu verwalten (Kontoebene)

   Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration für AWS Fargate (ECSnur) die Option Aktivieren aus. Wenn eine neue ECS Fargate-Amazon-Aufgabe gestartet GuardDuty wird, wird die Bereitstellung des Sicherheitsagenten verwaltet.

   - Wählen Sie Save (Speichern) aus.

b. Verwaltung der automatisierten Agentenkonfiguration durch Ausschluss einiger ECS Amazon-Cluster (Cluster-Ebene)

   i. Fügen Sie dem ECS Amazon-Cluster, für den Sie alle Aufgaben ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `false`

   ii. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
```

```
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Automatisierte Agentenkonfiguration die Option Aktivieren aus.

> **Note**
>
> Fügen Sie Ihrem ECS Amazon-Cluster immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der Security Agent bei allen Aufgaben eingesetzt, die innerhalb des entsprechenden ECS Amazon-Clusters gestartet werden.

Verwaltet für die ECS Amazon-Cluster, die nicht ausgeschlossen wurden, GuardDuty die Bereitstellung des Security Agents im Sidecar-Container.

iv. Wählen Sie Save (Speichern) aus.

c. Verwaltung der automatisierten Agentenkonfiguration durch Einbeziehung einiger ECS Amazon-Cluster (Cluster-Ebene)

i. Fügen Sie einem ECS Amazon-Cluster, für den Sie alle Aufgaben einbeziehen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`

ii. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
```

```
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

4. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist eine neue Dienstbereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

GuardDuty Agent für eine Umgebung mit mehreren Konten konfigurieren

In einer Umgebung mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto die automatische Agentenkonfiguration für die Mitgliedskonten aktivieren oder deaktivieren und die automatische Agentenkonfiguration für ECS Amazon-Cluster verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Ein GuardDuty Mitgliedskonto kann diese Konfiguration nicht ändern.

Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten in. GuardDuty

Aktivierung der automatisierten Agentenkonfiguration für ein delegiertes Administratorkonto GuardDuty

Manage for all Amazon ECS clusters (account level)

Wenn Sie für Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben, stehen Ihnen die folgenden Optionen zur Verfügung:

- Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty wird den Sicherheitsagenten für alle ECS Amazon-Aufgaben bereitstellen und verwalten, die gestartet werden.
- Wählen Sie Konten manuell konfigurieren.

Wenn Sie im Bereich Runtime Monitoring die Option Konten manuell konfigurieren ausgewählt haben, gehen Sie wie folgt vor:

1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Konten manuell konfigurieren aus.
2. Wählen Sie im Abschnitt Delegiertes GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.

Wählen Sie Save (Speichern) aus.

Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist eine neue Dienstbereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

- Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
- UpdateServicein der Amazon Elastic Container Service API Reference.

- update-service in der AWS CLI Befehlsreferenz.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem ECS Amazon-Cluster ein Tag mit dem Schlüssel-Wert-Paar als `GuardDutyManaged` - hinzu. `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
```

```
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.
> **Note**
>
> Fügen Sie Ihren ECS Amazon-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den ECS Amazon-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Registerkarte Konfiguration in der automatisierten Agentenkonfiguration die Option Aktivieren aus.

   Verwaltet für die ECS Amazon-Cluster, die nicht ausgeschlossen wurden, GuardDuty die Bereitstellung des Security Agents im Sidecar-Container.
6. Wählen Sie Save (Speichern) aus.
7. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist nach der Aktivierung von Runtime Monitoring eine neue Servicebereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Fügen Sie einem ECS Amazon-Cluster, für den Sie alle Aufgaben einbeziehen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged true`
2. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
```

```
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inclusion-Tags für Ihre ECS Amazon-Cluster verwenden, müssen Sie den GuardDuty Agenten nicht explizit über die automatische Agentenkonfiguration aktivieren.

3. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Services sind, ist nach der Aktivierung von Runtime Monitoring eine neue Servicebereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

- Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
- UpdateServicein der Amazon Elastic Container Service API Reference.
- update-service in der AWS CLI Befehlsreferenz.

Automatische Aktivierung für alle Mitgliedskonten

Manage for all Amazon ECS clusters (account level)

Bei den folgenden Schritten wird davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben.

1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty wird den Sicherheitsagenten für alle ECS Amazon-Aufgaben bereitstellen und verwalten, die gestartet werden.
2. Wählen Sie Save (Speichern) aus.
3. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Services sind, ist nach der Aktivierung von Runtime Monitoring ein neuer Service erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem ECS Amazon-Cluster ein Tag mit dem Schlüssel-Wert-Paar als `GuardDutyManaged` - hinzu. `false`

2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren ECS Amazon-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird

der GuardDuty Sidecar-Container an alle Container in den ECS Amazon-Aufgaben angehängt, die gestartet werden.

Wählen Sie auf der Registerkarte Konfiguration die Option Bearbeiten aus.

6. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus

   Verwaltet für die ECS Amazon-Cluster, die nicht ausgeschlossen wurden, GuardDuty die Bereitstellung des Security Agents im Sidecar-Container.
7. Wählen Sie Save (Speichern) aus.
8. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist nach der Aktivierung von Runtime Monitoring eine neue Servicebereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Unabhängig davon, wie Sie Runtime Monitoring aktivieren, helfen Ihnen die folgenden Schritte dabei, ausgewählte Amazon ECS Fargate-Aufgaben für alle Mitgliedskonten in Ihrer Organisation zu überwachen.

1. Aktivieren Sie im Abschnitt Automatisierte Agentenkonfiguration keine Konfiguration. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt ausgewählt haben.
2. Wählen Sie Save (Speichern) aus.
3. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte

Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inclusion-Tags für Ihre ECS Amazon-Cluster verwenden, müssen Sie die automatische Verwaltung der GuardDuty Agenten nicht explizit aktivieren.

4. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist nach der Aktivierung von Runtime Monitoring eine neue Servicebereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime

Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

- Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
- UpdateServicein der Amazon Elastic Container Service API Reference.
- update-service in der AWS CLI Befehlsreferenz.

Aktivierung der automatisierten Agentenkonfiguration für bestehende aktive Mitgliedskonten

Manage for all Amazon ECS clusters (account level)

1. Auf der Seite Runtime Monitoring können Sie auf der Registerkarte Konfiguration den aktuellen Status der automatisierten Agentenkonfiguration einsehen.
2. Wählen Sie im Bereich Automatisierte Agentenkonfiguration im Abschnitt Aktive Mitgliedskonten die Option Aktionen aus.
3. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
4. Wählen Sie Bestätigen aus.
5. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist eine neue Dienstbereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem ECS Amazon-Cluster ein Tag mit dem Schlüssel-Wert-Paar als `GuardDutyManaged` - hinzu. `false`

2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren ECS Amazon-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird

der GuardDuty Sidecar-Container an alle Container in den ECS Amazon-Aufgaben angehängt, die gestartet werden.

Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Automatisierte Agentenkonfiguration unter Aktive Mitgliedskonten die Option Aktionen aus.

6. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.

   Verwaltet für die ECS Amazon-Cluster, die nicht ausgeschlossen wurden, GuardDuty die Bereitstellung des Security Agents im Sidecar-Container.

7. Wählen Sie Bestätigen aus.
8. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist nach der Aktivierung von Runtime Monitoring eine neue Servicebereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Fügen Sie einem ECS Amazon-Cluster, für den Sie alle Aufgaben einbeziehen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged true`
2. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
```

```
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inclusion-Tags für Ihre ECS Amazon-Cluster verwenden, müssen Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

3. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

Automatische Aktivierung der automatischen Agentenkonfiguration für neue Mitglieder

Manage for all Amazon ECS clusters (account level)

1. Wählen Sie auf der Seite Runtime Monitoring die Option Bearbeiten aus, um die bestehende Konfiguration zu aktualisieren.
2. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren aus.
3. Wählen Sie Save (Speichern) aus.
4. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist eine neue Dienstbereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem ECS Amazon-Cluster ein Tag mit dem Schlüssel-Wert-Paar als `GuardDutyManaged` - hinzu. `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
```

```
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
```

```
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren ECS Amazon-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den ECS Amazon-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren aus.

   Verwaltet für die ECS Amazon-Cluster, die nicht ausgeschlossen wurden, GuardDuty die Bereitstellung des Security Agents im Sidecar-Container.
6. Wählen Sie Save (Speichern) aus.
7. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist nach der Aktivierung von Runtime Monitoring eine neue Servicebereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime

Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

- Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
- UpdateServicein der Amazon Elastic Container Service API Reference.
- update-service in der AWS CLI Befehlsreferenz.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Fügen Sie einem ECS Amazon-Cluster, für den Sie alle Aufgaben einbeziehen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`
2. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
```

```
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inclusion-Tags für Ihre ECS Amazon-Cluster verwenden, müssen Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

3. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

Selektives Aktivieren der automatisierten Agentenkonfiguration für aktive Mitgliedskonten

Manage for all Amazon ECS (account level)

1. Wählen Sie auf der Seite Konten die Konten aus, für die Sie die automatische Agentenkonfiguration von Runtime Monitoring (ECS-Fargate) aktivieren möchten. Sie können mehrere Konten auswählen. Stellen Sie sicher, dass die Konten, die Sie in diesem Schritt auswählen, bereits für Runtime Monitoring aktiviert sind.
2. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um Runtime Monitoring-Automated Agent-Konfiguration (ECS-Fargate) zu aktivieren.
3. Wählen Sie Bestätigen aus.

4. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist nach der Aktivierung von Runtime Monitoring eine neue Dienstbereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Fügen Sie diesem ECS Amazon-Cluster ein Tag mit dem Schlüssel-Wert-Paar als `GuardDutyManaged` - hinzu. `false`
2. Verhindern Sie die Änderung von Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
5.

> **Note**
>
> Fügen Sie Ihren ECS Amazon-Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Sidecar-Container an alle Container in den ECS Amazon-Aufgaben angehängt, die gestartet werden.

   Wählen Sie auf der Seite Konten die Konten aus, für die Sie die automatische Agentenkonfiguration von Runtime Monitoring (ECS-Fargate) aktivieren möchten. Sie können mehrere Konten auswählen. Stellen Sie sicher, dass die Konten, die Sie in diesem Schritt auswählen, bereits für Runtime Monitoring aktiviert sind.

   Verwaltet für die ECS Amazon-Cluster, die nicht ausgeschlossen wurden, GuardDuty die Bereitstellung des Security Agents im Sidecar-Container.
6. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um Runtime Monitoring-Automated Agent-Konfiguration (ECS-Fargate) zu aktivieren.
7. Wählen Sie Save (Speichern) aus.
8. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Dienstes sind, ist nach der Aktivierung von Runtime Monitoring eine neue Dienstbereitstellung erforderlich. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

- Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
- UpdateServicein der Amazon Elastic Container Service API Reference.
- update-service in der AWS CLI Befehlsreferenz.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Stellen Sie sicher, dass Sie die automatische Agentenkonfiguration (oder Runtime Monitoring-Automated Agent-Konfiguration (ECS-Fargate)) nicht für die ausgewählten Konten aktivieren, die die ECS Amazon-Cluster haben, die Sie überwachen möchten.
2. Fügen Sie einem ECS Amazon-Cluster, für den Sie alle Aufgaben einbeziehen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar muss - sein. `GuardDutyManaged` `true`
3. Verhindern Sie die Änderung dieser Tags, außer durch vertrauenswürdige Entitäten. Die im AWS Organizations Benutzerhandbuch unter Verhindern, dass Tags nicht durch autorisierte Prinzipien geändert werden, beschriebene Richtlinie wurde dahingehend geändert, dass sie hier gilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
```

```
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
```

```
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Inclusion-Tags für Ihre ECS Amazon-Cluster verwenden, müssen Sie die automatische Agentenkonfiguration nicht explizit aktivieren.

4. Wenn Sie Aufgaben überwachen GuardDuty möchten, die Teil eines Service sind, ist eine neue Servicebereitstellung erforderlich, nachdem Sie Runtime Monitoring aktiviert haben. Wenn die letzte Bereitstellung für einen bestimmten ECS Dienst gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben, können Sie den Dienst entweder neu starten oder den Dienst aktualisieren, indem Sie`forceNewDeployment`.

   Schritte zum Aktualisieren des Dienstes finden Sie in den folgenden Ressourcen:

   - Aktualisierung eines ECS Amazon-Service mithilfe der Konsole im Amazon Elastic Container Service Developer Guide.
   - UpdateServicein der Amazon Elastic Container Service API Reference.
   - update-service in der AWS CLI Befehlsreferenz.

Automatisches Verwalten des Security Agents für EKS Amazon-Cluster

Konfiguration eines automatisierten Agenten für ein eigenständiges Konto

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Runtime Monitoring aus.
3. Wählen Sie auf der Registerkarte Konfiguration die Option Aktivieren aus, um die automatische Agentenkonfiguration für Ihr Konto zu aktivieren.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS Cluster)	1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Aktivieren aus. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle vorhandenen und potenziell neuen EKS Cluster in Ihrem Konto. 2. Wählen Sie Save (Speichern) aus.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS Cluster von der Überwachung auszuschl ießen, obwohl der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzer handbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* `miteks:TagRe source` . • Ersetzen *`ec2:DeleteTags`* `miteks:Untag Resource` . • Ersetzen *`access-project`* mit `GuardDuty Managed` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/. 4. Wählen Sie im Navigationsbereich Runtime Monitoring aus. **Note** Fügen Sie Ihren EKS Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert. 5. Wählen Sie auf der Registerkarte Konfiguration im Bereich GuardDuty Agentenverwaltung die Option Aktivieren aus. Verwaltet für die EKS Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty die Verteilung und die Updates des GuardDuty Security Agents. 6. Wählen Sie Save (Speichern) aus.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
	Um einen EKS Cluster von der Überwachung auszuschl ießen, nachdem der GuardDuty Security Agent bereits auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzer handbuch. Nach diesem Schritt GuardDuty wird der Security Agent für diesen Cluster nicht aktualisiert. Der Security Agent bleibt jedoch installiert und empfängt GuardDuty weiterhin Runtime-Ereignisse von diesem EKS Cluster. Dies kann sich auf Ihre Nutzungss tatistiken auswirken. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* `miteks:TagResource` . • Ersetzen *`ec2:DeleteTags`* `miteks:UntagResource` .

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
	• Ersetzen *access-project* mit `GuardDuty Managed` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Um die Runtime-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Security Agent aus diesem EKS Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster mithilfe von Inclusion-Tags	1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Deaktivieren auswählen. Lassen Sie Runtime Monitoring aktiviert. 2. Wählen Sie Speichern. 3. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und seinem Wert als hinzu`true`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* `miteks:TagResource` . • Ersetzen *`ec2:DeleteTags`* `miteks:UntagResource` . • Ersetzen *`access-project`* mit `GuardDutyManaged` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz für die Installation des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den Agent manuell verwalten	1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Deaktivieren auswählen. Lassen Sie Runtime Monitoring aktiviert. 2. Wählen Sie Save (Speichern) aus. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Konfiguration eines automatisierten Agenten für Umgebungen mit mehreren Konten

In Umgebungen mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto die automatische Agentenkonfiguration für die Mitgliedskonten aktivieren oder deaktivieren und den automatisierten Agenten für die EKS Cluster verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten.

Konfiguration der automatisierten Agentenkonfiguration für das delegierte Administratorkonto GuardDuty

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS Cluster)	Wenn Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben, stehen Ihnen die folgenden Optionen zur Verfügung: • Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty verteilt und verwaltet den Security Agent für alle EKS Cluster, die zum delegierten GuardDuty Administratorkonto gehören, sowie für alle EKS Cluster, die zu allen bestehenden und potenziell neuen Mitgliedskonten in der Organisation gehören. • Wählen Sie Konten manuell konfigurieren. Wenn Sie im Bereich Runtime Monitoring die Option Konten manuell konfigurieren ausgewählt haben, gehen Sie wie folgt vor: 1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Konten manuell konfigurieren aus. 2. Wählen Sie im Abschnitt Delegiertes GuardDuty Administr atorkonto (dieses Konto) die Option Aktivieren aus. Wählen Sie Save (Speichern) aus.
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe von Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Um einen EKS Cluster von der Überwachung auszuschließen, obwohl der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Cl usters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* mit `eks:TagResource` . • Ersetzen *`ec2:DeleteTags`* mit `eks:UntagResource` . • Ersetzen *`access-project`* mit `GuardDutyManaged` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/. 4. Wählen Sie im Navigationsbereich Runtime Monitoring aus. **Note** Fügen Sie Ihren EKS Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische GuardDuty Agentenverwaltung für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert. 5. Wählen Sie auf der Registerkarte Konfiguration im Bereich GuardDuty Agentenverwaltung die Option Aktivieren aus. Verwaltet für die EKS Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty die Verteilung und die Updates des GuardDuty Security Agents. 6. Wählen Sie Save (Speichern) aus. Um einen EKS Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit `eks:TagResource`. • Ersetzen *ec2:DeleteTags* mit `eks:UntagResource`. • Ersetzen *access-project* mit `GuardDutyManaged` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Wenn Sie den Automated Agent für diesen EKS Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisiert. Der Security Agent bleibt jedoch installiert und empfängt GuardDuty weiterhin Runtime-Ereignisse von diesem EKS Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Runtime-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Security Agent aus diesem EKS Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	4. Wenn Sie den GuardDuty Security Agent für diesen EKS Cluster manuell verwaltet haben, finden Sie weitere Informationen unterAuswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster mithilfe von Inclusion-Tags	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, helfen Ihnen die folgenden Schritte bei der Überwachung EKS ausgewählter Cluster in Ihrem Konto: 1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für delegiertes GuardDuty Administratorkonto (dieses Konto) deaktivieren auswählen. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt konfiguriert haben. 2. Wählen Sie Save (Speichern) aus. 3. Fügen Sie Ihrem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und seinem Wert als hinzu`true`. Weitere Informationen zum Taggen Ihres EKS Amazon-Cl usters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit `eks:TagResource` . • Ersetzen *ec2:DeleteTags* mit `eks:UntagResource` . • Ersetzen *access-project* mit `GuardDutyManaged` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den GuardDuty Security Agent manuell verwalten	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, können Sie den Security Agent für Ihre EKS Cluster manuell verwalten. 1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für delegiertes GuardDuty Administratorkonto (dieses Konto) deaktivieren auswählen. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt konfiguriert haben. 2. Wählen Sie Save (Speichern) aus. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Automatischer Agent für alle Mitgliedskonten automatisch aktivieren

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS Cluster)	In diesem Thema geht es darum, Runtime Monitoring für alle Mitgliedskonten zu aktivieren. Daher wird bei den folgenden Schritten davon ausgegangen, dass Sie im Abschnitt Runtime Monitoring die Option Für alle Konten aktivieren ausgewählt haben. 1. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. GuardDuty verteilt und verwaltet den Security Agent für alle EKS Cluster, die zum delegierten GuardDuty Administratorkonto gehören, sowie für alle EKS Cluster, die zu allen bestehenden und potenziell neuen Mitgliedskonten in der Organisation gehören. 2. Wählen Sie Save (Speichern) aus.
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe von Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS Cluster von der Überwachung auszuschließen, obwohl der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Cl usters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

- Ersetzen *ec2:CreateTags* miteks:TagResource .
- Ersetzen *ec2:DeleteTags* miteks:UntagResource .
- Ersetzen *access-project* mit GuardDutyManaged
- Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität.

  Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere PrincipalArn hinzuzufügen:

```
"aws:PrincipalArn":["arn:aws:iam::12345678901
2:role/org-admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/iam-admin"]
```

3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
4. Wählen Sie im Navigationsbereich Runtime Monitoring aus.

> **Note**
>
> Fügen Sie Ihren EKS Clustern immer das Ausschluss-Tag hinzu, bevor Sie Automated Agent für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert.

5. Wählen Sie auf der Registerkarte Konfiguration im Abschnitt Runtime Monitoring-Konfiguration die Option Bearbeiten aus.
6. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Für alle Konten aktivieren aus. Verwaltet für die EKS Cluster, die nicht von der Überwachung ausgeschlossen wurden,

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	GuardDuty die Verteilung und die Updates des GuardDuty Security Agents. 7. Wählen Sie Save (Speichern) aus. Um einen EKS Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Cl usters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. 2. Wenn Sie die automatische Agentenkonfiguration für diesen EKS Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisiert. Der Security Agent bleibt jedoch installiert und empfängt GuardDuty weiterhin Runtime-Ereignisse von diesem EKS Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Runtime-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Security Agent aus diesem EKS Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen 3. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen *ec2:CreateTags* miteks:TagResource . • Ersetzen *ec2:DeleteTags* miteks:UntagResource . • Ersetzen *access-project* mit GuardDutyManaged • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere PrincipalArn hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 4. Wenn Sie den GuardDuty Security Agent für diesen EKS Cluster manuell verwaltet haben, finden Sie weitere Informationen unterAuswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster mithilfe von Inclusion-Tags	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, helfen Ihnen die folgenden Schritte dabei, selektive EKS Cluster für alle Mitgliedskonten in Ihrer Organisation zu überwachen: 1. Aktivieren Sie im Abschnitt Automatisierte Agentenkonfiguration keine Konfiguration. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt konfiguriert haben. 2. Wählen Sie Save (Speichern) aus. 3. Fügen Sie Ihrem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und seinem Wert als hinzu`true`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* mit `eks:TagResource` . • Ersetzen *`ec2:DeleteTags`* mit `eks:UntagResource` . • Ersetzen *`access-project`* mit `GuardDutyManaged` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den GuardDuty Security Agent manuell verwalten	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, können Sie den Security Agent für Ihre EKS Cluster manuell verwalten. 1. Aktivieren Sie im Abschnitt Automatisierte Agentenkonfiguration keine Konfiguration. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt konfiguriert haben. 2. Wählen Sie Save (Speichern) aus. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Aktivierung des automatisierten Agenten für alle vorhandenen aktiven Mitgliedskonten

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Um den GuardDuty Security Agent für bestehende aktive Mitgliedskonten in Ihrem Unternehmen zu verwalten

- GuardDuty Um Runtime-Ereignisse von den EKS Clustern zu empfangen, die zu den bestehenden aktiven Mitgliedskonten in der Organisation gehören, müssen Sie einen bevorzugten Ansatz für die Verwaltung des GuardDuty Security Agents für diese EKS Cluster wählen. Weitere Informationen zu diesen Ansätzen finden Sie unter Methoden zur Verwaltung des GuardDuty Security Agents.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS Cluster)	Um alle EKS Cluster für alle vorhandenen aktiven Mitgliedskonten zu überwachen 1. Auf der Seite Runtime Monitoring können Sie auf der Registerkarte Konfiguration den aktuellen Status der automatisierten Agentenkonfiguration einsehen. 2. Wählen Sie im Bereich Automatisierte Agentenkonfiguration im Abschnitt Aktive Mitgliedskonten die Option Aktionen aus. 3. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten. 4. Wählen Sie Bestätigen aus.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe des Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS Cluster von der Überwachung auszuschl ießen, obwohl der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzer handbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* `miteks:TagRe source` . • Ersetzen *`ec2:DeleteTags`* `miteks:Untag Resource` . • Ersetzen *`access-project`* mit `GuardDuty Managed` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/. 4. Wählen Sie im Navigationsbereich Runtime Monitoring aus. **Note** Fügen Sie Ihren EKS Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert. 5. Wählen Sie auf der Registerkarte Konfiguration im Bereich Automatisierte Agentenkonfiguration unter Aktive Mitgliedskonten die Option Aktionen aus. 6. Wählen Sie bei Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten. 7. Wählen Sie Bestätigen aus.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Um einen EKS Cluster von der Überwachung auszuschl ießen, nachdem der GuardDuty Security Agent bereits auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzer handbuch. Nach diesem Schritt GuardDuty wird der Security Agent für diesen Cluster nicht aktualisiert. Der Security Agent bleibt jedoch installiert und empfängt GuardDuty weiterhin Runtime-Ereignisse von diesem EKS Cluster. Dies kann sich auf Ihre Nutzungss tatistiken auswirken. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* `miteks:TagRe source` . • Ersetzen *`ec2:DeleteTags`* `miteks:Untag Resource` .

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen *access-project* mit `GuardDuty Managed` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Unabhängig davon, wie Sie den Security Agent verwalten (über GuardDuty oder manuell), müssen Sie den installierten Security Agent aus diesem Cluster entfernen, um den Empfang von Runtime-Ereignissen von diesem EKS Cluster zu beenden. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster mithilfe von Inclusion-Tags	1. Aktivieren Sie auf der Seite „Konten“ die Option Runtime Monitoring — Automatisierte Agentenkonfiguration nicht, nachdem Sie Runtime Monitoring aktiviert haben. 2. Fügen Sie dem EKS Cluster ein Tag hinzu, das zu dem ausgewählten Konto gehört, das Sie überwachen möchten. Das Schlüssel-Wert-Paar des Tags muss `GuardDutyManaged -true` sein. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS Cluster, die Sie überwachen möchten. 3. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit `eks:TagResource` . • Ersetzen *ec2:DeleteTags* mit `eks:UntagResource` . • Ersetzen *access-project* mit `GuardDutyManaged`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den GuardDuty Security Agent manuell verwalten	1. Stellen Sie sicher, dass Sie im Abschnitt Automatisierte Agentenkonfiguration nicht die Option Aktivieren auswählen. Lassen Sie Runtime Monitoring aktiviert. 2. Wählen Sie Save (Speichern) aus. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Automatische Aktivierung der automatischen Agentenkonfiguration für neue Mitglieder

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS Cluster)	1. Wählen Sie auf der Seite Runtime Monitoring die Option Bearbeiten aus, um die bestehende Konfiguration zu aktualisieren. 2. Wählen Sie im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren aus.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. Wählen Sie Save (Speichern) aus.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe von Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS Cluster von der Überwachung auszuschließen, obwohl der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* mit `eks:TagResource`. • Ersetzen *`ec2:DeleteTags`* mit `eks:UntagResource`. • Ersetzen *`access-project`* mit `GuardDutyManaged` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	<pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> 3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/. 4. Wählen Sie im Navigationsbereich Runtime Monitoring aus. **Note** Fügen Sie Ihren EKS Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert. 5. Wählen Sie auf der Registerkarte Konfiguration im Bereich GuardDuty Agentenverwaltung die Option Automatisch für neue Mitgliedskonten aktivieren aus. Verwaltet für die EKS Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty die Verteilung und die Updates des GuardDuty Security Agents. 6. Wählen Sie Save (Speichern) aus.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Um einen EKS Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster installiert wurde 1. Unabhängig davon, ob Sie den GuardDuty Security Agent über GuardDuty oder manuell verwalten, fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. Wenn Sie Automated Agent für diesen EKS Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisiert. Der Security Agent bleibt jedoch installiert und empfängt GuardDuty weiterhin Runtime-Ereignisse von diesem EKS Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Runtime-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Security Agent aus diesem EKS Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben:

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen *ec2:CreateTags* mit `eks:TagResource`. • Ersetzen *ec2:DeleteTags* mit `eks:UntagResource`. • Ersetzen *access-project* mit `GuardDutyManaged` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Wenn Sie den GuardDuty Security Agent für diesen EKS Cluster manuell verwaltet haben, finden Sie weitere Informationen unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster mithilfe von Inclusion-Tags	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, helfen Ihnen die folgenden Schritte dabei, ausgewählte EKS Cluster auf die neuen Mitgliedskonten in Ihrer Organisation zu überwachen. 1. Stellen Sie sicher, dass im Abschnitt Automatisierte Agentenkonfiguration die Option Automatisch für neue Mitgliedskonten aktivieren deaktiviert ist. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt konfiguriert haben. 2. Wählen Sie Save (Speichern) aus. 3. Fügen Sie Ihrem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und seinem Wert als hinzu`true`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS Cluster, die Sie überwachen möchten. 4. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* miteks:TagResource . • Ersetzen *ec2:DeleteTags* miteks:UntagResource .

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen *access-project* mit GuardDuty Managed • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere PrincipalArn hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den GuardDuty Security Agent manuell verwalten	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, können Sie den Security Agent für Ihre EKS Cluster manuell verwalten. 1. Stellen Sie sicher, dass das Kontrollkästchen Automatisch für neue Mitgliedskonten aktivieren im Abschnitt Automatische Agentenkonfiguration deaktiviert ist. Behalten Sie die Runtime Monitoring-Konfiguration bei, die Sie im vorherigen Schritt konfiguriert haben. 2. Wählen Sie Save (Speichern) aus. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Selektives Konfigurieren des automatisierten Agenten für aktive Mitgliedskonten

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Verwalten Sie den Security Agent über GuardDuty (Überwachen Sie alle EKS Cluster)	1. Wählen Sie auf der Seite Konten die Konten aus, für die Sie die automatische Agentenkonfiguration aktivieren möchten. Sie können mehr als ein Konto zur gleichen Zeit auswählen. Stellen Sie sicher, dass EKS Runtime Monitoring für die Konten, die Sie in diesem Schritt auswählen, bereits aktiviert ist. 2. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um Runtime Monitoring — Automatisierte Agentenkonfiguration zu aktivieren. 3. Wählen Sie Bestätigen aus.
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe von Ausschluss-Tags)	Wählen Sie aus den folgenden Verfahren eines der Szenarien aus, das auf Sie zutrifft. Um einen EKS Cluster von der Überwachung auszuschließen, obwohl der GuardDuty Security Agent nicht auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* `miteks:TagResource` .

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	• Ersetzen *ec2:DeleteTags* miteks:UntagResource . • Ersetzen *access-project* mit GuardDutyManaged • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere PrincipalArn hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/. **Note** Fügen Sie Ihren EKS Clustern immer das Ausschluss-Tag hinzu, bevor Sie die automatische Agentenkonfiguration für Ihr Konto aktivieren. Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert. 4. Wählen Sie auf der Kontenseite das Konto aus, für das Sie Agent automatisch verwalten aktivieren möchten. Sie können mehr als ein Konto zur gleichen Zeit auswählen. 5. Wählen Sie unter Schutzpläne bearbeiten die entsprechende Option aus, um die automatische Agentenkonfiguration mit Runtime Monitoring für das ausgewählte Konto zu aktivieren.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Verwaltet für die EKS Cluster, die nicht von der Überwachung ausgeschlossen wurden, GuardDuty die Verteilung des Security Agents und die GuardDuty Updates für ihn. 6. Wählen Sie Save (Speichern) aus. Um einen EKS Cluster von der Überwachung auszuschließen, wenn der GuardDuty Security Agent auf diesem Cluster installiert wurde 1. Fügen Sie diesem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und dem Wert as hinzu`false`. Weitere Informationen zum Taggen Ihres EKS Amazon-Cl usters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. Wenn Sie zuvor die automatische Agentenkonfiguration für diesen EKS Cluster aktiviert hatten, GuardDuty wird der Security Agent für diesen Cluster nach diesem Schritt nicht aktualisi ert. Der Security Agent bleibt jedoch installiert und empfängt GuardDuty weiterhin die Runtime-Ereignisse von diesem EKS Cluster. Dies kann sich auf Ihre Nutzungsstatistiken auswirken. Um die Runtime-Ereignisse von diesem Cluster nicht mehr zu empfangen, müssen Sie den bereitgestellten Security Agent aus diesem EKS Cluster entfernen. Weitere Informationen zum Entfernen des bereitgestellten Sicherheitsagenten finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit `eks:TagResource`. • Ersetzen *ec2:DeleteTags* mit `eks:UntagResource`. • Ersetzen *access-project* mit `GuardDutyManaged` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Wenn Sie den GuardDuty Security Agent für diesen EKS Cluster manuell verwaltet haben, müssen Sie ihn entfernen. Weitere Informationen finden Sie unter Auswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster mithilfe von Inclusion-Tags	Unabhängig davon, wie Sie Runtime Monitoring aktiviert haben, helfen Ihnen die folgenden Schritte bei der Überwachung ausgewählter EKS Cluster, die zu den ausgewählten Konten gehören: 1. Stellen Sie sicher, dass Sie die automatische Agentenkonfiguration mit Runtime Monitoring nicht für die ausgewählten Konten aktivieren, die über die EKS Cluster verfügen, die Sie überwachen möchten. 2. Fügen Sie Ihrem EKS Cluster ein Tag mit dem Schlüssel as `GuardDutyManaged` und seinem Wert als hinzu. `true` Weitere Informationen zum Taggen Ihres EKS Amazon-Clusters finden Sie unter Arbeiten mit Tags mithilfe der Konsole im EKSAmazon-Benutzerhandbuch. Nach dem Hinzufügen des Tags verwaltet er die Bereitstellung und Aktualisierung des Security Agents für die ausgewählten EKS Cluster, die Sie überwachen möchten. GuardDuty 3. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* miteks:TagResource . • Ersetzen *ec2:DeleteTags* miteks:UntagResource . • Ersetzen *access-project* mit GuardDutyManaged • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Den GuardDuty Security Agent manuell verwalten	1. Behalten Sie für die Runtime Monitoring-Konfiguration dieselbe wie im vorherigen Schritt bei. Stellen Sie sicher, dass Sie für keines der ausgewählten Konten die automatische Agentenkonfiguration von Runtime Monitoring aktivieren. 2. Wählen Sie Bestätigen aus. 3. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Manuelles Verwalten des Security Agents für EKS Amazon-Cluster

In diesem Abschnitt wird beschrieben, wie Sie Ihren EKS Amazon-Zusatz-Agenten (GuardDuty Agenten) verwalten können, nachdem Sie Runtime Monitoring aktiviert haben. Um Runtime Monitoring verwenden zu können, müssen Sie Runtime Monitoring aktivieren und das EKS Amazon-Add-on konfigurieren`aws-guardduty-agent`. Wenn Sie nur einen dieser beiden Schritte ausführen, können Sie potenzielle Bedrohungen nicht GuardDuty erkennen oder Ergebnisse generieren.

Voraussetzungen für die Installation des GuardDuty Security Agents

In diesem Abschnitt werden die Voraussetzungen für die manuelle Installation des GuardDuty Security Agents für Ihre EKS Cluster beschrieben. Bevor Sie fortfahren, stellen Sie sicher, dass Sie Runtime Monitoring bereits für Ihre Konten konfiguriert haben. Der GuardDuty Security Agent (EKSAdd-on) funktioniert nicht, wenn Sie Runtime Monitoring nicht konfigurieren. Weitere

Informationen finden Sie unter GuardDuty Runtime Monitoring aktivieren. Nachdem Sie diese Schritte abgeschlossen haben, sehen Sie Der Security Agent wird bereitgestellt GuardDuty .

Wählen Sie Ihre bevorzugte Zugriffsmethode, um einen VPC Amazon-Endpunkt zu erstellen.

Console

VPCEndpunkt erstellen

1. Öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsmenü unter Virtual Private Cloud die Option Endpunkte.
3. Klicken Sie auf Endpunkt erstellen.
4. Wählen Sie auf der Seite Endpunkt erstellen für Servicekategorie die Option Andere Endpunkt-Services.
5. Geben Sie unter Servicename **`com.amazonaws.`*`us-east-1`*`.guardduty-data`** ein.

   Stellen Sie sicher, dass Sie es austauschen *`us-east-1`* mit der richtigen Region. Dies muss dieselbe Region sein wie der EKS Cluster, der zu Ihrer AWS-Konto ID gehört.
6. Wählen Sie Service verifizieren.
7. Nachdem der Dienstname erfolgreich verifiziert wurde, wählen Sie den VPCOrt aus, an dem sich Ihr Cluster befindet. Fügen Sie die folgende Richtlinie hinzu, um die VPC Endpunktnutzung nur auf das angegebene Konto zu beschränken. Unter Angabe der unter dieser Richtlinie angegebenen Organisations-`Condition` können Sie die folgende Richtlinie aktualisieren, um den Zugriff auf Ihren Endpunkt einzuschränken. Informationen zur Bereitstellung von VPC Endpunktunterstützung für ein bestimmtes Konto IDs in Ihrer Organisation finden Sie unterOrganization condition to restrict access to your endpoint.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
```

```
      "aws:PrincipalAccount": "111122223333"
     }
    },
    "Action": "*",
    "Resource": "*",
    "Effect": "Deny",
    "Principal": "*"
   }
  ]
}
```

Die `aws:PrincipalAccount` Konto-ID muss mit dem Konto übereinstimmen, das den VPC Endpunkt VPC und enthält. Die folgende Liste zeigt, wie Sie den VPC Endpunkt mit anderen teilen können AWS-Konto IDs:

Organisationsbedingung , um den Zugriff auf Ihren Endpunkt einzuschränken

- Wenn Sie mehrere Konten für den Zugriff auf den VPC Endpunkt angeben möchten, `"aws:PrincipalAccount": "111122223333"` ersetzen Sie ihn durch Folgendes:

  ```
  "aws:PrincipalAccount": [
            "666666666666",
            "555555555555"
      ]
  ```

- Um allen Mitgliedern einer Organisation den Zugriff auf den VPC Endpunkt zu ermöglichen, `"aws:PrincipalAccount": "111122223333"` ersetzen Sie ihn durch folgenden Wortlaut:

  ```
  "aws:PrincipalOrgID": "o-abcdef0123"
  ```

- Um den Zugriff auf eine Ressource auf eine Organisations-ID zu beschränken, fügen Sie Ihre `ResourceOrgID` zur Richtlinie hinzu.

  Weitere Informationen finden Sie unter ResourceOrgID.

  ```
  "aws:ResourceOrgID": "o-abcdef0123"
  ```

8. Wählen Sie unter Zusätzliche Einstellungen die Option DNSNamen aktivieren aus.
9. Wählen Sie unter Subnetze die Subnetze aus, in denen sich Ihr Cluster befindet.

10. Wählen Sie unter Sicherheitsgruppen eine Sicherheitsgruppe aus, für die der eingehende Port 443 von Ihrem VPC (oder Ihrem EKS Cluster) aus aktiviert ist. Wenn Sie noch keine Sicherheitsgruppe haben, für die der eingehende Port 443 aktiviert ist, Erstellen Sie eine Sicherheitsgruppe.

    Wenn bei der Beschränkung der eingehenden Zugriffsberechtigungen für Sie VPC (oder Ihren Cluster) ein Problem auftritt, stellen Sie die Unterstützung für den eingehenden Port 443 von einer beliebigen IP-Adresse () bereit. `0.0.0.0/0`

API/CLI

- CreateVpcEndpointAufrufen.
- Verwenden Sie die folgenden Werte für die Parameter:
  - Geben Sie unter Servicename **`com.amazonaws.`*`us-east-1`*`.guardduty-data`** ein.

    Stellen Sie sicher, dass Sie es ersetzen *`us-east-1`* mit der richtigen Region. Dies muss dieselbe Region sein wie der EKS Cluster, der zu Ihrer AWS-Konto ID gehört.
  - Aktivieren Sie die private DNS Option für DNSOptions, indem Sie sie auf setzen`true`.
- AWS Command Line Interface Näheres dazu finden Sie unter create-vpc-endpoint.

Konfigurieren Sie die Parameter des GuardDuty Security Agents (Add-on) für Amazon EKS

Sie können spezifische Parameter Ihres GuardDuty Security Agents für Amazon konfigurierenEKS. Diese Unterstützung ist für GuardDuty Security Agent Version 1.5.0 und höher verfügbar. Informationen zu den neuesten Add-On-Versionen finden Sie unterGuardDuty Sicherheitsagent für EKS Amazon-Cluster.

Warum sollte ich das Security Agent Konfigurationsschema aktualisieren

Das Konfigurationsschema für den GuardDuty Security Agent ist für alle Container in Ihren EKS Amazon-Clustern dasselbe. Wenn die Standardwerte nicht mit den zugehörigen Workloads und der Instance-Größe übereinstimmen, sollten Sie die Konfiguration der CPU Einstellungen, Speichereinstellungen und `dnsPolicy` Einstellungen in Betracht ziehen. `PriorityClass` Unabhängig davon, wie Sie den GuardDuty Agenten für Ihre EKS Amazon-Cluster verwalten, können Sie die bestehende Konfiguration dieser Parameter konfigurieren oder aktualisieren.

Automatisiertes Verhalten der Agentenkonfiguration mit konfigurierten Parametern

Wenn der Security Agent (EKSAdd-on) in Ihrem Namen GuardDuty verwaltet wird, aktualisiert er das Add-on bei Bedarf. GuardDuty setzt den Wert der konfigurierbaren Parameter auf einen Standardwert. Sie können die Parameter jedoch immer noch auf einen gewünschten Wert aktualisieren. Wenn dies zu einem Konflikt führt, resolveConflictsist die Standardoption aufNone.

Konfigurierbare Parameter und Werte

Informationen zu den Schritten zur Konfiguration der Zusatzparameter finden Sie unter:

- Der Security Agent wird bereitgestellt GuardDuty oder
- Manuelles Aktualisieren des Security Agents

Die folgenden Tabellen enthalten die Bereiche und Werte, die Sie verwenden können, um das EKS Amazon-Add-on manuell bereitzustellen oder die vorhandenen Add-On-Einstellungen zu aktualisieren.

CPUEinstellungen

Parameter	Standardwert	Konfigurierbarer Bereich
Anforderungen	200m	Zwischen 200 m und 10000 m, beide inklusive
Einschränkungen	1000m	

Speicher-Einstellungen

Parameter	Standardwert	Konfigurierbarer Bereich
Anforderungen	256 Mi	Zwischen 256Mi und 20000Mi, beide inklusive
Einschränkungen	1024 Mi	

`PriorityClass`-Einstellungen

Wenn ein EKS Amazon-Add-on für Sie GuardDuty erstellt wird, `PriorityClass` ist das zugewieseneaws-guardduty-agent.priorityclass. Das bedeutet, dass aufgrund

der Priorität des Agenten-Pods keine Maßnahmen ergriffen werden. Sie können diesen Zusatzparameter konfigurieren, indem Sie eine der folgenden `PriorityClass` Optionen wählen:

Konfigurierbar **`PriorityClass`**	**`preemptionPolicy`** Wert	**`preemptionPolicy`** Beschreibung	Pod-Wert
`aws-guardduty-agent.priorityclass`	`Never`	Keine Aktion	1000000
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	Durch die Zuweisung dieses Werts wird verhindert, dass ein Pod ausgeführt wird, dessen Prioritätswert unter dem Pod-Wert des Agenten liegt.	100000000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2000000000
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] Kubernetes bietet diese beiden `PriorityClass` Optionen — und. `system-cluster-critical` `system-node-critical` Weitere Informationen finden Sie PriorityClassin der Kubernetes-Dokumentation.

`dnsPolicy`-Einstellungen

Wählen Sie eine der folgenden DNS Richtlinienoptionen, die Kubernetes unterstützt. Wird als Standardwert verwendet, wenn keine Konfiguration angegeben `ClusterFirst` ist.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Informationen zu diesen Richtlinien finden Sie unter Pods DNS Policy in der Kubernetes-Dokumentation.

Der Security Agent wird bereitgestellt GuardDuty

In diesem Abschnitt wird beschrieben, wie Sie den GuardDuty Security Agent zum ersten Mal für bestimmte EKS Cluster einsetzen können. Bevor Sie mit diesem Abschnitt fortfahren, stellen Sie sicher, dass Sie die Voraussetzungen bereits eingerichtet und Runtime Monitoring für Ihre Konten aktiviert haben. Der GuardDuty Security Agent (EKSAdd-on) funktioniert nicht, wenn Sie Runtime Monitoring nicht aktivieren.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty Security Agent zum ersten Mal zu installieren.

Console

1. Öffnen Sie die EKS Amazon-Konsole unter https://console.aws.amazon.com/eks/home#/clusters.
2. Wählen Sie Ihren Clusternamen aus.
3. Wählen Sie die Registerkarte Add-ons.
4. Wählen Sie Weitere Add-Ons erhalten.
5. Wählen Sie auf der Seite „Add-Ons auswählen“ Amazon GuardDuty Runtime Monitoring aus.
6. Verwenden Sie auf der Seite Ausgewählte Add-On-Einstellungen konfigurieren die Standardeinstellungen. Wenn der Status Ihres EKS Add-ons Aktivierung erfordert lautet, wählen Sie Aktivieren aus GuardDuty. Diese Aktion öffnet die GuardDuty Konsole, in der Sie Runtime Monitoring für Ihre Konten konfigurieren können.
7. Nachdem Sie Runtime Monitoring für Ihre Konten konfiguriert haben, kehren Sie zur EKS Amazon-Konsole zurück. Der Status Ihres EKS Add-ons sollte sich auf Bereit zur Installation geändert haben.
8. (Optional) Bereitstellung des EKS Add-On-Konfigurationsschemas

   Wenn Sie für die Add-On-Version Version v1.5.0 und höher wählen, unterstützt Runtime Monitoring die Konfiguration bestimmter GuardDuty Agentenparameter. Hinweise zu Parameterbereichen finden Sie unterKonfigurieren Sie die EKS Zusatzparameter.

   a. Erweitern Sie Optionale Konfigurationseinstellungen, um die konfigurierbaren Parameter sowie deren erwarteten Wert und Format anzuzeigen.

   b. Stellen Sie die Parameter ein. Die Werte müssen in dem unter angegebenen Bereich liegenKonfigurieren Sie die EKS Zusatzparameter.

c. Wählen Sie Änderungen speichern, um das Add-on auf der Grundlage der erweiterten Konfiguration zu erstellen.

d. Bei der Methode zur Konfliktlösung wird die von Ihnen gewählte Option verwendet, um einen Konflikt zu lösen, wenn Sie den Wert eines Parameters auf einen anderen Wert als den Standardwert aktualisieren. Weitere Informationen zu den aufgelisteten Optionen finden Sie resolveConflictsin der EKSAPIAmazon-Referenz.

9. Wählen Sie Weiter.
10. Überprüfen Sie auf der Seite Überprüfen und erstellen alle Details und wählen Sie dann Erstellen.
11. Gehen Sie zurück zu den Cluster-Details und wählen Sie die Registerkarte Ressourcen.
12. Sie können die neuen Pods mit dem Präfix anzeigen aws-guardduty-agent.

API/CLI

Sie können den EKS Amazon-Zusatz-Agenten (`aws-guardduty-agent`) mit einer der folgenden Optionen konfigurieren:

- CreateAddonFür Ihr Konto ausführen.
-

> **Note**
>
> Wenn Sie für das Add-on `version` Version 1.5.0 und höher wählen, unterstützt Runtime Monitoring die Konfiguration bestimmter GuardDuty Agentenparameter. Weitere Informationen finden Sie unter Konfigurieren Sie die EKS Zusatzparameter.

Verwenden Sie die folgenden Werte für die Parameter:

- Geben Sie unter `addonName` den Wert `aws-guardduty-agent` ein.

Sie können das folgende AWS CLI Beispiel verwenden, wenn Sie konfigurierbare Werte verwenden, die für die Addon-Versionen v1.5.0 und höher unterstützt werden. Achten Sie darauf, die rot markierten Platzhalterwerte und die `Example.json` mit den konfigurierten Werten verknüpften Werte zu ersetzen.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example example.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- Weitere Informationen zu unterstützten `addonVersion` finden Sie unter Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty .

- Alternativ können Sie verwenden. AWS CLI Weitere Informationen finden Sie unter create-addon.

Manuelles Aktualisieren des Security Agents

Wenn Sie den GuardDuty Security Agent manuell verwalten, sind Sie dafür verantwortlich, ihn für Ihr Konto zu aktualisieren. Um über neue Agent-Versionen informiert zu werden, können Sie einen RSS Feed abonnierenGuardDuty Versionsverlauf des Agenten.

Sie können den Security Agent auf die neueste Version aktualisieren, um von der zusätzlichen Unterstützung und den Verbesserungen zu profitieren. Wenn der Standardsupport für Ihre aktuelle Agent-Version ausläuft, müssen Sie Ihre aktuelle Agent-Version aktualisieren, um EKS Runtime Monitoring (oder Runtime Monitoring) weiterhin verwenden zu können. Informationen zu Release-Versionen finden Sie unterGuardDuty Sicherheitsagent für EKS Amazon-Cluster.

Voraussetzung

Bevor Sie die Security Agent-Version aktualisieren, stellen Sie sicher, dass die Agent-Version, die Sie jetzt verwenden möchten, mit Ihrer Kubernetes-Version kompatibel ist. Weitere Informationen finden Sie unter Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty .

Console

1. Öffnen Sie die EKS Amazon-Konsole unter https://console.aws.amazon.com/eks/home#/clusters.
2. Wählen Sie Ihren Clusternamen aus.
3. Wählen Sie Add-Ons.
4. Wählen Sie unter Add-Ons die Option GuardDutyRuntime Monitoring aus.
5. Wählen Sie Bearbeiten, um die Agentendetails zu aktualisieren.
6. Aktualisieren Sie auf der Seite GuardDuty Runtime Monitoring konfigurieren die Details.
7. (Optional) Aktualisierung der Konfigurationsparameter des Add-ons

   Wenn Ihre EKS Add-On-Version 1.5.0 oder höher ist, können Sie auch die Add-On-Konfigurationseinstellungen aktualisieren.

   a. Erweitern Sie Optionale Konfigurationseinstellungen, um das Konfigurationsschema anzuzeigen.

   b. Aktualisieren Sie die Parameterwerte basierend auf dem angegebenen Bereich unterKonfigurieren Sie die EKS Zusatzparameter.

   c. Wählen Sie Änderungen speichern, um das Update zu starten.

   d. Bei der Methode zur Konfliktlösung wird die von Ihnen gewählte Option verwendet, um einen Konflikt zu lösen, wenn Sie den Wert eines Parameters auf einen Wert aktualisieren, der nicht dem Standard entspricht. Weitere Informationen zu den aufgelisteten Optionen finden Sie resolveConflictsin der EKSAPIAmazon-Referenz.

API/CLI

Informationen zum Update des GuardDuty Security Agents für Ihre EKS Amazon-Cluster finden Sie unter Ein Add-on aktualisieren.

> **Note**
>
> Wenn Sie für das Add-on `version` Version 1.5.0 und höher wählen, unterstützt Runtime Monitoring die Konfiguration bestimmter GuardDuty Agentenparameter. Hinweise zu Parameterbereichen finden Sie unterKonfigurieren Sie die EKS Zusatzparameter.

Sie können das folgende AWS CLI Beispiel verwenden, wenn Sie konfigurierbare Werte verwenden, die für die Addon-Versionen v1.5.0 und höher unterstützt werden. Achten Sie darauf, die rot markierten Platzhalterwerte und die `Example.json` mit den konfigurierten Werten verknüpften Werte zu ersetzen.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example example.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Wenn Ihre EKS Amazon-Add-On-Version 1.5.0 oder höher ist und Sie das Add-On-Schema konfiguriert haben, können Sie überprüfen, ob die Werte für Ihren Cluster korrekt angezeigt werden. Weitere Informationen finden Sie unter Aktualisierungen des Konfigurationsschemas werden überprüft.

Aktualisierungen des Konfigurationsschemas werden überprüft

Nachdem Sie die Parameter konfiguriert haben, führen Sie die folgenden Schritte aus, um zu überprüfen, ob das Konfigurationsschema aktualisiert wurde:

1. Öffnen Sie die EKS Amazon-Konsole unter https://console.aws.amazon.com/eks/home#/clusters.
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Wählen Sie auf der Cluster-Seite den Clusternamen aus, für den Sie die Updates überprüfen möchten.

4. Wählen Sie die Registerkarte Resources (Ressourcen) aus.
5. Wählen Sie im Bereich Ressourcentypen unter Workloads die Option DaemonSets.
6. Wählen Sie aus aws-guardduty-agent.
7. Wählen Sie auf der aws-guardduty-agentSeite „Rohansicht“, um die unformatierte Antwort JSON anzuzeigen. Stellen Sie sicher, dass die konfigurierbaren Parameter den von Ihnen angegebenen Wert anzeigen.

Wechseln Sie nach der Überprüfung zur GuardDuty Konsole. Wählen Sie das entsprechende aus AWS-Region und sehen Sie sich den Deckungsstatus für Ihre EKS Amazon-Cluster an. Weitere Informationen finden Sie unter Abdeckung für EKS Amazon-Cluster.

Konfiguration der EKS Laufzeitüberwachung (APInur)

Bevor Sie EKS Runtime Monitoring in Ihrem Konto konfigurieren, stellen Sie sicher, dass Sie eine der verifizierten Plattformen verwenden, die die derzeit verwendete Kubernetes-Version unterstützt. Weitere Informationen finden Sie unter Validierung der architektonischen Anforderungen.

GuardDuty hat die Konsolenerfahrung für EKS Runtime Monitoring in Runtime Monitoring zusammengefasst. GuardDuty empfiehlt Überprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring undMigration von EKS Runtime Monitoring zu Runtime Monitoring.

Stellen Sie im Rahmen der Migration zu Runtime Monitoring sicher, dass Deaktivieren Sie die Laufzeitüberwachung EKS Dies ist wichtig, denn wenn Sie sich später dafür entscheiden, Runtime Monitoring zu deaktivieren und EKS Runtime Monitoring nicht zu deaktivieren, werden Ihnen weiterhin Nutzungskosten für EKS Runtime Monitoring entstehen.

EKSRuntime Monitoring für ein eigenständiges Konto konfigurieren

Informationen zu den Konten, die AWS Organizations zugeordnet sind, finden Sie unterKonfiguration von EKS Runtime Monitoring für Umgebungen mit mehreren Konten.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Runtime Monitoring für Ihr Konto zu aktivieren.

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS Cluster überwachen)	1. Führen Sie den aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features` Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben `ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster in Ihrem Konto. 2. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`
Überwachen Sie alle EKS Cluster, schließen Sie jedoch	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
einige davon aus (mithilfe des Ausschluss-Tags)	`Managed -false`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon -Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit. `eks:TagResource` • Ersetzen *ec2:DeleteTags* miteks:`UntagResource` . • Ersetzen *access-project* mit `GuardDuty Managed` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. **Note** Fügen Sie Ihrem EKS Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS` von `EKS_RUNTIME_MONITORING` auf setzen. `ENABLED` Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert. Führen Sie den aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features` Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben `ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster (mithilfe des Inclusion-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -true`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon -Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* mit. `eks:TagResource` • Ersetzen *`ec2:DeleteTags`* miteks:`UntagResource` . • Ersetzen *`access-project`* mit `GuardDuty Managed` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. Führen Sie das aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features` Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben `ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die mit dem `true` -Paar `GuardDutyManaged` - gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Führen Sie den aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features` Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben `ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Konfiguration von EKS Runtime Monitoring für Umgebungen mit mehreren Konten

In Umgebungen mit mehreren Konten kann nur das delegierte GuardDuty Administratorkonto EKS Runtime Monitoring für die Mitgliedskonten aktivieren oder deaktivieren und die GuardDuty Agentenverwaltung für die EKS Cluster verwalten, die zu den Mitgliedskonten in ihrer Organisation gehören. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten.

Konfiguration der EKS Laufzeitüberwachung für das delegierte Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Runtime Monitoring zu aktivieren und den GuardDuty Security Agent für die EKS Cluster zu verwalten, die zum delegierten GuardDuty Administratorkonto gehören.

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS Cluster überwachen)	Führen Sie den aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features` Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben`ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster in Ihrem Konto.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -false`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon -Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit. `eks:TagResource` • Ersetzen *ec2:DeleteTags* miteks:Untag `Resource` . • Ersetzen *access-project* mit `GuardDuty Managed` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. **Note** Fügen Sie Ihrem EKS Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS` von `EKS_RUNTIME_MONITORING` auf setzen. `ENABLED` Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert. Führen Sie den aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features` Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben `ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster (mithilfe des Inclusion-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -true`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon -Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit. `eks:TagResource` • Ersetzen *ec2:DeleteTags* mit`eks:UntagResource` . • Ersetzen *access-project* mit `GuardDuty Managed` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. Führen Sie das aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features` Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben `ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die mit dem `true` -Paar `GuardDutyManaged` - gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Führen Sie den aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features` Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben `ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Automatische Aktivierung der EKS Laufzeitüberwachung für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Runtime Monitoring für alle Mitgliedskonten zu aktivieren. Dazu gehören das delegierte GuardDuty Administratorkonto, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten. Wählen Sie Ihren bevorzugten Ansatz zur Verwaltung des GuardDuty Security Agents für die EKS Cluster, die zu diesen Mitgliedskonten gehören.

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS Cluster überwachen)	Um die EKS Laufzeitüberwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen aus *`detector ID`*. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` :

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT",
 "Status" : "ENABLED"}] ]'
```

> **Note**
>
> Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -false`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon-Benutzer handbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* mit. `eks:TagResource` • Ersetzen *`ec2:DeleteTags`* mit`eks:UntagResource` . • Ersetzen *`access-project`* mit `GuardDutyManaged` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. **Note** Fügen Sie Ihrem EKS Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS` von `EKS_RUNTIME_MONITORING` auf `ENABLED` setzen. Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert. Führen Sie den aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features` Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben`ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

```
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM
ENT", "Status" : " ENABLED"}] ]'
```

> **Note**
>
> Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster (mithilfe des Inclusion-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -true`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon-Benutzer handbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* mit. `eks:TagResource` • Ersetzen *`ec2:DeleteTags`* miteks`:UntagResource` . • Ersetzen *`access-project`* mit `GuardDutyManaged` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Führen Sie das aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben`ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die mit dem `true` -Paar `GuardDutyManaged` - gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Führen Sie das aus, updateDetectorAPIindem Sie Ihre eigene regionale Melder-ID verwenden und den `features` Objektnamen als `EKS_RUNTIME_MONITORING` und den Status als übergeben`ENABLED`. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Konfiguration der EKS Laufzeitüberwachung für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um EKS Runtime Monitoring zu aktivieren und den GuardDuty Security Agent für bestehende aktive Mitgliedskonten in Ihrem Unternehmen zu verwalten.

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS Cluster überwachen)	Um die EKS Laufzeitüberwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen aus *detector ID*. Stellen Sie den Status für EKS_ADDON_MANAGEMENT als ENABLED ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den detectorId für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert sowohl EKS_RUNTIME_MONITORING als auch EKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "Addition``

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

```
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT",
 "Status" : "ENABLED"}] ]'
```

> **Note**
>
> Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -false`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon-Benutzer handbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit. `eks:TagResource` • Ersetzen *ec2:DeleteTags* mit`eks:UntagResource` . • Ersetzen *access-project* mit `GuardDutyManaged` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3.

> **Note**
>
> Fügen Sie Ihrem EKS Cluster immer das Ausschluss-Tag hinzu, bevor Sie das STATUS von EKS_RUNTIME_MONITORING auf setzen. ENABLED Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert.

Um EKS Runtime Monitoring selektiv für Ihre Mitglieds konten zu aktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen aus *detector ID*.

Stellen Sie den Status für EKS_ADDON_MANAGEMENT als ENABLED ein.

GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die nicht von der Überwachung ausgeschlossen wurden.

Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Den detectorId für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

Das folgende Beispiel aktiviert sowohl EKS_RUNTIME_MONITORING als auch EKS_ADDON_MANAGEMENT :

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
```

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM ENT", "Status" : " *ENABLED*"}]]' **Note** Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster (mithilfe des Inclusion-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDutyManaged -true`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon-Benutzer handbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* mit. `eks:TagResource` • Ersetzen *`ec2:DeleteTags`* miteks`:UntagResource` . • Ersetzen *`access-project`* mit `GuardDutyManaged` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Um die EKS Laufzeitüberwachung selektiv für Ihre Mitglieds konten zu aktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihren eigenen aus *`detector ID`*.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte

Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein.

GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die mit dem `true` -Paar `GuardDutyManaged` - gekennzeichnet wurden.

Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0    --account-
ids 111122223333  --features '[{"Name" : "EKS_RUNT
IME_MONITORING", "Status" : "  ENABLED", "Addition
alConfiguration" : [{"Name" : "EKS_ADDON_MANAGEM
ENT", "Status" : " DISABLED"}] ]'
```

> **Note**
>
> Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.
Den Sicherheitsagent manuell verwalten	1. Um die EKS Laufzeitüberwachung selektiv für Ihre Mitglieds konten zu aktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen aus *detector ID*. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden , indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Automatische Aktivierung der EKS Laufzeitüberwachung für neue Mitglieder

Das delegierte GuardDuty Administratorkonto kann EKS Runtime Monitoring automatisch aktivieren und einen Ansatz für die Verwaltung des GuardDuty Security Agents für neue Konten wählen, die Ihrem Unternehmen beitreten.

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS Cluster überwachen)	Um die EKS Laufzeitüberwachung selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den UpdateOrganization ConfigurationAPIVorgang mit Ihren eigenen Konten auf *detector ID*. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Im folgenden Beispiel werden beide Optionen `EKS_RUNTIME_MONITORING` und `EKS_ADDON_MANAGEMENT` für ein einzelnes Konto aktiviert. Sie können auch eine

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	durch ein IDs Leerzeichen getrennte Liste von Konten übergeben. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -false`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon -Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit. `eks:TagResource` • Ersetzen *ec2:DeleteTags* mit`eks:UntagResource` . • Ersetzen *access-project* mit `GuardDuty Managed` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	3. **Note** Fügen Sie Ihrem EKS Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS` von `EKS_RUNTIME_MONITORING` auf setzen. `ENABLED` Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert. Um EKS Runtime Monitoring selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den UpdateOrganizationConfigurationAPIVorgang mit Ihrem eigenen Konto auf *`detector ID`*. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Im folgenden Beispiel werden beide Optionen `EKS_RUNTIME_MONITORING` und `EKS_ADDON_MANAGEMENT` für ein einzelnes Konto aktiviert

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	. Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Überwachen Sie ausgewählte EKS Cluster (mithilfe des Inclusion-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -true`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon -Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *`ec2:CreateTags`* mit. `eks:TagResource` • Ersetzen *`ec2:DeleteTags`* miteks:`UntagResource` . • Ersetzen *`access-project`* mit `GuardDuty Managed` • Ersetzen *`123456789012`* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	3. Um die EKS Laufzeitüberwachung selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den UpdateOrganizationConfigurationAPIVorgang mit Ihren eigenen auf *detector ID*. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die mit dem `true` -Paar `GuardDutyManaged` - gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` für ein einzelnes Konto. Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]' Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
Den Sicherheitsagent manuell verwalten	1. Um die EKS Laufzeitüberwachung selektiv für Ihre neuen Konten zu aktivieren, rufen Sie den UpdateOrganizationConfigurationAPIVorgang mit Ihrem eigenen Konto auf *detector ID*. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` für ein einzelnes Konto. Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben. Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu`

Bevorzugter Ansatz zur Verwaltung des Security Agents GuardDuty	Schritte
	ration" : [{"Name" : "EKS_ADDON_MANAGEM ENT", "AutoEnable": "NEW"}]]' Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellu ngen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenf assung des Problems aufgeführt. 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Aktivieren Sie die EKS Laufzeitüberwachung für einzelne aktive Mitgliedskonten

API/CLI

Auf der Grundlage von Methoden zur Verwaltung des GuardDuty Security Agents können Sie einen bevorzugten Ansatz wählen und die in der folgenden Tabelle aufgeführten Schritte ausführen.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Security Agent verwalten über GuardDuty (Alle EKS Cluster überwachen)	Um die EKS Laufzeitüberwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMem berDetectorsAPIVorgang mit Ihrem eigenen aus *`detector ID`*. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster in Ihrem Konto. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie alle EKS Cluster, schließen Sie jedoch einige davon aus (mithilfe des Ausschluss-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -false`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon -Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauen swürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit. `eks:TagResource` • Ersetzen *ec2:DeleteTags* mit`eks:UntagResource` . • Ersetzen *access-project* mit `GuardDuty Managed` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. **Note** Fügen Sie Ihrem EKS Cluster immer das Ausschluss-Tag hinzu, bevor Sie das `STATUS` von `EKS_RUNTIME_MONITORING` auf `ENABLED` setzen. Andernfalls wird der GuardDuty Security Agent auf allen EKS Clustern in Ihrem Konto installiert. Um EKS Runtime Monitoring selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen aus *`detector ID`*. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `ENABLED` ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die nicht von der Überwachung ausgeschlossen wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert sowohl `EKS_RUNTIME_MONITORING` als auch `EKS_ADDON_MANAGEMENT` :

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	`aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'` **Note** Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Überwachen Sie ausgewählte EKS Cluster (mithilfe des Inclusion-Tags)	1. Fügen Sie dem EKS Cluster, den Sie von der Überwachung ausschließen möchten, ein Tag hinzu. Das Schlüssel-Wert-Paar ist `GuardDuty Managed -true`. Weitere Informationen zum Hinzufügen des Tags finden Sie unter Arbeiten mit Tags mithilfe von CLIAPI, oder eksctl im EKSAmazon -Benutzerhandbuch. 2. Um zu verhindern, dass Tags, außer durch vertrauenswürdige Entitäten, geändert werden, verwenden Sie die Richtlinie im Benutzerhandbuch für AWS Organizations im Abschnitt Änderungen von Tags verhindern, außer durch autorisierte Prinzipale. Ersetzen Sie in dieser Richtlinie die folgenden Angaben: • Ersetzen *ec2:CreateTags* mit. `eks:TagResource` • Ersetzen *ec2:DeleteTags* miteks:`Untag Resource` . • Ersetzen *access-project* mit `GuardDuty Managed` • Ersetzen *123456789012* mit der AWS-Konto ID der vertrauenswürdigen Entität. Wenn Sie mehr als eine vertrauenswürdige Entität haben, verwenden Sie das folgende Beispiel, um mehrere `PrincipalArn` hinzuzufügen: `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	3. Um die EKS Laufzeitüberwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihren eigenen aus *detector ID*. Stellen Sie den Status für EKS_ADDON_MANAGEMENT als DISABLED ein. GuardDuty verwaltet die Bereitstellung und Aktualisierung des Security Agents für alle EKS Amazon-Cluster, die mit dem true -Paar GuardDutyManaged - gekennzeichnet wurden. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den detectorId für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert EKS_RUNTIME_MONITORING und deaktiviert EKS_ADDON_MANAGEMENT : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
	Note Sie können auch eine durch ein IDs Leerzeich en getrennte Liste von Konten übergeben. Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellu ngen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenf assung des Problems aufgeführt.

Bevorzugter Ansatz zur Verwaltung des GuardDuty Security Agents	Schritte
Den Sicherheitsagent manuell verwalten	1. Um die EKS Laufzeitüberwachung selektiv für Ihre Mitgliedskonten zu aktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen aus *`detector ID`*. Stellen Sie den Status für `EKS_ADDON_MANAGEMENT` als `DISABLED` ein. Alternativ können Sie den AWS CLI Befehl verwenden, indem Sie Ihre eigene regionale Melder-ID verwenden. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI. Das folgende Beispiel aktiviert `EKS_RUNTIME_MONITORING` und deaktiviert `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Informationen zur Verwaltung des Sicherheitsagenten finden Sie unter Manuelles Verwalten des Security Agents für EKS Amazon-Cluster.

Migration von EKS Runtime Monitoring zu Runtime Monitoring

Mit der Einführung von GuardDuty Runtime Monitoring wurde der Geltungsbereich der Bedrohungserkennung auf ECS Amazon-Container und EC2 Amazon-Instances ausgeweitet. EKSDie Erfahrung mit Runtime Monitoring wurde nun in Runtime Monitoring zusammengefasst. Sie können Runtime Monitoring aktivieren und einzelne GuardDuty Security Agents für jeden Ressourcentyp (EC2Amazon-Instance, ECS Amazon-Cluster und EKS Amazon-Cluster) verwalten, für den Sie das Laufzeitverhalten überwachen möchten.

GuardDuty hat die Konsolenerfahrung für EKS Runtime Monitoring in Runtime Monitoring zusammengefasst. GuardDuty empfiehlt Überprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring undMigration von EKS Runtime Monitoring zu Runtime Monitoring.

Stellen Sie im Rahmen der Migration zu Runtime Monitoring sicher, dass Deaktivieren Sie die Laufzeitüberwachung EKS Dies ist wichtig, denn wenn Sie sich später dafür entscheiden, Runtime Monitoring zu deaktivieren und EKS Runtime Monitoring nicht zu deaktivieren, werden Ihnen weiterhin Nutzungskosten für EKS Runtime Monitoring entstehen.

Um von EKS Runtime Monitoring zu Runtime Monitoring zu migrieren

1. Die GuardDuty Konsole unterstützt EKS Runtime Monitoring als Teil von Runtime Monitoring.

   Sie können damit beginnen, Runtime Monitoring Überprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring von Ihrer Organisation und Ihren Konten aus zu verwenden.

   Stellen Sie sicher, dass Sie EKS Runtime Monitoring nicht deaktivieren, bevor Sie Runtime Monitoring aktivieren. Wenn Sie EKS Runtime Monitoring deaktivieren, wird auch die EKS Amazon-Zusatzverwaltung deaktiviert. Fahren Sie mit den folgenden Schritten in der angegebenen Reihenfolge fort.
2. Stellen Sie sicher, dass Sie alle erfüllenVoraussetzungen für die Aktivierung von Runtime Monitoring.
3. Aktivieren Sie Runtime Monitoring, indem Sie dieselben Organisationskonfigurationseinstellungen für Runtime Monitoring replizieren wie für EKS Runtime Monitoring. Weitere Informationen finden Sie unter Laufzeitüberwachung aktivieren.
   - Wenn Sie ein eigenständiges Konto haben, müssen Sie Runtime Monitoring aktivieren.

     Wenn Ihr GuardDuty Security Agent bereits installiert ist, werden die entsprechenden Einstellungen automatisch repliziert und Sie müssen die Einstellungen nicht erneut konfigurieren.

- Wenn Sie eine Organisation mit Einstellungen für die automatische Aktivierung haben, stellen Sie sicher, dass Sie dieselben Einstellungen für die automatische Aktivierung für Runtime Monitoring replizieren.
- Wenn Sie ein Unternehmen haben, dessen Einstellungen für bestehende aktive Mitgliedskonten einzeln konfiguriert sind, stellen Sie sicher, dass Sie Runtime Monitoring aktivieren und den GuardDuty Security Agent für diese Mitglieder individuell konfigurieren.

4. Nachdem Sie sichergestellt haben, dass die Einstellungen für Runtime Monitoring und GuardDuty Security Agent korrekt sind, deaktivieren Sie EKS Runtime Monitoring, indem Sie entweder den Befehl API oder den AWS CLI Befehl verwenden.
5. (Optional) Wenn Sie alle mit dem GuardDuty Security Agent verknüpften Ressourcen säubern möchten, finden Sie weitere Informationen unterAuswirkungen der Deaktivierung und Bereinigung von Ressourcen.

Wenn Sie Runtime Monitoring weiterhin verwenden möchten, ohne EKS Runtime Monitoring zu aktivieren, finden Sie weitere Informationen unterKonfiguration der EKS Laufzeitüberwachung (APInur).

Überprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring

Verwenden Sie die folgenden AWS CLI Befehle APIs oder, um den aktuellen Konfigurationsstatus von EKS Runtime Monitoring zu überprüfen.

Um den bestehenden EKS Runtime Monitoring-Konfigurationsstatus in Ihrem Konto zu überprüfen

- Führen Sie den Befehl aus GetDetector, um den Konfigurationsstatus Ihres eigenen Kontos zu überprüfen.
- Alternativ können Sie den folgenden Befehl ausführen, indem Sie Folgendes verwenden AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

Achten Sie darauf, die Melder-ID Ihrer Region AWS-Konto und der aktuellen Region zu ersetzen. Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite Einstellungen oder führen Sie den aus ListDetectorsAPI.

So überprüfen Sie den aktuellen EKS Runtime Monitoring-Konfigurationsstatus für Ihr Unternehmen (nur als delegiertes GuardDuty Administratorkonto)

- Führen Sie DescribeOrganizationConfigurationden Befehl aus, um den Konfigurationsstatus Ihrer Organisation zu überprüfen.

  Alternativ können Sie den folgenden Befehl ausführen mit AWS CLI:

  ```
  aws guardduty describe-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
  ```

  Achten Sie darauf, die Melder-ID durch die Melder-ID Ihres delegierten GuardDuty Administratorkontos und die Region durch Ihre aktuelle Region zu ersetzen. Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

Deaktivieren von EKS Runtime Monitoring nach der Migration zu Runtime Monitoring

Nachdem Sie sichergestellt haben, dass die vorhandenen Einstellungen für Ihr Konto oder Ihre Organisation in Runtime Monitoring repliziert wurden, können Sie EKS Runtime Monitoring deaktivieren.

Um EKS Runtime Monitoring zu deaktivieren

- Um EKS Runtime Monitoring in Ihrem eigenen Konto zu deaktivieren

  Führen Sie das UpdateDetectorAPImit Ihrer eigenen Region aus *`detector-id`*.

  Alternativ können Sie den folgenden AWS CLI Befehl verwenden. Ersetzen *`12abc34d567e8fa901bc2d34e56789f0`* mit Ihrer eigenen Region *`detector-id`*.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
  ```

- Um die EKS Laufzeitüberwachung für Mitgliedskonten in Ihrer Organisation zu deaktivieren

  Führen Sie das UpdateMemberDetectorsAPImit dem regionalen *`detector-id`* des delegierten GuardDuty Administratorkontos der Organisation.

Alternativ können Sie den folgenden AWS CLI Befehl verwenden. Ersetzen *12abc34d567e8fa901bc2d34e56789f0* mit der regionalen *detector-id* des delegierten GuardDuty Administratorkontos der Organisation und *111122223333* mit der AWS-Konto ID des Mitgliedskontos, für das Sie diese Funktion deaktivieren möchten.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "DISABLED"}]'
```

- Um die Einstellungen für die automatische Aktivierung von EKS Runtime Monitoring für Ihr Unternehmen zu aktualisieren

  Führen Sie den folgenden Schritt nur aus, wenn Sie die Einstellungen für die automatische Aktivierung von EKS Runtime Monitoring entweder auf neue (NEW) oder alle (ALL) Mitgliedskonten in der Organisation konfiguriert haben. Wenn Sie es bereits als konfiguriert habenNONE, können Sie diesen Schritt überspringen.

  > **Note**
  >
  > Wenn Sie die Konfiguration für die automatische Aktivierung von EKS Runtime NONE Monitoring auf einstellen, wird EKS Runtime Monitoring nicht automatisch für ein vorhandenes Mitgliedskonto aktiviert oder wenn ein neues Mitgliedskonto Ihrer Organisation beitritt.

  Führen Sie das UpdateOrganizationConfigurationAPImit dem regionalen *detector-id* des delegierten GuardDuty Administratorkontos der Organisation.

  Alternativ können Sie den folgenden AWS CLI Befehl verwenden. Ersetzen *12abc34d567e8fa901bc2d34e56789f0* mit der regionalen *detector-id* des delegierten GuardDuty Administratorkontos der Organisation. Ersetzen Sie das *EXISTING_VALUE* mit Ihrer aktuellen Konfiguration für die automatische Aktivierung GuardDuty.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
   --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
  ```

Bewertung der Laufzeitabdeckung Ihrer Ressourcen

Nachdem Sie Runtime Monitoring aktiviert haben und der GuardDuty Security Agent auf Ihrer Ressource installiert wurde, GuardDuty liefert er Deckungsstatistiken für den entsprechenden Ressourcentyp und den individuellen Schutzstatus für die Ressourcen, die zu Ihrem Konto gehören. Der Deckungsstatus wird bestimmt, indem Sie sicherstellen, dass Sie Runtime Monitoring aktiviert haben, Ihr VPC Amazon-Endpunkt erstellt wurde und der GuardDuty Security Agent für die entsprechende Ressource bereitgestellt wurde. Der Status „Fehlerfrei“ bedeutet, dass, wenn es ein Laufzeitereignis im Zusammenhang mit Ihrer Ressource gibt, GuardDuty das besagte Laufzeitereignis über den VPC Amazon-Endpunkt empfangen und das Verhalten überwachen kann. Wenn bei der Konfiguration von Runtime Monitoring, der Erstellung eines VPC Amazon-Endpunkts oder der Bereitstellung des GuardDuty Security Agents ein Problem aufgetreten ist, wird der Deckungsstatus als Ungesund angezeigt. Wenn der Schutzstatus fehlerhaft ist, kann GuardDuty das Laufzeitverhalten der entsprechenden Ressource nicht empfangen oder überwacht werden, und es können auch keine Runtime Monitoring-Ergebnisse generiert werden.

Die folgenden Themen helfen Ihnen dabei, Deckungsstatistiken zu überprüfen, EventBridge Benachrichtigungen zu konfigurieren und Probleme mit der Abdeckung für einen bestimmten Ressourcentyp zu beheben.

Inhalt

Deckung für EC2 Amazon-Instance

Für eine EC2 Amazon-Ressource wird die Laufzeitabdeckung auf Instance-Ebene bewertet. Ihre EC2 Amazon-Instances können unter anderem mehrere Arten von Anwendungen und Workloads in Ihrer AWS Umgebung ausführen. Diese Funktion unterstützt auch von Amazon ECS verwaltete EC2 Amazon-Instances. Wenn Sie ECS Amazon-Cluster auf einer EC2 Amazon-Instance ausführen, werden die Deckungsprobleme auf Instance-Ebene unter Amazon EC2 Runtime Coverage angezeigt.

Themen

- Benachrichtigungen über Änderungen des Abdeckungsstatus konfigurieren
- Fehlerbehebung bei Abdeckungsproblemen

Überprüfen der Abdeckungsstatistiken

Die Deckungsstatistik für die EC2 Amazon-Instances, die mit Ihren eigenen Konten oder Ihren Mitgliedskonten verknüpft sind, gibt den Prozentsatz der fehlerfreien EC2 Instances an allen EC2 Instances in den ausgewählten Instances an AWS-Region. Die folgende Gleichung stellt dies wie folgt dar:

(Fehlerfreie Instanzen/Alle Instances) *100

Wenn Sie den GuardDuty Security Agent auch für Ihre ECS Amazon-Cluster bereitgestellt haben, wird jedes Problem mit der Abdeckung auf Instance-Ebene, das mit ECS Amazon-Clustern in Verbindung steht, die auf einer EC2 Amazon-Instance ausgeführt werden, als Problem mit der Runtime-Coverage von Amazon EC2 Instance angezeigt.

Wählen Sie eine der Zugriffsmethoden, um die Abdeckungsstatistiken für Ihre Konten einzusehen.

Console

- Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
- Wählen Sie im Navigationsbereich Runtime Monitoring aus.
- Wählen Sie die Registerkarte Runtime Coverage aus.
- Auf der Registerkarte EC2Instance-Laufzeitabdeckung können Sie die Deckungsstatistiken einsehen, die nach dem Deckungsstatus jeder EC2 Amazon-Instance aggregiert sind, die in der Instance-Listentabelle verfügbar sind.
  - Sie können die Tabelle mit der Instance-Liste nach den folgenden Spalten filtern:
    - Konto-ID
    - Agentenverwaltungs-Typ
    - Version des Agenten
    - Abdeckungsstatus
    - Instanz-ID
    - Cluster ARN

- Wenn eine Ihrer EC2 Instances den Coverage-Status als Ungesund hat, enthält die Spalte Problem zusätzliche Informationen über den Grund für den Status Ungesund.

API/CLI

- Führen Sie den ListCoverageAPImit Ihrer eigenen gültigen Melder-ID, Ihrer aktuellen Region und Ihrem Service-Endpunkt aus. Damit können Sie die Instanzliste filtern und sortierenAPI.
  - Sie können das Beispiel `filter-criteria` ändern mit einer der folgenden Optionen für `CriterionKey`:
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `AGENT_VERSION`
    - `MANAGEMENT_TYPE`
    - `INSTANCE_ID`
    - `CLUSTER_ARN`
  - Wenn der `RESOURCE_TYPE` als `filter-criteria` beinhaltet EC2, unterstützt Runtime Monitoring die Verwendung von ISSUEas nicht`AttributeName`. Wenn Sie es verwenden, führt die API Antwort zu`InvalidInputException`.

    Sie können das Beispiel `AttributeName` in `sort-criteria` ändern mit einer der folgenden Optionen:
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`
    - `INSTANCE_ID`
    - `UPDATED_AT`
  - Sie können das ändern *`max-results`* (bis zu 50).
  - Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
"EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
```

```
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Führen Sie den aus GetCoverageStatisticsAPI, um aggregierte Statistiken zur Abdeckung abzurufen, die `statisticsType` auf dem basieren.
  - Sie können das Beispiel `statisticsType` zu einer der folgenden Optionen ändern:
    - `COUNT_BY_COVERAGE_STATUS`— Stellt Deckungsstatistiken für EKS Cluster dar, die nach dem Deckungsstatus aggregiert sind.
    - `COUNT_BY_RESOURCE_TYPE`— Deckungsstatistiken, die auf der Grundlage des AWS Ressourcentyps in der Liste aggregiert wurden.
    - Sie können das Beispiel `filter-criteria` im Befehl ändern. Sie können die folgenden Optionen für `CriterionKey` verwenden:
      - `ACCOUNT_ID`
      - `RESOURCE_TYPE`
      - `COVERAGE_STATUS`
      - `AGENT_VERSION`
      - `MANAGEMENT_TYPE`
      - `INSTANCE_ID`
      - `CLUSTER_ARN`
  - Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Wenn der Abdeckungsstatus Ihrer EC2 Instance fehlerhaft ist, finden Sie weitere Informationen unterFehlerbehebung bei Abdeckungsproblemen.

Benachrichtigungen über Änderungen des Abdeckungsstatus konfigurieren

Der Deckungsstatus Ihrer EC2 Amazon-Instance wird möglicherweise als Ungesund angezeigt. Um zu wissen, wann sich der Deckungsstatus ändert, empfehlen wir Ihnen, den Deckungsstatus

regelmäßig zu überprüfen und Fehler zu beheben, falls der Status auf Ungesund umgestellt wird. Alternativ können Sie eine EventBridge Amazon-Regel erstellen, um eine Benachrichtigung zu erhalten, wenn sich der Versicherungsstatus von „Ungesund“ in „Fehlerfrei“ oder anderweitig ändert. GuardDuty Veröffentlicht dies standardmäßig im EventBridge Bus für Ihr Konto.

Beispiel für ein Benachrichtigungsschema

In einer EventBridge Regel können Sie die vordefinierten Beispielereignisse und Ereignismuster verwenden, um eine Benachrichtigung über den Versicherungsstatus zu erhalten. Weitere Informationen zum Erstellen einer EventBridge Regel finden Sie unter Regel erstellen im EventBridge Amazon-Benutzerhandbuch.

Darüber hinaus können Sie mithilfe des folgenden Beispiel-Benachrichtigungsschemas ein benutzerdefiniertes Ereignismuster erstellen. Achten Sie darauf, die Werte für Ihr Konto zu ersetzen. Um benachrichtigt zu werden, wenn sich der Deckungsstatus Ihrer EC2 Amazon-Instance von `Healthy` zu ändert`Unhealthy`, `detail-type` sollte *`GuardDuty Runtime Protection Unhealthy`*. Um benachrichtigt zu werden, wenn sich der Versicherungsstatus von `Unhealthy` zu ändert`Healthy`, ersetzen Sie den Wert von `detail-type` durch *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS-Konto ID",
  "time": "event timestamp (string)",
  "region": "AWS-Region",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
          "clusterArn": "",
          "agentDetails": {
```

```
            "version":""
          },
          "managementType":""
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Fehlerbehebung bei Abdeckungsproblemen

Wenn der Deckungsstatus Ihrer EC2 Amazon-Instance „Ungesund“ lautet, können Sie den Grund in der Spalte Problem einsehen.

Wenn Ihre EC2 Instance einem EKS Cluster zugeordnet ist und der Security Agent für entweder manuell oder über eine automatische Agentenkonfiguration installiert EKS wurde, finden Sie Informationen zur Behebung des Deckungsproblems unterAbdeckung für EKS Amazon-Cluster.

In der folgenden Tabelle sind die Problemtypen und die entsprechenden Schritte zur Fehlerbehebung aufgeführt.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Keine Agentenberichterstattung	Ich warte auf die SSM Benachrichtigung	Der Empfang der SSM Benachrichtigung kann einige Minuten dauern. Stellen Sie sicher, dass die EC2 Amazon-Instance SSM verwaltet wird. Weitere Informationen finden Sie in den Schritten unter Methode 1 — Mithilfe von AWS Systems Manager inManuelles Installieren des Security Agents.
	(Absichtlich leer)	Wenn Sie den GuardDuty Security Agent manuell verwalten, stellen Sie sicher, dass Sie die Schritte unter befolgt habenManuelles Verwalten des Security Agents für EC2 Amazon-Instance.
		Wenn Sie die automatische Agentenkonfiguration aktiviert haben:

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
		• Ihre EC2 Instanz wird SSM verwaltet. • Sehen Sie sich regelmäßig den Status Ihres Security Agents an. Weitere Informationen finden Sie unter Der Installationsstatus des GuardDuty Security Agents wird überprüft.
		Stellen Sie sicher, dass der VPC Endpunkt für Ihre EC2 Amazon-Instance korrekt konfiguriert ist. Weitere Informationen finden Sie unter Wie überprüfe ich, ob die VPC Endpunktkonfiguration korrekt ist?.
		Wenn Ihre Organisation über eine Richtlinie zur Servicekontrolle (SCP) verfügt, stellen Sie sicher, dass die Berechtigungen nicht durch die Grenze der `guardduty:SendSecurityTelemetry` Berechtigungen eingeschränkt werden. Weitere Informationen finden Sie unter Überprüfung der Servicesteuerungsrichtlinie Ihres Unternehmens.
	Die Verbindung des Agenten wurde unterbrochen	• Sehen Sie sich den Status Ihres Security Agents an. Weitere Informationen finden Sie unter Der Installationsstatus des GuardDuty Security Agents wird überprüft. • Sehen Sie sich die Security Agent-Protokolle an, um die mögliche Ursache zu ermitteln. Die Protokolle enthalten detaillierte Fehler, anhand derer Sie das Problem selbst beheben können. Die Protokolldateien sind verfügbar unter`/var/log/amzn-guardduty-agent/` . `Tunsudo journalctl -u amazon-guardduty-agent .`

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
SSMDie Erstellung der Assoziation ist fehlgeschlagen	GuardDuty SSMIn Ihrem Konto ist bereits eine Assoziation vorhanden	1. Löschen Sie die bestehende Zuordnung manuell. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Löschen von Verknüpfungen. 2. Nachdem Sie die Zuordnung gelöscht haben, deaktivieren Sie die GuardDuty automatische Agentenkonfiguration für Amazon EC2 und aktivieren Sie sie anschließend erneut.
	Ihr Konto hat zu viele Verknüpfungen SSM	Wählen Sie eine der folgenden zwei Optionen: • Löschen Sie alle ungenutzten SSM Verknüpfungen. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Löschen von Verknüpfungen. • Prüfen Sie, ob Ihr Konto für eine Erhöhung des Kontingents in Frage kommt. Weitere Informationen finden Sie unter Systems Manager Manager-Dienstkontingente in der Allgemeine AWS-Referenz.
SSMDie Aktualisierung der Assoziation ist fehlgeschlagen	GuardDuty SSMIn Ihrem Konto ist keine Assoziation vorhanden	GuardDuty SSMDie Assoziation ist in Ihrem Konto nicht vorhanden. Deaktivieren Sie Runtime Monitoring und aktivieren Sie es anschließend erneut.
SSMDas Löschen der Assoziation ist fehlgeschlagen	GuardDuty SSMDie Zuordnung ist in Ihrem Konto nicht vorhanden	Die SSM Assoziation ist in Ihrem Konto nicht vorhanden. Wenn die SSM Zuordnung absichtlich gelöscht wurde, ist keine Aktion erforderlich.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
SSMDie Ausführung der Instanzzu weisung ist fehlgeschlagen	Architektonische Anforderungen oder andere Vorausset zungen sind nicht erfüllt.	Informationen zu verifizierten Betriebssystemverteilungen finden Sie unterVoraussetzungen für die Unterstützung Amazon EC2 Amazon-Instances. Wenn dieses Problem weiterhin auftritt, helfen Ihnen die folgenden Schritte dabei, das Problem zu identifizieren und möglicherweise zu lösen: 1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/. 2. Wählen Sie im Navigationsbereich unter Node Management die Option State Manager aus. 3. Filtern Sie nach der Eigenschaft Dokumentname und geben Sie ein AmazonGuardDuty-ConfigureRu ntimeMonitoringSsmPlugin. 4. Wählen Sie die entsprechende Zuordnungs-ID aus und sehen Sie sich den zugehörigen Ausführun gsverlauf an. 5. Sehen Sie sich anhand des Ausführungsverlaufs die Fehler an, identifizieren Sie die potenzielle Ursache und versuchen Sie, sie zu beheben.
VPCDie Endpunkte rstellung ist fehlgeschlagen	VPCDie Erstellung von Endpunkten wird für Shared nicht unterstützt VPC *vpcId*	Runtime Monitoring unterstützt die Verwendung eines VPC innerhalb einer Organisation gemeinsam genutzten Geräts. Weitere Informationen finden Sie unter Wird gemeinsam VPC mit automatisierten Security Agents verwendet.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
	Nur bei Verwendung von Shared VPC mit automatisierter Agentenkonfiguration Konto-ID des Besitzers *111122223333* zur gemeinsamen Nutzung VPC *vpcId* hat weder Runtime Monitoring noch automatische Agentenkonfiguration oder beides aktiviert	Das gemeinsame VPC Besitzerkonto muss Runtime Monitoring und automatische Agentenkonfiguration für mindestens einen Ressourcentyp (Amazon EKS oder Amazon ECS (AWS Fargate)) aktivieren. Weitere Informationen finden Sie unter Spezifische Voraussetzungen für GuardDuty Runtime Monitoring.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
	Für die Aktivierung von privat DNS sind beide erforderlich `enableDnsSupport` und die `enableDnsHostnames` VPC Attribute müssen auf „`true`for“ gesetzt sein *`vpcId`* (Dienst: Ec2, Statuscode: 400, Anforderungs-ID: *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Stellen Sie sicher, dass die folgenden VPC Attribute auf `true` — `enableDnsSupport` und gesetzt sind. `enableDnsHostnames` Weitere Informationen finden Sie unter DNSAttribute in Ihrem VPC. Wenn Sie Amazon VPC Console unter verwenden , https://console.aws.amazon.com/vpc/um Amazon zu erstellen, stellen Sie sicherVPC, dass Sie sowohl DNSHostnamen aktivieren als auch DNSAuflösung aktivieren auswählen. Weitere Informationen finden Sie unter VPCKonfigurationsoptionen.

Art des Problems	Meldung ausgeben	Fehlerbehebungsschritte
Das Löschen des gemeinsamen VPC Endpunkts ist fehlgeschlagen	Das Löschen eines gemeinsamen VPC Endpunkts ist für die Konto-ID nicht zulässig *111122223333* , geteilt VPC *vpcId*, Konto-ID des Besitzers *555555555555* .	Mögliche Schritte: • Die Deaktivierung des Runtime Monitoring-Status des gemeinsamen VPC Teilnehmerkontos hat keine Auswirkungen auf die Richtlinie für gemeinsame VPC Endgeräte und die Sicherheitsgruppe, die im Besitzerkonto vorhanden ist. Um den gemeinsamen VPC Endpunkt und die Sicherheitsgruppe zu löschen, müssen Sie Runtime Monitoring oder den Status der automatisierten Agentenkonfiguration im gemeinsamen VPC Besitzerkonto deaktivieren. • Das gemeinsame VPC Teilnehmerkonto kann den gemeinsamen VPC Endpunkt und die Sicherheitsgruppe, die im gemeinsamen VPC Besitzerkonto gehostet werden, nicht löschen.
Der Agent meldet sich nicht	(Absichtlich leer)	Der Support für diesen Problemtyp hat das Ende des Supports erreicht. Wenn dieses Problem weiterhin auftritt und dies noch nicht geschehen ist, aktivieren Sie den GuardDuty automatisierten Agenten für AmazonEC2. Wenn das Problem weiterhin besteht, sollten Sie in Erwägung ziehen, Runtime Monitoring für einige Minuten zu deaktivieren und es dann erneut zu aktivieren.

Abdeckung für ECS Amazon-Cluster

Die Laufzeitabdeckung für ECS Amazon-Cluster umfasst die Aufgaben, die auf AWS Fargate (Fargate) ECS Amazon-Container-Instances ausgeführt werden [1].

Für einen ECS Amazon-Cluster, der auf Fargate läuft, wird die Laufzeitabdeckung auf Aufgabenebene bewertet. Die Runtime-Abdeckung des ECS Clusters umfasst die Fargate-Aufgaben,

die gestartet wurden, nachdem Sie Runtime Monitoring und automatisierte Agentenkonfiguration für Fargate aktiviert haben (ECSnur). Standardmäßig ist eine Fargate-Aufgabe unveränderlich. GuardDuty kann den Security Agent nicht installieren, um Container bei bereits laufenden Aufgaben zu überwachen. Um eine solche Fargate-Aufgabe einzubeziehen, müssen Sie die Aufgabe beenden und erneut starten. Stellen Sie sicher, dass Sie überprüfen, ob der zugehörige Dienst unterstützt wird.

Informationen zu ECS Amazon-Containern finden Sie unter Kapazitätserstellung.

Inhalt

Überprüfen der Abdeckungsstatistiken

Die Deckungsstatistik für die ECS Amazon-Ressourcen, die mit Ihrem eigenen Konto oder Ihren Mitgliedskonten verknüpft sind, ist der Prozentsatz der fehlerfreien ECS Amazon-Cluster im Vergleich zu allen ECS Amazon-Clustern in den ausgewählten AWS-Region. Dies beinhaltet die Abdeckung für ECS Amazon-Cluster, die sowohl mit Fargate- als auch mit EC2 Amazon-Instances verknüpft sind. Die folgende Gleichung stellt dies wie folgt dar:

(Fehlerfreie Cluster/Alle Cluster)*100

Überlegungen

- Die Deckungsstatistiken für den ECS Cluster beinhalten den Abdeckungsstatus der Fargate-Aufgaben oder ECS Container-Instances, die diesem ECS Cluster zugeordnet sind. Der Deckungsstatus der Fargate-Aufgaben umfasst Aufgaben, die sich entweder im Status Running befinden oder deren Ausführung vor Kurzem abgeschlossen wurde.
- Auf der Registerkarte ECSClusters Runtime Coverage gibt das Feld Abgedeckte Container-Instances den Abdeckungsstatus der Container-Instances an, die Ihrem ECS Amazon-Cluster zugeordnet sind.

  Wenn Ihr ECS Amazon-Cluster nur Fargate-Aufgaben enthält, wird die Anzahl als 0/0 angezeigt.
- Wenn Ihr ECS Amazon-Cluster mit einer EC2 Amazon-Instance verknüpft ist, die keinen Sicherheitsagenten hat, hat der ECS Amazon-Cluster auch den Deckungsstatus Unhealthy.

Informationen zur Identifizierung und Behebung des Deckungsproblems für die zugehörige EC2 Amazon-Instance finden Sie unter Fehlerbehebung bei Abdeckungsproblemen Für EC2 Amazon-Instances.

Wählen Sie eine der Zugriffsmethoden, um die Abdeckungsstatistiken für Ihre Konten einzusehen.

Console

- Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
- Wählen Sie im Navigationsbereich Runtime Monitoring aus.
- Wählen Sie die Registerkarte Runtime Coverage aus.
- Auf der Registerkarte ECSCluster-Laufzeitabdeckung können Sie die Deckungsstatistiken einsehen, die nach dem Abdeckungsstatus jedes ECS Amazon-Clusters zusammengefasst sind, der in der Cluster-Listentabelle verfügbar ist.
  - Sie können die Tabelle mit der Cluster-Liste nach den folgenden Spalten filtern:
    - Konto-ID
    - Cluster-Name
    - Agentenverwaltungs-Typ
    - Abdeckungsstatus
- Wenn einer Ihrer ECS Amazon-Cluster den Deckungsstatus „Ungesund“ hat, enthält die Spalte „Problem“ zusätzliche Informationen über den Grund für den Status „Fehlerhaft“.

  Wenn Ihre ECS Amazon-Cluster mit einer EC2 Amazon-Instance verknüpft sind, navigieren Sie zur Registerkarte EC2Instance-Laufzeitabdeckung und filtern Sie nach dem Feld Clustername, um das zugehörige Problem anzuzeigen.

API/CLI

- Führen Sie den ListCoverageAPImit Ihrer eigenen gültigen Melder-ID, Ihrer aktuellen Region und Ihrem Service-Endpunkt aus. Damit können Sie die Instanzliste filtern und sortierenAPI.
  - Sie können das Beispiel `filter-criteria` ändern mit einer der folgenden Optionen für `CriterionKey`:
    - `ACCOUNT_ID`

    - ECS_CLUSTER_NAME
    - COVERAGE_STATUS
    - MANAGEMENT_TYPE
  - Sie können das Beispiel AttributeName in sort-criteria ändern mit einer der folgenden Optionen:
    - ACCOUNT_ID
    - COVERAGE_STATUS
    - ISSUE
    - ECS_CLUSTER_NAME
    - UPDATED_AT

      Das Feld wird nur aktualisiert, wenn entweder eine neue Aufgabe im zugehörigen ECS Amazon-Cluster erstellt wird oder wenn sich der entsprechende Deckungsstatus ändert.
  - Sie können das ändern *max-results* (bis zu 50).
  - Den detectorId für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Führen Sie den aus GetCoverageStatisticsAPI, um aggregierte Statistiken zur Abdeckung abzurufen, die statisticsType auf dem basieren.
  - Sie können das Beispiel statisticsType zu einer der folgenden Optionen ändern:
    - COUNT_BY_COVERAGE_STATUS— Stellt Deckungsstatistiken für ECS Cluster dar, die nach dem Deckungsstatus aggregiert sind.
    - COUNT_BY_RESOURCE_TYPE— Deckungsstatistiken, die auf der Grundlage des AWS Ressourcentyps in der Liste aggregiert wurden.
    - Sie können das Beispiel filter-criteria im Befehl ändern. Sie können die folgenden Optionen für CriterionKey verwenden:
      - ACCOUNT_ID

    - ECS_CLUSTER_NAME
    - COVERAGE_STATUS
    - MANAGEMENT_TYPE
    - INSTANCE_ID
- Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Weitere Informationen zu Problemen mit der Netzabdeckung finden Sie unterFehlerbehebung bei Abdeckungsproblemen.

Benachrichtigungen über Änderungen des Abdeckungsstatus konfigurieren

Der Abdeckungsstatus Ihres ECS Amazon-Clusters wird möglicherweise als Ungesund angezeigt. Um zu wissen, wann sich der Deckungsstatus ändert, empfehlen wir Ihnen, den Deckungsstatus regelmäßig zu überprüfen und Fehler zu beheben, falls der Status auf Ungesund umgestellt wird. Alternativ können Sie eine EventBridge Amazon-Regel erstellen, um eine Benachrichtigung zu erhalten, wenn sich der Versicherungsstatus von „Ungesund“ in „Fehlerfrei“ oder anderweitig ändert. GuardDuty Veröffentlicht dies standardmäßig im EventBridge Bus für Ihr Konto.

Beispiel für ein Benachrichtigungsschema

In einer EventBridge Regel können Sie die vordefinierten Beispielereignisse und Ereignismuster verwenden, um eine Benachrichtigung über den Versicherungsstatus zu erhalten. Weitere Informationen zum Erstellen einer EventBridge Regel finden Sie unter Regel erstellen im EventBridge Amazon-Benutzerhandbuch.

Darüber hinaus können Sie mithilfe des folgenden Beispiel-Benachrichtigungsschemas ein benutzerdefiniertes Ereignismuster erstellen. Achten Sie darauf, die Werte für Ihr Konto zu ersetzen. Um benachrichtigt zu werden, wenn sich der Abdeckungsstatus Ihres ECS Amazon-Clusters von `Healthy` zu ändert`Unhealthy`, `detail-type` sollten Sie *`GuardDuty Runtime Protection Unhealthy`*. Um benachrichtigt zu werden, wenn sich der Versicherungsstatus von `Unhealthy`

zu ändert`Healthy`, ersetzen Sie den Wert von `detail-type` durch *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS-Konto ID",
  "time": "event timestamp (string)",
  "region": "AWS-Region",
  "resources": [
      ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
            "issues":[],
            "managementType":""
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Fehlerbehebung bei Abdeckungsproblemen

Wenn der Abdeckungsstatus Ihres ECS Amazon-Clusters fehlerhaft ist, können Sie den Grund in der Spalte Problem einsehen.

Die folgende Tabelle enthält die empfohlenen Schritte zur Fehlerbehebung bei Problemen mit Fargate (ECSnur Amazon). Informationen zu Problemen mit der Abdeckung von EC2 Amazon-Instances finden Sie unter Fehlerbehebung bei Abdeckungsproblemen Für EC2 Amazon-Instances.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
Der Agent meldet sich nicht	Der Agent meldet sich nicht für Aufgaben in `TaskDefinition - '`*`TASK_DEFINITION`*`'`	Stellen Sie sicher, dass der VPC Endpunkt für die Aufgabe Ihres ECS Amazon-Clusters korrekt konfiguriert ist. Weitere Informationen finden Sie unter Wie überprüfe ich, ob die VPC Endpunktkonfiguration korrekt ist?. Wenn Ihre Organisation über eine Richtlinie zur Servicekontrolle (SCP) verfügt, überprüfen Sie, ob die Zugriffsr echte nicht durch die Grenze der `guardduty:SendSecurityTelem etry` Berechtigungen eingeschränkt werden. Weitere Informationen finden Sie unter Validierung der Service-C ontrol-Richtlinie Ihres Unternehmens.
	`VPC_ISSUE` `; for task in TaskDefin ition - '` *`TASK_DEFI NITION`*` '`	Die VPC Problemdetails finden Sie in den zusätzlichen Informationen.
Der Agent wurde beendet	ExitCode: `EXIT_CODE` für Aufgaben in `TaskDefinition - '`*`TASK_DEFINITION`*`'`	Die Problemdetails finden Sie in den zusätzlichen Informationen.
	Grund: *`REASON`* für Aufgaben in `TaskDefin`	

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
	`ition - ' TASK_DEFI NITION '`	
	ExitCode: `EXIT_CODE` mit Grund: '*EXIT_CODE* 'für Aufgaben in `TaskDefinition - '`*TASK_DEFINITION* '	
	Der Agent wurde beendet: `GrundCannotPul lContainerError` : Das Abrufen des Image-Manifests wurde erneut versucht...	Die Aufgabenausführungsrolle muss über die folgenden Amazon Elastic Container Registry (AmazonECR) - Berechtigungen verfügen: `... "ecr:GetAuthorizat ionToken", "ecr:BatchCheckLay erAvailability", "ecr:GetDownloadUr lForLayer", "ecr:BatchGetImage", ...` Weitere Informationen finden Sie unter Geben Sie ECR Berechtigungen und Subnetzdetails an. Nachdem Sie die ECR Amazon-Be rechtigungen hinzugefügt haben, müssen Sie die Aufgabe neu starten. Wenn das Problem weiterhin besteht, finden Sie weitere Informationen unterMein AWS Step Functions Workflow schlägt unerwartet fehl.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
VPCDie Endpunkte rstellung ist fehlgesch lagen	Für die Aktivierung von privat DNS sind beide erforderlich `enableDns Support` und die `enableDnsHostnames` VPC Attribute müssen auf `true` for gesetzt sein *`vpcId`* (Dienst:ECS, Statuscod e: 400, Anforderu ngs-ID: *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Stellen Sie sicher, dass die folgenden VPC Attribute auf `true` — `enableDns Support` und `enableDns Hostnames` gesetzt sind. Weitere Informationen finden Sie unter DNSAttribute in Ihrem VPC. Wenn Sie Amazon VPC Console unter verwenden, https://console.aws.amazon .com/vpc/um Amazon zu erstellen, stellen Sie sicherVPC, dass Sie sowohl DNSHostnamen aktivieren als auch DNSAuflösung aktivieren auswählen. Weitere Informationen finden Sie unter VPCKonfigurationsoptionen.
Der Agent wurde nicht bereitgestellt	Der Aufruf von *`SERVICE`* for Task (n) in wird nicht unterstützt `TaskDefin ition - '` *`TASK_DEFI NITION`* `'`	Diese Aufgabe wurde von einem aufgerufen*`SERVICE`*, der nicht unterstüt zt wird.
	Nicht unterstützte Architektur 'CPU*`TYPE`*'für Aufgabe (n) in `TaskDefinition - '`*`TASK_DEFINITION`* `'`	Diese Aufgabe wird auf einer nicht unterstützten CPU Architektur ausgeführ t. Hinweise zu unterstützten CPU Architekturen finden Sie unter. Validieru ng der architektonischen Anforderungen
	`TaskExecu tionRole` fehlt bei `TaskDefinition - '`*`TASK_DEFINITION`* `'`	Die Rolle zur ECS Aufgabenausführung fehlt. Informationen zur Bereitstellung der Aufgabenausführungsrolle und der erforderlichen Berechtigungen finden Sie unterGeben Sie ECR Berechtig ungen und Subnetzdetails an.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
	Fehlende Netzwerkk onfiguration *CONFIGURA TION_DETAILS* " für Aufgabe (n) in `TaskDefinition - '`*TASK_DEFINITION* `'`	Probleme mit der Netzwerkkonfigurat ion können aufgrund fehlender VPC Konfiguration oder fehlender oder leerer Subnetze auftreten. Stellen Sie sicher, dass Ihre Netzwerkk onfiguration korrekt ist. Weitere Informati onen finden Sie unter Geben Sie ECR Berechtigungen und Subnetzdetails an. Weitere Informationen finden Sie unter ECSAmazon-Aufgabendefinitio nsparametern im Amazon Elastic Container Service Developer Guide.

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
Weitere	Unbekanntes Problem, für Aufgaben in `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Ermitteln Sie anhand der folgenden Fragen die Ursache des Problems: • Wurde die Aufgabe gestartet, bevor Sie Runtime Monitoring aktiviert haben? In Amazon sind ECS die Aufgaben unveränderlich. Um das Laufzeitv erhalten einer laufenden Fargate-Aufgabe zu beurteilen, stellen Sie sicher, dass Runtime Monitoring bereits aktiviert ist, und starten Sie dann die Aufgabe neu, GuardDuty um den Container-Sidecar hinzuzufügen. • Ist diese Aufgabe Teil einer Servicebe reitstellung, die gestartet wurde, bevor Sie Runtime Monitoring aktiviert haben? Falls ja, können Sie den Dienst entweder neu starten oder den Dienst mit aktualisieren, `forceNewD eployment` indem Sie die Schritte unter Dienst aktualisieren ausführen. Sie können auch UpdateServiceoder verwenden AWS CLI. • Wurde die Aufgabe gestartet, nachdem der ECS Cluster von Runtime Monitoring ausgeschlossen wurde? Wenn Sie das vordefinierte GuardDuty Tag von `GuardDuty`

Art des Problems	Zusatzinformation	Empfohlene Schritte zur Fehlerbeh ebung
		`Managed` - in - `true` ändern`false`, GuardDuty werden die Runtime-E reignisse für den ECS Cluster nicht empfangen. `GuardDutyManaged` • Enthält Ihr Service eine Aufgabe, die das alte Format von `taskArn` hat? GuardDuty Runtime Monitoring unterstützt die Abdeckung von Aufgaben nicht, die das alte Format von haben`taskArn`. Informationen zu Amazon Resource Names (ARNs) für ECS Amazon-Re ssourcen finden Sie unter Amazon Resource Names (ARNs) und IDs.

Abdeckung für EKS Amazon-Cluster

Nachdem Sie Runtime Monitoring aktiviert und den GuardDuty Security Agent (Add-on) EKS entweder manuell oder über die automatische Agentenkonfiguration installiert haben, können Sie mit der Bewertung der Abdeckung für Ihre EKS Cluster beginnen.

Inhalt

Überprüfen der Abdeckungsstatistiken

Die Abdeckungsstatistik für die EKS Cluster, die Ihren eigenen Konten oder Ihren Mitgliedskonten zugeordnet sind, gibt den Prozentsatz der fehlerfreien EKS Cluster an allen EKS Clustern in den ausgewählten Clustern an AWS-Region. Die folgende Gleichung stellt dies wie folgt dar:

(Fehlerfreie Cluster/Alle Cluster)*100

Wählen Sie eine der Zugriffsmethoden, um die Abdeckungsstatistiken für Ihre Konten einzusehen.

Console

- Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
- Wählen Sie im Navigationsbereich Runtime Monitoring aus.
- Wählen Sie die Registerkarte Runtime Coverage des EKS Clusters aus.
- Auf der Registerkarte EKSCluster-Laufzeitabdeckung können Sie die Coverage-Statistiken einsehen, die nach dem Coverage-Status aggregiert sind, der in der Cluster-Listentabelle verfügbar ist.
  - Sie können die Tabelle mit der Cluster-Liste nach den folgenden Spalten filtern:
    - Cluster name
    - Konto-ID
    - Agentenverwaltungs-Typ
    - Abdeckungsstatus
    - Add-On-Version
- Wenn einer Ihrer EKS Cluster den Deckungsstatus „Ungesund“ hat, kann die Spalte „Problem“ zusätzliche Informationen über den Grund für den Status „Fehlerhaft“ enthalten.

API/CLI

- Führen Sie den ListCoverageAPImit Ihrer eigenen gültigen Melder-ID, Region und Service-Endpunkt aus. Sie können die Clusterliste damit filtern und sortierenAPI.
  - Sie können das Beispiel `filter-criteria` ändern mit einer der folgenden Optionen für `CriterionKey`:
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `ADDON_VERSION`
    - `MANAGEMENT_TYPE`

- Sie können das Beispiel `AttributeName` in `sort-criteria` ändern mit einer der folgenden Optionen:
  - `ACCOUNT_ID`
  - `CLUSTER_NAME`
  - `COVERAGE_STATUS`
  - `ISSUE`
  - `ADDON_VERSION`
  - `UPDATED_AT`
- Sie können das ändern *`max-results`* (bis zu 50).
- Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Führen Sie den aus GetCoverageStatisticsAPI, um aggregierte Statistiken zur Abdeckung abzurufen, die `statisticsType` auf dem basieren.
  - Sie können das Beispiel `statisticsType` zu einer der folgenden Optionen ändern:
    - `COUNT_BY_COVERAGE_STATUS`— Stellt Deckungsstatistiken für EKS Cluster dar, die nach dem Deckungsstatus aggregiert sind.
    - `COUNT_BY_RESOURCE_TYPE`— Deckungsstatistiken, die auf der Grundlage des AWS Ressourcentyps in der Liste aggregiert wurden.
    - Sie können das Beispiel `filter-criteria` im Befehl ändern. Sie können die folgenden Optionen für `CriterionKey` verwenden:
      - `ACCOUNT_ID`
      - `CLUSTER_NAME`
      - `RESOURCE_TYPE`
      - `COVERAGE_STATUS`
      - `ADDON_VERSION`
      - `MANAGEMENT_TYPE`

- Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Wenn der Abdeckungsstatus Ihres EKS Clusters fehlerhaft ist, finden Sie weitere Informationen unterBehebung von Problemen mit dem EKS Versicherungsschutz.

Benachrichtigungen über Änderungen des Abdeckungsstatus konfigurieren

Der Abdeckungsstatus eines EKS Clusters in Ihrem Konto wird möglicherweise als Ungesund angezeigt. Um zu erkennen, wann der Abdeckungsstatus Fehlerhaft wird, empfehlen wir Ihnen, den Abdeckungsstatus regelmäßig zu überwachen und Fehler zu beheben, falls der Status Fehlerhaft ist. Alternativ können Sie eine EventBridge Amazon-Regel erstellen, die Sie benachrichtigt, wenn sich der Deckungsstatus von einem `Unhealthy` auf `Healthy` oder einem anderen Wert ändert. GuardDuty Veröffentlicht dies standardmäßig im EventBridgeBus für Ihr Konto.

Beispiel für ein Benachrichtigungsschema

In einer EventBridge Regel können Sie die vordefinierten Beispielereignisse und Ereignismuster verwenden, um eine Benachrichtigung über den Versicherungsstatus zu erhalten. Weitere Informationen zum Erstellen einer EventBridge Regel finden Sie unter Regel erstellen im EventBridge Amazon-Benutzerhandbuch.

Darüber hinaus können Sie mithilfe des folgenden Beispiel-Benachrichtigungsschemas ein benutzerdefiniertes Ereignismuster erstellen. Achten Sie darauf, die Werte für Ihr Konto zu ersetzen. Um benachrichtigt zu werden, wenn sich der Abdeckungsstatus Ihres EKS Amazon-Clusters von `Healthy` zu ändertUnhealthy, `detail-type` sollten Sie *`GuardDuty Runtime Protection Unhealthy`*. Um benachrichtigt zu werden, wenn sich der Versicherungsstatus von `Unhealthy` zu ändert`Healthy`, ersetzen Sie den Wert von `detail-type` durch *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
```

```
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "AWS-Konto ID",
  "time": "event timestamp (string)",
  "region": "AWS-Region",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EKS",
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Behebung von Problemen mit dem EKS Versicherungsschutz

Wenn der Abdeckungsstatus für Ihren EKS Cluster lautet`Unhealthy`, können Sie den entsprechenden Fehler entweder in der Spalte Problem in der GuardDuty Konsole oder mithilfe des CoverageResourceDatentyps anzeigen.

Wenn Sie mit Ein- oder Ausschluss-Tags arbeiten, um Ihre EKS Cluster selektiv zu überwachen, kann es einige Zeit dauern, bis die Tags synchronisiert sind. Dies kann sich auf den Abdeckungsstatus des zugehörigen EKS Clusters auswirken. Sie können erneut versuchen, das entsprechende Tag (Einschluss oder Ausschluss) zu entfernen und hinzuzufügen. Weitere Informationen finden Sie unter Taggen Ihrer EKS Amazon-Ressourcen im EKSAmazon-Benutzerhandbuch.

Die Struktur eines Abdeckungsproblems ist `Issue type:Extra information`. In der Regel verfügen die Probleme über optionale Zusatzinformationen, die eine spezifische Ausnahme oder eine Beschreibung des Problems enthalten können. Basierend auf zusätzlichen Informationen enthalten

die folgenden Tabellen die empfohlenen Schritte zur Behebung von Problemen mit der Abdeckung Ihrer EKS Cluster.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Die Erstellung des Addons ist fehlgeschlagen	Das Addon `aws-guardduty-agent` ist mit der aktuellen Clusterversion des Clusters nicht kompatibel *`ClusterName`* . Das angegebene Addon wird nicht unterstützt.	Stellen Sie sicher, dass Sie eine der Kubernetes-Versionen verwenden, die die Bereitstellung des Add-ons unterstützen. `aws-guardduty-agent` EKS Weitere Informationen finden Sie unter Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty . Informationen zur Aktualisierung Ihrer Kubernetes-Version finden Sie unter Aktualisieren einer EKS Amazon-Cluster-Kubernetes-Version.
Die Erstellung des Addons ist fehlgeschlagen Die Aktualisierung des Addons ist fehlgeschlagen Der Status des Addons ist fehlerhaft	EKSProblem mit dem Addon -: `AddonIssueCode` `AddonIssueMessage`	Informationen zu empfohlenen Schritten für einen bestimmten Problemcode eines Add-ons finden Sie unterTroubleshooting steps for Addon creation/updatation error with Addon issue code. Eine Liste der Addon-Problemcodes, die bei

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
		diesem Problem auftreten können, finden Sie unter AddonIssue.
VPCDie Endpunkterstellung ist fehlgeschlagen	VPCDie Erstellung von Endpunkten wird für Shared nicht unterstützt VPC *vpcId*	Runtime Monitoring unterstützt jetzt die Verwendung eines VPC innerhalb einer Organisation gemeinsam genutzten Geräts. Stellen Sie sicher, dass Ihre Konten alle Voraussetzungen erfüllen. Weitere Informationen finden Sie unter Voraussetzungen für die Nutzung von Shared VPC.
	Nur bei Verwendung von Shared VPC mit automatisierter Agentenkonfiguration Konto-ID des Besitzers *111122223333* zur gemeinsamen Nutzung VPC *vpcId* hat weder Runtime Monitoring noch automatische Agentenkonfiguration oder beides aktiviert.	Das gemeinsame VPC Besitzerkonto muss Runtime Monitoring und automatische Agentenkonfiguration für mindestens einen Ressourcentyp (Amazon EKS oder Amazon ECS (AWS Fargate)) aktivieren. Weitere Informationen finden Sie unter Spezifische Voraussetzungen für GuardDuty Runtime Monitoring.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
	Für die Aktivierung von privat DNS sind beide erforderlich `enableDnsSupport` und die `enableDnsHostnames` VPC Attribute müssen auf „`true`for“ gesetzt sein *`vpcId`* (Dienst: Ec2, Statuscode: 400, Anforderungs-ID: *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Stellen Sie sicher, dass die folgenden VPC Attribute auf `true` — `enableDnsSupport` und gesetzt sind. `enableDnsHostnames` Weitere Informationen finden Sie unter DNSAttribute in Ihrem VPC. Wenn Sie Amazon VPC Console unter verwenden, https://console.aws.amazon.com/vpc/um Amazon zu erstellen, stellen Sie sicherVPC, dass Sie sowohl DNSHostnamen aktivieren als auch DNSAuflösung aktivieren auswählen. Weitere Informationen finden Sie unter VPCKonfigurationsoptionen.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Das Löschen des gemeinsamen VPC Endpunkts ist fehlgeschlagen	Das Löschen eines gemeinsamen VPC Endpunkts ist für die Konto-ID nicht zulässig *111122223333* , geteilt VPC *vpcId*, Konto-ID des Besitzers *555555555555* .	Mögliche Schritte: • Die Deaktivierung des Runtime Monitoring-Status des gemeinsamen VPC Teilnehmerkontos hat keine Auswirkungen auf die Richtlinie für gemeinsame VPC Endgeräte und die Sicherheitsgruppe, die im Besitzerkonto vorhanden ist. Um den gemeinsamen VPC Endpunkt und die Sicherheitsgruppe zu löschen, müssen Sie Runtime Monitoring oder den Status der automatisierten Agentenkonfiguration im gemeinsamen VPC Besitzerkonto deaktivieren. • Das gemeinsame VPC Teilnehmerkonto kann den gemeinsamen VPC Endpunkt und die Sicherheitsgruppe, die im gemeinsamen VPC Besitzerkonto gehostet werden, nicht löschen.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
Lokale EKS Cluster	EKSAddons werden auf lokalen Outpost-Clustern nicht unterstützt.	Nicht umsetzbar. Weitere Informationen finden Sie EKSauf Amazon on AWS Outposts.
EKSDie Genehmigung zur Aktivierung von Runtime Monitoring wurde nicht erteilt	(kann zusätzliche Informationen anzeigen oder auch nicht)	1. Wenn die zusätzlichen Informationen für dieses Problem verfügbar sind, beheben Sie die Ursache und folgen Sie dem nächsten Schritt. 2. Schalten Sie EKS Runtime Monitoring ein, um es auszuschalten und dann wieder einzuschalten. Stellen Sie sicher, dass der GuardDuty Agent ebenfalls bereitgestellt wird, entweder automatisch GuardDuty oder manuell.

Art des Problems (Präfix)	Zusatzinformation	Empfohlene Schritte zur Fehlerbehebung
EKSDie Bereitstellung der Ressourcen zur Aktivierung der Runtime Monitoring ist im Gange	(zeigt möglicherweise zusätzliche Informationen an oder auch nicht)	Nicht umsetzbar. Nachdem Sie EKS Runtime Monitoring aktiviert haben, bleibt der Deckungsstatus möglicherweise bestehen, `Unhealthy` bis der Schritt zur Ressource nbereitstellung abgeschlo ssen ist. Der Abdeckung sstatus wird regelmäßig überwacht und aktualisi ert.
Andere (jedes andere Problem)	Fehler aufgrund eines Autorisierungsfehlers	Schalten Sie EKS Runtime Monitoring um, um es auszuschalten und dann wieder einuscha lten. Stellen Sie sicher, dass der GuardDuty Agent ebenfalls bereitges tellt wird, entweder automatisch GuardDuty oder manuell.

Fehler bei der Erstellung oder Aktualisierung des Addons	Fehlerbehebungsschritte
EKSAddon-Problem -`InsufficientNumber OfReplicas` : Das Add-on ist fehlerhaft, da	• Mithilfe der Problemmeldung können Sie die Ursache identifizieren und beheben. Sie

Fehler bei der Erstellung oder Aktualisierung des Addons	Fehlerbehebungsschritte
es nicht die gewünschte Anzahl von Replikaten hat.	können damit beginnen, Ihren Cluster zu beschreiben. Verwenden Sie dies beispiels weise, `kubectl describe pods`um die Hauptursache für den Pod-Ausfall zu ermitteln. Nachdem Sie die Ursache behoben haben, wiederholen Sie den Schritt (Erstellung oder Aktualisierung des Add-ons). • Wenn das Problem weiterhin besteht, überprüfen Sie, ob der VPC Endpunkt für Ihren EKS Amazon-Cluster korrekt konfiguri ert ist. Weitere Informationen finden Sie unter Wie überprüfe ich, ob die VPC Endpunktk onfiguration korrekt ist?.
EKSAddon-Problem —`Admission RequestDenied` : Der Zulassungs-Webhook `"validate.kyverno.svc-fail"` hat die Anfrage abgelehnt: Richtlinie `DaemonSet /amazon-guardduty/aws-guard duty-agent` wegen Ressourcenverletzu ng:::... restrict-image-registries `autogen-v alidate-registries`	1. Amazon EKS Cluster oder der Sicherhei tsadministrator müssen die Sicherheitsrichtli nie überprüfen, die das Addon-Update blockiert. 2. Sie müssen entweder den Controller (webhook) deaktivieren oder den Controlle r die Anfragen von Amazon annehmen lassenEKS.

Fehler bei der Erstellung oder Aktualisierung des Addons	Fehlerbehebungsschritte
EKSZusatzproblem —`ConfigurationConflict` : Beim Versuch, sich zu bewerben, wurden Konflikte festgestellt. Wird aufgrund des Konfliktlösungsmodus nicht fortgesetzt. `Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image`	Wenn Sie das Addon erstellen oder aktualisieren, geben Sie das `OVERWRITE` Konfliktlösungskennzeichen an. Dadurch werden möglicherweise alle Änderungen überschrieben, die mithilfe von Kubernetes direkt an den zugehörigen Ressourcen in Kubernetes vorgenommen wurden. API Sie können das Addon zuerst löschen und dann erneut installieren.

Fehler bei der Erstellung oder Aktualisierung des Addons	Fehlerbehebungsschritte

EKSProblem mit dem Addon - `AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope`	Sie müssen die fehlende Berechtigung `eks:addon-cluster-admin ClusterRoleBinding` manuell hinzufügen. Fügen Sie Folgendes `yaml` hinzu`eks:addon-cluster-admin` :
	
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`
	`metadata:`
	`  name: eks:addon-cluster-admin`
	`subjects:`
	`- kind: User`
	`  name: eks:addon-manager`
	`  apiGroup: rbac.authorization.k8s.io`
	`roleRef:`
	`  kind: ClusterRole`
	`  name: cluster-admin`
	`  apiGroup: rbac.authorization.k8s.io`
	`---`
	
	Sie können dies jetzt mit `yaml` dem folgenden Befehl auf Ihren EKS Amazon-Cluster anwenden:
	
	`kubectl apply -f eks-addon-cluster-admin.yaml`

Fehler bei der Erstellung oder Aktualisierung des Addons	Fehlerbehebungsschritte
EKSProblem mit dem Add-on - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	Sie müssen entweder den Controller deaktivieren oder den Controller die Anfragen vom EKS Amazon-Cluster annehmen lassen. Bevor Sie das Add-on erstellen oder aktualisieren, können Sie auch einen GuardDuty Namespace erstellen und ihn als `owner` kennzeichnen.

Häufig gestellte Fragen () FAQs

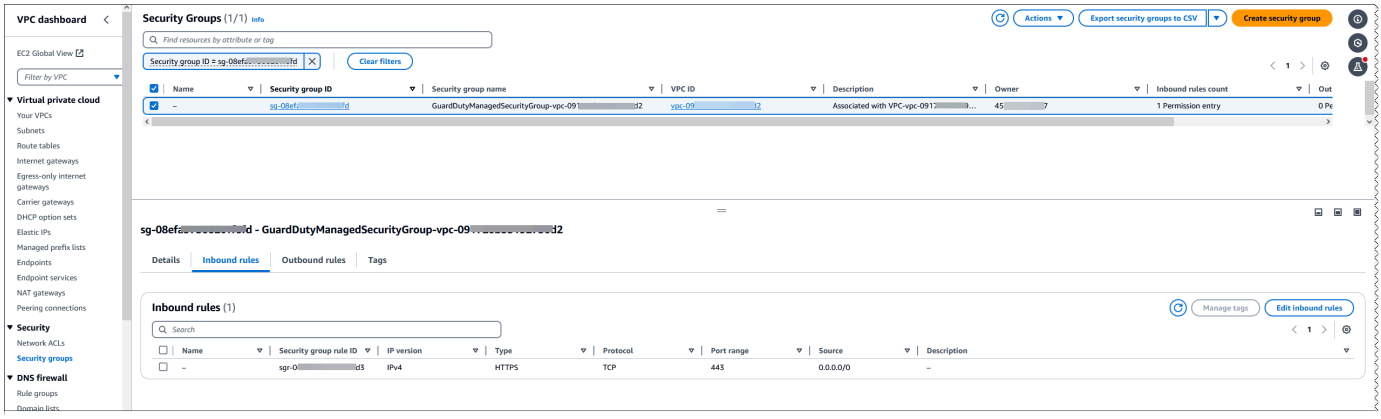
Inhalt

Wie überprüfe ich, ob die VPC Endpunktkonfiguration korrekt ist?

Gehen Sie wie folgt vor, um zu überprüfen, ob die VPC Endpunktkonfiguration für Ihren Ressourcentyp im VPC Besitzerkonto korrekt eingerichtet ist:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die VPC Amazon-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsmenü unter Virtual Private Cloud die Option Endpunkte.
3. Wählen Sie in der Tabelle Endpoints die Zeile mit dem Servicenamen aus, der com.amazonaws ähnelt.***us-east-1***.guardduty-data. Die Region (`us-east-1`) kann für Ihren Endpunkt unterschiedlich sein.

4. Ein Fenster mit Endpunktdetails wird angezeigt. Wählen Sie auf der Registerkarte Sicherheitsgruppen den zugehörigen Gruppen-ID-Link aus, um weitere Informationen zu erhalten.
5. Wählen Sie in der Tabelle Sicherheitsgruppen die Zeile mit der zugehörigen Sicherheitsgruppen-ID aus, um die Details anzuzeigen.
6. Stellen Sie auf der Registerkarte Regeln für eingehenden Datenverkehr sicher, dass es eine Eingangsrichtlinie mit dem Portbereich 443 und der Quelle mit 0.0.0.0/0 gibt. Regeln für eingehenden Datenverkehr steuern den eingehenden Datenverkehr, der die Instance erreichen darf. Die folgende Abbildung zeigt die Regeln für eingehende Nachrichten für eine Sicherheitsgruppe, die mit der vom GuardDuty Security VPC Agent verwendeten verknüpft ist.



Wenn Sie noch keine Sicherheitsgruppe haben, für die ein eingehender Port 443 aktiviert ist, erstellen Sie im EC2Amazon-Benutzerhandbuch eine Sicherheitsgruppe.

Wenn bei der Einschränkung der eingehenden Zugriffsberechtigungen für Sie VPC (oder Ihren Cluster) ein Problem auftritt, stellen Sie die Unterstützung für den eingehenden Port 443 von einer beliebigen IP-Adresse (0.0.0.0/0) aus bereit.

Warum ist der Abdeckungsstatus für meine Ressource? **`Unhealthy`**

Wenn Sie den GuardDuty Security Agent gerade installiert haben (entweder durch automatische Agentenkonfiguration oder manuell) oder die empfohlenen Schritte zur Behebung eines Deckungsproblems befolgt haben, kann es einige Minuten dauern, bis der Schutzstatus wieder fehlerfrei ist. Sie können den Deckungsstatus entweder regelmäßig überprüfen oder Amazon EventBridge (EventBridge) so konfigurieren, dass Sie eine Benachrichtigung erhalten, wenn sich der Deckungsstatus ändert.

Darüber hinaus können Sie überprüfen, ob die VPC Endpunktkonfiguration für Ihre Ressource korrekt ist. Weitere Informationen finden Sie unter Wie überprüfe ich, ob die VPC Endpunktkonfiguration korrekt ist?.

Wer kann den Runtime-Coverage-Status für eine Ressource einsehen, die mir gehört AWS-Konto?

Als Mitgliedskonto oder eigenständiges Konto können Sie die Deckungsstatistiken der Ressourcen einsehen, die Ihren eigenen Konten zugeordnet sind. Als delegiertes GuardDuty Administratorkonto einer Organisation können Sie die Deckungsstatistiken für die mit Ihrem Konto verknüpften Ressourcen und die Mitgliedskonten, die zu Ihrer Organisation gehören, einsehen.

Wie kann ich überprüfen, ob der GuardDuty Security Agent auf einer Fargate-Aufgabe ausgeführt wird?

Der GuardDuty Security Agent läuft als Sidecar-Container für die Fargate-Aufgaben.

Wählen Sie eine bevorzugte Methode, um zu überprüfen, ob der Sidecar-Container angezeigt wird, während die Task ausgeführt wird.

Amazon ECS console

1. Öffnen Sie die Konsole auf Version 2. https://console.aws.amazon.com/ecs/
2. Klicken Sie im Navigationsbereich auf Cluster.
3. Wählen Sie auf der Seite Cluster den zugehörigen Clusternamen aus, um weitere Informationen zu erhalten.
4. Wählen Sie die Registerkarte Tasks aus.
5. Wählen Sie den Link zur zugehörigen Aufgabe aus, um die Aufgabendetails anzuzeigen.
6. Auf der Seite mit den Aufgabendetails enthält die Tabelle Container die Sidecar-Details. Der Container-Runtime-ID wird das Präfix Ihrer Task-ID zugewiesen.

CLI

Führen Sie den Vorgang aus `describe-tasks` und suchen Sie nach dem Container, dessen Name auf `aws-gd-agent` und der Wert auf lastStatusgesetzt ist`RUNNING`.

Das folgende Beispiel zeigt die Ausgabe für den Standardcluster für Aufgaben `aws:ecs:`*`us-east-1`*`:`*`123456789012`*`:`*`task/0b69d5c0-d655-4695-98cd-5d2d5EXAMPLE`*

Output

Der angegebene Container aws-gd-agentbefindet sich im RUNNING Status.

```
"containers": [
      {
        "containerArn": "arn:aws:ecs:us-east-1:123456789012:container/4df26bb4-
f057-467b-a079-96167EXAMPLE",
        "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/0b69d5c0-
d655-4695-98cd-5d2d5EXAMPLE",
        "lastStatus": "RUNNING",
        "healthStatus": "UNKNOWN",
        "memory": "1 GB",
        "name": "aws-gd-agent"
      }
    ]
```

Weitere Informationen finden Sie unter describe-tasks.

Weitere Fragen zur Fehlerbehebung

Weitere Fragen zur Fehlerbehebung in Bezug auf Ihre Fargate-Aufgaben finden Sie unter Runtime Monitoring Troubleshooting FAQs im Amazon Elastic Container Service Developer Guide.

Einrichtung CPU und Speicherüberwachung

Nachdem Sie Runtime Monitoring aktiviert und festgestellt haben, dass der Abdeckungsstatus Ihres Clusters fehlerfrei ist, können Sie die Insight-Metriken einrichten und einsehen.

Anhand der folgenden Themen können Sie beurteilen, wie der bereitgestellte Agent im Vergleich zu den CPU Speicherlimits für den GuardDuty Agenten abschneidet.

Überwachung auf ECS Amazon-Cluster einrichten

Mithilfe der folgenden Schritte aus dem CloudWatch Amazon-Benutzerhandbuch können Sie beurteilen, wie der bereitgestellte Agent im Vergleich zu den CPU Speicherlimits für den GuardDuty Agenten abschneidet:

1. Einrichtung von Container Insights auf Amazon ECS für Metriken auf Cluster- und Serviceebene
2. Amazon ECS Container Insights-Metriken

Überwachung auf EKS Amazon-Cluster einrichten

Nachdem der GuardDuty Security Agent bereitgestellt wurde und Sie festgestellt haben, dass der Schutzstatus Ihres Clusters fehlerfrei ist, können Sie die Container Insight-Metriken einrichten und anzeigen.

Bewerten Sie die Leistung des Security Agents

1. Einrichtung von Container Insights auf Amazon EKS und Kubernetes im Amazon-Benutzerhandbuch CloudWatch
2. Amazon EKS - und Kubernetes Container Insights-Metriken im Amazon-Benutzerhandbuch CloudWatch

Verwalten Sie die Leistung mit dem Security Agent v1.5.0 und höher

Bei Security Agent v1.5.0 und höher können Sie bestimmte Parameter konfigurieren, wenn die Erkenntnisse darauf hindeuten, dass der zugehörige GuardDuty Agent die zugewiesenen Grenzwerte erreicht. Weitere Informationen finden Sie unter Konfigurieren Sie die EKS Zusatzparameter.

Gesammelte Runtime-Ereignistypen, die verwendet GuardDuty

Der GuardDuty Security Agent sammelt die folgenden Ereignistypen und sendet sie zur Erkennung und Analyse von Bedrohungen an das GuardDuty Backend. GuardDuty macht Ihnen diese Ereignisse nicht zugänglich. Wenn eine potenzielle Bedrohung GuardDuty erkannt und ein Runtime Monitoring-Ergebnis generiert wird, können Sie die entsprechenden Ergebnisdetails einsehen. Weitere Hinweise zur GuardDuty Verwendung der gesammelten Ereignistypen finden Sie unterAbmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung.

Ereignisse verarbeiten

Feldname	Beschreibung
Prozessname	Name des beobachteten Prozesses.
Prozesspfad	Absoluter Pfad der ausführbaren Datei des Prozesses.

Feldname	Beschreibung
Prozess-ID	Die ID, die dem Prozess vom Betriebssystem zugewiesen wurde.
Namespace PID	Die Prozess-ID des Prozesses in einem anderen sekundären PID Namespace als dem Namespace auf HostebenePID. Bei Prozessen innerhalb eines Containers ist dies die Prozess-ID, die innerhalb des Containers beobachtet wird.
Prozess-Benutzer-ID	Die eindeutige ID des Benutzers, der den Prozess ausgeführt hat.
Prozess UUID	Die eindeutige ID, die dem Prozess von zugewiesen wurde GuardDuty.
Prozess GID	Prozess-ID der Prozessgruppe.
Prozess EGID	Effektive Gruppen-ID der Prozessgruppe.
Prozess EUID	Effektive Benutzer-ID des Prozesses.
Prozess-Benutzername	Der Benutzername, der den Prozess ausgeführ t hat.
Prozesses-Startzeit	Die Zeit, zu der der Prozess erstellt wurde. Dieses Feld hat das Format einer UTC Datumszeichenfolge (`2023-03-22T19:37:2 0.168Z`).
Ausführbarer Prozess SHA -256	Der Hash `SHA256` der ausführbaren Prozesses datei.
Prozess-Skriptpfad	Pfad der Skriptdatei, die ausgeführt wurde.

Feldname	Beschreibung
Prozess-Umgebungsvariable	Die Umgebungsvariable, die dem Prozess zur Verfügung gestellt wurde. Nur `LD_PRELOAD` und `LD_LIBRARY_PATH` werden gesammelt.
Verarbeiten Sie das aktuelle Arbeitsverzeichnis () PWD	Derzeitiges Arbeitsverzeichnis des Prozesses.
Übergeordneter Prozess	Prozessdetails des übergeordneten Prozesses . Ein übergeordneter Prozess ist ein Prozess, der den beobachteten Prozess erzeugt hat.
Befehlszeilenargumente Derzeit ist dieses Feld auf bestimmte Agentenversionen beschränkt, die dem Ressourcentyp entsprechen: • Fargate (ECSnur Amazon) mit GuardDuty Security Agent v1.0.0 und höher. • EC2Amazon-Instances mit GuardDuty Security Agent v1.0.0 und höher. • EKSAmazon-Cluster mit Security Agent v1.4.0 und höher. Weitere Informationen finden Sie unter GuardDuty Versionsverlauf des Agenten.	Befehlszeilenargumente, die zum Zeitpunkt der Prozessausführung bereitgestellt wurden. Dieses Feld kann vertrauliche Kundendaten enthalten.

Container-Ereignisse

Feldname	Beschreibung
Container-Name	Name des Containers.

Feldname	Beschreibung
	Falls verfügbar, zeigt dieses Feld den Wert des Labels `io.kubenetes.container.name` an.
Behälter UID	Die eindeutige ID des Containers, die von der Container-Laufzeit zugewiesen wurde.
Container-Laufzeit	Die Container-Laufzeit (wie z. B. `docker` oder `containerd`), die zum Ausführen des Containers verwendet wurde.
Container-Image-ID	Die ID des Container-Images.
Container-Image-Name	Name des Container-Images.

AWS Fargate (ECSnur Amazon) Aufgabenereignisse

Feldname	Beschreibung
Amazon-Ressourcenname der Aufgabe (ARN)	Die ARN der Aufgabe.
Cluster-Name	Der Name des ECS Amazon-Clusters.
Familienname	Der Familienname der Aufgabendefinition. Der `family` wird als Name für die Aufgabendefinition verwendet, mit der die Aufgabe gestartet wird.
Service-Name	Der Name des ECS Amazon-Dienstes, wenn die Aufgabe als Teil eines Dienstes gestartet wurde.
Starttyp	Die Infrastruktur, auf der Ihre Aufgabe ausgeführt wird. Für Runtime Monitoring mit dem Ressourcentyp as `ECSCluster` könnte der Starttyp entweder `EC2` oder sein`FARGATE`.
CPU	Die Anzahl der von der Aufgabe verwendeten CPU Einheiten, wie in der Aufgabendefinition angegeben.

Kubernetes-Pod-Ereignisse

Feldname	Beschreibung
Pod-ID	Die ID des Kubernetes-Pods.
Pod-Name	Name des Kubernetes-Pods.
Pod-Namespace	Name des Kubernetes-Namespace, zu dem der Kubernetes-Workload gehört.
Kubernetes-Cluster-Name	Name des Kubernetes-Clusters.

DNSEreignisse

Feldname	Beschreibung
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. Beispiel, `SOCK_RAW`.
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IP-v4-Protokoll verwendet.
Richtungs-ID	Die ID der Verbindungsrichtung.
Protokollnummer	Die Layer-4-Protokollnummer, z. B. 17 für UDP und 6 fürTCP.
DNSRemote-Endpunkt-IP	Die Remote-IP-Informationen der Verbindung.
DNSPort für Remote-Endgeräte	Die Portnummer der Verbindung.
DNSLokale Endpunkt-IP	Die lokale IP der Verbindung.
DNSLokaler Endpunkt-Port	Die Portnummer der Verbindung.

Feldname	Beschreibung
DNSNutzlast	Die Nutzlast von DNS Paketen, die DNS Abfragen und Antworten enthält.

Offene Ereignisse

Feldname	Beschreibung
Dateipfad	Pfad der Datei, die in diesem Ereignis geöffnet wird.
Flags	Beschreibt den Dateizugriffsmodus, z. B. Schreibgeschützt, Nur-Schreiben und Lesen-Schreiben.

Lastmodul-Ereignis

Feldname	Beschreibung
Modulname	Name des in den Kernel geladenen Moduls.

Mprotect-Ereignisse

Feldname	Beschreibung
Adressbereiche	Der Adressbereich, für den der Zugriffsschutz geändert wurde.
Arbeitsspeicherregionen	Gibt die Region des Adressraums eines Prozesses an, z. B. Stapel und Heap.
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.

Mount-Ereignisse

Feldname	Beschreibung
Mount-Ziel	Der Pfad, in dem die Mount-Quelle gemountet ist.
Mount-Quelle	Der Pfad auf dem Host, der am Mount-Ziel gemountet ist.
Typ des Dateisystems	Stellt den Typ der bereitgestellten fileSystem Datei dar.
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.

Verknüpfungs-Ereignisse

Feldname	Beschreibung
Verknüpfungs-Pfad	Pfad, in dem der Hardlink erstellt wird.
Zielpfad	Pfad der Datei, auf die der Hardlink verweist.

Symlink-Ereignisse

Feldname	Beschreibung
Verknüpfungs-Pfad	Pfad, in dem der symbolische Link erstellt wird.
Zielpfad	Pfad der Datei, auf die der symbolische Link verweist.

Dup-Ereignisse

Feldname	Beschreibung
Alter Dateideskriptor	Ein Dateideskriptor, der ein geöffnetes Dateiobjekt darstellt.

Feldname	Beschreibung
Neuer Dateideskriptor	Ein neuer Dateideskriptor, der ein Duplikat des alten Dateidesk riptors ist. Sowohl der alte als auch der neue Dateideskriptor stehen für dasselbe offene Dateiobjekt.
DNS-Remote-Endpunkt-IP	Die Remote-IP-Adresse des Netzwerk-Sockets, dargestel lt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.
DNS-Remote-Endpunkt-Port	Die Remote-IP-Adresse des Netzwerk-Sockets, dargestel lt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.
Lokale Dup-Endpunkt-IP	Die lokale IP-Adresse des Netzwerk-Sockets, dargestellt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.
Lokaler Dup-Endpunkt-Port	Der lokale Port des Netzwerk-Sockets, dargestellt durch den alten Dateideskriptor. Gilt nur, wenn der alte Dateideskriptor einen Netzwerk-Socket darstellt.

Arbeitsspeicherzuordnungs-Ereignis

Feldname	Beschreibung
Dateipfad	Pfad der Datei, der der Arbeitsspeicher zugeordnet ist.

Socket-Ereignisse

Feldname	Beschreibung
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IP-v4-Protokoll verwendet.

Feldname	Beschreibung
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. Beispiel, `SOCK_RAW`.
Protokollnummer	Spezifiziert ein bestimmtes Protokoll innerhalb der Adressfam ilie. Normalerweise gibt es ein einziges Protokoll in Adressfam ilien. Beispielsweise hat die Adressfamilie `AF_INET` nur das IP-Protokoll.

Verbindungs-Ereignisse

Feldname	Beschreibung
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IP-v4-Protokoll verwendet.
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. Beispiel, `SOCK_RAW`.
Protokollnummer	Spezifiziert ein bestimmtes Protokoll innerhalb der Adressfam ilie. Normalerweise gibt es ein einziges Protokoll in Adressfam ilien. Beispielsweise hat die Adressfamilie `AF_INET` nur das IP-Protokoll.
Dateipfad	Pfad der Socket-Datei, falls die Adressfamilie `AF_UNIX` ist.
Remote-Endpunkt-IP	Die Remote-IP-Informationen der Verbindung.
Remote-Endpunkt-Port	Die Portnummer der Verbindung.
Lokale Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler Endpunkt-Port	Die Portnummer der Verbindung.

Prozess-VM-Readv-Ereignisse

Feldname	Beschreibung
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.
Ziel PID	Prozess-ID des Prozesses, aus dessen Arbeitsspeicher gelesen wird.
Zielprozess UUID	Die eindeutige ID des Zielprozesses.
Pfad der ausführbaren Zieldatei	Absoluter Pfad der ausführbaren Zieldatei des Prozesses.

Prozess-VM-Writev-Ereignisse

Feldname	Beschreibung
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.
Ziel PID	Prozess-ID des Prozesses, in den Arbeitsspeicher geschrieben wird.
Zielprozess UUID	Die eindeutige ID des Zielprozesses.
Pfad der ausführbaren Zieldatei	Absoluter Pfad der ausführbaren Zieldatei des Prozesses.

Ptrace-Ereignisse

Feldname	Beschreibung
Ziel PID	Prozess-ID des Zielprozesses.

Feldname	Beschreibung
Zielprozess UUID	Die eindeutige ID des Zielprozesses.
Pfad der ausführbaren Zieldatei	Absoluter Pfad der ausführbaren Zieldatei des Prozesses.
Flags	Stellt Optionen dar, die das Verhalten dieses Ereignisses steuern.

Ereignisse binden

Feldname	Beschreibung
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IP-v4-Protokoll verwendet.
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. Beispiel, `SOCK_RAW`.
Protokollnummer	Die Layer-4-Protokollnummer, z. B. 17 für UDP und 6 fürTCP.
Lokale Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler Endpunkt-Port	Die Portnummer der Verbindung.

Ereignisse abhören

Feldname	Beschreibung
Adress-Familie	Stellt das der Adresse zugeordnete Kommunikationsprotokoll dar. Die Adressfamilie `AF_INET` wird beispielsweise für das IP-v4-Protokoll verwendet.

Feldname	Beschreibung
Socket-Typ	Socket-Typ zur Angabe der Kommunikationssemantik. Beispiel, `SOCK_RAW`.
Protokollnummer	Die Layer-4-Protokollnummer, z. B. 17 für UDP und 6 fürTCP.
Lokale Endpunkt-IP	Die lokale IP der Verbindung.
Lokaler Endpunkt-Port	Die Portnummer der Verbindung.

Ereignisse umbenennen

Feldname	Beschreibung
Dateipfad	Pfad, in dem die Datei umbenannt wurde.
Ziel	Der neue Pfad der Datei.

UIDEreignisse festlegen

Feldname	Beschreibung
Neu EUID	Die neue effektive Benutzer-ID des Prozesses.
Neu UID	Die neue Benutzer-ID des Prozesses.

Chmod-Ereignisse

Feldname	Beschreibung
Dateipfad	Pfad der Datei, die dieses Ereignis auslöst.
Dateimodus	Die aktualisierten Zugriffsberechtigungen für die zugehörige Datei.

Amazon ECR GuardDuty Repository-Hosting-Agent

In den folgenden Abschnitten sind die Amazon Elastic Container Registry (AmazonECR) -Repositorys aufgeführt, in denen der Security Agent GuardDuty gehostet wird, der auf Ihren Amazon EKS - und ECS Amazon-Clustern bereitgestellt wird.

Inhalt

Repository für die EKS Agentenversion 1.6.0 oder höher

In der folgenden Tabelle sind die ECR Amazon-Repositorys aufgeführt, die jeweils den EKS Amazon-Zusatz-Agenten der Version (`aws-guardduty-agent`) 1.6.0 und höher hosten. AWS-Region

AWS-Region	ECRAmazon-Repositorium URI
USA West (Oregon)	`602401143452.dkr.ecr.us-west-2.amazonaws.com`
Europa (Paris)	`602401143452.dkr.ecr.eu-west-3.amazonaws.com`
Asien-Pazifik (Mumbai)	`602401143452.dkr.ecr.ap-south-1.amazonaws.com`
Asien-Pazifik (Hyderabad)	`900889452093.dkr.ecr.ap-south-2.amazonaws.com`
Kanada (Zentral)	`602401143452.dkr.ecr.ca-central-1.amazonaws.com`
Kanada West (Calgary)	`761377655185.dkr.ecr.ca-west-1.amazonaws.com`
Naher Osten (UAE)	`759879836304.dkr.ecr.me-central-1.amazonaws.com`
Europa (London)	`602401143452.dkr.ecr.eu-west-2.amazonaws.com`

AWS-Region	ECRAmazon-Repositorium URI
USA West (Nordkalifornien)	602401143452.dkr.ecr.us-west-1.amazonaws.com
USA Ost (Nord-Virginia)	602401143452.dkr.ecr.us-east-1.amazonaws.com
USA Ost (Ohio)	602401143452.dkr.ecr.us-east-2.amazonaws.com
Europa (Irland)	602401143452.dkr.ecr.eu-west-1.amazonaws.com
Südamerika (São Paulo)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
Europa (Stockholm)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
Europa (Frankfurt)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zürich)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
Asien-Pazifik (Singapur)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com
Asien-Pazifik (Sydney)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
Asien-Pazifik (Jakarta)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
Asien-Pazifik (Tokio)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
Asien-Pazifik (Seoul)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
Asien-Pazifik (Osaka)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com

AWS-Region	ECRAmazon-Repositorium URI
Asien-Pazifik (Hongkong)	`800184023465.dkr.ecr.ap-east-1.amazonaws.com`
Naher Osten (Bahrain)	`759879836304.dkr.ecr.me-south-1.amazonaws.com`
Europa (Milan)	`590381155156.dkr.ecr.eu-south-1.amazonaws.com`
Europa (Spain)	`455263428931.dkr.ecr.eu-south-2.amazonaws.com`
Afrika (Kapstadt)	`877085696533.dkr.ecr.af-south-1.amazonaws.com`
Asien-Pazifik (Melbourne)	`491585149902.dkr.ecr.ap-southeast-4.amazonaws.com`
Israel (Tel Aviv)	`066635153087.dkr.ecr.il-central-1.amazonaws.com`

Repository für EKS Agentenversion 1.5.0 und früher

In der folgenden Tabelle sind die ECR Amazon-Repositorys aufgeführt, die jeweils den EKS Amazon-Zusatzagenten der Version (`aws-guardduty-agent`) 1.5.0 und früher hosten. AWS-Region

AWS-Region	ECRAmazon-Repositorium URI
USA West (Oregon)	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Europa (Paris)	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`
Asien-Pazifik (Mumbai)	`610108029387.dkr.ecr.ap-south-1.amazonaws.com`
Asien-Pazifik (Hyderabad)	`618745550137.dkr.ecr.ap-south-2.amazonaws.com`
Kanada (Zentral)	`001188825231.dkr.ecr.ca-central-1.amazonaws.com`

AWS-Region	ECRAmazon-Repositorium URI
Naher Osten (UAE)	601769779514.dkr.ecr.me-central-1.amazonaws.com
Europa (London)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
USA West (Nordkalifornien)	373421517865.dkr.ecr.us-west-1.amazonaws.com
USA Ost (Nord-Virginia)	031903291036.dkr.ecr.us-east-1.amazonaws.com
USA Ost (Ohio)	591382732059.dkr.ecr.us-east-2.amazonaws.com
Europa (Irland)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
Südamerika (São Paulo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europa (Stockholm)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europa (Frankfurt)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zürich)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asien-Pazifik (Singapur)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asien-Pazifik (Sydney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asien-Pazifik (Jakarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com
Asien-Pazifik (Tokio)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com

AWS-Region	ECRAmazon-Repositorium URI
Asien-Pazifik (Seoul)	`732248494576.dkr.ecr.ap-northeast-2.amazonaws.com`
Asien-Pazifik (Osaka)	`810724417379.dkr.ecr.ap-northeast-3.amazonaws.com`
Asien-Pazifik (Hongkong)	`790429075973.dkr.ecr.ap-east-1.amazonaws.com`
Naher Osten (Bahrain)	`541829937850.dkr.ecr.me-south-1.amazonaws.com`
Europa (Milan)	`528450769569.dkr.ecr.eu-south-1.amazonaws.com`
Europa (Spain)	`531047660167.dkr.ecr.eu-south-2.amazonaws.com`
Afrika (Kapstadt)	`379032919888.dkr.ecr.af-south-1.amazonaws.com`
Asien-Pazifik (Melbourne)	`750462861327.dkr.ecr.ap-southeast-4.amazonaws.com`
Israel (Tel Aviv)	`292660727137.dkr.ecr.il-central-1.amazonaws.com`

Repository für GuardDuty Agenten auf AWS Fargate (ECSnur Amazon)

Die folgende Tabelle zeigt die ECR Amazon-Repositorys, die jeweils AWS-Region den GuardDuty Agenten für AWS Fargate (ECSnur Amazon) hosten.

AWS-Region	ECRAmazon-Repositorium URI
USA West (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Paris)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate`

AWS-Region	ECRAmazon-Repositorium URI
Asien-Pazifik (Mumbai)	`251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Hyderabad)	`950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Kanada (Zentral)	`354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Naher Osten (UAE)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (London)	`892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate`
USA West (Nordkalifornien)	`684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate`
USA Ost (Nord-Virginia)	`593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate`
USA Ost (Ohio)	`307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Irland)	`694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate`
Südamerika (São Paulo)	`758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Stockholm)	`591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Frankfurt)	`323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Zürich)	`529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate`

AWS-Region	ECRAmazon-Repositorium URI
Asien-Pazifik (Singapur)	`174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Sydney)	`005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Jakarta)	`510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Tokio)	`533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Seoul)	`914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Osaka)	`273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Hongkong)	`258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Naher Osten (Bahrain)	`536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Milan)	`266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Spain)	`919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Afrika (Kapstadt)	`197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asien-Pazifik (Melbourne)	`251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate`
Israel (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate`

GuardDuty Versionsverlauf des Agenten

Die folgenden Abschnitte enthalten die Release-Version für den GuardDuty Agenten, der auf EC2 Amazon-Instances, ECS Amazon-Clustern und EKS Amazon-Clustern bereitgestellt wird.

GuardDuty Sicherheitsagent für EC2 Amazon-Instances

Agent-Version	Versionshinweise	Datum der Verfügbarkeit
v1.3.0	Allgemeine Leistungsoptimierung und -verbesserungen Beinhaltet Unterstützung für die Erfassung zusätzlicher Sicherheitssignale für die futureRuntime Monitoring: Typen finden.	19. August 2024
v1.2.0	Unterstützt die Betriebssystem-Distributionen Ubuntu 20.04, Ubuntu 22.04, Debian 11 und Debian 12 Unterstützt Kernel 6.5 und 6.8 Allgemeine Leistungsoptimierung und -verbesserungen	13. Juni 2024
v1.1.0	Unterstützt die GuardDuty automatische Agentenkonfiguration in Runtime Monitoring für EC2 Amazon-Instances Unterstützt neue Sicherheitssignale und Erkenntnisse, die mit der Ankündigung der allgemeinen Verfügbarkeit von Runtime Monitoring für	26. März 2024

Agent-Version	Versionshinweise	Datum der Verfügbarkeit
	EC2 Instances veröffentlicht wurden Allgemeine Leistungsoptimierung und -verbesserungen	
v1.0.2	Unterstützt die neueste Version von Amazon ECSAMIs.	2. Februar 2024
v1.0.1	Agentenversionen, die vor Version 1.0.2 veröffentlicht wurden, sind nicht mit Amazon kompatibel, die nach dem 31. Januar 2024 auf den ECS AMIs Markt gebracht wurden. Allgemeine Leistungsoptimierung und -verbesserungen	23. Januar 2024
v1.0.0	Erste Version der RPM Installation Agentenversionen, die vor Version 1.0.2 veröffentlicht wurden, sind nicht mit Amazon kompatibel, die nach dem 31. Januar 2024 auf den ECS AMIs Markt gebracht wurden.	26. November 2023

RPM S3 bucket example script

Der öffentliche Schlüssel, die Signatur von x86_64RPM, die Signatur von arm64 RPM und der entsprechende Zugriffslink zu den in Amazon S3 S3-Buckets gehosteten RPM Skripten können aus den folgenden Vorlagen gebildet werden. Ersetzen Sie den Wert von AWS-Region, der AWS

Konto-ID und der GuardDuty Agentenversion, um auf die Skripts zuzugreifen. RPM Die folgenden Vorlagen enthalten die neueste Agentenversion für EC2 Amazon-Instances.

- Öffentlicher Schlüssel:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/publickey.pem
```

- GuardDuty RPMSignatur des Sicherheitsagenten:

  Signatur von x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.sig
```

  Signatur von arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.sig
```

- Greifen Sie auf Links zu den RPM Skripten im Amazon S3 S3-Bucket zu:

  Zugangslink für x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/x86_64/amazon-guardduty-agent-1.3.0.x86_64.rpm
```

  Zugangslink für arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.rpm
```

Debian S3 bucket example script

Der öffentliche Schlüssel, die Signatur mit arm64 und der entsprechende Zugriffslink zu den in Amazon S3 S3-Buckets gehosteten Skripten können aus den folgenden Vorlagen gebildet werden. Ersetzen Sie den Wert von AWS-Region, der AWS Konto-ID und der GuardDuty Agentenversion, um auf die Skripts zuzugreifen. Die folgenden Vorlagen enthalten die neueste Agentenversion für EC2 Amazon-Instances.

- Öffentlicher Schlüssel:

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/publickey.pem
```

- GuardDuty Signatur des Sicherheitsagenten:

  Signatur von amd64

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/amazon-guardduty-agent-1.3.0.amd64.sig
  ```

  Signatur von arm64

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.sig
  ```

- Greifen Sie auf Links zu den Skripten im Amazon S3 S3-Bucket zu:

  Zugangslink für amd64

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/amd64/amazon-guardduty-agent-1.3.0.amd64.deb
  ```

  Zugangslink für arm64

  ```
  s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.3.0/arm64/amazon-guardduty-agent-1.3.0.arm64.deb
  ```

AWS-Region	Name der Region	AWS Konto-ID
eu-west-1	Europa (Irland)	694911143906
us-east-1	USA Ost (Nord-Virginia)	593207742271
us-east-2	USA Ost (Ohio)	733349766148
eu-west-3	Europa (Paris)	665651866788
us-east-2	USA Ost (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986

ap-northeast-2	Asien-Pazifik (Seoul)	914738172881
eu-north-1	Europa (Stockholm)	591436053604
ap-east-1	Asien-Pazifik (Hongkong)	258348409381
me-south-1	Naher Osten (Bahrain)	536382113932
eu-west-2	Europa (London)	892757235363
ap-northeast-1	Asien-Pazifik (Tokio)	533107202818
ap-southeast-1	Asien-Pazifik (Singapur)	174946120834
ap-south-1	Asien-Pazifik (Mumbai)	251508486986
ap-southeast-3	Asien-Pazifik (Jakarta)	510637619217
sa-east-1	Südamerika (São Paulo)	758426053663
ap-northeast-3	Asien-Pazifik (Osaka)	273192626886
eu-south-1	Europa (Milan)	266869475730
af-south-1	Afrika (Kapstadt)	197869348890
ap-southeast-2	Asien-Pazifik (Sydney)	005257825471
me-central-1	Naher Osten () UAE	000014521398
us-west-1	USA West (Nordkalifornien)	684579721401
ca-central-1	Kanada (Zentral)	354763396469
ap-south-2	Asien-Pazifik (Hyderabad)	950823858135
eu-south-2	Europa (Spain)	919611009337
eu-central-2	Europa (Zürich)	529164026651
ap-southeast-4	Asien-Pazifik (Melbourne)	251357961535

il-central-1	Israel (Tel Aviv)	870907303882

GuardDuty Sicherheitsagent für AWS Fargate (ECSnur Amazon)

Die folgende Tabelle zeigt den Versionsverlauf der Versionen des GuardDuty Security Agents für Fargate (ECSnur Amazon).

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit
v1.3.0	x86_64 (): AMD64 sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831 Graviton (): ARM64 sha256:ff81a755d46681e409f55a95beedae9ebbcf5336e1c0b1e6348af7c6518bdbb1	Allgemeine Leistungsoptimierung und -verbesserungen. Beinhaltet Unterstützung für die Erfassung zusätzlicher Sicherheitssignale für die future GuardDuty Runtime Monitoring: Typen finden.	9. August 2024
v1.2.0	x86_64 (): AMD64 sha256:1dbad20ac2dc66d52d00bb28dde4281fe0d3c5f261b1649b247c2369d9e26b93 Graviton (): ARM64 sha256:91930f8446f5f95b93b8ccb18773992affa401	Allgemeine Leistungsoptimierung und -verbesserungen.	31. Mai 2024

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit
	eb3f42da89d68077a56bafa6cd		
v1.1.0	x86_64 (): AMD64 sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c9f673f2835823957e9dcf71657 Graviton (): ARM64 sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dcccfe8c9383dc7	Unterstützt neue Sicherheitssignale und Erkenntnisse. Allgemeine Leistungsoptimierung und -verbesserungen.	01. Mai 2024
v1.0.1	x86_64 (): AMD64 sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68 Graviton (): ARM64 sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7	Allgemeine Leistungsoptimierung und -verbesserungen.	26. Januar 2024

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit
v1.0.0	x86_64 (): AMD64 `sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017` Graviton (): ARM64 `sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984`	Erste Version des GuardDuty Security Agents für AWS Fargate (ECSnur Amazon).	26. November 2023

GuardDuty Sicherheitsagent für EKS Amazon-Cluster

Die folgende Tabelle zeigt den Versionsverlauf des Amazon EKS Add-on GuardDuty Agents.

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.7.0	x86_64 (): AMD64 `sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffcd7e68554a423d610cea8c7e8f2185ec` Graviton (): ARM64 `sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a`	Allgemeine Leistungsoptimierung und -verbesserungen. Beinhaltet Unterstützung für die Erfassung zusätzlicher Sicherheitssignale	17. August 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
		für die futureRuntime Monitoring: Typen finden.		
v1.6.1	x86_64 (): AMD64 `sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1` Graviton (): ARM64 `sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019`	Allgemeine Leistungsoptimierung und -verbesserungen.	14. Mai 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]

v1.6.0	x86_64 (): AMD64
	`sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010`
	
	Graviton (): ARM64
	`sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650`
		• Unterstützt die GuardDuty automatische Agentenkonfiguration für EKS EC2 /-Ressourcen.
		• Unterstützt die neuen Sicherheitssignale und Ergebnisse. Weitere Informationen erhalten Sie unter Gesammelte Runtime-Ereignistypen, die verwendet GuardDuty und Runtime Monitorin
			29. April 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
		g: Typen finden. • Allgemeine Leistungsoptimierung und -verbesserungen.		
v1.5.0	x86_64 (): AMD64 sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d Graviton (): ARM64 sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6	• Allgemeine Leistungsoptimierung und -verbesserungen. • Sicherheitsverbesserungen, einschließlich neuer Ereignistypen unterGesamte Laufzeit-Ereignistypen. • Leistungsverbesserungen rund um CPU die Nutzung.	07. März 2024	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.4.1	x86_64 (): AMD64 `sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c` Graviton (): ARM64 `sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40`	Allgemeine Leistungsoptimierung und -verbesserungen.	16. Januar 2024	–
v1.4.0	x86_64 (): AMD64 `sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f` Graviton (): ARM64 `sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e`	Manifest Mount Point unterstützt eine bessere Datenerfassung AppArmor Konfiguration im Manifest Sammle das Befehlszeilenargument Allgemeine Leistungsoptimierung und -verbesserungen	21. Dezember 2	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.3.1	x86_64 (): AMD64 `sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29` Graviton (): ARM64 `sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd`	Wichtige Sicherheitspatches und Updates.	23. Oktober 202	–
v1.3.0	x86_64 (): AMD64 `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Graviton (): ARM64 `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Unterstützt die Ubuntu-Plattform Unterstützt Kubernetes-Version 1.28 Allgemeine Leistungsverbesserungen und Stabilitätsverbesserungen.	5. Oktober 2023	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.2.0	x86_64 (): AMD64 `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Graviton (): ARM64 `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	Zusätzlich zu AMD64 basierten Instances unterstützt v1.2.0 jetzt auch ARM64 basierte Instances . Unterstützung für Bottlerocket hinzugefügt und verifiziert Unterstützt Kubernetes-Version 1.27 Allgemeine Leistungsverbesserungen und Stabilitätsverbesserungen.	16. Juni 2023	–

Agent-Version	Container-Image	Versionshinweise	Datum der Verfügbarkeit	Ende des Standard-Supports [1]
v1.1.0	`sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c`	Über Kubernetes-Versionen, die vom Security Agent unterstützt werden GuardDuty hinaus unterstützt zt diese Agentenversion auch Kubernetes Version 1.26. Allgemeine Leistungsverbesserungen und Stabilitätsverbesserungen.	2. Mai 2023	14. Mai 2024
v1.0.0	`sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e`	Erste Version des EKS Amazon-Zusatz-Agenten.	30. März 2023	14. Mai 2024

[1] Informationen zur Aktualisierung Ihrer aktuellen Agentenversion, für die der Standardsupport bald ausläuft, finden Sie unterManuelles Aktualisieren des Security Agents.

Auswirkungen der Deaktivierung und Bereinigung von Ressourcen

Dieser Abschnitt bezieht sich darauf, AWS-Konto ob Sie die Laufzeitüberwachung oder nur die GuardDuty automatische Agentenkonfiguration für einen Ressourcentyp deaktivieren möchten.

Deaktivierung der GuardDuty automatisierten Agentenkonfiguration

GuardDuty entfernt den Security Agent, der auf Ihrer Ressource installiert ist, nicht. GuardDuty Beendet jedoch die Verwaltung der Updates für den Security Agent.

GuardDuty empfängt weiterhin die Runtime-Ereignisse von Ihrem Ressourcentyp. Um Auswirkungen auf Ihre Nutzungsstatistiken zu vermeiden, sollten Sie den GuardDuty Security Agent unbedingt von Ihrer Ressource entfernen.

Unabhängig davon, ob ein gemeinsam genutzter VPC Endpunkt AWS-Konto verwendet wird oder GuardDuty nicht, wird der VPC Endpunkt nicht gelöscht. Falls erforderlich, müssen Sie den VPC Endpunkt manuell löschen.

Laufzeitüberwachung und EKS Laufzeitüberwachung deaktivieren

Dieser Abschnitt gilt für Sie in den folgenden Szenarien:

- Sie haben EKS Runtime Monitoring nie separat aktiviert und jetzt haben Sie Runtime Monitoring deaktiviert.
- Sie deaktivieren sowohl Runtime Monitoring als auch EKS Runtime Monitoring. Wenn Sie sich über den Konfigurationsstatus von EKS Runtime Monitoring nicht sicher sind, finden Sie weitere Informationen unterÜberprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring.

> **Runtime Monitoring deaktivieren, ohne Runtime Monitoring zu deaktivieren EKS**
>
> In diesem Szenario haben Sie zu einem bestimmten Zeitpunkt Runtime Monitoring aktiviert und später auch EKS Runtime Monitoring aktiviert, ohne Runtime Monitoring zu deaktivierenEKS.
> Wenn Sie jetzt Runtime Monitoring deaktivieren, müssen Sie EKS Runtime Monitoring auch deaktivieren. Andernfalls fallen weiterhin Nutzungskosten für EKS Runtime Monitoring an.

Wenn die zuvor aufgelisteten Szenarien auf Sie zutreffen, GuardDuty wird in Ihrem Konto die folgenden Maßnahmen ergriffen:

- GuardDuty löscht dasVPC, das das `true` Tag`GuardDutyManaged`: hat. Dies ist derVPC, der zur Verwaltung des automatisierten Security Agents erstellt GuardDuty wurde.
- GuardDuty löscht die Sicherheitsgruppe, die als gekennzeichnet wurde`GuardDutyManaged`:`true`.
- Bei einer geteilten VPC Ressource, die von mindestens einem Teilnehmerkonto verwendet wurde, werden GuardDuty weder der VPC Endpunkt noch die Sicherheitsgruppe gelöscht, die der gemeinsam genutzten VPC Ressource zugeordnet sind.
- GuardDuty Löscht für eine EKS Amazon-Ressource den Security Agent. Dies ist unabhängig davon, ob die Verwaltung manuell oder über erfolgt GuardDuty.

  Bei einer ECS Amazon-Ressource GuardDuty kann der Security Agent nicht von dieser Ressource deinstalliert werden, da eine ECS Aufgabe unveränderlich ist. Dies ist unabhängig davon, wie Sie den Security Agent verwalten — manuell oder automatisch. GuardDuty Nachdem Sie Runtime Monitoring deaktiviert haben, GuardDuty wird kein Sidecar-Container angehängt, wenn eine neue ECS Aufgabe ausgeführt wird. Hinweise zur Arbeit mit ECS Fargate-Aufgaben finden Sie unterSo funktioniert Runtime Monitoring mit Fargate (ECSnur Amazon).

  GuardDuty Deinstalliert bei einer EC2 Amazon-Ressource den Security Agent nur dann von allen Systems Manager (SSM) verwalteten EC2 Amazon-Instances, wenn er die folgenden Bedingungen erfüllt:

  - Ihre Ressource ist nicht mit dem Tag`GuardDutyManaged`: `false` exclusion gekennzeichnet.
  - GuardDuty muss über Berechtigungen für den Zugriff auf die Tags in den Instanzmetadaten verfügen. Für diese EC2 Ressource ist der Zugriff auf Tags in Instanzmetadaten auf Zulassen gesetzt.

Wenn Sie die manuelle Verwaltung des Security Agents beenden

Unabhängig davon, welche Methode Sie für die Installation und Verwaltung des GuardDuty Security Agents verwenden, müssen Sie den Security Agent entfernen, um die Überwachung der GuardDuty Runtime-Ereignisse in Ihrer Ressource zu beenden. Wenn Sie die Überwachung der Runtime-Ereignisse von einem Ressourcentyp in einem Konto beenden möchten, können Sie auch den VPC Amazon-Endpunkt löschen.

Prozess zur Bereinigung der Ressourcen des Security Agents

Um den VPC Amazon-Endpunkt zu löschen

- Ohne geteilte Ressource VPC — Wenn Sie eine Ressource in einem Konto nicht mehr überwachen möchten, sollten Sie erwägen, den VPC Amazon-Endpunkt zu löschen.
- Mit geteiltem Konto VPC — Wenn ein Konto mit geteiltem VPC Eigentümer die gemeinsam genutzte VPC Ressource löscht, die noch genutzt wurde, kann der Deckungsstatus der EKS Runtime Monitoring (und gegebenenfalls Runtime Monitoring) für die Ressourcen in Ihrem gemeinsamen VPC Besitzerkonto und dem teilnehmenden Konto fehlerhaft werden. Informationen zum Deckungsstatus finden Sie unter. Bewertung der Laufzeitabdeckung Ihrer Ressourcen

  Weitere Informationen finden Sie unter Löschen eines Schnittstellenendpunkts.

Um die Sicherheitsgruppe zu löschen

- Ohne gemeinsam genutzt VPC — Wenn Sie einen Ressourcentyp in einem Konto nicht mehr überwachen möchten, sollten Sie erwägen, die dem Amazon zugeordnete Sicherheitsgruppe zu löschenVPC.
- Mit geteiltem Konto VPC — Wenn das Konto des gemeinsamen VPC Besitzers die Sicherheitsgruppe löscht, kann es sein, dass jedes Teilnehmerkonto, das derzeit die Sicherheitsgruppe verwendet, die mit dem geteilten Konto verknüpft istVPC, der Runtime Monitoring-Abdeckungsstatus für die Ressourcen in Ihrem Konto mit gemeinsamem VPC Besitzer und das teilnehmende Konto fehlerhaft wird. Weitere Informationen finden Sie unter Bewertung der Laufzeitabdeckung Ihrer Ressourcen.

  Weitere Informationen finden Sie unter Löschen einer Sicherheitsgruppe.

Um den GuardDuty Security Agent aus einem EKS Cluster zu entfernen

Informationen zum Entfernen des Security Agents aus Ihrem EKS Cluster, den Sie nicht mehr überwachen möchten, finden Sie unter Löschen eines Add-ons.

Durch das Entfernen des EKS Add-On-Agents wird der `amazon-guardduty` Namespace nicht aus dem EKS Cluster entfernt. Um einen `amazon-guardduty`-Namespace zu löschen, sehen Sie Einen Namespace löschen.

Um den **`amazon-guardduty`** Namespace (EKSCluster) zu löschen

Wenn Sie die automatische Agentenkonfiguration deaktivieren, wird der `amazon-guardduty` Namespace nicht automatisch aus Ihrem Cluster entfernt. EKS Um einen `amazon-guardduty`-Namespace zu löschen, sehen Sie Einen Namespace löschen.

GuardDuty Malware-Schutz für EC2

Malware Protection for EC2 hilft Ihnen dabei, das potenzielle Vorhandensein von Malware zu erkennen, indem es die Amazon Elastic Block Store (AmazonEBS) -Volumes scannt, die an die Amazon Elastic Compute Cloud (AmazonEC2) -Instances und Container-Workloads angehängt sind. Malware Protection for EC2 bietet Scanoptionen, mit denen Sie entscheiden können, ob Sie bestimmte EC2 Amazon-Instances und Container-Workloads beim Scannen ein- oder ausschließen möchten. Es bietet auch die Möglichkeit, die Snapshots der EBS Amazon-Volumes, die den EC2 Amazon-Instances oder Container-Workloads zugeordnet sind, in Ihren GuardDuty Konten zu speichern. Die Snapshots werden nur gespeichert, wenn Malware gefunden wird, und der Malware-Schutz für EC2 Ergebnisse wird generiert.

Malware Protection for EC2 ist eine optionale Erweiterung von und wurde so konzipiert, dass die Leistung Ihrer Ressourcen nicht beeinträchtigt wird. GuardDuty Informationen zur EC2 Funktionsweise von Malware Protection for finden Sie unterFunktion im Malware-Schutz für EC2. GuardDuty Informationen zur Verfügbarkeit von Malware Protection for EC2 in verschiedenen AWS-Regionen Ländern finden Sie unterRegionen und Endpunkte.

> **Hinweis**
>
> GuardDuty Malware Protection for EC2 unterstützt Fargate EKS weder bei Amazon noch bei AmazonECS.

Malware Protection for EC2 bietet zwei Arten von Scans zur Erkennung potenziell bösartiger Aktivitäten in Ihren EC2 Amazon-Instances und Container-Workloads: den GuardDuty initiierten Malware-Scan und den On-Demand-Malware-Scan. Die folgende Tabelle zeigt den Vergleich zwischen den beiden Scan-Typen.

Faktor	GuardDuty-initiierter Malware-Scan	Malware-Scan auf Abruf
Wie der Scan aufgerufen wird	Sobald Sie den GuardDuty -initiierten Malware-Scan aktiviert haben, GuardDuty wird jedes Mal, wenn ein Ergebnis generiert wird,	Sie können einen On-Demand-Malware-Scan initiieren, indem Sie den Amazon-Ressourcennamen (ARN) angeben, der Ihrer

Faktor	GuardDuty-initiierter Malware-Scan	Malware-Scan auf Abruf
	das auf das potenzielle Vorhandensein von Malware in einer EC2 Amazon-Instance oder einem Container-Workload hinweist, GuardDuty automatisch ein agentenloser Malware-Scan auf den EBS Amazon-Volumes initiiert, die Ihrer potenziell betroffenen Ressource zugeordnet sind. Weitere Informationen finden Sie unter GuardDuty-hat einen Malware-Scan initiiert.	EC2 Amazon-Instance- oder Container-Workload zugeordnet ist. Sie können einen On-Demand-Malware-Scan auch dann initiieren, wenn für Ihre Ressource kein GuardDuty Ergebnis generiert wurde. Weitere Informationen finden Sie unter Malware-Scan auf Abruf.
Konfiguration erforderlich	Um den GuardDuty -initiierten Malware-Scan verwenden zu können, müssen Sie ihn für Ihr Konto aktivieren. Weitere Informationen finden Sie unter Konfiguration des GuardDuty -initiierten Malware-Scans.	Ihr Konto muss GuardDuty aktiviert sein. Um den On-Demand-Malware-Scan zu verwenden, ist keine Konfiguration auf Funktionsebene erforderlich.
Wartezeit zum Initiieren eines neuen Scanvorgangs	Immer wenn ein Malware-Scan GuardDuty generiert wirdErgebnisse, die einen GuardDuty -initiierten Malware-Scan auslösen, wird nur einmal alle 24 Stunden automatisch ein Malware-Scan gestartet.	Sie können einen On-Demand -Malware-Scan für dieselbe Ressource jederzeit nach dem Start des vorherigen Scans starten.

Faktor	GuardDuty-initiierter Malware-Scan	Malware-Scan auf Abruf
Verfügbarkeit der 30-tägigen kostenlosen Testphase	Wenn Sie den GuardDuty -initiierten Malware-Scan in Ihrem Konto zum ersten Mal aktivieren, können Sie eine 30-tägige kostenlose Testphase nutzen*. Weitere Informationen zum GuardDuty -initiierten Malware-Scan finden Sie unter. Kostenlose 30-Tage-Testversion	Es gibt keine kostenlose Testzeit* mit Malware-Scan auf Abruf für neue oder bestehende GuardDuty Konten.
Scan-Optionen	Nachdem Sie den GuardDuty -initiierten Malware-Scan konfiguriert haben, hilft Ihnen Malware Protection for EC2 auch dabei, auszuwählen, welche Ressourcen gescannt oder übersprungen werden sollen. Malware Protection for EC2 initiiert keinen automatischen Scan der Ressourcen, die Sie vom Scan ausschließen möchten.	Der Malware-Scan auf Abruf unterstützt ein globales Tag —`GuardDutyExcluded` . Scan-Optionen mit benutzerdefinierten Tagsgilt nicht für den Malware-Scan auf Abruf, da Sie die Ressource ARN manuell bereitstellen.

*Für die Erstellung von EBS Volumen-Snapshots und die Aufbewahrung von Snapshots fallen Nutzungskosten an. Weitere Informationen zur Konfiguration Ihres Kontos für die Aufbewahrung von Snapshots finden Sie unter. Snapshot-Beibehaltung

Funktion im Malware-Schutz für EC2

Elastisches Blockspeicher-Volumen (EBS)

In diesem Abschnitt wird erklärt, wie Malware Protection forEC2, einschließlich GuardDuty initiierter Malware-Scans und On-Demand-Malware-Scans, die EBS Amazon-Volumes scannt, die Ihren EC2

Amazon-Instances und Container-Workloads zugeordnet sind. Berücksichtigen Sie die folgenden Anpassungen, bevor Sie fortfahren:

- Scanoptionen — Malware Protection for EC2 bietet die Möglichkeit, Tags anzugeben, um EC2 Amazon-Instances und EBS Amazon-Volumes entweder vom Scanvorgang ein- oder auszuschließen. Nur durch einen GuardDuty -initiierten Malware-Scan werden Scanoptionen mit benutzerdefinierten Tags unterstützt. Sowohl der GuardDuty -initiierte Malware-Scan als auch der On-Demand-Malware-Scan unterstützen das globale Tag. `GuardDutyExcluded` Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.
- Aufbewahrung von Snapshots — Malware Protection for EC2 bietet die Möglichkeit, die Snapshots Ihrer EBS Amazon-Volumes in Ihrem AWS Konto aufzubewahren. Diese Option ist standardmäßig ausgeschaltet. Sie können sich für die Aufbewahrung von Snapshots sowohl für GuardDuty initiierte als auch für On-Demand-Malware-Scans entscheiden. Weitere Informationen finden Sie unter Snapshot-Beibehaltung.

Wenn ein Ergebnis GuardDuty generiert wird, das auf das potenzielle Vorhandensein von Malware in einer EC2 Amazon-Instance oder einem Container-Workload hinweist, und Sie den Typ des GuardDuty initiierten Scans in Malware Protection for aktiviert habenEC2, kann ein GuardDuty -initiierter Malware-Scan auf der Grundlage Ihrer Scanoptionen aufgerufen werden.

Um einen On-Demand-Malware-Scan auf den EBS Amazon-Volumes zu initiieren, die einer EC2 Amazon-Instance zugeordnet sind, geben Sie den Amazon-Ressourcennamen (ARN) der EC2 Amazon-Instance an.

Als Reaktion auf einen On-Demand-Malware-Scan oder einen automatisch aufgerufenen, durch GuardDuty ihn initiierten Malware-Scan GuardDuty erstellt es Snapshots der relevanten EBS Volumes, die an die potenziell betroffene Ressource angehängt sind, und gibt sie an die weiter. GuardDuty Dienstkonto GuardDuty Erstellt aus diesen Snapshots ein verschlüsseltes EBS Replikat-Volume im Dienstkonto.

Informationen zur Methode zur GuardDuty Malware-Erkennung und zu den verwendeten Scan-Engines finden Sie unter. GuardDuty Scan-Engine zur Malware-Erkennung

GuardDuty Löscht nach Abschluss des Scans die verschlüsselten EBS Replikat-Volumes und die Snapshots Ihrer Volumes. EBS Wenn Malware gefunden wird und Sie die Einstellung zur Aufbewahrung von Snapshots aktiviert haben, werden die Snapshots Ihrer EBS Volumes nicht gelöscht, sondern automatisch in Ihrem Konto gespeichert. AWS Wenn keine Malware gefunden wird, werden die Snapshots Ihrer EBS Volumes nicht aufbewahrt, unabhängig von der

Aufbewahrungseinstellung für Snapshots. Standardmäßig ist die Aufbewahrungseinstellung für Snapshots deaktiviert. Informationen zu den Kosten von Snapshots und deren Aufbewahrung finden Sie unter EBSAmazon-Preise.

GuardDuty speichert jedes EBS Replikat-Volume im Servicekonto für bis zu 55 Stunden. Im Falle eines Dienstausfalls oder eines Fehlers bei einem EBS Replikat-Volume und dessen Malware-Scan GuardDuty wird ein solches EBS Volume nicht länger als sieben Tage aufbewahrt. Die verlängerte Aufbewahrungsfrist für das Volume dient der Suche und Behebung des Ausfalls oder Fehlers. GuardDuty Malware Protection for EC2 löscht die EBS Replikat-Volumes aus dem Dienstkonto, nachdem der Ausfall oder Fehler behoben wurde oder wenn die erweiterte Aufbewahrungsfrist abgelaufen ist.

Unterstützte EBS Amazon-Volumes für Malware-Scans

In allen Ländern, in AWS-Regionen denen die EC2 Funktion Malware-Schutz für GuardDuty unterstützt wird, können Sie die unverschlüsselten oder verschlüsselten EBS Amazon-Volumes scannen. Sie können EBS Amazon-Volumes verwenden, die entweder mit einem Von AWS verwalteter Schlüsseloder mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Derzeit AWS-Regionen unterstützen einige Programme beide Methoden zur Verschlüsselung Ihrer EBS Amazon-Volumes, während andere nur vom Kunden verwaltete Schlüssel unterstützen.

Weitere Informationen, wo diese Funktion noch nicht unterstützt wird, finden Sie unter China Regions

In der folgenden Liste wird der Schlüssel beschrieben, der GuardDuty verwendet, unabhängig davon, ob Ihre EBS Amazon-Volumes verschlüsselt sind oder nicht:

- EBSAmazon-Volumes, die entweder unverschlüsselt oder mit verschlüsselt sind Von AWS verwalteter Schlüssel — GuardDuty verwendet einen eigenen Schlüssel, um die Replikat-Amazon-Volumes zu verschlüsseln. EBS

  Wenn Ihr Konto zu einem gehört AWS-Region , das das Scannen von EBS Amazon-Volumes nicht unterstützt, die mit der Von AWS verwalteter Schlüssel Standardform verschlüsselt sindEBS, finden Sie unterÄndern der AWS KMS Standardschlüssel-ID eines EBS Amazon-Volumes.
- EBSAmazon-Volumes, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind, GuardDuty verwenden denselben Schlüssel, um das EBS Replikat-Volume zu verschlüsseln.

Malware Protection for unterstützt das Scannen von EC2 Amazon-Instances mit `productCode` as EC2 nicht`marketplace`. Wenn ein Malware-Scan für eine solche EC2 Amazon-

Instance initiiert wird, wird der Scan übersprungen. Weitere Informationen finden Sie unter `UNSUPPORTED_PRODUCT_CODE_TYPE` in Gründe für das Überspringen von Ressourcen beim Malware-Scan.

Ändern der AWS KMS Standardschlüssel-ID eines EBS Amazon-Volumes

Standardmäßig wird beim Aufrufen von CreateVolumeAPImit auf `true` eingestellter Verschlüsselung ohne Angabe der KMS Schlüssel-ID ein EBS Amazon-Volume erstellt, das mit dem AWS KMS Standardschlüssel für die EBS Verschlüsselung verschlüsselt wird. Wenn ein Verschlüsselungsschlüssel jedoch nicht explizit angegeben wird, können Sie den Standardschlüssel ändern, indem Sie ModifyEbsDefaultKmsKeyIdAPIoder aufrufen, indem Sie den entsprechenden AWS CLI Befehl verwenden.

Um die EBS Standardschlüssel-ID zu ändern, fügen Sie Ihrer IAM Richtlinie die folgende erforderliche Berechtigung hinzu:`ec2:modifyEbsDefaultKmsKeyId`. Jedes neu erstellte EBS Amazon-Volume, das Sie für die Verschlüsselung auswählen, aber keine zugehörige KMS Schlüssel-ID angeben, verwendet die Standardschlüssel-ID. Verwenden Sie eine der folgenden Methoden, um die EBS Standardschlüssel-ID zu aktualisieren:

So ändern Sie die KMS Standardschlüssel-ID eines EBS Amazon-Volumes

Führen Sie eine der folgenden Aktionen aus:

- Mit einem API — Sie können den verwenden ModifyEbsDefaultKmsKeyIdAPI. Informationen darüber, wie Sie den Verschlüsselungsstatus Ihres Volumes einsehen können, finden Sie unter EBSAmazon-Volume erstellen.
- AWS CLI Befehl verwenden — Im folgenden Beispiel wird die KMS Standardschlüssel-ID geändert, mit der EBS Amazon-Volumes verschlüsselt werden, wenn Sie keine KMS Schlüssel-ID angeben. Achten Sie darauf, die Region durch die AWS-Region Ihrer KM-Schlüssel-ID zu ersetzen.

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
id AKIAIOSFODNN7EXAMPLE
```

Der obige Befehl wird eine Ausgabe erzeugen, die folgendermaßen aussieht:

```
{
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

Weitere Informationen finden Sie unter modify-ebs-default-kms-key-id.

Anpassungen im Malware-Schutz für EC2

In diesem Abschnitt wird beschrieben, wie Sie die Scanoptionen für Ihre EC2 Amazon-Instances oder Container-Workloads anpassen können, wenn ein Malware-Scan ausgelöst wird, entweder bei Bedarf oder über. GuardDuty

Allgemeine Einstellungen

Snapshot-Beibehaltung

GuardDuty bietet Ihnen die Möglichkeit, die Snapshots Ihrer EBS Volumes in Ihrem Konto zu speichern. AWS Standardmäßig ist die Aufbewahrungseinstellung für Snapshots deaktiviert. Die Snapshots werden nur beibehalten, wenn Sie diese Einstellung aktiviert haben, bevor der Scan gestartet wird.

Bei Beginn des Scans werden die EBS Replikat-Volumes auf der Grundlage der Snapshots Ihrer Volumes GuardDuty generiert. EBS Nachdem der Scan abgeschlossen ist und die Einstellung zur Aufbewahrung von Snapshots in Ihrem Konto bereits aktiviert wurde, werden die Snapshots Ihrer EBS Volumes nur dann aufbewahrt, wenn Malware gefunden und generiert wird. Malware-Schutz für EC2-Suchtypen Unabhängig davon, ob Sie die Einstellung zur Aufbewahrung von Snapshots aktiviert haben oder nicht, werden die Snapshots Ihrer Volumes GuardDuty automatisch gelöscht, wenn keine Malware erkannt wird. EBS

Nutzungskosten für Snapshots

Während des Malware-Scans, bei dem die Snapshots Ihrer EBS Amazon-Volumes GuardDuty erstellt werden, fallen mit diesem Schritt Nutzungskosten an. Wenn Sie die Einstellung zur Aufbewahrung von Snapshots für Ihr Konto aktivieren, fallen für Sie Nutzungskosten an, wenn Malware gefunden wird und die Snapshots beibehalten werden. Informationen zu den Kosten von Snapshots und deren Aufbewahrung finden Sie unter EBSAmazon-Preise.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die Aufbewahrungseinstellung für Snapshots zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware-Schutz für ausEC2.
3. Wählen Sie im unteren Bereich der Konsole Allgemeine Einstellungen. Um die Snapshots beizubehalten, aktivieren Sie die Option Beibehaltung von Snapshots.

API/CLI

1. Ausführen UpdateMalwareScanSettings, um die aktuelle Konfiguration für die Einstellung zur Aufbewahrung von Snapshots zu aktualisieren.
2. Alternativ können Sie den folgenden AWS CLI Befehl ausführen, um Snapshots automatisch beizubehalten, wenn GuardDuty Malware Protection for Ergebnisse EC2 generiert.

   Stellen Sie sicher, dass Sie das ersetzen *detector-id* mit Ihrem eigenen gültigen`detectorId`.
3. Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Einstellungsseite in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

   ```
   aws guardduty update-malware-scan-settings --detector-
   id 60b87779336485625 54d637e0e4bb3b2 --ebs-snapshot-preservation
    "RETENTION_WITH_FINDING"
   ```
4. Wenn Sie die Beibehaltung von Snapshots deaktivieren möchten, ersetzen Sie sie `RETENTION_WITH_FINDING` durch `NO_RETENTION`.

Scan-Optionen mit benutzerdefinierten Tags

Mithilfe des GuardDuty -initiierten Malware-Scans können Sie auch Tags angeben, um EC2 Amazon-Instances und EBS Amazon-Volumes vom Scan- und Bedrohungserkennungsprozess entweder ein- oder auszuschließen. Sie können jeden GuardDuty -initiierten Malware-Scan individuell anpassen, indem Sie die Tags entweder in der Liste der Inklusions- oder Ausschlusstags bearbeiten. Jede Liste kann bis zu 50 Tags enthalten.

Wenn Sie noch keine benutzerdefinierten Tags mit Ihren EC2 Ressourcen verknüpft haben, finden Sie weitere Informationen unter Taggen Sie Ihre EC2 Amazon-Ressourcen im EC2Amazon-Benutzerhandbuch oder Taggen Sie Ihre EC2 Amazon-Ressourcen im EC2Amazon-Benutzerhandbuch.

> **Note**
>
> Der Malware-Scan auf Abruf unterstützt keine Scan-Optionen mit benutzerdefinierten Tags. Er unterstützt Globales `GuardDutyExcluded`-Tag.

Um EC2 Instances vom Malware-Scan auszuschließen

Wenn Sie eine EC2 Amazon-Instance oder ein EBS Amazon-Volume während des Scanvorgangs ausschließen möchten, können Sie das `GuardDutyExcluded` Tag `true` für jede EC2 Amazon-Instance oder jedes EBS Amazon-Volume auf setzen und es GuardDuty wird nicht gescannt. Weitere Informationen über das `GuardDutyExcluded`-Tag finden Sie unter Servicebezogene Rollenberechtigungen für Malware Protection für EC2. Sie können auch ein EC2 Amazon-Instance-Tag zu einer Ausschlussliste hinzufügen. Wenn Sie der Liste der Ausschluss-Tags mehrere Tags hinzufügen, wird jede EC2 Amazon-Instance, die mindestens eines dieser Tags enthält, vom Malware-Scanvorgang ausgeschlossen.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um ein mit einer EC2 Amazon-Instance verknüpftes Tag zu einer Ausschlussliste hinzuzufügen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware-Schutz für ausEC2.
3. Erweitern Sie den Abschnitt Einschluss-/Ausschluss-Tags. Wählen Sie Tags hinzufügen aus.
4. Wählen Sie Ausschluss-Tags und anschließend Bestätigen.
5. Geben Sie das **`Key`**- und **`Value`**-Paar des Tags an, das Sie ausschließen möchten. Die Angabe von **`Value`** ist optional. Nachdem Sie alle Tags hinzugefügt haben, wählen Sie Speichern.

> **Important**
>
> Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter Tag-Einschränkungen im EC2Amazon-Benutzerhandbuch oder Tag-Einschränkungen im EC2Amazon-Benutzerhandbuch.

Wenn kein Wert für einen Schlüssel angegeben wird und die EC2 Instance mit dem angegebenen Schlüssel gekennzeichnet ist, wird diese EC2 Instance unabhängig vom zugewiesenen Wert des Tags vom GuardDuty -initiierten Malware-Scanvorgang ausgeschlossen.

API/CLI

- Aktualisieren Sie die Einstellungen für den Malware-Scan, indem Sie eine EC2 Instanz oder einen Container-Workload vom Scanvorgang ausschließen.

  Mit dem folgenden AWS CLI Beispielbefehl wird der Liste der Ausschluss-Tags ein neues Tag hinzugefügt. Achten Sie darauf, das Beispiel zu ersetzen *`detector-id`* mit Ihrem eigenen gültigen`detectorId`.

  `MapEquals` ist eine Liste von `Key`/`Value`-Paaren.

  Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Einstellungsseite in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

  ```
  aws guardduty update-malware-scan-settings --detector-
  id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
   {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
   "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
   "RETENTION_WITH_FINDING"
  ```

  Important

  Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter Tag-Einschränkungen im EC2Amazon-Benutzerhandbuch oder Tag-Einschränkungen im EC2Amazon-Benutzerhandbuch.

Um EC2 Instances in den Malware-Scan einzubeziehen

Wenn Sie eine EC2 Instanz scannen möchten, fügen Sie ihr Tag zur Aufnahmeliste hinzu. Wenn Sie ein Tag zu einer Liste mit Einschlusstags hinzufügen, wird eine EC2 Instanz, die keines der hinzugefügten Tags enthält, aus dem Malware-Scan übersprungen. Wenn Sie der Liste der Einschlusstags mehrere Tags hinzufügen, wird eine EC2 Instanz, die mindestens eines dieser Tags enthält, in den Malware-Scan aufgenommen. Manchmal kann es vorkommen, dass eine EC2 Instanz während des Scanvorgangs übersprungen wird. Weitere Informationen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um ein mit einer EC2 Instanz verknüpftes Tag zu einer Aufnahmeliste hinzuzufügen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware-Schutz für ausEC2.
3. Erweitern Sie den Abschnitt Einschluss-/Ausschluss-Tags. Wählen Sie Tags hinzufügen aus.
4. Wählen Sie Einschluss-Tags und dann Bestätigen.
5. Wählen Sie Neues Einschluss-Tag hinzufügen und geben Sie das **`Key`**- und **`Value`**-Paar des Tags an, das Sie einbeziehen möchten. Die Angabe von **`Value`** ist optional.

   Nachdem Sie alle Einschluss-Tags hinzugefügt haben, wählen Sie Speichern.

   Wenn kein Wert für einen Schlüssel angegeben wird, ist eine EC2 Instanz mit dem angegebenen Schlüssel gekennzeichnet, wird die EC2 Instanz unabhängig vom zugewiesenen Wert in den Malware-Schutz für den EC2 Scanvorgang aufgenommen.

API/CLI

- Aktualisieren Sie die Einstellungen für den Malware-Scan, um eine EC2 Instanz oder einen Container-Workload in den Scanvorgang einzubeziehen.

  Mit dem folgenden AWS CLI Beispielbefehl wird der Liste der Einschlusstags ein neues Tag hinzugefügt. Stellen Sie sicher, dass Sie das Beispiel ersetzen *`detector-id`* mit Ihrem eigenen gültigen`detectorId`. Ersetze das Beispiel *`TestKey`* and *`TestValue`* durch das `Value` Paar `Key` und des Tags, das mit Ihrer EC2 Ressource verknüpft ist.

`MapEquals` ist eine Liste von `Key`/`Value`-Paaren.

Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite „Einstellungen“ oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625554d637e0e4bb3b2 --scan-resource-criteria '{"Include":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

Important

Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter Tag-Einschränkungen im EC2Amazon-Benutzerhandbuch oder Tag-Einschränkungen im EC2Amazon-Benutzerhandbuch.

Note

Es kann bis zu 5 Minuten dauern GuardDuty , bis ein neues Tag erkannt wird.

Sie können jederzeit entweder Einschluss-Tags oder Ausschluss-Tags wählen, aber nicht beides. Wenn Sie zwischen den Tags wechseln möchten, wählen Sie dieses Tag aus dem Drop-down-Menü aus, wenn Sie neue Tags hinzufügen, und Bestätigen Sie Ihre Auswahl. Diese Aktion löscht alle Ihre aktuellen Tags.

Globales **`GuardDutyExcluded`**-Tag

Standardmäßig werden die Snapshots Ihrer EBS Volumes mit einem `GuardDutyScanId` Tag erstellt. Entfernen Sie dieses Tag nicht, da dadurch der Zugriff auf die Snapshots GuardDuty verhindert wird. Beide Scantypen in Malware Protection for scannen EC2 nicht die EC2 Amazon-Instances oder EBS Amazon-Volumes, auf die das `GuardDutyExcluded` Tag gesetzt ist`true`. Wenn ein Malware-Schutz für eine solche Ressource EC2 scannt, wird zwar eine Scan-ID generiert, der Scan wird jedoch mit Angabe eines `EXCLUDED_BY_SCAN_SETTINGS` Grundes übersprungen.

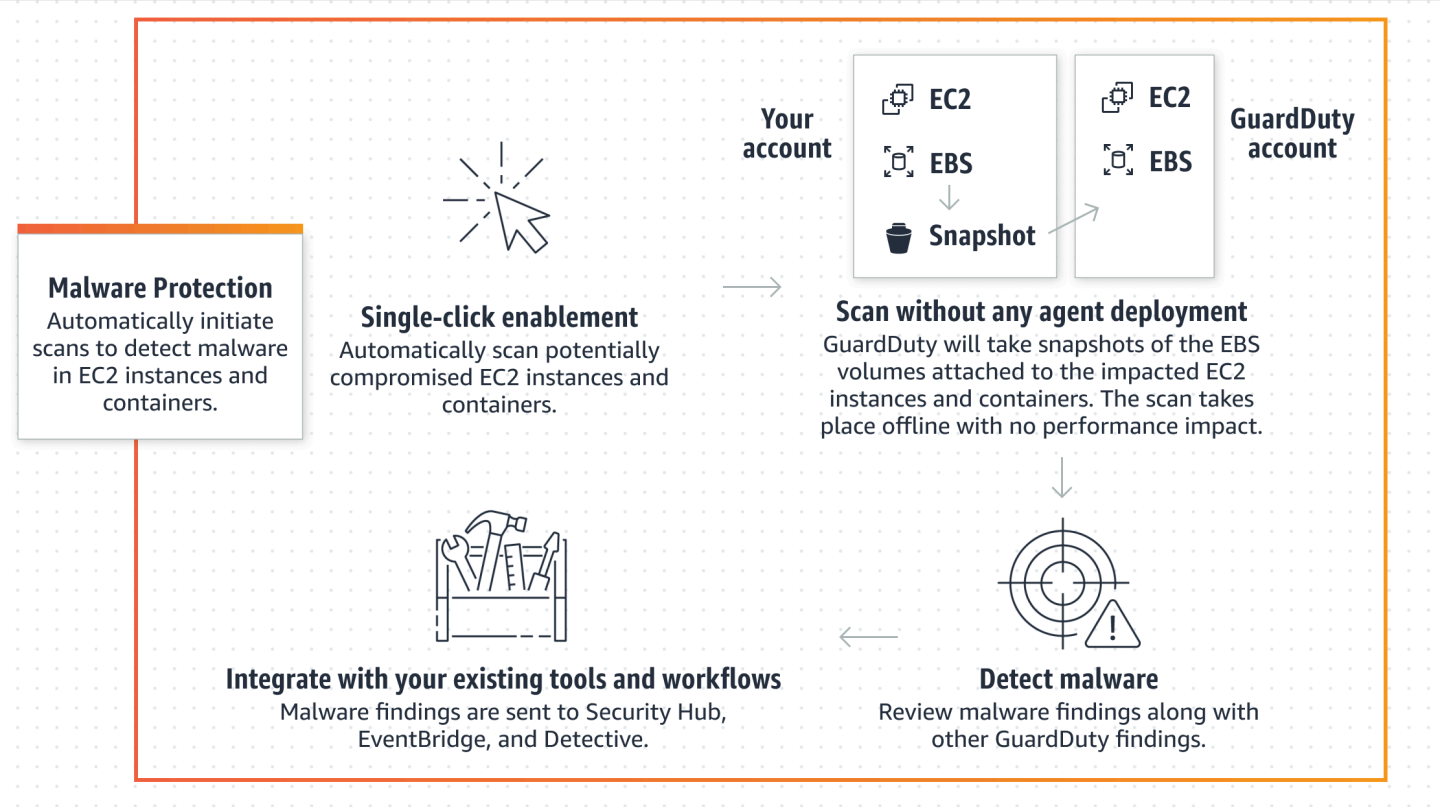
Weitere Informationen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan.

GuardDuty-hat einen Malware-Scan initiiert

Wenn der GuardDuty -initiierte Malware-Scan aktiviert ist, wird bei jeder GuardDuty Erkennung bösartiger Aktivitäten, die auf das potenzielle Vorhandensein von Malware in Ihrer EC2 Amazon-Instance- oder Container-Workload hinweisenErgebnisse, die einen GuardDuty -initiierten Malware-Scan auslösen, GuardDuty automatisch ein agentenloser Scan auf den Amazon Elastic Block Store (AmazonEBS) -Volumes initiiert, die an die potenziell betroffene EC2 Amazon-Instance oder Container-Workload angehängt sind, um das Vorhandensein von Malware zu erkennen. GuardDuty Mit den Scan-Optionen können Sie Einschluss-Tags hinzufügen, die mit den Ressourcen verknüpft sind, die Sie scannen möchten, oder Ausschluss-Tags hinzufügen, die mit den Ressourcen verknüpft sind, die Sie aus dem Scanvorgang auslassen möchten. Bei der automatischen Initiierung des Scans werden immer Ihre Scan-Optionen berücksichtigt. Sie können auch die Einstellung für die Aufbewahrung von Snapshots aktivieren, sodass die Snapshots Ihrer EBS Volumes nur dann aufbewahrt werden, wenn Malware Protection for EC2 das Vorhandensein von Malware erkennt. Weitere Informationen finden Sie unter Anpassungen im Malware-Schutz für EC2.

Für jede EC2 Amazon-Instance und Container-Workload, für die Ergebnisse GuardDuty generiert werden, wird alle 24 Stunden ein automatisch GuardDuty initiierter Malware-Scan aufgerufen. Informationen darüber, wie die EBS Amazon-Volumes gescannt werden, die Ihrer EC2 Amazon-Instance- oder Container-Workload zugeordnet sind, finden Sie unterFunktion im Malware-Schutz für EC2.

In der folgenden Abbildung wird beschrieben, wie der von GuardDuty -initiierte Malware-Scan funktioniert.



Informationen zur Methode zur GuardDuty Malware-Erkennung und zu den verwendeten Scan-Engines finden Sie unterGuardDuty Scan-Engine zur Malware-Erkennung.

Wenn Malware gefunden wird, wird GuardDuty generiertMalware-Schutz für EC2-Suchtypen. Wenn GuardDuty kein Ergebnis generiert wird, das auf Malware auf derselben Ressource hinweist, wird kein GuardDuty -initiierter Malware-Scan ausgeführt. Sie können auf derselben Ressource auch einen Malware-Scan auf Abruf starten. Weitere Informationen finden Sie unter Malware-Scan auf Abruf.

Kostenlose 30-Tage-Testversion

Sie können jederzeit wählen, ob Sie den von GuardDuty uns initiierten Malware-Scan für ein unterstütztes AWS-Konto AWS-Region Gerät aktivieren oder deaktivieren möchten. Wenn Sie ein Unternehmen haben, hat jedes Mitgliedskonto eine eigene kostenlose 30-Tage-Testversion.

Um zu verstehen, wie die kostenlose 30-Tage-Testversion funktioniert, sollten Sie sich die folgenden Szenarien ansehen:

- Wenn Sie den Dienst GuardDuty zum ersten Mal aktivieren (neues GuardDuty Konto), wird auch der von GuardDuty uns initiierte Malware-Scan aktiviert. Er ist in der kostenlosen 30-Tage-Testversion des Dienstes enthalten. GuardDuty
- Ein vorhandenes GuardDuty Konto kann im Rahmen einer kostenlosen GuardDuty 30-Tage-Testversion zum ersten Mal den -initiierten Malware-Scan aktivieren. Wenn Sie diese Funktion zum ersten Mal in einer anderen Region aktivieren, erhalten Sie in dieser Region eine kostenlose 30-Tage-Testversion.
- Wenn Sie bereits über ein GuardDuty Konto verfügen, für das der Malware-Schutz EC2 vor der Ankündigung des On-Demand-Malware-Scans verwendet wurde, und für dieses GuardDuty Konto bereits das Preismodell gilt AWS-Region, können Sie den GuardDuty -initiierten Malware-Scan weiterhin verwenden.

> **Note**
>
> Selbst wenn Sie eine 30-tägige kostenlose Testphase haben, fallen die Standardnutzungskosten für die Erstellung der Amazon EBS Volume Snapshots und deren Aufbewahrung an. Weitere Informationen finden Sie unter EBSAmazon-Preise.

Informationen zur Aktivierung des GuardDuty -initiierten Malware-Scans finden Sie unterKonfiguration des GuardDuty -initiierten Malware-Scans.

Konfiguration des GuardDuty -initiierten Malware-Scans

Konfiguration des GuardDuty -initiierten Malware-Scans für ein eigenständiges Konto

Für Konten, die mit verknüpft sind AWS Organizations, können Sie diesen Vorgang über die Konsoleneinstellungen automatisieren, wie im nächsten Abschnitt beschrieben.

Um den GuardDuty -initiierten Malware-Scan zu aktivieren oder zu deaktivieren

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty -initiierten Malware-Scan für ein eigenständiges Konto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware-Schutz für ausEC2.

3. Im EC2 Bereich Malware-Schutz für wird der aktuelle Status des GuardDuty -initiierten Malware-Scans für Ihr Konto aufgeführt. Sie können das jederzeit aktivieren oder deaktivieren, indem Sie Aktivieren oder Deaktivieren auswählen.
4. Wählen Sie Save (Speichern) aus.

API/CLI

- Führen Sie den updateDetectorAPIVorgang mit Ihrer eigenen regionalen Melder-ID aus und übergeben Sie das `dataSources` Objekt mit der `EbsVolumes` Einstellung auf `true` oder`false`.

  Sie können den GuardDuty -initiierten Malware-Scan auch mithilfe von AWS Befehlszeilentools aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie Ihr eigenes gültiges *`detector ID`*.

  > **Note**
  >
  > Der folgende Beispielcode aktiviert den GuardDuty -initiierten Malware-Scan. Um die Funktion zu deaktivieren, ersetzen Sie `true` durch `false`.

  Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

Konfiguration des GuardDuty -initiierten Malware-Scans in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten können nur GuardDuty Administratorkonten den -initiierten Malware-Scan konfigurieren. GuardDuty GuardDuty Administratorkonten können die Verwendung des GuardDuty -initiierten Malware-Scans für ihre Mitgliedskonten aktivieren oder deaktivieren. Sobald das Administratorkonto den GuardDuty -initiierten Malware-Scan für ein Mitgliedskonto konfiguriert hat, folgt das Mitgliedskonto den Einstellungen des Administratorkontos und kann diese Einstellungen nicht über die Konsole ändern. GuardDuty Administratorkonten, die ihre

Mitgliedskonten beim AWS Organizations Support verwalten, können festlegen, dass der GuardDuty -initiierte Malware-Scan automatisch für alle vorhandenen und neuen Konten in der Organisation aktiviert wird. Weitere Informationen finden Sie unter GuardDuty Konten verwalten mit AWS Organizations.

Einrichtung eines vertrauenswürdigen Zugriffs zur Aktivierung des GuardDuty -initiierten Malware-Scans

Wenn das GuardDuty delegierte Administratorkonto nicht mit dem Verwaltungskonto in Ihrer Organisation identisch ist, muss das Verwaltungskonto den GuardDuty -initiierten Malware-Scan für die Organisation aktivieren. Auf diese Weise kann das delegierte Administratorkonto die Servicebezogene Rollenberechtigungen für Malware Protection für EC2 internen Mitgliedskonten erstellen, über die verwaltet werden. AWS Organizations

> **Note**
>
> Bevor Sie ein delegiertes GuardDuty Administratorkonto festlegen, finden Sie weitere Informationen unter. Überlegungen und Empfehlungen

Wählen Sie Ihre bevorzugte Zugriffsmethode, damit das delegierte GuardDuty Administratorkonto die von Ihnen GuardDuty initiierte Malware-Suche für Mitgliedskonten in der Organisation aktivieren kann.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Verwenden Sie das Verwaltungskonto Ihrer AWS Organizations Organisation, um sich anzumelden.

2. a. Wenn Sie kein delegiertes GuardDuty Administratorkonto angegeben haben, gehen Sie wie folgt vor:

      Geben Sie auf der Seite Einstellungen unter Delegiertes GuardDuty Administratorkonto die 12-stellige Zahl ein, **`account ID`** die Sie für die Verwaltung der GuardDuty Richtlinie in Ihrer Organisation angeben möchten. Wählen Sie Delegieren.

   b. i. Wenn Sie bereits ein delegiertes GuardDuty Administratorkonto festgelegt haben, das sich vom Verwaltungskonto unterscheidet, gehen Sie wie folgt vor:

Aktivieren Sie auf der Seite Einstellungen unter Delegierter Administrator die Einstellung Berechtigungen. Diese Aktion ermöglicht es dem delegierten GuardDuty Administratorkonto, den Mitgliedskonten entsprechende Berechtigungen zuzuweisen und in diesen Mitgliedskonten den von GuardDuty Hand initiierten Malware-Scan zu aktivieren.

ii. Wenn Sie bereits ein delegiertes GuardDuty Administratorkonto eingerichtet haben, das mit dem Verwaltungskonto identisch ist, können Sie den GuardDuty -initiierten Malware-Scan für die Mitgliedskonten direkt aktivieren. Weitere Informationen finden Sie unter Automatisch aktivieren GuardDuty — initiierter Malware-Scan für alle Mitgliedskonten.

> **Tip**
>
> Wenn sich das delegierte GuardDuty Administratorkonto von Ihrem Verwaltungskonto unterscheidet, müssen Sie dem delegierten GuardDuty Administratorkonto Berechtigungen zuweisen, um die Aktivierung des GuardDuty -initiierten Malware-Scans für Mitgliedskonten zu ermöglichen.

3. Wenn Sie dem delegierten GuardDuty Administratorkonto erlauben möchten, den GuardDuty -initiierten Malware-Scan für Mitgliedskonten in anderen Regionen zu aktivieren, ändern Sie Ihr Konto und wiederholen Sie die AWS-Region obigen Schritte.

API/CLI

1. Mit den Anmeldeinformationen für Ihr Verwaltungskonto führen Sie den folgenden Befehl aus:

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (Optional) Um den GuardDuty -initiierten Malware-Scan für das Verwaltungskonto zu aktivieren, bei dem es sich nicht um ein delegiertes Administratorkonto handelt, erstellt das Verwaltungskonto zuerst das Servicebezogene Rollenberechtigungen für Malware Protection für EC2 explizit in seinem Konto und aktiviert dann den GuardDuty -initiierten Malware-Scan vom delegierten Administratorkonto aus, ähnlich wie bei jedem anderen Mitgliedskonto.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. Sie haben das delegierte GuardDuty Administratorkonto im aktuell ausgewählten Konto angegeben. AWS-Region Wenn Sie in einer Region ein Konto als delegiertes GuardDuty Administratorkonto festgelegt haben, muss dieses Konto Ihr delegiertes GuardDuty Administratorkonto in allen anderen Regionen sein. Wiederholen Sie den obigen Schritt für alle anderen Regionen.

Konfiguration des GuardDuty -initiierten Malware-Scans für das delegierte Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty -initiierten Malware-Scan für ein GuardDuty delegiertes Administratorkonto zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen des Verwaltungskontos verwenden.
2. Wählen Sie im Navigationsbereich die Option Malware-Schutz für ausEC2.
3. Wählen Sie auf der EC2 Seite Malware-Schutz für neben GuardDuty-initiierter Malware-Scan die Option Bearbeiten aus.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Save (Speichern) aus.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.

- Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Save (Speichern) aus.

API/CLI

Führen Sie den updateDetectorAPIVorgang mit Ihrer eigenen regionalen Melder-ID aus und übergeben Sie das `features` Objekt `name` als `EBS_MALWARE_PROTECTION` und `status` als `ENABLED` oder`DISABLED`.

Sie können den GuardDuty -initiierten Malware-Scan aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie ein gültiges delegiertes GuardDuty Administratorkonto verwenden *`detector ID`*.

> **Note**
>
> Der folgende Beispielcode aktiviert den GuardDuty -initiierten Malware-Scan. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Automatisch aktivieren GuardDuty — initiierter Malware-Scan für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die GuardDuty -initiierte Malware-Scan-Funktion für alle Mitgliedskonten zu aktivieren. Dazu gehören der delegierte Administrator, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   Seite „Malware-Schutz für EC2“ verwenden

   1. Wählen Sie im Navigationsbereich die Option Malware-Schutz für ausEC2.
   2. Wählen Sie auf der EC2 Seite Malware-Schutz für im Abschnitt GuardDuty-initiierter Malware-Scan die Option Bearbeiten aus.
   3. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch den GuardDuty -initiierten Malware-Scan sowohl für bestehende als auch für neue Konten in der Organisation.
   4. Wählen Sie Save (Speichern) aus.

   > **Note**
   >
   > Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

   Verwenden der Seite Konten

   1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
   2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
   3. Wählen Sie im Fenster „Einstellungen für automatische Aktivierung verwalten“ die Option „Für alle Konten unter GuardDuty-initiiertem Malware-Scan aktivieren“ aus.
   4. Wählen Sie auf der EC2 Seite Malware-Schutz für im Bereich GuardDuty-initiierter Malware-Scan die Option Bearbeiten aus.
   5. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch den GuardDuty -initiierten Malware-Scan sowohl für bestehende als auch für neue Konten in der Organisation.
   6. Wählen Sie Save (Speichern) aus.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwenden der Seite Konten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
3. Wählen Sie im Fenster „Einstellungen für automatische Aktivierung verwalten“ die Option „Für alle Konten unter GuardDuty-initiiertem Malware-Scan aktivieren“ aus.
4. Wählen Sie Save (Speichern) aus.

Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Aktiviere oder deaktiviere selektiv den von GuardDuty dir initiierten Malware-Scan für Mitgliedskonten.

API/CLI

- Um den GuardDuty -initiierten Malware-Scan für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, starten Sie den Vorgang mit Ihrem eigenen updateMemberDetectorsAPI *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie den GuardDuty -initiierten Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können. Um ein Mitgliedskonto zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie den GuardDuty -initiierten Malware-Scan für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty -initiierten Malware-Scan für alle vorhandenen aktiven Mitgliedskonten in der Organisation zu aktivieren.

So konfigurieren Sie den GuardDuty -initiierten Malware-Scan für alle vorhandenen aktiven Mitgliedskonten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich die Option Malware-Schutz für EC2 aus.
3. Im Fenster Malware-Schutz für EC2 können Sie den aktuellen Status der Konfiguration des GuardDuty-initiierten Malware-Scans einsehen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Save (Speichern) aus.

Automatische Aktivierung des GuardDuty -initiierten Malware-Scans für neue Mitgliedskonten

Die neu hinzugefügten Mitgliedskonten müssen aktiviert werden, GuardDuty bevor die Konfiguration des GuardDuty -initiierten Malware-Scans ausgewählt werden kann. Die auf Einladung verwalteten Mitgliedskonten können den GuardDuty -initiierten Malware-Scan für ihre Konten manuell konfigurieren. Weitere Informationen finden Sie unter Step 3 - Accept an invitation.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty -initiierten Malware-Scan für neue Konten zu aktivieren, die Ihrer Organisation beitreten.

Console

Das delegierte GuardDuty Administratorkonto kann den GuardDuty -initiierten Malware-Scan für neue Mitgliedskonten in einer Organisation entweder über die Seite Malware-Schutz für EC2 oder Konten aktivieren.

So aktivieren Sie automatisch den GuardDuty -initiierten Malware-Scan für neue Mitgliedskonten

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Führen Sie eine der folgenden Aktionen aus:
   - EC2Seite „Malware-Schutz für“ verwenden:
     1. Wählen Sie im Navigationsbereich die Option Malware-Schutz für ausEC2.
     2. Wählen Sie auf der EC2 Seite Malware-Schutz für beim GuardDuty-initiierten Malware-Scan die Option Bearbeiten aus.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Durch diesen Schritt wird sichergestellt, dass jedes Mal, wenn ein neues Konto Ihrer Organisation beitritt, der von einem neuen Konto GuardDuty initiierte Malware-Scan automatisch für das Konto aktiviert wird. Nur das vom Unternehmen delegierte GuardDuty Administratorkonto kann diese Konfiguration ändern.
     5. Wählen Sie Save (Speichern) aus.
   - Verwenden der Seite Konten:
     1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
     2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren.
     3. Wählen Sie im Fenster „Einstellungen für automatische Aktivierung verwalten“ die Option „Für neue Konten aktivieren“ unter „GuardDuty-initiierter Malware-Scan“ aus.
     4. Wählen Sie Save (Speichern) aus.

API/CLI

- Um den GuardDuty -initiierten Malware-Scan für neue Mitgliedskonten zu aktivieren oder zu deaktivieren, starten Sie den Vorgang mit Ihrem eigenen UpdateOrganizationConfigurationAPI *detector ID*.
- Das folgende Beispiel zeigt, wie Sie den GuardDuty -initiierten Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können. Informationen zur Deaktivierung finden Sie unter Aktiviere oder deaktiviere selektiv den von GuardDuty dir initiierten Malware-Scan für Mitgliedskonten. Wenn Sie es nicht für alle neuen Konten aktivieren möchten, die der Organisation beitreten, legen Sie die Einstellung `AutoEnable` auf `NONE` fest.

  Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name":
   "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
  ```

  Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.
- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktiviere oder deaktiviere selektiv den von GuardDuty dir initiierten Malware-Scan für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den GuardDuty -initiierten Malware-Scan für Mitgliedskonten selektiv zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Prüfen Sie auf der Kontoseite in der Spalte „GuardDuty-initiierter Malware-Scan“ den Status Ihres Mitgliedskontos.

4. Wählen Sie das Konto aus, für das Sie den GuardDuty -initiierten Malware-Scan konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
5. Wählen Sie im Menü Schutzpläne bearbeiten die entsprechende Option für den GuardDuty-initiierten Malware-Scan aus.

API/CLI

Um den GuardDuty -initiierten Malware-Scan für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, starten Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen *detector ID*.

Das folgende Beispiel zeigt, wie Sie den GuardDuty -initiierten Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "Status": "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Um den von Ihnen GuardDuty initiierten Malware-Scan für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, führen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen aus *detector ID*. Das folgende Beispiel zeigt, wie Sie den GuardDuty -initiierten Malware-Scan für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `true` durch `false`.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

> **Note**
>
> Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie den GuardDuty -initiierten Malware-Scan für bestehende Konten in der Organisation, die per Einladung verwaltet werden

Die Rolle „ GuardDuty Malware-Schutz für EC2 den Service“ (SLR) muss in den Mitgliedskonten erstellt werden. Das Administratorkonto kann die Funktion „ GuardDuty-initiierter Malware-Scan“ nicht in Mitgliedskonten aktivieren, die nicht von verwaltet werden. AWS Organizations

Derzeit können Sie über die GuardDuty Konsole unter die folgenden Schritte ausführen, https://console.aws.amazon.com/guardduty/um den GuardDuty -initiierten Malware-Scan für die vorhandenen Mitgliedskonten zu aktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Melden Sie sich mit den Anmeldeinformationen Ihres Administratorkontos an.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie das Mitgliedskonto aus, für das Sie den GuardDuty -initiierten Malware-Scan aktivieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
4. Wählen Sie Aktionen.
5. Wählen Sie Mitglied trennen.

6. Wählen Sie im Mitgliedskonto im Navigationsbereich Malware Protection unter Schutzpläne.
7. Wählen Sie „ GuardDuty-initiierten Malware-Scan aktivieren“. GuardDuty erstellt ein Konto SLR für das Mitglied. Weitere Informationen zu finden SLR Sie unterServicebezogene Rollenberechtigungen für Malware Protection für EC2.
8. Wählen Sie in Ihrem Administratorkonto im Navigationsbereich Konten aus.
9. Wählen Sie das Mitgliedskonto aus, das der Organisation wieder hinzugefügt werden muss.
10. Wählen Sie Aktionen und dann Mitglied hinzufügen.

API/CLI

1. Verwenden Sie das Administratorkonto, um die Ausführung DisassociateMembersAPIauf die Mitgliedskonten durchzuführen, die den durch den Benutzer GuardDuty initiierten Malware-Scan aktivieren möchten.
2. Verwenden Sie Ihr Mitgliedskonto, um den GuardDuty -initiierten Malware-Scan aufzurufen und UpdateDetectorzu aktivieren.

   Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus. ListDetectorsAPI

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
   {"EbsVolumes":true}}}'
   ```
3. Verwenden Sie das Administratorkonto, CreateMembersAPIum den auszuführen, um das Mitglied wieder zur Organisation hinzuzufügen.

Ergebnisse, die einen GuardDuty -initiierten Malware-Scan auslösen

Ein GuardDuty -initiierter Malware-Scan wird ausgelöst, wenn verdächtiges Verhalten GuardDuty entdeckt wird, das auf Malware in EC2 Amazon-Instance- oder Container-Workloads hindeutet.

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp

- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce (Nur ausgehend)
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/RDPBruteForce (Nur ausgehend)
- UnauthorizedAccess:EC2/SSHBruteForce (Nur ausgehend)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B!DNS

- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

Malware-Scan auf Abruf

Der On-Demand-Malware-Scan hilft Ihnen dabei, das Vorhandensein von Malware auf Amazon Elastic Block Store (AmazonEBS) -Volumes zu erkennen, die an Ihre EC2 Amazon-Instances angehängt sind. Ohne Konfiguration können Sie einen On-Demand-Malware-Scan initiieren, indem Sie den Amazon-Ressourcennamen (ARN) der EC2 Amazon-Instance angeben, die Sie scannen

möchten. Sie können einen On-Demand-Malware-Scan entweder über die GuardDuty Konsole oder startenAPI. Bevor Sie einen Malware-Scan auf Abruf starten, können Sie Ihre bevorzugte Snapshot-Beibehaltung-Einstellung festlegen. Anhand der folgenden Szenarien können Sie ermitteln, wann Sie den Malware-Scan auf Abruf verwenden sollten GuardDuty:

- Sie möchten das Vorhandensein von Malware in Ihren EC2 Amazon-Instances erkennen, ohne den GuardDuty -initiierten Malware-Scan zu aktivieren.
- Sie haben den GuardDuty -initiierten Malware-Scan aktiviert und ein Scan wurde automatisch gestartet. Wenn Sie die empfohlene Abhilfemaßnahme für den Typ „Generierter Malware-Schutz für die EC2 Suche“ befolgt haben, können Sie, wenn Sie einen Scan auf derselben Ressource starten möchten, einen Malware-Scan auf Anforderung starten, nachdem 1 Stunde nach der Startzeit des vorherigen Scans vergangen ist.

  Der Malware-Scan auf Abruf setzt nicht voraus, dass seit dem Zeitpunkt, an dem der vorherige Malware-Scan initiiert wurde, 24 Stunden vergangen sind. Es sollte eine Stunde vergangen sein, bevor ein Malware-Scan auf Abruf auf derselben Ressource gestartet wird. Informationen dazu, wie Sie vermeiden können, dass ein Malware-Scan auf derselben EC2 Instanz dupliziert wird, finden Sie unter. Dieselbe EC2 Amazon-Instance erneut scannen

> **Note**
>
> Der On-Demand-Malware-Scan ist in der 30-tägigen kostenlosen Testphase von nicht enthalten. GuardDuty Die Nutzungskosten beziehen sich auf das gesamte EBS Amazon-Volumen, das bei jedem Malware-Scan gescannt wurde. Weitere Informationen finden Sie unter GuardDuty Amazon-Preise. Informationen zu den Kosten für die Erstellung der Amazon EBS Volume Snapshots und deren Aufbewahrung finden Sie unter EBSAmazon-Preise.

So funktioniert der Malware-Scan auf Abruf

Mit dem On-Demand-Malware-Scan können Sie eine Malware-Scan-Anfrage für Ihre EC2 Amazon-Instance initiieren, auch wenn sie gerade verwendet wird. Nachdem Sie einen On-Demand-Malware-Scan initiiert haben, GuardDuty erstellt Snapshots der EBS Amazon-Volumes, die an die EC2 Amazon-Instance angehängt sind, deren Amazon-Ressourcenname (ARN) für den Scan angegeben wurde. Als Nächstes GuardDuty teilt diese Schnappschüsse mit dem. GuardDuty Dienstkonto GuardDuty erstellt verschlüsselte EBS Replikat-Volumes aus diesen Snapshots im GuardDuty

Dienstkonto. Weitere Informationen darüber, wie die EBS Amazon-Volumes gescannt werden, finden Sie unterElastisches Blockspeicher-Volumen (EBS).

> **Note**
>
> GuardDuty erstellt die Snapshots der Daten, die bereits auf die EBS Amazon-Volumes geschrieben wurden, point-in-time wenn Sie einen On-Demand-Malware-Scan starten.

Wenn Malware gefunden wird und Sie die Aufbewahrungseinstellung für Snapshots aktiviert haben, werden die Snapshots Ihres EBS Volumes automatisch in Ihrem gespeichert. AWS-Konto Der Malware-Scan auf Abruf generiert die Malware-Schutz für EC2-Suchtypen. Wenn keine Malware gefunden wird, werden die Snapshots Ihrer EBS Volumes unabhängig von der Einstellung zur Aufbewahrung von Snapshots gelöscht.

Standardmäßig werden die Snapshots Ihrer EBS Volumes mit einem Tag erstellt. `GuardDutyScanId` Entfernen Sie dieses Tag nicht, da dadurch der Zugriff auf die Snapshots GuardDuty verhindert wird. Beide Scantypen in Malware Protection for scannen EC2 nicht die EC2 Amazon-Instances oder EBS Amazon-Volumes, auf die das `GuardDutyExcluded` Tag gesetzt ist`true`. Wenn ein Malware-Schutz für eine solche Ressource EC2 scannt, wird zwar eine Scan-ID generiert, der Scan wird jedoch mit Angabe eines `EXCLUDED_BY_SCAN_SETTINGS` Grundes übersprungen. Weitere Informationen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan.

AWS Organizations Richtlinie zur Dienststeuerung — Zugriff verweigert

Mithilfe der Service-Kontrollrichtlinien (SCPs) in AWS Organizations kann das delegierte GuardDuty Administratorkonto Berechtigungen einschränken und Aktionen wie das Initiieren eines On-Demand-Malware-Scans für EC2 Amazon-Instances, die Ihren Konten gehören, verweigern.

Als GuardDuty Mitgliedskonto erhalten Sie möglicherweise eine Fehlermeldung, wenn Sie einen On-Demand-Malware-Scan für Ihre EC2 Amazon-Instances starten. Sie können sich mit dem Verwaltungskonto verbinden, um zu erfahren, warum für Ihr Mitgliedskonto ein Konto eingerichtet SCP wurde. Weitere Informationen finden Sie unter SCPAuswirkungen auf Berechtigungen.

Erste Schritte mit dem Malware-Scan auf Abruf

Als GuardDuty Administratorkonto können Sie im Namen Ihrer aktiven Mitgliedskonten, für deren Konten die folgenden Voraussetzungen erfüllt sind, einen On-Demand-Malware-Scan initiieren.

Eigenständige Konten und aktive Mitgliedskonten in GuardDuty können auch einen On-Demand-Malware-Scan für ihre eigenen EC2 Amazon-Instances einleiten.

Voraussetzungen

- GuardDuty muss in dem Bereich aktiviert sein, in AWS-Regionen dem Sie den On-Demand-Malware-Scan starten möchten.
- Stellen Sie sicher, AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess dass der dem IAM Benutzer oder der IAM Rolle zugeordnet ist. Sie benötigen den Zugriffsschlüssel und den geheimen Schlüssel, die dem IAM Benutzer oder der IAM Rolle zugeordnet sind.
- Als delegiertes GuardDuty Administratorkonto haben Sie die Möglichkeit, im Namen eines aktiven Mitgliedskontos einen On-Demand-Malware-Scan zu starten.
- Wenn Sie ein Mitgliedskonto sind, das nicht über das verfügtServicebezogene Rollenberechtigungen für Malware Protection für EC2, wird bei der Initiierung eines On-Demand-Malware-Scans für eine EC2 Amazon-Instance, die zu Ihrem Konto gehört, automatisch das SLR für den Malware-Schutz für EC2 erstellt.

> **Important**
>
> Stellen Sie sicher, dass niemand die SLRBerechtigungen für den Malware-Schutz löscht, EC2 solange der Malware-Scan, ob GuardDuty initiiert oder auf Abruf, noch läuft. Dadurch wird verhindert, dass der Scan erfolgreich abgeschlossen wird und es wird kein definitives Scanergebnis angezeigt.

Bevor Sie einen Malware-Scan auf Abruf starten, stellen Sie sicher, dass in den letzten Stunde kein Scan auf derselben Ressource gestartet wurde. Andernfalls wird der Scan dedupliziert. Weitere Informationen finden Sie unter Dieselbe Ressource erneut scannen.

Starten eines Malware-Scans auf Abruf

Wählen Sie Ihre bevorzugte Zugriffsmethode, um einen Malware-Scan auf Abruf zu starten.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Initiieren Sie den Scanvorgang mithilfe einer der folgenden Optionen:

a. EC2Seite „Malware-Schutz für“ verwenden:

   i. Wählen Sie im Navigationsbereich unter Schutzpläne die Option Malware-Schutz für ausEC2.

   ii. Geben Sie auf der EC2 Seite Malware-Schutz für die EC2Amazon-Instance ARN [1] an, für die Sie den Scan initiieren möchten.

b. Verwendung der Seite Malware-Scans:

   i. Wählen Sie im Navigationsbereich Malware-Scans.

   ii. Wählen Sie On-Demand-Scan starten und geben Sie die EC2Amazon-Instance ARN [1] an, für die Sie den Scan initiieren möchten.

   iii. Wenn es sich um einen erneuten Scan handelt, wählen Sie auf der Seite Malware-Scans eine EC2Amazon-Instance-ID aus.

   Erweitern Sie das Drop-down-Menü Scan auf Abruf starten und wählen Sie Ausgewählte Instance erneut scannen.

3. Nachdem Sie einen Scan mit einer der beiden Methoden erfolgreich initiiert haben, wird eine Scan-ID generiert. Sie können diese Scan-ID verwenden, um den Scan-Fortschritt zu verfolgen. Weitere Informationen finden Sie unter Überwachen von Scanstatus und Ergebnissen.

API/CLI

Rufen Sie auf StartMalwareScan, `resourceArn` der die EC2 Amazon-Instance [1] akzeptiert, für die Sie einen On-Demand-Malware-Scan initiieren möchten.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

Nachdem Sie einen Scan erfolgreich initiiert haben, gibt `StartMalwareScan` `scanId` zurück. Invoke DescribeMalwareScansüberwacht den Fortschritt des initiierten Scans.

[1] Informationen zum Format Ihrer EC2 Amazon-Instance ARN finden Sie unter Amazon-Ressourcenname (ARN). Für EC2 Amazon-Instances können Sie das folgende ARN Beispielformat verwenden, indem Sie die Werte für die Partition, Region, AWS-Konto ID und EC2 Amazon-Instance-ID ersetzen. Informationen zur Länge Ihrer Instance-ID finden Sie unter Ressource IDs.

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

Dieselbe EC2 Amazon-Instance erneut scannen

Unabhängig davon, ob ein Scan GuardDuty initiiert oder ein On-Demand-Scan durchgeführt wird, können Sie einen neuen On-Demand-Malware-Scan auf derselben EC2 Instance innerhalb einer Stunde nach dem Start des vorherigen Malware-Scans starten. Wenn der neue Malware-Scan innerhalb von einer Stunde nach dem Start des vorherigen Malware-Scans initiiert wird, führt Ihre Anfrage zu dem folgenden Fehler, und es wird keine Scan-ID für diese Anfrage generiert.

```
A scan was initiated on this resource recently. You can request a scan on the same resource one hour after the previous scan start time.
```

Informationen darüber, wie Sie einen neuen Scan für dieselbe Ressource starten, finden Sie unter Starten eines Malware-Scans auf Abruf.

Informationen zum Verfolgen des Status der Malware-Scans finden Sie unter Überwachung des Scanstatus und der Ergebnisse in GuardDuty Malware Protection für EC2.

Überwachung des Scanstatus und der Ergebnisse in GuardDuty Malware Protection für EC2

Sie können den Scanstatus jedes zu EC2 scannenden GuardDuty Malware-Schutzes überwachen. Die möglichen Werte für den Scan-Status sind `Completed`, `Running`, `Skipped` und `Failed`.

Nach Abschluss des Scans wird das Scanergebnis für Scans mit dem Status `Completed` aufgefüllt. Mögliche Werte für das Scanergebnis sind `Clean` und `Infected`. Anhand des Scan-Typs können Sie feststellen, ob es sich bei dem Malware-Scan um `GuardDuty initiated` oder `On demand` handelte.

Die Scan-Ergebnisse für jeden Malware-Scan werden 90 Tage aufbewahrt. Wählen Sie Ihre bevorzugte Zugriffsmethode, um den Status Ihres Malware-Scans zu verfolgen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Malware-Scans.
3. Sie können die Malware-Scans anhand der folgenden Eigenschaften filtern, die in den Filterkriterien verfügbar sind.

- Scan-ID
- Konto-ID
- EC2Instanz ARN
- Scan-Typ
- Scan-Status

Informationen zu Eigenschaften, die für Filterkriterien verwendet werden, finden Sie unter Erkenntnisdetails.

API/CLI

- Wenn für den Malware-Scan ein Scanergebnis vorliegt, können Sie die Malware-Scans auf der Grundlage von `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` und `SCAN_START_TIME` filtern.

  Die `GUARDDUTY_FINDING_ID` Filterkriterien sind verfügbar, wenn der GuardDuty initiiert `SCAN_TYPE` wird. Informationen zu allen Filterkriterien finden Sie unter Erkenntnisdetails.
- Sie können das Beispiel ändern *`filter-criteria`* im folgenden Befehl. Gegenwärtig können Sie auf der Grundlage von jeweils einem `CriterionKey` filtern. Die Optionen für `CriterionKey` sind `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` und `SCAN_START_TIME`.

  Wenn Sie dasselbe `CriterionKey` wie unten verwenden, stellen Sie sicher, dass Sie das Beispiel `EqualsValue` durch Ihr eigenes gültiges ersetzen AWS *`scan-id`*.

  Ersetzen Sie das Beispiel `detector-id` durch Ihre eigene gültige *`detector-id`*. Sie können das ändern *`max-results`* (bis zu 50) und die *`sort-criteria`*. Das `AttributeName` ist verpflichtend und muss es sein`scanStartTime`.

  ```
  aws guardduty describe-malware-scans --detector-
  id 60b87779336485625 54d637e0e4bb3b2 --max-results 1 --sort-criteria
   '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
   '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
  {"EqualsValue":"123456789012"}}] }'
  ```
- Die Antwort auf diesen Befehl zeigt maximal eine Erkenntnis mit Details zur betroffenen Ressource und zu den Malware-Erkenntnissen (wenn `Infected`) an.

GuardDuty Dienstkonten von AWS-Region

Wenn ein Snapshot erstellt und mit einem GuardDuty Dienstkonto geteilt wird, wird ein neues Ereignis in Ihren CloudTrail Protokollen erstellt. Dieses Ereignis spezifiziert das entsprechende `snapshotId` AND `userId` (GuardDuty Dienstkonto dafür AWS-Region). Weitere Informationen finden Sie unter Funktion im Malware-Schutz für EC2.

Das folgende Beispiel ist ein Ausschnitt aus einem CloudTrail Ereignis, das den Anfragetext für die `ModifySnapshotAttribute` Anfrage anzeigt:

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

Die folgende Tabelle zeigt die GuardDuty Dienstkonten für jede Region. Das `userId` ist das GuardDuty Dienstkonto und hängt von der ausgewählten Region ab.

AWS-Region	Regionscode	GuardDuty Dienstkonto-ID (**`userId`**)
USA Ost (Nord-Virginia)	us-east-1	652050842985
USA Ost (Ohio)	us-east-2	178123968615
USA West (Nordkali fornien)	us-west-1	669213148797
USA West (Oregon)	us-west-2	447226417196
Asien-Pazifik (Mumbai)	ap-south-1	913179291432

AWS-Region	Regionscode	GuardDuty Dienstkonto-ID (**`userId`**)
Asien-Pazifik (Osaka)	ap-northeast-3	089661699081
Asien-Pazifik (Seoul)	ap-northeast-2	039163547507
Asien-Pazifik (Tokio)	ap-northeast-1	874749492622
Asien-Pazifik (Singapur)	ap-southeast-1	247460962669
Asien-Pazifik (Sydney)	ap-southeast-2	124839743349
Kanada (Zentral)	ca-central-1	175877067165
Kanada West (Calgary)	ca-west-1	894794104037
Europa (Frankfurt)	eu-central-1	002294850712
Europa (Irland)	eu-west-1	283769539786
Europa (London)	eu-west-2	310125036783
Europa (Paris)	eu-west-3	866607715269
Europa (Stockholm)	eu-north-1	693780578038
China (Peking)	cn-north-1	448721096076
China (Ningxia)	cn-northwest-1	480864352451
Südamerika (São Paulo)	sa-east-1	546914126324
Asien-Pazifik (Hyderabad) (Opt-in)	ap-south-2	682251015962
Asien-Pazifik (Melbourne) (Opt-in)	ap-southeast-4	353488359550
Europa (Spanien) (Opt-In)	eu-south-2	936182149045
Europa (Zürich) (Opt-In)	eu-central-2	867642063380

AWS-Region	Regionscode	GuardDuty Dienstkonto-ID (**`userId`**)
Israel (Tel Aviv) (Opt-In)	il-central-1	619233833001
Europa (Mailand) (Opt-In)	eu-south-1	977238331021
Asien-Pazifik (Hongkong) (Opt-in)	ap-east-1	249472122084
Naher Osten (Bahrain) (Opt-In)	me-south-1	404001805210
Afrika (Kapstadt) (Opt-in)	af-south-1	957664736811
Asien-Pazifik (Jakarta) (Opt-in)	ap-southeast-3	452118225523
Naher Osten () (Opt-In) UAE	me-central-1	828603743433

Malware-Schutz für Kontingente EC2

Malware Protection for EC2 bietet die folgende Standardverfügbarkeit verschiedener Ressourcen, die von der Funktion verwendet werden.

Scope	Standard	Kommentare
Extraktion und Analyse von Daten in komprimierten oder archivierten Dateien	5	Die maximale Anzahl von verschachtelten Ebenen, die in einer archivierten Datei zulässig sind.
Anzahl der Dateien in einer archivierten Datei	1000	Die maximale Anzahl an Dateien, die in einem Archiv gescannt werden können. Diese Anzahl ist die Summe der aus dem Archiv extrahier ten Dateien und der Anzahl

Scope	Standard	Kommentare
		der aus allen verschachtelten Archiven extrahierten Dateien.
Anzahl der Bedrohungen	32	Die maximale Anzahl von Bedrohungen, die Sie im Ergebnisfenster anzeigen können. GuardDuty Der Malware-Schutz für hat EC2 möglicherweise mehr Bedrohungsnamen erkannt. Wenn die Anzahl der erkannten Bedrohungsnamen höher als der Standardwert ist, können Sie die JSON Details anzeigen, indem Sie im Detailbereich der GuardDuty Konsole unter dem Namen der gefundenen Bedrohung die Finding-ID auswählen.
Anzahl der Dateien pro erkannter Bedrohung	5	Die maximale Anzahl identifiz ierter Dateien pro erkannter Bedrohung. Wenn beispiels weise 10 Dateien GuardDuty erkannt werden, die mit einer einzigen Bedrohung verknüpft sind, zeigt die Bedrohung maximal 5 Dateien an.

Scope	Standard	Kommentare
EBSVolumen pro Scan pro Instanz	11	Die maximale Anzahl von EBS Volumes, die pro EC2 Instanz gescannt werden GuardDuty können. Wenn mehr als 11 EBS Volumes gescannt werden müssen, EC2 sortiert GuardDuty Malware Protectio n for die Volumes `deviceNam e` alphabetisch und wählt die ersten 11 EBS Volumes aus.
EBS-Volume-Größe	2048 GB	In Verbindung mit einer EC2 Amazon-Instance und einem Container-Workload EC2 kann GuardDuty Malware Protectio n for jedes EBS Amazon-Vo lume scannen, das bis zu 2048 GB groß ist. Dieses Kontingent gilt für alle AWS-Region , für die die Unterstüt zung von Malware Protection verfügbar EC2 ist.

Scope	Standard	Kommentare
Unterstützte Dateitypen	GuardDuty Malware Protection for EC2 kann die folgenden Dateisystemtypen scannen: • Dateisystem mit neuer Technologie (NTFS) • X-Dateisystem (XFS) • Zweites erweitertes Dateisystem (ext2) • Viertes erweitertes Dateisystem (ext4) • Dateizuordnungstabelle (FAT) Dateisystem • Virtuelle Dateizuordnungstabelle (VFAT) Dateisystem	NICHT ZUTREFFEND
Scan-Optionen-Tags	50	Die maximale Anzahl von Ressourcen-Tags, die Sie hinzufügen können, um die Einstellungen Ihrer Malware-Scan-Optionen anzupassen. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.
Aufbewahrungszeitraum für Ergebnisse	90	Die maximale Anzahl von Tagen, für die GuardDuty ein Ergebnis aufbewahrt wird. Die neuesten Informationen finden Sie unter GuardDuty Amazon-Kontingente.

Scope	Standard	Kommentare
Beibehaltungszeitraum für Malware-Scans	90	Die maximale Anzahl von Tagen, für die GuardDuty Malware Protection EC2 den Verlauf eines Scans aufbewahrt. Weitere Informationen zum Anzeigen der letzten Malware-Scans finden Sie unter Überwachung des Scanstatus und der Ergebnisse in GuardDuty Malware Protection für EC2.
Transaktionen pro Sekunde (TPS) für Malware-Scan auf Abruf	1	Die Anzahl der Anforderungen für Malware-Scan auf Abruf, die pro Sekunde in jeder Region initiiert werden können.
Burst-Limit für Malware-Scan auf Abruf	1	Die Anzahl der Anforderungen für Malware-Scan auf Abruf, die pro Sekunde in jeder Region initiiert werden können.

GuardDuty Malware-Schutz für S3

Malware Protection for S3 hilft Ihnen dabei, potenzielles Vorhandensein von Malware zu erkennen, indem neu hochgeladene Objekte in Ihren ausgewählten Amazon Simple Storage Service (Amazon S3) -Bucket gescannt werden. Wenn ein S3-Objekt oder eine neue Version eines vorhandenen S3-Objekts in den ausgewählten Bucket hochgeladen wird, wird GuardDuty automatisch ein Malware-Scan gestartet.

Malware-Schutz für S3 — Überblick und Demo

Zwei Ansätze zur Aktivierung von Malware Protection für S3

Sie können Malware Protection for S3 aktivieren, wenn AWS-Konto Sie den GuardDuty Dienst aktivieren und Malware Protection for S3 als Teil der GuardDuty Gesamterfahrung verwenden, oder wenn Sie die Funktion Malware Protection for S3 eigenständig verwenden möchten, ohne den GuardDuty Dienst zu aktivieren. Wenn Sie Malware Protection for S3 eigenständig aktivieren, wird in der GuardDuty Dokumentation darauf hingewiesen, dass Malware Protection for S3 als eigenständige Funktion verwendet wird.

Überlegungen zur eigenständigen Verwendung von Malware Protection for S3

- GuardDuty Sicherheitserkenntnisse — Die Detector-ID ist eine eindeutige Kennung, die Ihrem Konto in einer Region zugeordnet ist. Wenn Sie die Aktivierung GuardDuty in einer oder mehreren Regionen in einem Konto vornehmen, wird für dieses Konto in jeder Region, in der Sie die Aktivierung vornehmen, automatisch eine Melder-ID erstellt GuardDuty. Weitere Informationen finden Sie im Konzepte und Terminologie Dokument unter Detektor.

  Wenn Sie Malware Protection for S3 unabhängig in einem Konto aktivieren, ist diesem Konto keine Detektor-ID zugeordnet. Dies wirkt sich darauf aus, welche GuardDuty Funktionen Ihnen möglicherweise zur Verfügung stehen. Wenn beispielsweise ein S3-Malware-Scan das Vorhandensein von Malware erkennt, wird in Ihrem System kein GuardDuty Ergebnis generiert, AWS-Konto da alle GuardDuty Ergebnisse mit einer Detektor-ID verknüpft sind.
- Überprüfung, ob das gescannte Objekt bösartig ist — Standardmäßig werden die Malware-Scan-Ergebnisse in Ihrem standardmäßigen EventBridge Amazon-Event-Bus und einem CloudWatch Amazon-Namespace GuardDuty veröffentlicht. Wenn Sie das Tagging bei der Aktivierung von Malware Protection for S3 für einen Bucket aktivieren, erhält das gescannte S3-Objekt ein Tag, das das Scanergebnis erwähnt. Weitere Informationen über das Markieren

mit Tags finden Sie unter Optionales Markieren von Objekten auf der Grundlage des Scanergebnisses.

Allgemeine Überlegungen zur Aktivierung von Malware Protection for S3

Die folgenden allgemeinen Überlegungen gelten unabhängig davon, ob Sie Malware Protection for S3 unabhängig oder als Teil der GuardDuty Erfahrung verwenden:

- Sie können Malware Protection for S3 für einen Amazon S3 S3-Bucket aktivieren, der zu Ihrem eigenen Konto gehört. Als delegiertes GuardDuty Administratorkonto können Sie diese Funktion nicht in einem Amazon S3 S3-Bucket aktivieren, der zu einem Mitgliedskonto gehört.
- Sie können diese Funktion in den S3-Buckets aktivieren, die zu derselben Region gehören, die derzeit in der GuardDuty Konsole ausgewählt ist. GuardDuty unterstützt die Aktivierung dieser Funktion in regionsübergreifenden S3-Buckets nicht.
- Als delegiertes GuardDuty Administratorkonto erhalten Sie jedes Mal eine EventBridge Amazon-Benachrichtigung, wenn ein S3-Bucket geändert wird, den Ressourcenstatus des Malware-Schutzplans eines der Mitgliedskonten Ihrer Organisation für diese Funktion konfiguriert hat.

Inhalt

Preise für Malware Protection for S3

Kostenloses Kontingent (Kosten für das Scannen)

Jeder AWS-Konto erhält ein kostenloses Kontingent für 12 Monate, das die Nutzung bis zu einem bestimmten Limit pro Monat für jede Region beinhaltet. Wenn Ihre Nutzung das angegebene Limit überschreitet, fallen für Sie die Nutzungskosten für das Überschreitungslimit an. Informationen zu den angegebenen Grenzwerten und ein Preisbeispiel finden Sie unter Preise für GuardDuty Schutzpläne.

- Alle AWS-Konten Bestandskunden sind berechtigt, das 12-monatige kostenlose Kontingent für diese Funktion zu nutzen, das am 11. Juni 2024 beginnt und am 11. Juni 2025 endet. Dieses erweiterte kostenlose Kontingent für 12 Monate für Ihr Konto gilt für die Nutzung von Malware Protection for S3 und für keine andere AWS -Service oder andere GuardDuty Funktion.

  Wenn ein vorhandenes AWS-Konto Mitglied nach dem 11. Juni 2025 oder nach Ablauf des 12-monatigen kostenlosen Kontingents des Kontos mit der Nutzung von Malware Protection for S3 beginnt, fallen für Sie die entsprechenden Nutzungskosten an.
- Wenn Sie ein neues Abonnement haben AWS-Konto und Ihr 12-monatiges kostenloses Kontingent nach der allgemeinen Verfügbarkeit (11. Juni 2024) von Malware Protection for S3 beginnt, entspricht Ihr 12-monatiges kostenloses Kontingent für diese Funktion dem 12-monatigen kostenlosen Kontingent für Ihr Konto.

Informationen zu den Nutzungskosten nach der Aktivierung von Malware Protection for S3 finden Sie unter. Nutzung und Kosten für Malware Protection for S3 anzeigen

Kosten für die Nutzung von S3 Object Tagging

Wenn Sie den Malware-Schutz für S3 aktivieren, ist es optional, das Tagging für Ihre gescannten S3-Objekte zu aktivieren. Wenn Sie sich dafür entscheiden, S3 Object Tagging zu aktivieren, fallen damit Nutzungskosten an. Weitere Informationen zu den Kosten finden Sie auf der Amazon S3 S3-Preisseite unter dem Tab Management & Insights.

Die Nutzungskosten für S3 Object Tagging sind nicht im Tarif „Kostenloses Kontingent“ enthalten.

Amazon S3 APIs — GET und PUT Nutzungskosten

Je APIs nach IAM Rolle fallen Nutzungskosten an, wenn Amazon S3 GuardDuty ausgeführt wird. Wenn Sie beispielsweise die IAM Rolle übernommen haben, GuardDuty wird der ausgeführt, `PutObject` API um das Testobjekt zu Ihrem ausgewählten Bucket hinzuzufügen. Dies hilft bei der GuardDuty Beurteilung des aktivierten Status der Funktion.

Informationen zu den Preisen für API S3-Anrufe in Ihrem AWS-Region finden Sie unter Anfragen und Datenabrufe auf der Amazon S3 S3-Preisseite unter dem Tab Speicher und Anfragen.

Wie funktioniert Malware Protection for S3?

In diesem Abschnitt werden die Komponenten von Malware Protection for S3 und seine Funktionsweise beschrieben, nachdem Sie ihn für einen S3-Bucket aktiviert haben.

Übersicht

Sie können Malware Protection for S3 für einen Amazon S3 S3-Bucket aktivieren, der Ihnen gehört AWS-Konto. GuardDutybietet Ihnen die Flexibilität, diese Funktion für Ihren gesamten Bucket zu aktivieren oder den Umfang des Malware-Scans auf bestimmte Objektpräfixe zu beschränken. Dabei wird jedes hochgeladene Objekt GuardDuty gescannt, das mit einem der ausgewählten Präfixe beginnt. Sie können bis zu 5 Präfixe hinzufügen. Wenn Sie die Funktion für einen S3-Bucket aktivieren, wird dieser Bucket als geschützter Bucket bezeichnet.

IAMRollenberechtigungen

Malware Protection for S3 verwendet eine IAM Rolle, die es GuardDuty ermöglicht, die Malware-Scanaktionen in Ihrem Namen durchzuführen. Zu diesen Aktionen gehören die Benachrichtigung über die neu hochgeladenen Objekte in Ihrem ausgewählten Bucket, das Scannen dieser Objekte und das optionale Hinzufügen von Tags zu Ihren gescannten Objekten. Dies ist eine Voraussetzung für die Konfiguration Ihres S3-Buckets mit dieser Funktion.

Sie haben die Möglichkeit, entweder eine bestehende IAM Rolle zu aktualisieren oder zu diesem Zweck eine neue Rolle zu erstellen. Wenn Sie Malware Protection for S3 für mehr als einen Bucket aktivieren, können Sie die bestehende IAM Rolle nach Bedarf so aktualisieren, dass sie den anderen Bucket-Namen enthält. Weitere Informationen finden Sie unter Voraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren.

Optionales Markieren von Objekten auf der Grundlage des Scanergebnisses

Wenn Sie Malware Protection for S3 für Ihren Bucket aktivieren, gibt es einen optionalen Schritt, um das Tagging für gescannte S3-Objekte zu aktivieren. Die IAM Rolle beinhaltet bereits die Erlaubnis, Ihrem Objekt nach dem Scan Tags hinzuzufügen. Es GuardDuty werden jedoch nur Tags hinzugefügt, wenn Sie diese Option bei der Einrichtung aktivieren.

Sie müssen diese Option aktivieren, bevor ein Objekt hochgeladen wird. GuardDuty Fügt nach Abschluss des Scans dem gescannten S3-Objekt ein vordefiniertes Tag mit dem folgenden Schlüssel/Wert-Paar hinzu:

`GuardDutyMalwareScanStatus:`*`Potential scan result`*

Zu den möglichen Tagwerten für das Scanergebnis gehören`NO_THREATS_FOUND`,`THREATS_FOUND`, `UNSUPPORTEDACCESS_DENIED`, und. `FAILED` Weitere Informationen zu diesen Werten finden Sie unterS3 object potential scan result values.

Die Aktivierung von Tagging ist eine der Möglichkeiten, mehr über das Ergebnis des S3-Objektscans zu erfahren. Sie können diese Tags außerdem verwenden, um eine S3-Ressourcenrichtlinie für die Tag-basierte Zugriffskontrolle (TBAC) hinzuzufügen, sodass Sie Maßnahmen für die potenziell schädlichen Objekte ergreifen können. Weitere Informationen finden Sie unter Hinzufügen TBAC einer S3-Bucket-Ressource.

Wir empfehlen Ihnen, das Tagging bei der Konfiguration von Malware Protection for S3 für Ihren Bucket zu aktivieren. Wenn Sie das Tagging aktivieren, nachdem ein Objekt hochgeladen wurde und möglicherweise der Scan gestartet wurde, GuardDuty können dem gescannten Objekt keine Tags hinzugefügt werden. Informationen zu den damit verbundenen Kosten für das S3-Objekt-Tagging finden Sie unter. Preise für Malware Protection for S3

Vorgang, nachdem Sie Malware Protection for S3 für einen Bucket aktiviert haben

Nachdem Sie Malware Protection for S3 aktiviert haben, wird eine Ressource für den Malware-Schutzplan exklusiv für den ausgewählten S3-Bucket erstellt. Diese Ressource ist mit einer Paket-ID für den Malware-Schutz verknüpft, einer eindeutigen Kennung für Ihre geschützte Ressource. Mithilfe einer der IAM Berechtigungen wird GuardDuty anschließend eine EventBridge verwaltete Regel mit dem Namen erstellt und verwaltet`DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`.

Wie GuardDuty geht man mit Ihren Daten um — Leitplanken für den Datenschutz

Malware Protection for S3 hört sich die EventBridge Amazon-Benachrichtigungen an. Wenn ein Objekt in den ausgewählten Bucket oder eines der Präfixe hochgeladen wird, wird dieses Objekt mithilfe von aus dem S3-Bucket GuardDuty heruntergeladen AWS PrivateLinkund anschließend in einer isolierten Umgebung in derselben Region gelesen, entschlüsselt und gescannt. Die Scanumgebung wird in einer gesperrten virtuellen privaten Cloud (VPC) ohne Internetzugang ausgeführt. Die VPC ist an eine DNS Firewall-Regelgruppe angehängt, die nur die Kommunikation

mit den auf der Zulassungsliste aufgeführten Domänen erlaubt, AWS deren Eigentümer sie ist. Speichert das heruntergeladene S3-Objekt für die Dauer des Scans GuardDuty vorübergehend in der mit AWS Key Management Service (AWS KMS) -Schlüsseln verschlüsselten Scanumgebung.

Informationen zur Methode zur GuardDuty Malware-Erkennung und zu den verwendeten Scan-Engines finden Sie unterGuardDuty Scan-Engine zur Malware-Erkennung.

Nach Abschluss des Malware-Scans GuardDuty werden die Scan-Metadaten mit dem Scanstatus verarbeitet und anschließend die heruntergeladene Kopie des Objekts gelöscht.

GuardDuty reinigt die Scanumgebung jedes Mal, bevor ein neuer Scan beginnt. GuardDuty verwendet eine bedingte Autorisierung für den Benutzerzugriff auf die Scanumgebung, und jede Zugriffsanfrage wird geprüft, genehmigt und geprüft.

Das Ergebnis des S3-Objektscans wird überprüft

GuardDuty veröffentlicht das Ergebnisereignis des S3-Objektscans im EventBridge Amazon-Standardereignisbus. GuardDuty sendet auch die Scan-Metriken wie die Anzahl der gescannten Objekte und die Anzahl der gescannten Byte an Amazon CloudWatch. Wenn Sie Tagging aktiviert haben, GuardDuty werden das vordefinierte Tag `GuardDutyMalwareScanStatus` und ein potenzielles Scanergebnis als Tag-Wert hinzugefügt.

Weitere Informationen finden Sie unter Überwachung im Malware-Schutz für S3.

Überprüfung der generierten Ergebnisse

Die Überprüfung der Ergebnisse hängt davon ab, ob Sie Malware Protection for S3 mit verwenden oder nicht GuardDuty. Betrachten Sie folgende Szenarien:

Verwenden Sie Malware Protection for S3, wenn Sie den GuardDuty Dienst aktiviert haben (Detektor-ID)

> Wenn der Malware-Scan eine potenziell schädliche Datei in einem S3-Objekt erkennt, GuardDuty wird ein entsprechender Befund generiert. Sie können sich die Details des Befundes ansehen und die empfohlenen Schritte anwenden, um das Ergebnis möglicherweise zu beheben. Je nach Häufigkeit Ihrer Exportergebnisse wird das generierte Ergebnis in einen S3-Bucket und einen EventBridge Event-Bus exportiert.

Verwendung von Malware Protection for S3 als eigenständige Funktion (keine Detektor-ID)

> GuardDuty kann keine Ergebnisse generieren, da keine zugehörige Detektor-ID vorhanden ist. Um den Status des S3-Objekt-Malware-Scans zu erfahren, können Sie sich das Scanergebnis

ansehen, das GuardDuty automatisch in Ihrem Standard-Event-Bus veröffentlicht wird. Sie können sich auch die CloudWatch Metriken ansehen, um die Anzahl der Objekte und Byte einzuschätzen, die GuardDuty versucht haben, zu scannen. Sie können CloudWatch Alarme einrichten, um über die Scanergebnisse informiert zu werden. Wenn Sie S3 Object Tagging aktiviert haben, können Sie auch den Status des Malware-Scans einsehen, indem Sie das S3-Objekt auf den `GuardDutyMalwareScanStatus` Tag-Schlüssel und den Tag-Wert für das Scanergebnis überprüfen.

Funktionen des Malware-Schutzes für S3

Die folgende Liste bietet einen Überblick darüber, was Sie erwarten oder tun können, nachdem Sie Malware Protection for S3 für Ihren Bucket aktiviert haben:

- Wählen Sie aus, was gescannt werden soll — Dateien werden beim Hochladen auf alle oder bestimmte Präfixe (bis zu 5) gescannt, die Ihrem ausgewählten S3-Bucket zugeordnet sind.
- Automatische Scans hochgeladener Objekte — Sobald Sie Malware Protection for S3 für einen Bucket aktiviert haben, GuardDuty wird automatisch ein Scan gestartet, um potenzielle Malware in einem neu hochgeladenen Objekt zu erkennen.
- Aktivierung über die Konsole, mitAPI/AWS CLI, oder AWS CloudFormation — Wählen Sie eine bevorzugte Methode, um Malware Protection for S3 zu aktivieren.

  Sie können den Malware-Schutz für S3 aktivieren, indem Sie Infrastructure-as-Code-Plattformen (IaC) wie Terraform verwenden. Weitere Informationen finden Sie unter Ressource:. `aws_guardduty_malware_protection_plan`
- Unterstützte Dateiformate, Malware Protection for S3-Kontingente und Amazon S3 S3-Funktionen — Malware Protection for S3 unterstützt alle Dateiformate, die Sie in die S3-Buckets hochladen können. Wenn die hochgeladene Datei kennwortgeschützt ist, GuardDuty wird das Scannen der Datei übersprungen. Informationen zu den Kontingenten in Bezug auf Objektgröße, maximale Archivtiefe und weitere Informationen finden Sie unter. Kontingente im Malware-Schutz für S3

  Informationen darüber, ob eine Amazon S3 S3-Funktion unterstützt wird oder nicht, finden Sie unterUnterstützbarkeit der Amazon S3 S3-Funktionen.
- Unterstützt das Markieren von gescannten S3-Objekten — Wenn Sie diese Option aktivierenOptionales Markieren von Objekten auf der Grundlage des Scanergebnisses, GuardDuty wird nach jedem Malware-Scan ein Tag hinzugefügt, das den Scanstatus angibt. Sie können dieses Tag verwenden, um die Tag-basierte Zugriffskontrolle (TBAC) für die S3-Objekte

einzurichten. Sie können beispielsweise den Zugriff auf S3-Objekte einschränken, die als bösartig gekennzeichnet sind und den Tagwert als `THREATS_FOUND` haben.

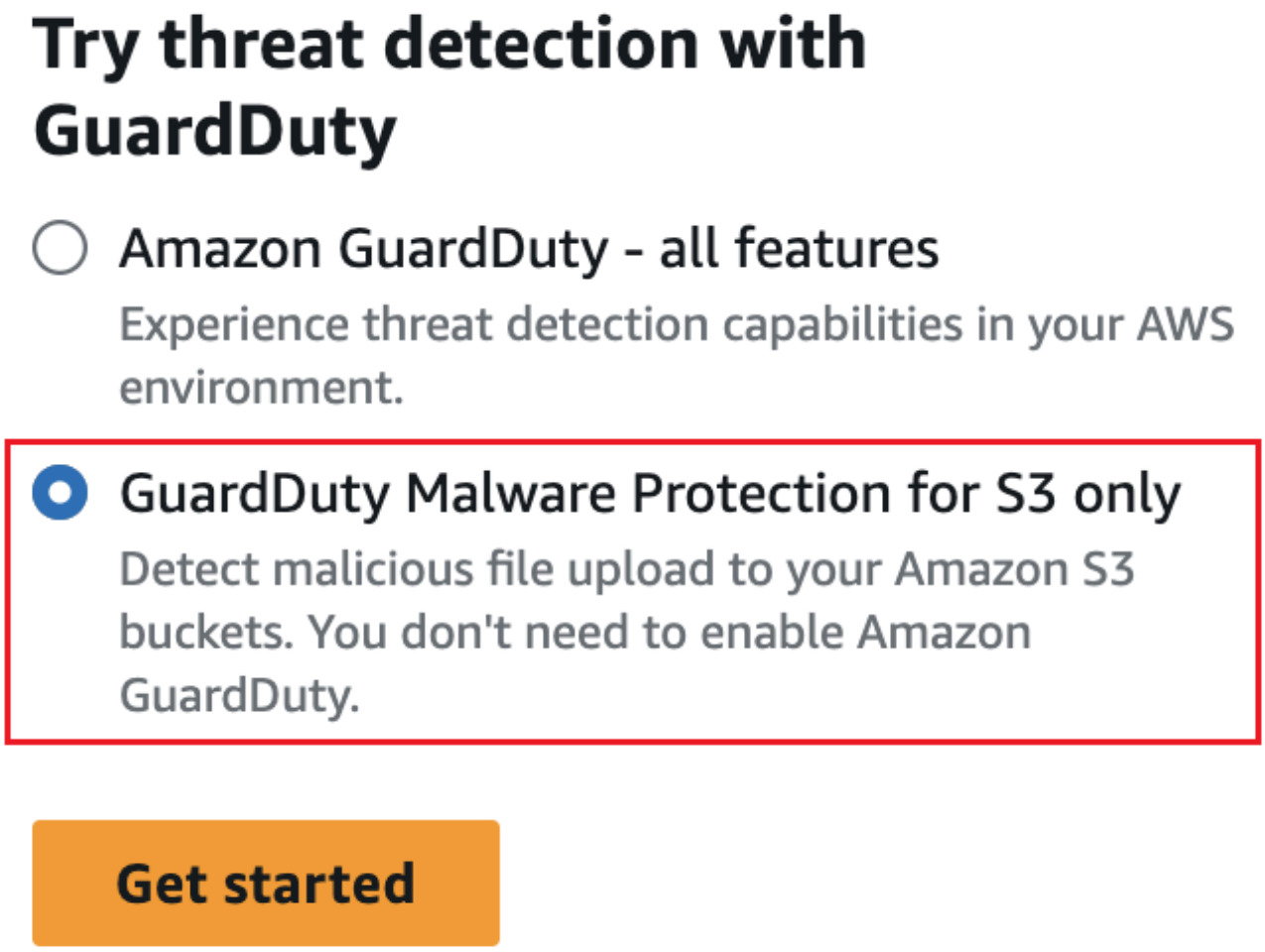
- EventBridge Amazon-Benachrichtigungen — GuardDuty sendet Ereignisse an Amazon EventBridge, wenn sich der Ressourcenstatus des Malware-Schutzplans ändert oder ein Malware-Scan des S3-Objekts abgeschlossen ist. Diese Ereignisse werden an den Standard-Event-Bus gesendet. Sie können diese Ereignisse verwenden EventBridge , um Regeln zu schreiben, die Aktionen ergreifen, z. B. die Überwachung, wann diese Ereignisse eintreten. Weitere Informationen finden Sie unter Überwachung mit Amazon EventBridge.
- CloudWatch Metriken — Zeigen Sie CloudWatch Metriken an, um Alarme bei einem bestimmten Malware-Scanstatus zu aktivieren. Weitere Informationen finden Sie unter Überwachung der Scanstatus-Metriken mithilfe von Amazon CloudWatch.

(Optional) Starten Sie eigenständig mit GuardDuty Malware Protection for S3 (nur Konsole)

Verwenden Sie diesen optionalen Schritt, wenn Sie unabhängig von Ihrem GuardDuty Status mit der Bedrohungserkennungsoption Malware Protection for S3 beginnen möchten AWS-Konto. Wenn Sie die Option GuardDuty in Ihrem Konto bereits aktiviert haben, können Sie diesen Schritt überspringen und mit fortfahrenKonfiguration des Malware-Schutzes für S3 für Ihren Bucket.

Schritte für den Einstieg in die Bedrohungserkennung nur für Malware Protection for S3

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie GuardDuty Malware-Schutz nur für S3 aus. Auf diese Weise können Sie erkennen, ob eine neu hochgeladene Datei in Ihrem Amazon Simple Storage Service (Amazon S3) -Bucket möglicherweise Malware enthält.



3. Wählen Sie Erste Schritte. Sie können nun mit den Schritten unter fortfahrenKonfiguration des Malware-Schutzes für S3 für Ihren Bucket.

Konfiguration des Malware-Schutzes für S3 für Ihren Bucket

Dieser Abschnitt enthält die Schritte zum Hinzufügen von Voraussetzungen und zum Aktivieren von Malware Protection for S3 für einen Amazon S3 S3-Bucket, der zu Ihrem eigenen Konto gehört. Die Schritte in den folgenden Abschnitten bleiben dieselben, unabhängig davon, ob Sie mit Malware Protection for S3 unabhängig beginnen oder es als Teil des GuardDuty Service aktivieren.

Gehen Sie jedes Mal, wenn Sie diese Bedrohungserkennung einem S3-Bucket hinzufügen möchten, die folgenden Schritte aus.

1. Voraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren
2. Aktivieren Sie den Malware-Schutz für S3 für Ihren Bucket

Voraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren

Damit Malware Protection for S3 Ihre S3-Objekte scannen und (optional) Tags hinzufügen kann, müssen Sie eine IAM Rolle erstellen und ihr zuordnen, die die folgenden erforderlichen Berechtigungen für Folgendes umfasst:

- Erlauben Sie Amazon EventBridge Actions, die EventBridge verwaltete Regel zu erstellen und zu verwalten, sodass Malware Protection for S3 Ihre S3-Objektbenachrichtigungen abhören kann.

  Weitere Informationen finden Sie unter Von Amazon EventBridge verwaltete Regeln im EventBridge Amazon-Benutzerhandbuch.
- Erlauben Sie Amazon S3 und EventBridge Aktionen, Benachrichtigungen EventBridge für alle Ereignisse in diesem Bucket zu senden

  Weitere Informationen finden Sie unter Enabling Amazon EventBridge im Amazon S3 S3-Benutzerhandbuch.
- Erlauben Sie Amazon S3 S3-Aktionen den Zugriff auf das hochgeladene S3-Objekt und fügen Sie dem gescannten S3-Objekt ein vordefiniertes Tag hinzu. `GuardDutyMalwareScanStatus` Wenn Sie ein Objektpräfix verwenden, fügen Sie eine `s3:prefix` Bedingung nur für die Zielpräfixe hinzu. Dadurch wird GuardDuty verhindert, dass Sie auf alle S3-Objekte in Ihrem Bucket zugreifen können.
- Erlauben Sie KMS wichtigen Aktionen den Zugriff auf das Objekt, bevor Sie ein Testobjekt scannen KMS und mit der unterstützten KMS Verschlüsselung DSSE in Buckets SSE platzieren.

> **Note**
>
> Dieser Schritt ist jedes Mal erforderlich, wenn Sie Malware Protection for S3 für einen Bucket in Ihrem Konto aktivieren. Wenn Sie bereits über eine bestehende IAM Rolle verfügen, können Sie deren Richtlinie so aktualisieren, dass sie die Details einer anderen S3-Bucket-Ressource enthält. Das Hinzufügen von IAM Richtlinienberechtigungen Thema enthält ein Beispiel dafür.

Verwenden Sie die folgenden Richtlinien, um eine IAM Rolle zu erstellen oder zu aktualisieren.

Richtlinien

- Hinzufügen von IAM Richtlinienberechtigungen
- Eine Vertrauensbeziehungsrichtlinie wird hinzugefügt

Hinzufügen von IAM Richtlinienberechtigungen

Sie können wählen, ob Sie die Inline-Richtlinie einer vorhandenen IAM Rolle aktualisieren oder eine neue IAM Rolle erstellen möchten. Informationen zu diesen Schritten finden Sie unter Erstellen einer IAM Rolle oder Ändern einer Rollenberechtigungsrichtlinie im IAMBenutzerhandbuch.

Fügen Sie Ihrer bevorzugten IAM Rolle die folgende Berechtigungsvorlage hinzu. Ersetzen Sie die folgenden Platzhalterwerte durch entsprechende Werte, die Ihrem Konto zugeordnet sind:

- Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. *amzn-s3-demo-bucket*, ersetzen Sie es durch Ihren Amazon S3 S3-Bucket-Namen.

  Um dieselbe IAM Rolle für mehr als eine S3-Bucket-Ressource zu verwenden, aktualisieren Sie eine bestehende Richtlinie, wie im folgenden Beispiel dargestellt:

  ```
  ...
  ...
  "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "arn:aws:s3:::amzn-s3-demo-bucket2/*"
  ],
  ...
  ...
  ```

  Stellen Sie sicher, dass Sie ein Komma (,) hinzufügen, bevor Sie ein neues hinzufügen, das dem S3-Bucket ARN zugeordnet ist. Tun Sie dies überall dort, wo Sie `Resource` in der Richtlinienvorlage auf einen S3-Bucket verweisen.
- Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. *111122223333*, ersetzen Sie es durch Ihre AWS-Konto ID.
- Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. *us-east-1*, ersetzen Sie durch Ihre AWS-Region.

- Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. *APKAEIBAERJR2EXAMPLE*, ersetzen Sie durch Ihre vom Kunden verwaltete Schlüssel-ID. Wenn Ihr Bucket mit einem verschlüsselt ist AWS KMS key, ersetzen Sie den Platzhalterwert durch einen*, wie im folgenden Beispiel gezeigt:

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

IAMVorlage für eine Rollenrichtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
            ],
            "Condition": {
                "StringLike": {
                    "events:ManagedBy": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
            "Effect": "Allow",
            "Action": [
                "events:DescribeRule",
                "events:ListTargetsByRule"
            ],
            "Resource": [
                "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
```

```
            ]
        },
        {
            "Sid": "AllowPostScanTag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:GetObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowEnableS3EventBridgeEvents",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketNotification",
                "s3:GetBucketNotification"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Sid": "AllowPutValidationObject",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-
validation-object"
            ]
        },
        {
            "Sid": "AllowCheckBucketOwnership",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
           "Sid": "AllowMalwareScan",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "AllowDecryptForMalwareScan",
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                }
            }
        }
    ]
}
```

Eine Vertrauensbeziehungsrichtlinie wird hinzugefügt

Fügen Sie Ihrer IAM Rolle die folgende Vertrauensrichtlinie hinzu. Informationen zu den einzelnen Schritten finden Sie unter Ändern einer Vertrauensrichtlinie für Rollen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
```

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Aktivieren Sie den Malware-Schutz für S3 für Ihren Bucket

Dieser Abschnitt enthält detaillierte Schritte zur Aktivierung von Malware Protection for S3 für einen ausgewählten Bucket in Ihren eigenen Konten.

Schritte zum Aktivieren von Malware Protection for S3 für einen Bucket

- Geben Sie die S3-Bucket-Details ein
- Aktivieren Sie das Tagging für gescannte Objekte
- Berechtigungen
- (Optional) Markieren Sie die ID des Malware-Schutzplans

Geben Sie die S3-Bucket-Details ein

Gehen Sie wie folgt vor, um die Amazon S3 S3-Bucket-Details bereitzustellen:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie mithilfe der AWS-Region Auswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie Malware Protection for S3 aktivieren möchten.
3. Wählen Sie im Navigationsbereich die Option Malware Protection for S3 aus.
4. Wählen Sie im Abschnitt Geschützte Buckets die Option Aktivieren aus, um Malware Protection for S3 für einen S3-Bucket zu aktivieren, der Ihrem eigenen AWS-Konto gehört.
5. Geben Sie unter S3-Bucket-Details eingeben den Namen des Amazon S3 S3-Buckets ein. Wählen Sie alternativ Browse S3, um einen S3-Bucket auszuwählen.

   Der AWS-Region Name des S3-Buckets und der Bereich AWS-Konto , in dem Sie den Malware-Schutz für S3 aktivieren, müssen identisch sein. Wenn Ihr Konto beispielsweise zur `us-east-1` Region gehört, muss dies auch Ihre Amazon S3 S3-Bucket-Region sein`us-east-1`.
6. Unter Präfix können Sie entweder Alle Objekte im S3-Bucket oder Objekte, die mit einem bestimmten Präfix beginnen, auswählen.

- Wählen Sie Alle Objekte im S3-Bucket aus, wenn Sie alle neu hochgeladenen Objekte im ausgewählten Bucket scannen möchten GuardDuty .
- Wählen Sie Objekte, die mit einem bestimmten Präfix beginnen, wenn Sie die neu hochgeladenen Objekte scannen möchten, die zu einem bestimmten Präfix gehören. Mit dieser Option können Sie den Umfang des Malware-Scans nur auf die ausgewählten Objektpräfixe konzentrieren. Weitere Informationen zur Verwendung von Präfixen finden Sie unter Objekte in der Amazon S3 S3-Konsole mithilfe von Ordnern organisieren im Amazon S3 S3-Benutzerhandbuch.

  Wählen Sie Präfix hinzufügen und geben Sie Präfix ein. Sie können bis zu fünf Präfixe hinzufügen.

Aktivieren Sie das Tagging für gescannte Objekte

Dies ist ein optionaler Schritt. Wenn Sie die Tagging-Option aktivieren, bevor ein Objekt in Ihren Bucket hochgeladen wird, GuardDuty wird nach Abschluss des Scans ein vordefiniertes Tag mit dem Schlüssel as `GuardDutyMalwareScanStatus` und dem Wert als Scanergebnis hinzugefügt. Um den Malware-Schutz für S3 optimal nutzen zu können, empfehlen wir, die Option zum Hinzufügen von Tags zu den S3-Objekten nach Abschluss des Scans zu aktivieren. Es fallen die Standardkosten für das S3-Objekt-Tagging an. Weitere Informationen finden Sie unter Preise für Malware Protection for S3.

Warum sollten Sie Tagging aktivieren?

- Das Aktivieren von Tagging ist eine der Möglichkeiten, sich über das Ergebnis des Malware-Scans zu informieren. Hinweise zu den Ergebnissen eines S3-Malware-Scans finden Sie unterÜberwachung im Malware-Schutz für S3.
- Richten Sie eine tagbasierte Zugriffskontrollrichtlinie (TBAC) für Ihren S3-Bucket ein, der das potenziell schädliche Objekt enthält. Informationen zu Überlegungen und zur Implementierung der tagbasierten Zugriffskontrolle (TBAC) finden Sie unter. Tag-basierte Zugriffskontrolle (TBAC) mit Malware Protection for S3 verwenden

Überlegungen GuardDuty zum Hinzufügen eines Tags zu Ihrem S3-Objekt:

- Standardmäßig können Sie einem Objekt bis zu 10 Tags zuordnen. Weitere Informationen finden Sie unter Kategorisieren Ihres Speichers mithilfe von Tags im Amazon S3 S3-Benutzerhandbuch.

Wenn alle 10 Tags bereits verwendet werden, GuardDuty kann das vordefinierte Tag dem gescannten Objekt nicht hinzugefügt werden. GuardDuty veröffentlicht das Scanergebnis auch in Ihrem EventBridge Standard-Event-Bus. Weitere Informationen finden Sie unter Überwachung mit Amazon EventBridge.

- Wenn die gewählte IAM Rolle nicht über die Berechtigung GuardDuty zum Taggen des S3-Objekts verfügt, können Sie diesem gescannten S3-Objekt auch dann kein Tag hinzufügen, GuardDuty wenn das Tagging für Ihren geschützten Bucket aktiviert ist. Weitere Informationen zu den erforderlichen IAM Rollenberechtigungen für das Tagging finden Sie unter. Voraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren

  GuardDuty veröffentlicht das Scanergebnis auch in Ihrem EventBridge Standard-Event-Bus. Weitere Informationen finden Sie unter Überwachung mit Amazon EventBridge.

Um eine Option unter Gescannte Objekte taggen auszuwählen

- Wenn Sie Ihren gescannten S3-Objekten Tags hinzufügen möchten GuardDuty , wählen Sie Objekte kennzeichnen.
- Wenn Sie Ihren gescannten S3-Objekten keine Tags hinzufügen möchten GuardDuty , wählen Sie Objekte nicht taggen.

Berechtigungen

Gehen Sie wie folgt vor, um eine IAM Rolle auszuwählen, die über die erforderlichen Berechtigungen verfügt, um in Ihrem Namen Malware-Suchaktionen durchzuführen. Zu diesen Aktionen können das Scannen der neu hochgeladenen S3-Objekte und (optional) das Hinzufügen von Tags zu diesen Objekten gehören.

Um einen IAM Rollennamen zu wählen

1. Wenn Sie die folgenden Schritte bereits ausgeführt habenVoraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren, gehen Sie wie folgt vor:

   - Wählen Sie im Abschnitt Berechtigungen für den IAM Rollennamen einen IAM Rollennamen aus, der die erforderlichen Berechtigungen enthält.

2. Wenn Sie die unten aufgeführten Schritte noch nicht ausgeführt habenVoraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren, gehen Sie wie folgt vor:

a. Wähle „Berechtigungen anzeigen“.

b. Wählen Sie unter Berechtigungsdetails den Tab Richtlinie aus. Dies zeigt eine Vorlage mit den erforderlichen IAM Berechtigungen.

   Kopieren Sie diese Vorlage und wählen Sie dann am Ende des Fensters mit den Berechtigungsdetails die Option Schließen aus.

c. Wählen Sie Richtlinie anhängen aus, um die IAM Konsole auf einer neuen Registerkarte zu öffnen. Sie können wählen, ob Sie eine neue IAM Rolle erstellen oder eine bestehende IAM Rolle mit den Berechtigungen aus der kopierten Vorlage aktualisieren möchten.

   Diese Vorlage enthält Platzhalterwerte, die Sie durch die entsprechenden Werte ersetzen müssen, die Ihrem Bucket und AWS-Konto zugeordnet sind.

d. Kehren Sie mit der GuardDuty Konsole zum Browser-Tab zurück. Wählen Sie erneut Berechtigungen anzeigen.

e. Wählen Sie unter Berechtigungsdetails die Registerkarte Vertrauensverhältnis aus. Dies zeigt eine Vorlage der Vertrauensbeziehungsrichtlinie für Ihre IAM Rolle.

   Kopieren Sie diese Vorlage und wählen Sie dann am Ende des Fensters mit den Berechtigungsdetails die Option Schließen aus.

f. Gehen Sie zu dem Browser-Tab, auf dem die IAM Konsole geöffnet ist. Fügen Sie diese Vertrauensbeziehungsrichtlinie zu Ihrer bevorzugten IAM Rolle hinzu.

3. Um Ihrer Paket-ID für den Malware-Schutz, die für diese geschützte Ressource erstellt wird, Tags hinzuzufügen, fahren Sie mit dem nächsten Abschnitt fort. Andernfalls wählen Sie am Ende dieser Seite die Option Aktivieren aus, um den S3-Bucket als geschützte Ressource hinzuzufügen.

(Optional) Markieren Sie die ID des Malware-Schutzplans

Dies ist ein optionaler Schritt, mit dem Sie der Ressource des Malware-Schutzplans, die für Ihre S3-Bucket-Ressource erstellt werden würde, Tags hinzufügen können.

Jedes Tag besteht aus zwei Teilen: einem Tag-Schlüssel und einem optionalen Tag-Wert. Weitere Informationen zu Tagging und seinen Vorteilen finden Sie unter Ressourcen zum Taggen AWS.

So fügen Sie Tags zur Ressource Ihres Malware-Schutzplans hinzu

1. Geben Sie einen Schlüssel und einen optionalen Wert für das Tag ein. Sowohl beim Tag-Schlüssel als auch beim Tag-Wert wird zwischen Groß- und Kleinschreibung unterschieden. Informationen zu den Namen von Tag-Schlüsseln und Tag-Werten finden Sie unter Einschränkungen und Anforderungen für die Benennung von Tags.
2. Um weitere Tags zur Ressource Ihres Malware-Schutzplans hinzuzufügen, wählen Sie Neues Tag hinzufügen und wiederholen Sie den vorherigen Schritt. Sie können bis zu 50 Tags für jede -Ressource hinzufügen.
3. Wählen Sie Enable (Aktivieren) aus.

Schritte nach der Aktivierung von Malware Protection for S3

Nachdem Sie Malware Protection for S3 für einen Bucket (oder bestimmte Objektpräfixe) aktiviert haben, führen Sie die folgenden Schritte in der aufgeführten Reihenfolge aus:

1. Ressourcenrichtlinie für Tag-basierte Zugriffskontrolle (TBAC) hinzufügen — Wenn Sie Tagging aktivieren und ein Objekt in den ausgewählten Bucket hochgeladen wird, stellen Sie sicher, dass Sie die TBAC Richtlinie zu Ihrer S3-Bucket-Ressource hinzufügen. Weitere Informationen finden Sie unter Hinzufügen TBAC einer S3-Bucket-Ressource.
2. Status des Malware-Schutzplans überwachen — Überwachen Sie die Statusspalte für jeden geschützten Bucket. Informationen zu möglichen Status und deren Bedeutung finden Sie unterRessourcenstatus des Malware-Schutzplans.
3. Laden Sie ein Objekt hoch:
    1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
    2. Laden Sie eine Datei in den S3-Bucket oder das Objektpräfix hoch, für das Sie diese Funktion aktiviert haben. Die Schritte zum Hochladen einer Datei finden Sie unter Hochladen eines Objekts in Ihren Bucket im Amazon S3 S3-Benutzerhandbuch.
4. S3-Objektscan-Status überwachen — Dieser Schritt beinhaltet Informationen darüber, wie Sie den Malware-Scan-Status des S3-Objekts überprüfen können.

GuardDuty Sowohl als auch der Malware-Schutz für S3 aktiviert	Malware-Schutz nur für S3 aktiviert
• Wenn diese Option aktiviert GuardDuty ist, kann sie generiert werden, Suchtyp „Malware-Schutz für S3“ um auf das Vorhandensein von Malware im gescannten S3-Objekt hinzuweisen. • Möglicherweise können Sie das Ergebnis des S3-Objektscans überprüfen, indem Sie eine oder mehrere Optionen unter verwendenÜberwachung im Malware-Schutz für S3. Dazu gehören die Nutzung von Amazon EventBridge, CloudWatch Metriken für den Malware-Schutzplan und das Markieren gescannter Objekte.	Möglicherweise können Sie das Ergebnis des S3-Objektscans überprüfen, indem Sie eine oder mehrere Optionen unter Überwachung im Malware-Schutz für S3 verwenden. Dazu gehören die Nutzung von Amazon EventBridge, CloudWatch Metriken für den Malware-Schutzplan und das Markieren gescannter Objekte.

Ressourcenstatus des Malware-Schutzplans

In diesem Abschnitt werden verschiedene Schutzstatuswerte beschrieben, die mit der Ressource Ihres Malware-Schutzplans verknüpft sind.

Status	Description
Aktiv	Ihr S3-Bucket wurde erfolgreich mit Malware Protection for S3 konfiguriert.
Warnung *	Der Malware-Schutz für S3 ist so konzipiert, dass er nicht beeinträchtigt wird, wenn eine Warnung angezeigt wird. Wenn GuardDuty ein neues S3-Objekt entdeckt wird, wird ein Malware-Scan eingeleitet. Nach erfolgreicher Initiierung des Scans kann es einige Minuten dauern, bis der Wert in der Spalte Status auf Aktiv geändert wird. Sie erhalten eine EventBridge Benachrichtigung, nachdem der Wert der Statusspalte aktualisiert wurde.

Status	Description
Fehler [*] -	Ihr Bucket ist nicht geschützt. Keiner der mit diesem S3-Bucket verknüpften Malware-Scans wird abgeschlossen. Es könnte eine oder mehrere mögliche Hauptursachen geben.

[*] Informationen zu potenziellen Problemen und den entsprechenden Schritten zu ihrer Behebung finden Sie unterStatusdetails zum Malware-Schutzplan zur Fehlerbehebung.

Statusdetails zum Malware-Schutzplan zur Fehlerbehebung

GuardDuty Zeigt für jeden geschützten Bucket den Status auf der Grundlage der Rangfolge an. Wenn ein geschützter Bucket beispielsweise Probleme sowohl in der Kategorie Fehler als auch in der Kategorie Warnung aufweist, GuardDuty wird zuerst das Problem angezeigt, das dem Fehlerstatus zugeordnet ist.

Die folgende Liste enthält die Fehler und die Warnung für den Status des Malware-Schutzplans.

Fehler

- EventBridge Die Benachrichtigung ist für diesen S3-Bucket deaktiviert
- EventBridge Eine verwaltete Regel zum Empfangen von S3-Bucket-Ereignissen fehlt
- Der S3-Bucket ist nicht mehr vorhanden

Warnung

Das Testobjekt konnte nicht platziert werden

EventBridge Die Benachrichtigung ist für diesen S3-Bucket deaktiviert

Der zugehörige Status-Ursachencode lautet`EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED`.

Detail zum Status

GuardDuty verwendet EventBridge , um eine Benachrichtigung zu erhalten, wenn ein neues Objekt in diesen S3-Bucket hochgeladen wird. Diese Berechtigung fehlt in Ihrer IAM Rolle.

Schritte zur Fehlerbehebung

Option 1: Fügen Sie Ihrer IAM Rolle die folgende Berechtigungserklärung hinzu:

```
{
          "Sid": "AllowEnableS3EventBridgeEvents",
          "Effect": "Allow",
          "Action": [
             "s3:PutBucketNotification",
             "s3:GetBucketNotification"
             ],
          "Resource": [
             "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
}
```

Ersetzen *amzn-s3-demo-bucket* mit Ihrem Amazon S3 S3-Bucket-Namen.

Option 2: EventBridge Benachrichtigung mithilfe der Amazon S3 S3-Konsole aktivieren

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie auf der Seite Buckets auf der Registerkarte Allgemeine Buckets den Bucket-Namen aus, der mit diesem Fehler verknüpft ist.
3. Wählen Sie auf dieser Bucket-Seite die Registerkarte Eigenschaften aus.
4. Wählen Sie im EventBridge Bereich Amazon die Option Bearbeiten aus.
5. Wählen Sie auf der EventBridge Seite Amazon bearbeiten für Benachrichtigung an Amazon senden EventBridge für alle Ereignisse in diesem Bucket die Option An.
6. Wählen Sie Änderungen speichern.

Es kann einige Minuten dauern, bis der Wert in der Spalte Status auf Aktiv geändert wird.

EventBridge Eine verwaltete Regel zum Empfangen von S3-Bucket-Ereignissen fehlt

Der zugehörige Status-Ursachencode lautet`EVENTBRIDGE_MANAGED_RULE_DISABLED`.

Detail zum Status

Die EventBridge verwalteten Regelberechtigungen zur Verwaltung des EventBridge Regel-Setups fehlen.

Schritte zur Fehlerbehebung

Fügen Sie Ihrer IAM Rolle die folgende Berechtigungserklärung hinzu:

```
{
         "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
        "Effect": "Allow",
        "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
        "Resource": [
           "arn:aws:events:*:*:rule/DO-NOT-DELETE-
AmazonGuardDutyMalwareProtectionS3*"
           ],
        "Condition": {
           "StringEquals": {
              "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
              }
           }
}
```

Es kann einige Minuten dauern, bis der Wert in der Spalte Status auf Aktiv geändert wird.

Der S3-Bucket ist nicht mehr vorhanden

Der zugehörige Status-Ursachencode lautet`PROTECTED_RESOURCE_DELETED`.

Detail zum Status

Dieser S3-Bucket wurde aus Ihrem Konto gelöscht und ist nicht mehr vorhanden.

Schritt zur Fehlerbehebung

Wenn das Löschen des S3-Buckets nicht beabsichtigt war, können Sie mithilfe der Amazon S3 S3-Konsole einen neuen Bucket erstellen.

Nachdem Sie den Bucket erfolgreich erstellt haben, aktivieren Sie den Malware-Schutz für S3, indem Sie die Schritte Konfiguration des Malware-Schutzes für S3 für Ihren Bucket auf der Seite befolgen.

Das Testobjekt konnte nicht platziert werden

Der zugehörige Status-Ursachencode lautet`INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

> **Note**
>
> Die Erlaubnis, ein Testobjekt hinzuzufügen, ist optional. Das Fehlen dieser Berechtigung in Ihrer IAM Rolle verhindert nicht, dass Malware Protection for S3 einen Malware-Scan für ein neu hochgeladenes Objekt initiiert. Nach dem erfolgreichen Start eines Scans kann es einige Minuten dauern, bis der Status des Malware-Schutzplans von Warnung auf Aktiv geändert wird.
> Wenn die IAM Rolle diese Berechtigung bereits enthält, weist diese Warnung auf eine restriktive Amazon S3 S3-Bucket-Richtlinie hin, die es der IAM Rolle nicht erlaubt, diese Berechtigung einzubeziehen.

Einzelheiten zum Status

GuardDuty Fügt ein Testobjekt in Ihren Bucket ein, um die Einrichtung des ausgewählten Buckets zu überprüfen.

Schritte zur Fehlerbehebung

Sie können sich dafür entscheiden, die IAM Rolle so zu aktualisieren, dass sie die fehlenden Berechtigungen enthält. Fügen Sie der ausgewählten IAM Rolle die folgenden Berechtigungen hinzu, damit das Testobjekt der ausgewählten Ressource zugewiesen werden GuardDuty kann:

```
{
         "Sid": "AllowPutValidationObject",
         "Effect": "Allow",
         "Action": [
           "s3:PutObject"
           ],
         "Resource": [
           "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-
object"
```

```
            ]
}
```

Ersetzen *amzn-s3-demo-bucket* mit Ihrem Amazon S3 S3-Bucket-Namen. Informationen zu IAM Rollenberechtigungen finden Sie unterVoraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren.

Es kann einige Minuten dauern, bis der Wert in der Spalte Status auf Aktiv geändert wird.

Überwachung im Malware-Schutz für S3

Wenn Sie Malware Protection for S3 mit einer GuardDuty Detektor-ID verwenden und Ihr Amazon S3 S3-Objekt potenziell bösartig ist, GuardDuty wird Folgendes generiertSuchtyp „Malware-Schutz für S3“. Mithilfe der GuardDuty Konsole und APIs können Sie sich die generierten Ergebnisse ansehen. Informationen zum Verständnis dieses Ergebnistyps finden Sie unterErkenntnisdetails.

Wenn Sie Malware Protection for S3 ohne Aktivierung verwenden GuardDuty (keine Detektor-ID), GuardDuty können auch dann keine Ergebnisse generiert werden, wenn Ihr gescanntes Amazon S3 S3-Objekt potenziell bösartig ist.

Die folgende Liste enthält die möglichen Statuswerte für die Ergebnisse des S3-Objektscans:

- `NO_THREATS_FOUND`— es GuardDuty wurde keine potenzielle Bedrohung im Zusammenhang mit dem gescannten Objekt festgestellt.
- `THREATS_FOUND`— hat eine potenzielle Bedrohung im Zusammenhang mit dem gescannten Objekt GuardDuty erkannt.
- `UNSUPPORTED`— Es gibt mehrere Gründe, warum Malware Protection for S3 einen Scan überspringt. Mögliche Gründe sind kennwortgeschützte Dateien, Malware-Schutz für S3-Kontingente und bestimmte Amazon S3 S3-Funktionen. Weitere Informationen finden Sie unter Funktionen des Malware-Schutzes für S3.
- `ACCESS_DENIED`— GuardDuty kann zum Scannen nicht auf dieses Objekt zugreifen. Überprüfen Sie die mit diesem Bucket verknüpften IAM Rollenberechtigungen. Weitere Informationen finden Sie unter Voraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren.
- `FAILED`— Dieses Objekt GuardDuty kann aufgrund eines internen Fehlers nicht nach Schadsoftware gescannt werden.

Die folgende Liste enthält mögliche Statuswerte für S3-Objektscans und deren Zuordnung zum Ergebnis des S3-Objektscans:

- Abgeschlossen — Der Scan wurde erfolgreich abgeschlossen und gibt an, ob das S3-Objekt Schadsoftware enthält. In diesem Fall könnte der potenzielle Ergebniswert des S3-Objektscans entweder `THREATS_FOUND` oder sein`NO_THREATS_FOUND`.
- GuardDuty Übersprungen — Überspringt einen Malware-Scan, wenn die S3-Objektdetails nicht mit dem Kontingente im Malware-Schutz für S3 hochgeladenen S3-Objekt im ausgewählten Bucket übereinstimmen oder GuardDuty kein Zugriff darauf besteht.

  In diesem Fall könnte der potenzielle Ergebniswert für den S3-Objektscan entweder oder `UNSUPPORTED` lauten. `ACCESS_DENIED`
- Fehlgeschlagen — Ähnlich wie der Ergebniswert des `FAILED` S3-Objektscans bedeutet dieser Scanstatus, GuardDuty dass das S3-Objekt aufgrund eines internen Fehlers nicht auf Schadsoftware geprüft werden konnte.

Themen

- Überwachung mit Amazon EventBridge
- Überwachung der Scanstatus-Metriken mithilfe von Amazon CloudWatch
- Überwachung mit S3-Objekt-Tags

Überwachung mit Amazon EventBridge

Amazon EventBridge ist ein serverloser Event-Bus-Service, der es einfach macht, Ihre Anwendungen mit Daten aus einer Vielzahl von Quellen zu verbinden. EventBridge liefert einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, oftware-as-a S-Service (SaaS) -Anwendungen und AWS Diensten und leitet diese Daten an Ziele wie Lambda weiter. Auf diese Weise können Sie Ereignisse überwachen, die in Services auftreten, und ereignisgesteuerte Architekturen erstellen. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Als Besitzerkonto eines S3-Buckets, der mit Malware Protection for S3 geschützt ist, GuardDuty veröffentlicht er in den folgenden Szenarien EventBridge Benachrichtigungen an den Standard-Event-Bus:

- Der Ressourcenstatus des Malware-Schutzplans ändert sich für jeden Ihrer geschützten Buckets. Informationen zu den verschiedenen Status finden Sie unter. Ressourcenstatus des Malware-Schutzplans
- Aus den folgenden Gründen ist ein Tag-Ereignis fehlgeschlagen:
  - In Ihrer IAM Rolle fehlen die Berechtigungen zum Markieren des Objekts.

    Die Hinzufügen von IAM Richtlinienberechtigungen Vorlage beinhaltet die Erlaubnis GuardDuty , ein Objekt zu taggen.
  - Die in der Rolle angegebene Bucket-Ressource oder das in der IAM Rolle angegebene Bucket-Objekt ist nicht mehr vorhanden.
  - Das zugehörige S3-Objekt hat bereits das maximale Tag-Limit erreicht. Weitere Informationen zum Tag-Limit finden Sie unter Kategorisieren Ihres Speichers mithilfe von Tags im Amazon S3 S3-Benutzerhandbuch.
- Das Ergebnis des S3-Objektscans wird in Ihrem EventBridge Standard-Event-Bus veröffentlicht.

Richten Sie EventBridge Regeln ein

Sie können in Ihrem Konto EventBridge Regeln einrichten, um entweder den Ressourcenstatus, Ereignisse nach dem Scan-Tag oder das Ergebnis des S3-Objektscans an ein anderes AWS -Service zu senden. Als delegiertes GuardDuty Administratorkonto erhalten Sie eine Benachrichtigung über den Ressourcenstatus des Malware-Schutzplans, wenn sich der Status ändert.

Es gelten die EventBridge Standardpreise. Weitere Informationen finden Sie unter EventBridge Amazon-Preise.

Alle Werte, die in angezeigt werden *red* sind Platzhalter für das Beispiel. Diese Werte ändern sich je nach den Werten in Ihrem Konto und je nachdem, ob Malware erkannt wurde oder nicht.

Ressourcenstatus des Malware-Schutzplans

Sie können ein EventBridge Ereignismuster erstellen, das auf den folgenden Szenarien basiert:

Mögliche **`detail-type`** Werte

- `"GuardDuty Malware Protection Resource Status Active"`
- `"GuardDuty Malware Protection Resource Status Warning"`
- `"GuardDuty Malware Protection Resource Status Error"`

Muster des Ereignisses

```
{
      "detail-type": ["potential detail-type"],
      "source": ["aws.guardduty"]
}
```

Beispiel für ein Benachrichtigungsschema für **`GuardDuty Malware Protection Resource Status Active`**:

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status Active",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "ACTIVE"
    }
}
```

Beispiel für ein Benachrichtigungsschema für **`GuardDuty Malware Protection Resource Status Warning`**:

```
{
    "version": "0",
    "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
    "detail-type": "GuardDuty Malware Protection Resource Status warning",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
```

```
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "WARNING",
        "statusReasons": [
         {
            "code": "INSUFFICIENT_TEST_OBJECT_PERMISSIONS"
         }
        ]
    }
}
```

Beispiel für ein Benachrichtigungsschema für **`GuardDuty Malware Protection Resource Status Error`**:

```
{
    "version": "0",
    "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
    "detail-type": "GuardDuty Malware Protection Resource Status Error",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-02-28T01:01:01Z",
        "s3BucketDetails": {
            "bucketName": "amzn-s3-demo-bucket"
        },
        "resourceStatus": "ERROR",
        "statusReasons": [
        {
            "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
        }
       ]
    }
```

```
}
```

Basierend auf dem Grund dafür `resourceStatus` ERROR wird der `statusReasons` Wert aufgefüllt.

Informationen zu den Schritten zur Problembehandlung bei den folgenden Warnungen und Fehlern finden Sie unterStatusdetails zum Malware-Schutzplan zur Fehlerbehebung.

Ergebnis des S3-Objektscans

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

Beispiel für ein Benachrichtigungsschema für **`NO_THREATS_FOUND`**:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "NO_THREATS_FOUND",
            "threats": null
        }
    }
}
```

Beispiel für ein Benachrichtigungsschema für **`THREATS_FOUND`**:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "COMPLETED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "THREATS_FOUND",
            "threats": [
                {
                    "name": "EICAR-Test-File (not a virus)"
                }
            ]
        }
    }
}
```

Beispiel für ein Benachrichtigungsschema für den Status der Scanergebnisse **`UNSUPPORTED`** (Übersprungen):

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
```

```
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "UNSUPPORTED",
            "threats": null
        }
    }
}
```

Beispiel für ein Benachrichtigungsschema für den Status der Scanergebnisse **`ACCESS_DENIED`** (Übersprungen):

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
```

```
        "scanResultDetails": {
            "scanResultStatus": "ACCESS_DENIED",
            "threats": null
        }
    }
}
```

Beispiel für ein Benachrichtigungsschema für den Status **`FAILED`** der Scanergebnisse:

```
{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": [arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "FAILED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "scanResultDetails": {
            "scanResultStatus": "FAILED",
            "threats": null
        }
    }
}
```

Ereignisse, bei denen das Tag nach dem Scannen ausfällt

Muster des Ereignisses:

```
{
      "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
      "source": "aws.guardduty"
```

```
 }
```

Beispiel für ein Benachrichtigungsschema für **`ACCESS_DENIED`**:

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "status": "FAILED",
            "failureReason": "ACCESS_DENIED"
        }]
    }
}
```

Beispiel für ein Benachrichtigungsschema für **`MAX_TAG_LIMIT_EXCEEDED`**:

```
{
    "version": "0",
    "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
    "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-06-10T16:16:08Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
```

```
    "detail": {
        "schemaVersion": "1.0",
        "eventTime": "2024-06-10T16:16:08Z",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
            "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE"
        },
        "postScanActions": [{
            "actionType": "TAGGING",
            "status": "FAILED",
            "failureReason": "MAX_TAG_LIMIT_EXCEEDED"
        }]
    }
}
```

Informationen zur Behebung dieser Fehlerursachen finden Sie unterBehebung von Fehlern bei S3-Objektkennzeichnungen nach dem Scannen.

Überwachung der Scanstatus-Metriken mithilfe von Amazon CloudWatch

Sie können die GuardDuty Nutzung CloudWatch überwachen. Dabei werden Rohdaten gesammelt und zu lesbaren Messwerten verarbeitet, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden 15 Monate lang aufbewahrt, sodass Sie auf historische Informationen zugreifen und sich einen besseren Überblick über die Leistung von Malware Protection for S3 verschaffen können. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Die CloudWatch Metriken für Malware Protection for S3 sind auf Ressourcenebene verfügbar. Sie können diese Metriken für jede geschützte Ressource separat abfragen. Die Metriken werden im `AWS/GuardDuty/MalwareProtection` Namespace gemeldet. Sie können Alarme für bestimmte Ressourcen einrichten, um den Sicherheitsstatus zu überwachen.

Statistiken zum Status von Malware-Scans

Metrik	Beschreibung

`CompletedScanCount`	Die Anzahl der S3-Objekt-Malware-Scans, die in einem bestimmten Zeitraum abgeschlossen wurden. Gültige Abmessungen: • `Malware Protection Plan Id` `Resource Name` Einheiten: Anzahl
`FailedScanCount`	Die Anzahl der S3-Objekt-Malware-Scans, die in einem bestimmten Zeitraum abgeschlossen wurden. Gültige Abmessungen: • `Malware Protection Plan Id` `Resource Name` Einheiten: Anzahl

`SkippedScanCount`	Die Anzahl der S3-Objekt-Malware-Scans, die in einem bestimmten Zeitraum übersprungen wurden.
	
	Gültige Abmessungen:
	
	• `Malware Protection Plan Id`
	
	`Resource Name`
	
	`Skipped Reason`
	
	Mögliche Werte
	
	• `UnSupported`
	• `MissingPermissions`
	
	Einheiten: Anzahl

Kennzahlen zu den Ergebnissen von Malware-Scans

`InfectedScanCount`	Die Anzahl der S3-Objekt-Malware-Scans, bei denen innerhalb eines bestimmten Zeitraums potenziell schädliche Objekte erkannt wurden. Gültige Abmessungen: • `Malware Protection Plan Id` `Resource Name` Einheiten: Anzahl

`CompletedScanBytes`	Die Anzahl der in einem bestimmten Zeitraum gescannten S3-Objektbytes. Gültige Abmessungen: • `Malware Protection Plan Id` `Resource Name` Einheiten: Anzahl

> **Note**
>
> Standardmäßig lauten die Statistiken in den CloudWatch MetrikenAVG.

Die folgenden Dimensionen werden für die Malware Protection for S3-Metriken unterstützt.

Dimension	Beschreibung
`Malware Protection Plan Id`	Die eindeutige Kennung, die der Ressource des Malware-Schutzplans zugeordnet ist, die für Ihre geschützte Ressource GuardDuty erstellt wird.
`Resource Name`	Der Name der geschützten Ressource.
`Skipped Reason`	Der Grund, warum ein S3-Objekt-Malware-Scan übersprungen wurde. Mögliche Werte • `UnSupported` • `MissingPermissions`

Informationen zum Zugriff auf und zur Abfrage dieser Messwerte finden Sie unter Verwenden von CloudWatch Amazon-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Informationen zum Einrichten von Alarmen finden Sie unter Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch.

Überwachung mit S3-Objekt-Tags

Verwenden Sie die Option „Tagging aktivieren“, GuardDuty damit Sie Ihrem Amazon S3 S3-Objekt nach Abschluss des Malware-Scans Tags hinzufügen können.

Überlegungen zur Aktivierung von Tagging

- Wenn Sie Ihre S3-Objekte taggen, GuardDuty fallen Nutzungskosten an. Weitere Informationen finden Sie unter Preise für Malware Protection for S3.
- Sie müssen die erforderlichen Tagging-Berechtigungen für Ihre bevorzugte IAM Rolle behalten, die mit diesem Bucket verknüpft ist. Andernfalls GuardDuty können Sie Ihren gescannten Objekten keine Tags hinzufügen. Die IAM Rolle umfasst bereits die Berechtigungen zum Hinzufügen von Tags zu den gescannten S3-Objekten. Weitere Informationen finden Sie unter Voraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren.
- Standardmäßig können Sie einem S3-Objekt bis zu 10 Tags zuordnen. Weitere Informationen finden Sie unter Verwenden der tagbasierten Zugriffskontrolle () TBAC.

Nachdem Sie das Tagging für einen S3-Bucket oder bestimmte Präfixe aktiviert haben, wird jedem neu hochgeladenen Objekt, das gescannt wird, ein zugeordnetes Tag im folgenden Schlüssel-Wert-Paarformat zugewiesen:

`GuardDutyMalwareScanStatus:`*`Scan-Status`*

Hinweise zu möglichen Tag-Werten finden Sie unter. Verwenden der tagbasierten Zugriffskontrolle () TBAC

Behebung von Fehlern bei S3-Objekten nach dem Scannen von Tags in Malware Protection for S3

Dieser Abschnitt gilt nur für Sie, wenn Sie sich Aktivieren Sie das Tagging für gescannte Objekte in Ihrem geschützten Bucket befinden.

Wenn GuardDuty versucht wird, Ihrem gescannten S3-Objekt ein Tag hinzuzufügen, kann die Aktion des Taggens zu einem Fehler führen. Die möglichen Gründe, warum dies Ihrem Bucket passieren kann, sind `ACCESS_DENIED` und`MAX_TAG_LIMIT_EXCEEDED`. In den folgenden Themen erfahren

Sie mehr über die möglichen Gründe für diese Fehlerursachen nach dem Scannen von Tags und deren Behebung.

ACCESS_DENIED

In der folgenden Liste sind mögliche Gründe aufgeführt, die zu diesem Problem führen können:

- Der IAM Rolle, die für diesen geschützten S3-Bucket verwendet wird, fehlt die AllowPostScanTagBerechtigung. Stellen Sie sicher, dass die zugehörige IAM Rolle diese Bucket-Richtlinie verwendet. Weitere Informationen finden Sie unter Voraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren.
- Die geschützte S3-Bucket-Richtlinie erlaubt es nicht GuardDuty , diesem Objekt Tags hinzuzufügen.
- Das gescannte S3-Objekt ist nicht mehr vorhanden.

MAX_TAG_LIMIT_EXCEEDED

Standardmäßig können Sie einem S3-Objekt bis zu 10 Tags zuordnen. Weitere Informationen finden Sie unter Überlegungen GuardDuty zum Hinzufügen eines Tags zu Ihrem S3-Objekt unterAktivieren Sie das Tagging für gescannte Objekte.

Tag-basierte Zugriffskontrolle (TBAC) mit Malware Protection for S3 verwenden

Wenn Sie Malware Protection for S3 für Ihren Bucket aktivieren, können Sie optional das Tagging aktivieren. Nach dem Versuch, ein neu hochgeladenes S3-Objekt im ausgewählten Bucket zu scannen, wird dem gescannten Objekt ein Tag GuardDuty hinzugefügt, um den Status des Malware-Scans anzugeben. Wenn Sie das Tagging aktivieren, fallen direkte Nutzungskosten an. Weitere Informationen finden Sie unter Preise für Malware Protection for S3.

GuardDuty verwendet ein vordefiniertes Tag mit dem Schlüssel als `GuardDutyMalwareScanStatus` und dem Wert als einem der Malware-Scan-Status. Hinweise zu diesen Werten finden Sie unterS3 object potential scan result values.

Überlegungen GuardDuty zum Hinzufügen eines Tags zu Ihrem S3-Objekt:

- Standardmäßig können Sie einem Objekt bis zu 10 Tags zuordnen. Weitere Informationen finden Sie unter Kategorisieren Ihres Speichers mithilfe von Tags im Amazon S3 S3-Benutzerhandbuch.

Wenn alle 10 Tags bereits verwendet werden, GuardDuty kann das vordefinierte Tag dem gescannten Objekt nicht hinzugefügt werden. GuardDuty veröffentlicht das Scanergebnis auch in Ihrem EventBridge Standard-Event-Bus. Weitere Informationen finden Sie unter Überwachung mit Amazon EventBridge.

- Wenn die gewählte IAM Rolle nicht über die Berechtigung GuardDuty zum Taggen des S3-Objekts verfügt, können Sie diesem gescannten S3-Objekt auch dann kein Tag hinzufügen, GuardDuty wenn das Tagging für Ihren geschützten Bucket aktiviert ist. Weitere Informationen zu den erforderlichen IAM Rollenberechtigungen für das Tagging finden Sie unter. Voraussetzung — IAM Rollenrichtlinie erstellen oder aktualisieren

  GuardDuty veröffentlicht das Scanergebnis auch in Ihrem EventBridge Standard-Event-Bus. Weitere Informationen finden Sie unter Überwachung mit Amazon EventBridge.

Hinzufügen TBAC einer S3-Bucket-Ressource

Sie können die S3-Bucket-Ressourcenrichtlinien verwenden, um die tagbasierte Zugriffskontrolle (TBAC) für Ihre S3-Objekte zu verwalten. Sie können bestimmten Benutzern Zugriff gewähren, damit sie auf das S3-Objekt zugreifen und es lesen können. Wenn Sie über eine Organisation verfügen, die mithilfe von erstellt wurde AWS Organizations, müssen Sie sicherstellen, dass niemand die von hinzugefügten Tags ändern kann GuardDuty. Weitere Informationen finden Sie im Benutzerhandbuch unter Verhindern, dass Tags nur von autorisierten AWS Organizations Benutzern geändert werden. Das Beispiel, das im verlinkten Thema verwendet wird, erwähnt`ec2`. Wenn Sie dieses Beispiel verwenden, ersetzen Sie *`ec2`* mits`3`.

In der folgenden Liste wird erklärt, was Sie tun können, indem Sie Folgendes verwendenTBAC:

- Verhindern Sie, dass alle Benutzer außer dem Service Principal von Malware Protection for S3 die S3-Objekte lesen, die noch nicht mit dem folgenden Tag-Schlüssel-Wert-Paar gekennzeichnet sind:

  `GuardDutyMalwareScanStatus:`*`Potential key value`*

- Erlaubt nur GuardDuty das Hinzufügen des Tag-Schlüssels `GuardDutyMalwareScanStatus` mit Wert als Scanergebnis zu einem gescannten S3-Objekt. Mit der folgenden Richtlinienvorlage können bestimmte Benutzer, die Zugriff haben, das Schlüssel-Wert-Paar des Tags möglicherweise außer Kraft setzen.

Beispiel für eine S3-Bucket-Ressourcenrichtlinie:

Ersetzen *IAM-role-name* mit der IAM Rolle, die Sie für die Konfiguration von Malware Protection for S3 in Ihrem Bucket verwendet haben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "NoReadExceptForClean",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                    "arn:aws:iam::555555555555:root",
                    "arn:aws:iam::555555555555:role/IAM-role-name",
                    "arn:aws:iam::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection"
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
 "NO_THREATS_FOUND"
                }
            }
        },
        {
            "Sid": "OnlyGuardDutyCanTag",
            "Effect": "Deny",
            "NotPrincipal": {
                "AWS": [
                    "arn:aws:iam::555555555555:root",
                    "arn:aws:iam::555555555555:role/IAM-role-name",
                    "arn:aws:iam::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection"
                ]
```

```
            },
            "Action": "s3:PutObjectTagging",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

Weitere Informationen zum Taggen Ihrer S3-Ressource finden Sie unter Tagging- und Zugriffskontrollrichtlinien.

Bearbeiten von Malware Protection for S3 für einen geschützten Bucket

Gehen Sie wie folgt vor, um das bestehende Setup Ihres geschützten S3-Buckets zu bearbeiten:

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich die Option Malware Protection for S3 aus.
3. Wählen Sie unter Geschützte Buckets den Bucket aus, für den Sie die bestehende Konfiguration bearbeiten möchten.
4. Wählen Sie Bearbeiten aus.
5. Aktualisieren Sie die bestehende Konfiguration und die Einstellungen für Ihren Bucket und bestätigen Sie die Änderungen. Informationen zur Beschreibung und zu den einzelnen Schritten für die einzelnen Abschnitte finden Sie unterAktivieren Sie den Malware-Schutz für S3 für Ihren Bucket.

   Überwachen Sie die Statusspalte für diesen geschützten Bucket. Wenn es entweder als Warnung oder als Fehler angezeigt wird, finden Sie weitere Informationen unterStatusdetails zum Malware-Schutzplan zur Fehlerbehebung.

Nutzung und Kosten für Malware Protection for S3 anzeigen

Für Ihr Konto fallen Nutzungskosten an, wenn Sie Malware Protection for S3 über das angegebene Limit im Rahmen des kostenlosen Kontingents hinaus nutzen oder wenn das 12-monatige kostenlose

Kontingent Ihres Kontos endet. Informationen zum kostenlosen Kontingent finden Sie unter. Preise für Malware Protection for S3

Um die Nutzungskosten anzuzeigen, navigieren Sie in der https://console.aws.amazon.com/billing/ -Konsole zu Cost Explorer. Informationen zur AWS-Konto Abrechnung finden Sie im AWS Billing Benutzerhandbuch.

Deaktivieren Sie den Malware-Schutz für S3 für einen geschützten Bucket

Wenn Sie Malware Protection for S3 für einen geschützten Bucket deaktivieren, GuardDuty wird die diesem Bucket zugeordnete Plan-ID für den Schadsoftware-Schutz gelöscht. GuardDuty startet keinen Malware-Scan mehr, wenn ein neues Objekt in diesen Bucket oder eines der ausgewählten Objektpräfixe hochgeladen wird.

Wenn Sie die Option aktiviert haben GuardDuty und nun den Vorgang unterbrechen oder deaktivieren möchten GuardDuty, finden Sie weitere Informationen unterAussetzen oder Deaktivieren GuardDuty. Da es in Malware Protection for S3 kein Konzept für die Detektor-ID gibt, wirkt sich die Deaktivierung oder Sperrung GuardDuty nicht auf den Status eines geschützten Buckets in Ihrem Konto aus. Sie können die Funktion Malware Protection for S3 unabhängig weiter nutzen, wobei der entsprechende Standardpreis anfällt. Weitere Informationen finden Sie unter Nutzung und Kosten für Malware Protection for S3 anzeigen. Um die Nutzung von Malware Protection for S3 zu beenden, müssen Sie ihn für alle geschützten Buckets in Ihrem Konto deaktivieren. Wenn Sie weiterhin nur Malware Protection for S3 für einen Bucket verwenden GuardDuty und deaktivieren möchten, wirken sich die folgenden Schritte nicht auf die Konfiguration des GuardDuty Dienstes und andere Schutzpläne aus, die Sie möglicherweise aktiviert haben.

Um Malware Protection for S3 für einen geschützten Bucket zu deaktivieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich die Option Malware Protection for S3 aus.
3. Wählen Sie unter Geschützte Buckets den Bucket aus, für den Sie Malware Protection for S3 deaktivieren möchten.

   Sie können jeweils nur einen geschützten Bucket auswählen. Um den Malware-Schutz für S3 für mehr als einen Bucket zu deaktivieren, führen Sie diese Schritte erneut für einen anderen S3-Bucket aus.

4. Wählen Sie Disable (deaktivieren) aus.
5. Wählen Sie Deaktivieren, um die Auswahl zu bestätigen.

Unterstützbarkeit der Amazon S3 S3-Funktionen

In der folgenden Tabelle wird angegeben, ob Malware Protection for S3 die aufgelisteten Amazon S3 S3-Funktionen unterstützt.

Ist der Support verfügbar?	Beschreibung
Ja	S3-Objekte können abgerufen werden, ohne dass sie asynchron wiederhergestellt werden müssen.

Ist der Support verfügbar?	Beschreibung
Bedingt	• Unterstützung für Intelligent Tiering ist für S3-Objekte in den Stufen „Häufig“, „Seltener Zugriff“ und „Archive-Instanzzugriff“ verfügbar. • Die Opt-in-Stufen Archive und Deep Archive werden nicht unterstützt. • Intelligent Tiering erstellt in der Stufe „Häufiger Zugriff“ immer ein neues Objekt. Daher wird der Objektscan bei der Erstellung unterstützt. • Künftige intelligente Tiering-Funktionen könnten zunächst Objekte im Archiv erstellen. Daher wird dies nicht unterstützt.

Ist der Support verfügbar?	Beschreibung
Nein	GuardDuty unterstützt nur Allzweck-Buckets für den Malware-Schutz für S3.
Nein	Die S3-Objekte müssen wiederhergestellt werden, bevor auf sie zugegriffen werden kann.

Ist der Support verfügbar?	Beschreibung
Nein	Der Malware-Schutz für S3 wird auf Outposts nicht unterstützt.
Ja	Alle hochgeladenen S3-Objekte werden auf Malware gescannt. Wenn Sie ein Objekt mit Dateiversion v1 hochgeladen haben und sofort eine weitere Versionsü berschreibung mit Version v2 hochgeladen haben, GuardDuty werden beide Objektdateiversionen v1 und v2 gescannt. Die Startzeit des Scans ist jedoch möglicher weise nicht in derselben Reihenfolge.
Ja	Wenn es sich bei dem Ziel-Bucket um eine geschützte Ressource handelt, GuardDuty werden alle S3-Objekte auf die geschützten und überwachten Präfixe repliziert.

Ist der Support verfügbar?	Beschreibung
Nein	Sie können keine Replikationsregel auf der Grundlage des Scanergebnis-Tags definieren. Amazon S3 unterstützt keine Replikation für Tags, außer bei der Erstellung.

Ist der Support verfügbar?	Beschreibung
Ja	GuardDuty unterstützt Malware-Scans nach S3-Objekten, die mit verwalteten und vom Kunden verwalteten Schlüsseln verschlüsselt sind. Stellen Sie sicher, dass die IAM Rolle die Berechtigung zur Verwendung des Schlüssels beinhaltet. Weitere Informationen finden Sie unter Hinzufügen von IAM Richtlinienberechtigungen.

Ist der Support verfügbar?	Beschreibung
Nein	Malware Protection for S3 unterstützt nicht das Scannen von S3-Objekten, die mit Schlüsseln verschlüsselt sind, auf die nicht zugegriffen werden kann.
Nein	Wenn Ihre S3-Objekte mithilfe des Amazon S3 Encryption Client verschlüsselt werden, werden Ihre Objekte nicht an Dritte weitergegeben, auch nicht AWS. Weitere Informationen darüber, warum dies nicht unterstützt wird, finden Sie unter Schützen von Daten durch clientseitige Verschlüsselung im Amazon S3 S3-Benutzerhandbuch.
Ja	Gesperrte S3-Objekte werden auf der Grundlage von WORM - Write Once Read Many gesperrt. Malware Protection for S3 kann auf die Objekte zugreifen und sie scannen.
Ja	Malware Protection for S3 kann die Buckets scannen, die mit Requester Pays eingerichtet wurden. Der Anforderer zahlt für die S3-Anrufe. Weitere Informationen finden Sie unter Verwendung von Anforderer zahlt Buckets für Speicherübertragungen und -nutzung im Amazon-S3-Benutzerhandbuch.

Ist der Support verfügbar?	Beschreibung
Ja	Sie können Lebenszyklusrichtlinien auf der Grundlage des Scanergebnis-Tags definieren. Löschen Sie beispielsweise bösartige Objekte automatisch. Weitere Informationen zur Lebenszykluskonfiguration finden Sie unter Verwaltung Ihres Speicherlebenszyklus im Amazon S3 S3-Benutzerhandbuch.
Ja	Sie können Bucket-Ressourcenrichtlinien auf der Grundlage Ihres Ergebnis-Tags für den S3-Objektscan definieren. Verhindern Sie beispielsweise den Zugriff auf S3-Objekte, die noch nicht gescannt wurden, oder auf GuardDuty erkannte Bedrohungen. Weitere Informationen finden Sie unter Tag-basierte Zugriffskontrolle (TBAC) mit Malware Protection for S3 verwenden.

Kontingente im Malware-Schutz für S3

Dieser Abschnitt enthält Standardkontingente, die oft als Grenzwerte bezeichnet werden. Sofern nicht anders angegeben, ist jedes Kontingent regionsspezifisch. Standardkontingente für die Nutzung des Basisdienstes (oder GuardDuty Kerndienstes) finden Sie unter. GuardDuty Amazon-Kontingente

In den folgenden Tabellen werden die verschiedenen Kontingente beschrieben, die für Sie AWS-Konto gelten.

AWS Standardkontingentwert	Ist er einstellbar?	Beschreibung
5 GB	Nein	Die maximale S3-Objektgröße, mit der versucht GuardDuty wird, nach Malware zu suchen.

AWS Standardkontingentwert	Ist er einstellbar?	Beschreibung
5 GB	Nein	Die maximale Datenmenge (in GB), die aus einer Archivdatei extrahiert und analysiert werden GuardDuty kann. Selbst wenn eine Archivdatei mehr als 5 GB enthält, GuardDuty wird der Inhalt, der diesen Wert überschreitet, übersprungen.
1.000	Nein	Die maximale Anzahl von Dateien, die in einer Archivdatei extrahiert und analysiert werden GuardDuty können. Wenn die Datei mehr als 1.000 Dateien enthält, muss die archivierte Datei übersprungen GuardDuty werden.
5	Nein	Die maximale Anzahl verschachtelter Archive, die extrahiert GuardDuty werden können. Wenn das Archiv Dateien enthält, deren Verschachtelung diesen Wert überschreitet, GuardDuty werden diese verschachtelten Dateien übersprungen.
25	Nein	Die maximale Anzahl von S3-Buckets, für die Sie Malware Protection for S3 aktivieren können. Diese Kontingentbegrenzung gilt pro Konto in jeder Region.

AWS Standardkontingentwert	Ist er einstellbar?	Beschreibung
25	Auf regionaler Ebene	Die maximale Anzahl von Operationen auf der Kontrollebene, die pro Sekunde in jeder Region ausgelöst werden können. Zu den API Vorgängen gehören das Erstellen, Lesen, Aktualisieren und Löschen von Ressourcen. Dieser Kontingentwert gilt auf Regionsebene.

GuardDuty RDSSchutz

RDSProtection in Amazon GuardDuty analysiert und protokolliert RDS Anmeldeaktivitäten im Hinblick auf potenzielle Zugriffsbedrohungen auf Ihre Amazon Aurora-Datenbanken (Amazon Aurora My SQL -Compatible Edition und Aurora Postgre SQL -Compatible Edition) und Amazon RDS for Postgre. SQL Mit dieses Feature können Sie potenziell verdächtiges Anmeldeverhalten identifizieren. RDSDer Schutz erfordert keine zusätzliche Infrastruktur. Er ist so konzipiert, dass er die Leistung Ihrer Datenbank-Instances nicht beeinträchtigt.

Wenn der RDS Schutz einen potenziell verdächtigen oder anomalen Anmeldeversuch erkennt, der auf eine Bedrohung für Ihre Datenbank hindeutet, GuardDuty generiert er ein neues Ergebnis mit Details über die potenziell gefährdete Datenbank.

Sie können die RDS Schutzfunktion für jedes Konto an jedem Ort, AWS-Region an dem diese Funktion bei Amazon verfügbar ist GuardDuty, jederzeit aktivieren oder deaktivieren. Ein vorhandenes GuardDuty Konto kann den RDS Schutz mit einer 30-tägigen Testphase aktivieren. Für ein neues GuardDuty Konto ist der RDS Schutz bereits aktiviert und in der 30-tägigen kostenlosen Testphase enthalten. Weitere Informationen finden Sie unter Einschätzen der Kosten.

> **Note**
>
> Wenn die RDS Schutzfunktion nicht aktiviert ist, werden GuardDuty weder Ihre RDS Anmeldeaktivitäten erfasst noch ein ungewöhnliches oder verdächtiges Anmeldeverhalten erkannt.

Informationen darüber, AWS-Regionen wo der RDS Schutz noch GuardDuty nicht unterstützt wird, finden Sie unter. Verfügbarkeit regionsspezifischer Feature

Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken

Die folgende Tabelle zeigt die unterstützten Aurora- und RDS Amazon-Datenbankversionen.

Amazon Aurora und Amazon RDS DB-Engine	Unterstützte Engine-Versionen
Aurora My SQL	• 2.10.2 oder höher

Amazon Aurora und Amazon RDS DB-Engine	Unterstützte Engine-Versionen
	• 3.02.1 oder höher
Aurora Postgret SQL	• 10.17 oder höher • 11.12 oder höher • 12.7 oder höher • 13.3 oder höher • 14.3 oder höher • 15.2 oder später • 16.1 oder später
RDSfür Postgre SQL	• 14.5 oder später • 13.8 oder später • 12.12 oder später • 11.17 oder später • 10.22 oder später • RDSfür Postgre-Version 15 SQL • RDSfür Postgre-Version 16 SQL

Wie verwendet RDS Protection die Überwachung der RDS Anmeldeaktivitäten

RDSDer Schutz in Amazon GuardDuty hilft Ihnen, die unterstützten Amazon Aurora (Aurora) - und RDS SQL Postgre-Datenbanken in Ihrem Konto zu schützen. Nachdem Sie die RDS Schutzfunktion aktiviert haben, beginnt GuardDuty sofort die Überwachung der RDS Anmeldeaktivitäten von Aurora-Datenbanken und Amazon RDS in Ihrem Konto. GuardDuty überwacht kontinuierlich RDS Anmeldeaktivitäten und erstellt Profile für verdächtige Aktivitäten, z. B. unbefugten Zugriff auf die Aurora-Datenbank in Ihrem Konto durch einen zuvor unbekannten externen Akteur. Wenn Sie den RDS Schutz zum ersten Mal aktivieren oder eine neu erstellte Datenbank-Instance haben, ist eine Lernphase erforderlich, um das normale Verhalten als Grundlage zu nehmen. Aus diesem Grund kann es sein, dass neu aktivierte oder neu erstellte Datenbank-Instances bis zu zwei Wochen lang keine anomalen Anmelde-Erkenntnisse aufweisen. Weitere Informationen finden Sie unter RDSÜberwachung der Login-Aktivitäten.

Wenn der RDS Schutz eine potenzielle Bedrohung erkennt, z. B. ein ungewöhnliches Muster bei einer Reihe erfolgreicher, fehlgeschlagener oder unvollständiger Anmeldeversuche, GuardDuty generiert er ein neues Ergebnis mit Details über die potenziell gefährdete Datenbank-Instance. Weitere Informationen finden Sie unter Erkenntnistypen für RDS Protection. Wenn Sie den RDS Schutz deaktivieren, wird die Überwachung der RDS Anmeldeaktivitäten GuardDuty sofort beendet und es kann keine potenzielle Bedrohung für Ihre unterstützten Datenbank-Instances erkannt werden.

> **Note**
>
> GuardDuty verwaltet Unterstützte Datenbanken weder Ihre Aktivitäten noch Ihre RDS Anmeldeaktivitäten und stellt Ihnen keine RDS Anmeldeaktivitäten zur Verfügung.

Funktion im RDS Schutzbereich

RDSÜberwachung der Login-Aktivitäten

RDSDie Anmeldeaktivität erfasst sowohl erfolgreiche als auch fehlgeschlagene Anmeldeversuche Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken in Ihrer AWS Umgebung. Um Sie beim Schutz Ihrer Datenbanken zu unterstützen, überwacht GuardDuty RDS Protection die Anmeldeaktivitäten kontinuierlich auf potenziell verdächtige Anmeldeversuche. Beispielsweise könnte ein Angreifer versuchen, Brute-Force-Zugriff auf eine Amazon-Aurora-Datenbank zu erlangen, indem er das Passwort der Datenbank errät.

Wenn Sie die RDS Schutzfunktion aktivieren, beginnt GuardDuty automatisch die Überwachung der RDS Anmeldeaktivitäten für Ihre Datenbanken direkt von den Aurora- und RDS Amazon-Diensten aus. Wenn es Hinweise auf ein ungewöhnliches Anmeldeverhalten gibt, GuardDuty generiert dies einen Befund mit Einzelheiten über die potenziell gefährdete Datenbank. Wenn Sie den RDS Schutz zum ersten Mal aktivieren oder wenn Sie eine neu erstellte Datenbank-Instance haben, ist eine Lernphase erforderlich, um das normale Verhalten als Grundlage zu nehmen. Aus diesem Grund kann es sein, dass neu aktivierte oder neu erstellte Datenbank-Instances bis zu zwei Wochen lang keine anomalen Anmelde-Erkenntnisse aufweisen.

Die RDS Schutzfunktion erfordert keine zusätzliche Einrichtung. Sie hat keine Auswirkungen auf Ihre bestehenden Amazon Aurora Aurora-Datenbanken oder RDS Amazon-Konfigurationen. GuardDuty verwaltet Ihre unterstützten Datenbanken oder RDS Anmeldeaktivitäten nicht und stellt Ihnen die RDS Anmeldeaktivität auch nicht zur Verfügung.

Wenn Sie sich dafür entscheiden, die RDS Schutzfunktion für neue Mitgliedskonten automatisch zu aktivieren, wenn diese Ihrer Organisation beitreten, wird diese Aktion automatisch GuardDuty für diese neuen Mitgliedskonten aktiviert. Weitere Informationen zur Konfiguration der Überwachung der RDS Anmeldeaktivitäten als Funktion finden Sie unterGuardDuty RDSSchutz.

RDSSchutz für ein eigenständiges Konto konfigurieren

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich RDSSchutz aus.
3. Auf der Seite RDSSchutz wird der aktuelle Status Ihres Kontos angezeigt. Sie können das Feature jederzeit aktivieren oder deaktivieren, indem Sie Aktivieren oder Deaktivieren auswählen. Bestätigen Sie Ihre Auswahl.

API/CLI

Führen Sie den updateDetectorAPIVorgang mit Ihrer eigenen regionalen Melder-ID aus und übergeben Sie das `features` Objekt `name` als `RDS_LOGIN_EVENTS` und `status` als `ENABLED` oder`DISABLED`.

Sie können den RDS Schutz auch aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie Ihren eigenen gültigen verwenden *`detector ID`*.

> **Note**
>
> Der folgende Beispielcode aktiviert RDS den Schutz. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

Konfiguration des RDS Schutzes in Umgebungen mit mehreren Konten

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, die RDS Schutzfunktion für die Mitgliedskonten in seiner Organisation zu aktivieren oder zu deaktivieren. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet seine Mitgliedskonten mithilfe von AWS Organizations. Dieses delegierte GuardDuty Administratorkonto kann festlegen, dass die Überwachung der RDS Anmeldeaktivitäten für alle neuen Konten automatisch aktiviert wird, wenn sie der Organisation beitreten. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten bei Amazon. GuardDuty

Konfiguration des RDS Schutzes für ein delegiertes Administratorkonto GuardDuty

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die Überwachung der RDS Anmeldeaktivität für das delegierte GuardDuty Administratorkonto zu konfigurieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen des Verwaltungskontos verwenden.
2. Wählen Sie im Navigationsbereich RDSSchutz aus.
3. Wählen Sie auf der Seite RDSSchutz die Option Bearbeiten aus.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Save (Speichern) aus.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.

- Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
- Wählen Sie Save (Speichern) aus.

API/CLI

Führen Sie den updateDetectorAPIVorgang mit Ihrer eigenen regionalen Melder-ID aus und übergeben Sie das `features` Objekt `name` als `RDS_LOGIN_EVENTS` und `status` als `ENABLED` oder`DISABLED`.

Sie können den RDS Schutz aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie ein gültiges delegiertes GuardDuty Administratorkonto verwenden *`detector ID`*.

> **Note**
>
> Der folgende Beispielcode aktiviert den RDS Schutz. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

Automatisches Aktivieren RDS des Schutzes für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die RDS Schutzfunktion für alle Mitgliedskonten zu aktivieren. Dazu gehören der delegierte Administrator, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   Verwenden Sie die RDSSchutzseite

   1. Wählen Sie im Navigationsbereich RDSSchutz aus.
   2. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch RDS den Schutz sowohl für bestehende als auch für neue Konten in der Organisation.
   3. Wählen Sie Save (Speichern) aus.

   > **Note**
   >
   > Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

   Verwenden der Seite Konten

   1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
   2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
   3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter Überwachung der RDS Anmeldeaktivität die Option Für alle Konten aktivieren aus.
   4. Wählen Sie Save (Speichern) aus.

   Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Aktiviere oder deaktiviere den RDS Schutz für Mitgliedskonten selektiv.

API/CLI

- Um den RDS Schutz für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, starten Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie den RDS Schutz für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivieren Sie RDS den Schutz für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um den RDS Schutz für alle vorhandenen aktiven Mitgliedskonten in Ihrer Organisation zu aktivieren.

Console

Um den RDS Schutz für alle vorhandenen aktiven Mitgliedskonten zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich RDSSchutz aus.
3. Auf der Seite RDSSchutz können Sie den aktuellen Status der Konfiguration einsehen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.

5. Wählen Sie Bestätigen aus.

API/CLI

- Um den RDS Schutz für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen Konto auf *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie den RDS Schutz für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Automatischer RDS Schutz für neue Mitgliedskonten aktivieren

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die RDS Anmeldeaktivität für neue Konten zu aktivieren, die Ihrer Organisation beitreten.

Console

Das delegierte GuardDuty Administratorkonto kann über die Konsole entweder über die Seite RDSSchutz oder Konten neue Mitgliedskonten in einer Organisation aktivieren.

So aktivieren Sie den RDS Schutz für neue Mitgliedskonten automatisch

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   - Verwenden Sie die RDSSchutzseite:

     1. Wählen Sie im Navigationsbereich RDSSchutz aus.
     2. Wählen Sie auf der Seite RDSSchutz die Option Bearbeiten aus.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass der RDS Schutz für das Konto automatisch aktiviert wird, wenn ein neues Konto Ihrer Organisation beitritt. Nur das vom Unternehmen delegierte GuardDuty Administratorkonto kann diese Konfiguration ändern.
     5. Wählen Sie Save (Speichern) aus.

   - Verwenden der Seite Konten:

     1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
     2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren.
     3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter Überwachung der RDS Anmeldeaktivität die Option Für neue Konten aktivieren aus.
     4. Wählen Sie Save (Speichern) aus.

API/CLI

- Um den RDS Schutz für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den UpdateOrganizationConfigurationAPIVorgang mit Ihrem eigenen Konto auf *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie den RDS Schutz für ein einzelnes Mitgliedskonto aktivieren können. Informationen zur Deaktivierung finden Sie unter Aktiviere oder deaktiviere den RDS Schutz für Mitgliedskonten selektiv. Wenn Sie es nicht für alle neuen Konten aktivieren möchten, die der Organisation beitreten, legen Sie die Einstellung `autoEnable` auf `NONE` fest.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktiviere oder deaktiviere den RDS Schutz für Mitgliedskonten selektiv

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die Überwachung der RDS Anmeldeaktivitäten für Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   Auf der Seite Konten finden Sie in der Spalte mit den RDSAnmeldeaktivitäten den Status Ihres Mitgliedskontos.
3. Um RDS Anmeldeaktivitäten selektiv zu aktivieren oder zu deaktivieren

   Wählen Sie das Konto aus, für das Sie den RDS Schutz konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen. Wählen Sie im Dropdownmenü Schutzpläne bearbeiten die Option RDSAnmeldeaktivität und dann die entsprechende Option aus.

API/CLI

Um den RDS Schutz für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen Konto auf *`detector ID`*.

Das folgende Beispiel zeigt, wie Sie den RDS Schutz für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

> **Note**
>
> Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

GuardDuty Lambda-Schutz

Lambda Protection hilft Ihnen dabei, potenzielle Sicherheitsbedrohungen zu identifizieren, wenn eine AWS Lambda-Funktion in Ihrer AWS -Umgebung aufgerufen wird. Wenn Sie Lambda Protection aktivieren, GuardDuty beginnt die Überwachung von Lambda-Netzwerkaktivitätsprotokollen, VPC-Flow-Protokolle beginnend mit allen Lambda-Funktionen für Account, einschließlich der Protokolle, die kein VPC Netzwerk verwenden, und die generiert werden, wenn die Lambda-Funktion aufgerufen wird. Wenn verdächtiger Netzwerkverkehr GuardDuty identifiziert wird, der auf das Vorhandensein eines potenziell schädlichen Codes in Ihrer Lambda-Funktion hinweist, GuardDuty wird ein Befund generiert.

> **Note**
>
> Lambda Network Activity Monitoring beinhaltet keine Protokolle für Lambda@Edge-Funktionen.

Sie können Lambda Protection für jedes Konto oder für jedes verfügbare AWS-Regionen Konto jederzeit konfigurieren. Standardmäßig kann ein vorhandenes GuardDuty Konto Lambda Protection mit einer 30-tägigen Testphase aktivieren. Für ein neues GuardDuty Konto ist Lambda Protection bereits aktiviert und in der 30-tägigen Testphase enthalten. Weitere Informationen zu Nutzungsstatistiken finden Sie unter Einschätzen der Kosten.

GuardDuty überwacht Netzwerkaktivitätsprotokolle, die durch den Aufruf der Lambda-Funktionen generiert wurden. Derzeit umfasst Lambda Network Activity Monitoring VPC Amazon-Flow-Protokolle von allen Lambda-Funktionen für Ihr Konto, einschließlich der Protokolle, die kein Netzwerk verwenden VPC und sich ändern können, einschließlich der Erweiterung auf andere Netzwerkaktivitäten wie DNS Abfragedaten, die durch das Aufrufen der Lambda-Funktionen generiert werden. Die Ausweitung auf andere Formen der Überwachung der Netzwerkaktivität wird das Datenvolumen erhöhen, das für Lambda Protection verarbeitet GuardDuty wird. Dies wird sich direkt auf die Nutzungskosten von Lambda Protection auswirken. Wenn GuardDuty mit der Überwachung eines zusätzlichen Netzwerkaktivitätsprotokolls begonnen wird, erhalten die Konten, die Lambda Protection aktiviert haben, mindestens 30 Tage vor der Veröffentlichung eine Benachrichtigung.

Feature in Lambda Protection

Lambda Network Activity Monitoring

Wenn Sie Lambda Protection aktivieren, GuardDuty überwacht Lambda-Netzwerkaktivitätsprotokolle, die generiert werden, wenn eine Ihrem Konto zugeordnete Lambda-Funktion aufgerufen wird. Auf diese Weise können Sie potenzielle Sicherheitsbedrohungen für die Lambda-Funktion erkennen. GuardDuty überwacht die VPC Flussprotokolle all Ihrer Lambda-Funktionen, einschließlich derer, die kein VPC Netzwerk verwenden. Für Lambda-Funktionen, die für die Verwendung von VPC Netzwerken konfiguriert sind, müssen Sie keine VPC Flow-Logs für die Elastic Network Interfaces (ENI) aktivieren, die von Lambda für erstellt wurden. GuardDuty GuardDuty berechnet nur die Menge an Lambda-Netzwerkaktivitätsprotokollen, die verarbeitet wurden (in GB), um ein Ergebnis zu generieren. GuardDuty optimiert die Kosten durch die Anwendung intelligenter Filter und die Analyse einer Teilmenge der Lambda-Netzwerkaktivitätsprotokolle, die für die Bedrohungserkennung relevant sind. Preisinformationen finden Sie unter GuardDuty Amazon-Preise.

GuardDuty verwaltet Ihre Lambda-Netzwerkaktivitätsprotokolle (einschließlich VPC und VPC Nicht-Flow-Logs) nicht und macht sie auch nicht in Ihrem Konto zugänglich.

Konfigurieren von Lambda Protection

Lambda Protection für ein einzelnes Konto konfigurieren

Für Konten, die mit verknüpft sind AWS Organizations, können Sie diesen Vorgang über die GuardDuty Konsole oder API Anweisungen automatisieren, wie im nächsten Abschnitt beschrieben.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Protection für ein einzelnes Konto zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Lambda Protection.
3. Auf der Lambda-Protection-Seite wird der aktuelle Status Ihres Kontos angezeigt. Sie können das Feature jederzeit aktivieren oder deaktivieren, indem Sie Aktivieren oder Deaktivieren auswählen.
4. Wählen Sie Save (Speichern) aus.

API/CLI

Führen Sie den updateDetectorAPIVorgang mit Ihrer eigenen regionalen Melder-ID aus und übergeben Sie das `features` Objekt `name` als `LAMBDA_NETWORK_LOGS` und `status` als `ENABLED` oder`DISABLED`.

Sie können Lambda Network Activity Monitoring auch aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie Ihren eigenen gültigen verwenden *`detector ID`*.

> **Note**
>
> Der folgende Beispielcode aktiviert Lambda Network Activity Monitoring. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" : "ENABLED"}]'
```

Lambda Protection in Umgebungen mit mehreren Konten konfigurieren

In einer Umgebung mit mehreren Konten hat nur das delegierte GuardDuty Administratorkonto die Möglichkeit, Lambda Protection für die Mitgliedskonten in seiner Organisation zu aktivieren oder zu deaktivieren. Die GuardDuty Mitgliedskonten können diese Konfiguration nicht von ihren Konten aus ändern. Das delegierte GuardDuty Administratorkonto verwaltet Mitgliedskonten mithilfe von AWS Organizations. Das delegierte GuardDuty Administratorkonto kann festlegen, dass Lambda Network Activity Monitoring für alle neuen Konten automatisch aktiviert wird, sobald sie der Organisation beitreten. Weitere Informationen zu Umgebungen mit mehreren Konten finden Sie unter Verwaltung mehrerer Konten bei Amazon GuardDuty.

Lambda-Schutz für ein delegiertes Administratorkonto GuardDuty konfigurieren

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für das delegierte GuardDuty Administratorkonto zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Stellen Sie sicher, dass Sie die Anmeldeinformationen des Verwaltungskontos verwenden.
2. Wählen Sie im Navigationsbereich unter Einstellungen die Option Lambda Protection.
3. Wählen Sie auf der Seite Lambda Protection die Option Bearbeiten.
4. Führen Sie eine der folgenden Aktionen aus:

   Verwendung von Für alle Konten aktivieren

   - Wählen Sie Für alle Konten aktivieren. Dadurch wird der Schutzplan für alle aktiven GuardDuty Konten in Ihrer AWS Organisation aktiviert, einschließlich der neuen Konten, die der Organisation beitreten.
   - Wählen Sie Save (Speichern) aus.

   Verwendung von Konten manuell konfigurieren

   - Um den Schutzplan nur für das delegierte GuardDuty Administratorkonto zu aktivieren, wählen Sie Konten manuell konfigurieren.
   - Wählen Sie im Abschnitt für das delegierte GuardDuty Administratorkonto (dieses Konto) die Option Aktivieren aus.
   - Wählen Sie Save (Speichern) aus.

API/CLI

Führen Sie den updateDetectorAPIVorgang mit Ihrer eigenen regionalen Melder-ID aus und übergeben Sie das `features` Objekt `name` als `LAMBDA_NETWORK_LOGS` und `status` als `ENABLED` oder`DISABLED`.

Sie können Lambda Network Activity Monitoring aktivieren oder deaktivieren, indem Sie den folgenden AWS CLI Befehl ausführen. Stellen Sie sicher, dass Sie ein gültiges delegiertes GuardDuty Administratorkonto verwenden *`detector ID`*.

> **Note**
>
> Der folgende Beispielcode aktiviert Lambda Network Activity Monitoring. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Das `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty update-detector --detector-
id 12abc34d567e8fa901bc2d34e56789f0 555555555555 --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Automatische Aktivierung von Lambda Network Activity Monitoring für alle Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring Feature für alle Mitgliedskonten zu aktivieren. Dazu gehören der delegierte Administrator, bestehende Mitgliedskonten und die neuen Konten, die der Organisation beitreten.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:

   Die Seite Lambda Protection verwenden

   1. Wählen Sie im Navigationsbereich Lambda Protection aus.
   2. Wählen Sie Für alle Konten aktivieren. Diese Aktion aktiviert automatisch Lambda Network Activity Monitoring sowohl für bestehende als auch für neue Konten in der Organisation.
   3. Wählen Sie Save (Speichern) aus.

> **Note**
>
> Die Aktualisierung der Konfiguration der Mitgliedskonten kann bis zu 24 Stunden dauern.

Verwenden der Seite Konten

1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren und anschließend Konten auf Einladung hinzufügen.
3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter Lambda Network Activity Monitoring die Option Für alle Konten aktivieren.

   > **Note**
   >
   > Standardmäßig aktiviert diese Aktion automatisch die Option Automatisch GuardDuty für neue Mitgliedskonten aktivieren.

4. Wählen Sie Save (Speichern) aus.

Falls Sie die Option Für alle Konten aktivieren nicht verwenden können, finden Sie weitere Informationen unter Selektives Aktivieren oder Deaktivieren von Lambda Network Activity Monitoring für Mitgliedskonten.

API/CLI

- Um Lambda Network Activity Monitoring für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen auf *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie Lambda Network Activity Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um ein Mitgliedskonto zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus. ListDetectorsAPI

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Aktivierung von Lambda Network Activity Monitoring für alle vorhandenen aktiven Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für alle vorhandenen aktiven Mitgliedskonten in der Organisation zu aktivieren.

Console

So konfigurieren Sie Lambda Network Activity Monitoring für alle vorhandenen aktiven Mitgliedskonten

1. Melden Sie sich bei an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Melden Sie sich mit den Anmeldeinformationen für das delegierte GuardDuty Administratorkonto an.
2. Wählen Sie im Navigationsbereich Lambda Protection.
3. Auf der Seite Lambda Protection können Sie den aktuellen Status der Konfiguration anzeigen. Wählen Sie im Abschnitt Aktive Mitgliedskonten die Option Aktionen.
4. Wählen Sie im Dropdownmenü Aktionen die Option Aktivieren für alle vorhandenen aktiven Mitgliedskonten.
5. Wählen Sie Bestätigen aus.

API/CLI

- Um Lambda Network Activity Monitoring für Ihre Mitgliedskonten selektiv zu aktivieren oder zu deaktivieren, rufen Sie den updateMemberDetectorsAPIVorgang mit Ihrem eigenen auf *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie Lambda Network Activity Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um ein Mitgliedskonto zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

  Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus. ListDetectorsAPI

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
  ```

  Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.
- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Automatische Aktivierung von Lambda Network Activity Monitoring für neue Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für neue Konten, die Ihrer Organisation beitreten, zu aktivieren.

Console

Das delegierte GuardDuty Administratorkonto kann Lambda Network Activity Monitoring für neue Mitgliedskonten in einer Organisation entweder über die Seite Lambda-Schutz oder Konten aktivieren.

Wie Sie die automatische Aktivierung von Lambda Network Activity Monitoring für neue Mitgliedskonten einrichten

1. Öffnen Sie die Konsole unter GuardDuty . https://console.aws.amazon.com/guardduty/

Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.

2. Führen Sie eine der folgenden Aktionen aus:
   - Verwenden der Seite Lambda Protection:
     1. Wählen Sie im Navigationsbereich Lambda Protection.
     2. Wählen Sie auf der Seite Lambda Protection die Option Bearbeiten.
     3. Wählen Sie Konten manuell konfigurieren.
     4. Wählen Sie Automatisch für neue Mitgliedskonten aktivieren. Dieser Schritt stellt sicher, dass Lambda Protection automatisch für das Konto aktiviert wird, wann immer ein neues Konto Ihrer Organisation beitritt. Nur das delegierte GuardDuty Administratorkonto der Organisation kann diese Konfiguration ändern.
     5. Wählen Sie Save (Speichern) aus.
   - Verwenden der Seite Konten:
     1. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
     2. Wählen Sie auf der Seite Konten die Option Einstellungen automatisch aktivieren.
     3. Wählen Sie im Fenster Einstellungen für automatische Aktivierung verwalten unter Lambda Network Activity Monitoring die Option Für neue Konten aktivieren.
     4. Wählen Sie Save (Speichern) aus.

API/CLI

- Um Lambda Network Activity Monitoring für neue Mitgliedskonten zu aktivieren oder zu deaktivieren, rufen Sie den UpdateOrganizationConfigurationAPIVorgang mit Ihrem eigenen auf *`detector ID`*.
- Das folgende Beispiel zeigt, wie Sie Lambda Network Activity Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Informationen zur Deaktivierung finden Sie unter Selektives Aktivieren oder Deaktivieren von Lambda Network Activity Monitoring für Mitgliedskonten. Wenn Sie es nicht für alle neuen Konten aktivieren möchten, die der Organisation beitreten, legen Sie die Einstellung `AutoEnable` auf `NONE` fest.

  Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Einstellungsseite in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus. ListDetectorsAPI

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
```

- Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Selektives Aktivieren oder Deaktivieren von Lambda Network Activity Monitoring für Mitgliedskonten

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Lambda Network Activity Monitoring für ausgewählte Mitgliedskonten zu aktivieren oder zu deaktivieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Stellen Sie sicher, dass Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto verwenden.
2. Klicken Sie im Navigationsbereich unter Settings auf Accounts.

   Sehen Sie sich auf der Seite Konten die Spalte Lambda Network Activity Monitoring an. Sie gibt an, ob Lambda Network Activity Monitoring aktiviert ist oder nicht.
3. Wählen Sie das Konto aus, für das Sie Lambda Protection konfigurieren möchten. Sie können mehrere Konten gleichzeitig auswählen.
4. Wählen Sie im Dropdownmenü Schutzpläne bearbeiten die Option Lambda Network Activity Monitoring und wählen Sie dann eine entsprechende Aktion aus.

API/CLI

Rufen Sie das updateMemberDetectorsAPImit Ihrem eigenen auf *`detector ID`*.

Das folgende Beispiel zeigt, wie Sie Lambda Network Activity Monitoring für ein einzelnes Mitgliedskonto aktivieren können. Um die Funktion zu deaktivieren, ersetzen Sie `ENABLED` durch `DISABLED`.

Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

Sie können auch eine durch ein IDs Leerzeichen getrennte Liste von Konten übergeben.

Wenn der Code erfolgreich ausgeführt wurde, gibt er eine leere Liste von `UnprocessedAccounts` zurück. Wenn beim Ändern der Detektor-Einstellungen für ein Konto Probleme aufgetreten sind, wird diese Konto-ID zusammen mit einer Zusammenfassung des Problems aufgeführt.

Schutz von KI-Workloads mit GuardDuty

Amazon GuardDuty Foundational Threat Detection and Lambda Protection hilft Ihnen dabei, Bedrohungen für KI-Workloads, auf denen aufbaut, besser zu schützen und zu erkennen. AWS

Die grundlegende GuardDuty Bedrohungserkennung überwacht AWS CloudTrail Verwaltungsereignisse, um verdächtige und böswillige Aktivitäten in generativen KI-Workloads zu erkennen, die mithilfe von AWS Diensten wie Amazon Bedrock und Amazon erstellt wurden. SageMaker GuardDuty Kann beispielsweise Aktivitäten identifizieren wie:

- Ungewöhnliche Entfernung der Sicherheitsleitplanken von Amazon Bedrock
- Änderung der Datenquelle für Modelltraining, die möglicherweise zu Datenvergiftungsangriffen führen kann
- Verdächtiger Aufruf des Amazon Bedrock-Modells
- Ungewöhnlicher Notebookinstanz oder Schaffung eines Schulungsauftrags in SageMaker
- Exfiltrierte Amazon Elastic Compute Cloud-Anmeldeinformationen, die möglicherweise zum Aufrufen APIs von Amazon Bedrock-, Amazon- oder selbstverwalteten KI-Workloads auf EC2 Instances SageMaker, EKS Clustern oder Aufgaben verwendet wurden. ECS

GuardDuty Lambda Protection kann dabei helfen, potenzielle Bedrohungen im Zusammenhang mit Amazon Bedrock-Agenten zu erkennen. Dazu können verdächtige Netzwerkaktivitäten wie Cryptomining und die Kommunikation mit böswilligen Command-and-Control-Servern gehören, die durch Angriffe auf die Lieferkette oder komplexe Eingabeaufforderungen verursacht werden können.

Das folgende Video zeigt, wie die damit verbundenen Ergebnisse aussehen würden.

Das folgende Video zeigt, wie die zugehörigen Ergebnisse aussehen würden. Nutzung von Amazon GuardDuty zur Überwachung und Sicherung Ihrer KI-Workloads, die darauf aufbauen AWS

Verwaltung mehrerer Konten bei Amazon GuardDuty

Wenn Ihre AWS Umgebung über mehrere Konten verfügt, können Sie diese verwalten, indem Sie eines AWS-Konto als Administratorkonto festlegen. Anschließend können Sie mehrere AWS-Konten Konten diesem Administratorkonto als Mitgliedskonten zuordnen. Bei dieser Konfiguration kann ein zugewiesenes GuardDuty Administratorkonto die allgemeine Sicherheit Ihres Unternehmens beurteilen und überwachen. Mit dem Administratorkonto können auch Aufgaben zur Kontoverwaltung ausgeführt werden, z. B. die Überprüfung aller generierten Ergebnisse und die Konfiguration der Schutzpläne innerhalb des Kontos GuardDuty.

GuardDutyIn besteht eine Organisation aus einem delegierten GuardDuty Administratorkonto und einem oder mehreren zugehörigen Mitgliedskonten. Sie können die Konten auf zwei Arten verknüpfen: durch Integration oder durch Verwendung einer älteren Methode zum Senden und Annehmen von Mitgliedschaftseinladungen in der GuardDuty Konsole. AWS Organizations GuardDuty empfiehlt die Integration mit AWS Organizations.

AWS Organizations ist ein globaler Kontoverwaltungsdienst, der es AWS Administratoren ermöglicht, mehrere Konten zu konsolidieren und zentral zu verwalten AWS-Konten. Er bietet Funktionen zur Kontoverwaltung und konsolidierten Fakturierung, die auf die Erfüllung von Haushalts-, Sicherheits- und Compliance-Anforderungen zugeschnitten sind. Es wird ohne zusätzliche Kosten angeboten und lässt sich in mehrere integrieren AWS -Services, darunter Macie AWS Security Hub, und Amazon GuardDuty. Weitere Informationen finden Sie im AWS Organizations -Benutzerhandbuch.

Inhalt

Die Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten verstehen

Wenn Sie GuardDuty in einer Umgebung mit mehreren Konten arbeiten, kann das Administratorkonto bestimmte Aspekte von im Namen der GuardDuty Mitgliedskonten verwalten. Ein Administratorkonto kann die folgenden Hauptfunktionen erfüllen:

- Hinzufügen und Entfernen zugehöriger Mitgliedskonten. Das Verfahren, mit dem ein Administratorkonto dies tun kann, hängt davon ab, wie Sie die Konten verwalten — über Organisationen oder auf Einladung.
- Aktivierung des delegierten GuardDuty Administratorkontos GuardDuty im Verwaltungskonto

  Wenn das AWS Organizations Verwaltungskonto jemals deaktiviert wird GuardDuty, kann das delegierte GuardDuty Administratorkonto GuardDuty im Verwaltungskonto aktiviert werden. Es ist jedoch erforderlich, dass das Verwaltungskonto das nicht ausdrücklich gelöscht hat. Dienstbezogene Rollenberechtigungen für GuardDuty
- Verwaltet den Status der GuardDuty zugehörigen Mitgliedskonten, einschließlich Aktivierung und Sperrung GuardDuty.

  > **Note**
  >
  > Delegierte Administratorkonten, die GuardDuty in Konten, die als Mitglieder hinzugefügt werden, AWS Organizations automatisch aktiviert werden.

- Passen Sie die Ergebnisse innerhalb des GuardDuty Netzwerks an, indem Sie Unterdrückungsregeln, Listen vertrauenswürdiger IP-Adressen und Bedrohungslisten erstellen und verwalten. In einer Umgebung mit mehreren Konten ist die Konfiguration dieser Funktionen nur für ein GuardDuty delegiertes Administratorkonto verfügbar. Ein Mitgliedskonto kann diese Konfiguration nicht aktualisieren.

In der folgenden Tabelle wird die Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten detailliert beschrieben.

In dieser Tabelle:

- Selbst — Ein Konto kann die aufgelistete Aktion nur für sein eigenes Konto ausführen.
- Beliebig — Ein Konto kann die aufgelistete Aktion für jedes zugehörige Konto ausführen.
- Alle — Ein Konto kann die aufgelistete Aktion ausführen und sie gilt für alle zugehörigen Konten. In der Regel handelt es sich bei dem Konto, das diese Aktion ausführt, um ein GuardDuty designiertes Administratorkonto

Tabellenzellen mit einem Bindestrich (—) weisen darauf hin, dass das Konto die aufgelistete Aktion nicht ausführen kann.

Action (Aktion)	Durch AWS Organizations		Auf Einladung	
	Delegiertes GuardDuty Administratorkonto	Zugeordnetes Mitgliedskonto	Delegiertes GuardDuty Administratorkonto	Zugeordnetes Mitgliedskonto
Aktivieren GuardDuty	Any	–	Selbst	Selbst
GuardDuty Automatisch für die gesamte Organisation aktivieren (`ALL`,`NEW`,`NONE`)	Alle	–	–	–
Alle Mitgliedskonten von Organizations unabhängig vom GuardDuty Status anzeigen	Any	–	–	–
Generieren von Stichprobenergebnissen	Selbst	Selbst	Selbst	Selbst
Alle GuardDuty Ergebnisse anzeigen	Any	Selbst	Any	Selbst
GuardDuty Ergebnisse archivieren	Any	–	Any	–

Anwenden von Unterdrückungsregeln	Alle	–	Alle	–
Erstellen Sie eine Liste vertrauenswürdiger IP-Adressen oder Bedrohungslisten	Alle	–	Alle	–
Aktualisieren Sie die Liste vertrauenswürdiger IP-Adressen oder Bedrohungslisten	Alle	–	Alle	–
Löschen Sie die Liste vertrauenswürdiger IP-Adressen oder Bedrohungslisten	Alle	–	Alle	–
Stellen Sie die Häufigkeit der EventBridge Benachrichtigungen ein	Alle	–	Alle	Selbst
Festlegen des Amazon-S3-Standorts für den Export von Erkenntnissen	Alle	–	Alle	Selbst

Aktivieren Sie einen oder mehrere optionale Schutzpläne für die gesamte Organisation (`ALL`,`NEW`,`NONE`) Dies beinhaltet nicht den Malware-Schutz für S3.	Alle	–	–	–
Aktivieren Sie einen beliebigen GuardDuty Schutzplan für einzelne Konten Dies beinhaltet nicht den Malware-Schutz für EC2 und den Malware-Schutz für S3.	Any	–	Any	–
Malware-Schutz für EC2	Any	–	Selbst	Selbst
Malware-Schutz für S3	–	Selbst	–	Selbst
Trennen Sie die Zuordnung eines Mitgliedskontos	Any	–	Any	–

Trennen Sie die Verbindung zu einem Administratorkonto	–	Selbst +	–	Selbst
Löschen Sie ein getrenntes Mitgliedskonto	Any	–	Any	–
Sperren GuardDuty	Irgendein *	–	Irgendein *	–
Deaktivieren GuardDuty	Irgendein *	–	Irgendein *	–

+ Zeigt an, dass das Konto diese Aktion nur ausführen kann, wenn das delegierte GuardDuty Administratorkonto nicht die automatische Aktivierung für `ALL` die Organisationsmitglieder eingerichtet hat.

* Weist darauf hin, dass ein delegiertes GuardDuty Administratorkonto nicht direkt GuardDuty in einem Mitgliedskonto deaktiviert werden kann. Das delegierte GuardDuty Administratorkonto muss zuerst die Zuordnung zum Mitgliedskonto aufheben und dann löschen. Danach kann jedes Mitgliedskonto GuardDuty in seinen eigenen Konten deaktiviert werden. Weitere Informationen zur Durchführung dieser Aufgaben in Ihrer Organisation finden Sie unterAufrechterhaltung Ihrer Organisation innerhalb GuardDuty.

GuardDuty Konten verwalten mit AWS Organizations

In einer AWS Organisation kann das Verwaltungskonto jedes Konto innerhalb dieser Organisation als delegiertes Administratorkonto festlegen. GuardDuty GuardDuty Wird für dieses Administratorkonto nur im aktuellen Konto automatisch aktiviert. AWS-Region Standardmäßig kann das Administratorkonto GuardDuty für alle Mitgliedskonten in der Organisation in dieser Region aktiviert und verwaltet werden. Das Administratorkonto kann Mitglieder dieser AWS Organisation anzeigen und ihr hinzufügen.

In den folgenden Abschnitten werden Sie durch verschiedene Aufgaben geführt, die Sie als delegiertes GuardDuty Administratorkonto ausführen können.

Überlegungen und Empfehlungen zur Verwendung mit GuardDuty AWS Organizations

Die folgenden Überlegungen und Empfehlungen können Ihnen helfen zu verstehen, wie ein delegiertes GuardDuty Administratorkonto funktioniert in GuardDuty:

Ein delegiertes GuardDuty Administratorkonto kann maximal 50.000 Mitglieder verwalten.

Es gibt ein Limit von 50.000 Mitgliedskonten pro delegiertem GuardDuty Administratorkonto. Dies schließt Mitgliedskonten ein, die über die Einladung des Administratorkontos zum Beitritt zu ihrer Organisation hinzugefügt wurden, AWS Organizations oder solche, die die Einladung des GuardDuty Administratorkontos angenommen haben. In Ihrer AWS Organisation kann es jedoch mehr als 50.000 Konten geben.

Wenn Sie das Limit von 50.000 Mitgliedskonten überschreiten, erhalten Sie eine Benachrichtigung von CloudWatch AWS Health Dashboard, und eine E-Mail an das angegebene delegierte GuardDuty Administratorkonto.

Ein delegiertes GuardDuty Administratorkonto ist Regional.

Im Gegensatz AWS Organizations dazu GuardDuty handelt es sich um einen Regionaldienst. Die delegierten GuardDuty Administratorkonten und ihre Mitgliedskonten müssen AWS Organizations in jeder gewünschten Region, in der Sie sie GuardDuty aktiviert haben, hinzugefügt werden. Wenn das Organisationsverwaltungskonto ein delegiertes GuardDuty Administratorkonto nur für USA Ost (Nord-Virginia) festlegt, verwaltet das delegierte GuardDuty Administratorkonto nur Mitgliedskonten, die der Organisation in dieser Region hinzugefügt wurden. Weitere Informationen zur Funktionsparität in Regionen, in denen GuardDuty sie verfügbar ist, finden Sie unter. Regionen und Endpunkte

Sonderfälle für Opt-in-Regionen

- Wenn sich ein delegiertes GuardDuty Administratorkonto von einer Opt-in-Region abmeldet, GuardDuty kann es für kein Mitgliedskonto in der Organisation aktiviert werden, das derzeit deaktiviert ist, auch wenn in Ihrer Organisation die Konfiguration für die GuardDuty automatische Aktivierung entweder auf nur neue Mitgliedskonten (`NEWALL`) oder auf alle Mitgliedskonten () eingestellt ist. GuardDuty Informationen zur Konfiguration Ihrer Mitgliedskonten finden Sie im Navigationsbereich der GuardDuty Konsole unter Konten oder verwenden Sie den. ListMembersAPI
- Wenn Sie mit der Konfiguration für GuardDuty automatische Aktivierung arbeiten, stellen Sie sicher`NEW`, dass die folgende Reihenfolge eingehalten wird:

1. Die Mitgliedskonten melden sich für eine Opt-in-Region an.
2. Fügen Sie die Mitgliedskonten Ihrer Organisation in hinzu. AWS Organizations

Wenn Sie die Reihenfolge dieser Schritte ändern, funktioniert die Einstellung für die GuardDuty automatische Aktivierung mit `NEW` in der jeweiligen Opt-in-Region nicht mehr, da das Mitgliedskonto für die Organisation nicht mehr neu ist. GuardDuty bietet zwei alternative Lösungen:

- Stellen Sie die Konfiguration für die GuardDuty automatische Aktivierung auf ein`ALL`, die neue und bestehende Mitgliedskonten einschließt. In diesem Fall ist die Reihenfolge dieser Schritte nicht relevant.
- Wenn ein Mitgliedskonto bereits Teil Ihrer Organisation ist, verwalten Sie die GuardDuty Konfiguration für dieses Konto individuell in der jeweiligen Opt-in-Region mithilfe der GuardDuty Konsole oder derAPI.

Erforderlich, damit eine AWS Organisation für alle über dasselbe delegierte GuardDuty Administratorkonto verfügt. AWS-Regionen

Sie müssen ein Mitgliedskonto als delegiertes GuardDuty Administratorkonto für alle aktivierten AWS-Regionen Bereiche GuardDuty festlegen. Zum Beispiel, wenn Sie ein Mitgliedskonto angeben *`111122223333`* in *`Europe (Ireland)`*, Sie können kein anderes Mitgliedskonto angeben *`555555555555`* in *`Canada (Central)`*. Es ist erforderlich, dass Sie in allen anderen Regionen dasselbe Konto wie das delegierte GuardDuty Administratorkonto verwenden.

Sie können jederzeit ein neues delegiertes GuardDuty Administratorkonto einrichten. Weitere Informationen zum Entfernen des vorhandenen delegierten GuardDuty Administratorkontos finden Sie unter. Ändern des delegierten GuardDuty Administratorkontos

Es wird nicht empfohlen, das Verwaltungskonto Ihrer Organisation als delegiertes GuardDuty Administratorkonto festzulegen.

Das Verwaltungskonto Ihrer Organisation kann das delegierte GuardDuty Administratorkonto sein. Die bewährten AWS -Sicherheitsmethoden folgen jedoch dem Prinzip der geringsten Berechtigung und empfehlen diese Konfiguration nicht.

Durch das Ändern eines delegierten GuardDuty Administratorkontos werden Mitgliedskonten nicht deaktiviert GuardDuty .

Wenn Sie ein delegiertes GuardDuty Administratorkonto entfernen, werden alle Mitgliedskonten GuardDuty entfernt, die diesem delegierten GuardDuty Administratorkonto zugeordnet sind. GuardDuty bleibt weiterhin für all diese Mitgliedskonten aktiviert.

Für die Benennung eines delegierten GuardDuty Administratorkontos sind Berechtigungen erforderlich

Um GuardDuty mit der Nutzung von Amazon zu beginnen AWS Organizations, legt das AWS Organizations Verwaltungskonto der Organisation ein Konto als delegiertes GuardDuty Administratorkonto fest. Dies wird GuardDuty als vertrauenswürdiger Service in aktiviert. AWS Organizations Es aktiviert GuardDuty auch das delegierte GuardDuty Administratorkonto und ermöglicht es dem delegierten Administratorkonto, andere Konten in der Organisation in der aktuellen Region zu aktivieren und zu verwalten GuardDuty . Informationen darüber, wie diese Berechtigungen gewährt werden, finden Sie unter Zusammen AWS Organizations mit anderen AWS Diensten verwenden.

Bevor Sie das delegierte GuardDuty Administratorkonto für Ihre Organisation als AWS Organizations Verwaltungskonto festlegen, stellen Sie sicher, dass Sie die folgende GuardDuty Aktion ausführen können:. `guardduty:EnableOrganizationAdminAccount` Mit dieser Aktion können Sie das delegierte GuardDuty Administratorkonto für Ihre Organisation festlegen, indem Sie. GuardDuty Sie müssen außerdem sicherstellen, dass Sie die AWS Organizations Aktionen ausführen dürfen, mit denen Sie Informationen über Ihre Organisation abrufen können.

Um diese Berechtigungen zu gewähren, fügen Sie die folgende Aussage in eine AWS Identity and Access Management (IAM) -Richtlinie für Ihr Konto ein:

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

Wenn Sie Ihr AWS Organizations Verwaltungskonto als delegiertes GuardDuty Administratorkonto festlegen möchten, benötigt Ihr Konto auch die folgende IAM Aktion:. `CreateServiceLinkedRole` Mit dieser Aktion können Sie das Verwaltungskonto initialisieren GuardDuty . Überprüfen Sie dies jedoch, Überlegungen und Empfehlungen zur Verwendung mit GuardDuty AWS Organizations bevor Sie die Berechtigungen hinzufügen.

Um mit der Festlegung des Verwaltungskontos als delegiertes GuardDuty Administratorkonto fortzufahren, fügen Sie der IAM Richtlinie die folgende Erklärung hinzu und ersetzen Sie *111122223333* mit der AWS-Konto ID des Verwaltungskontos Ihrer Organisation:

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
 }
}
```

Benennen eines delegierten Administratorkontos GuardDuty

Wählen Sie eine bevorzugte Zugriffsmethode, um ein delegiertes GuardDuty Administratorkonto für Ihre Organisation festzulegen. Nur ein Verwaltungskonto kann diesen Schritt ausführen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Um sich anzumelden, verwenden Sie die Anmeldeinformationen für das Verwaltungskonto Ihrer AWS Organizations Organisation.

2. Wählen Sie mithilfe der AWS-Region Auswahltaste in der oberen rechten Ecke der Seite die Region aus, in der Sie das delegierte GuardDuty Administratorkonto für Ihre Organisation festlegen möchten.

3. Führen Sie je nachdem, ob es für Ihr Verwaltungskonto in der aktuellen Region aktiviert GuardDuty ist, einen der folgenden Schritte aus:

   - Wenn GuardDuty aktiviert, wählen Sie Amazon GuardDuty — all features und wählen Sie Get started. Diese Aktion führt Sie zur GuardDuty Seite Willkommen auf.
   - Wenn diese Option aktiviert GuardDuty ist, wählen Sie im Navigationsbereich Einstellungen aus.

4. Geben Sie unter Delegierter Administrator die 12-stellige AWS-Konto ID des Kontos ein, das Sie als delegiertes GuardDuty Administratorkonto für die Organisation festlegen möchten.

   Stellen Sie sicher, dass Sie GuardDuty die Aktivierung für Ihr neu benanntes delegiertes GuardDuty Administratorkonto vornehmen, da es sonst keine Aktion ausführen kann.

5. Wählen Sie Delegieren.

6. (Empfohlen) Wiederholen Sie die vorherigen Schritte, um das delegierte GuardDuty Administratorkonto für jedes Konto festzulegen, das Sie AWS-Region aktiviert haben. GuardDuty

API/CLI

1. Führen Sie die Ausführung enableOrganizationAdminAccountmit den Anmeldeinformationen AWS-Konto des Verwaltungskontos der Organisation aus.

   - Alternativ können Sie AWS Command Line Interface dies verwenden. Der folgende AWS CLI Befehl bestimmt ein delegiertes GuardDuty Administratorkonto nur für Ihre aktuelle Region. Führen Sie den folgenden AWS CLI Befehl aus und stellen Sie sicher, dass Sie ihn ersetzen *111111111111* mit der AWS-Konto ID des Kontos, das Sie als delegiertes GuardDuty Administratorkonto festlegen möchten:

     ```
     aws guardduty enable-organization-admin-account --admin-account-
     id 111111111111
     ```

     Um das delegierte GuardDuty Administratorkonto für andere Regionen festzulegen, geben Sie die Region im Befehl an. AWS CLI Das folgende Beispiel zeigt, wie ein delegiertes GuardDuty Administratorkonto in US West (Oregon) aktiviert wird. Stellen Sie sicher, dass Sie es ersetzen *us-west-2* mit der Region, für die Sie das delegierte GuardDuty Administratorkonto zuweisen möchten.

```
aws guardduty enable-organization-admin-account --admin-account-
id 111111111111 --region us-west-2
```

Informationen darüber, AWS-Regionen wo verfügbar GuardDuty ist, finden Sie unterRegionen und Endpunkte.

Wenn GuardDuty es für Ihr delegiertes GuardDuty Administratorkonto nicht aktiviert ist, kann es keine Aktion ausführen. Falls dies noch nicht geschehen ist, stellen Sie sicher, dass Sie die Aktivierung GuardDuty für das neu benannte delegierte GuardDuty Administratorkonto vorgenommen haben.

2. (Empfohlen) Wiederholen Sie die vorherigen Schritte, um das delegierte GuardDuty Administratorkonto AWS-Region in allen Bereichen festzulegen, die Sie aktiviert haben. GuardDuty

Aktualisierung der Einstellungen für die automatische Aktivierung der Organisation

GuardDuty Mit der Funktion zur automatischen Aktivierung von Organisationen in können Sie in einem einzigen Schritt den gleichen GuardDuty und den Status der Schutzpläne für `ALL` bestehende Konten oder `NEW` Mitgliedskonten in Ihrer Organisation festlegen. In ähnlicher Weise können Sie auch angeben, wann Sie keine Maßnahmen für die Mitgliedskonten ergreifen möchten, indem Sie wählen`NEW`. In den folgenden Schritten werden diese Einstellungen erklärt und es wird auch angegeben, wann Sie eine bestimmte Einstellung verwenden möchten.

Wählen Sie eine bevorzugte Zugriffsmethode, um die Einstellungen für die automatische Aktivierung für die Organisation zu aktualisieren.

Console

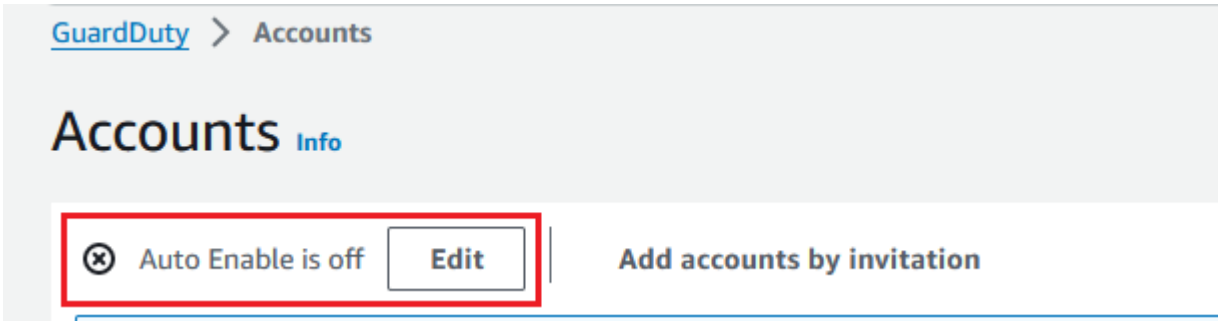
1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Verwenden Sie die Anmeldeinformationen des GuardDuty Administratorkontos, um sich anzumelden.

2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

Auf der Seite Konten finden Sie Konfigurationsoptionen für das GuardDuty Administratorkonto zur automatischen Aktivierung GuardDuty sowie optionale Schutzpläne für die Mitgliedskonten, die zur Organisation gehören.

3. Um die vorhandenen Einstellungen für die automatische Aktivierung zu aktualisieren, wählen Sie Bearbeiten.



Dieser Support kann konfiguriert werden, GuardDuty ebenso wie alle unterstützten optionalen Schutzpläne in Ihrem. AWS-Region Sie können im Namen Ihrer Mitgliedskonten eine der folgenden Konfigurationsoptionen auswählen: GuardDuty

- Für alle Konten aktivieren (**`ALL`**) — Wählen Sie diese Option, um die entsprechende Option für alle Konten in einer Organisation zu aktivieren. Dazu gehören neue Konten, die der Organisation beitreten, und Konten, die möglicherweise gesperrt oder aus der Organisation entfernt wurden. Dazu gehört auch das delegierte GuardDuty Administratorkonto.

  > **Note**
  >
  > Es kann bis zu 24 Stunden dauern, bis die Konfiguration für alle Mitgliedskonten aktualisiert ist.

- Automatische Aktivierung für neue Konten (**`NEW`**) — Wählen Sie aus, GuardDuty ob die optionalen Schutzpläne nur für neue Mitgliedskonten automatisch aktiviert werden sollen, wenn diese Ihrer Organisation beitreten.
- Nicht aktivieren (**`NONE`**) — Wählen Sie diese Option, um zu verhindern, dass die entsprechende Option für neue Konten in Ihrer Organisation aktiviert wird. In diesem Fall verwaltet das GuardDuty Administratorkonto jedes Konto einzeln.

  Wenn Sie die Einstellung für die automatische Aktivierung von `ALL` oder `NEW` auf aktualisieren`NONE`, deaktiviert diese Aktion nicht die entsprechende Option für Ihre vorhandenen Konten. Diese Konfiguration gilt für die neuen Konten, die der Organisation

beitreten. Nachdem Sie die Einstellungen für die automatische Aktivierung aktualisiert haben, wird die entsprechende Option für kein neues Konto aktiviert sein.

> **Note**
>
> Wenn sich ein delegiertes GuardDuty Administratorkonto von einer Opt-in-Region abmeldet, GuardDuty kann es für kein Mitgliedskonto in der Organisation aktiviert werden, das derzeit deaktiviert ist, auch wenn in Ihrer Organisation die Konfiguration für die GuardDuty automatische Aktivierung entweder auf nur neue Mitgliedskonten (`NEWALL`) oder auf alle Mitgliedskonten () eingestellt ist. GuardDuty Informationen zur Konfiguration Ihrer Mitgliedskonten finden Sie im Navigationsbereich der GuardDuty Konsole unter Konten oder verwenden Sie den. ListMembersAPI

4. Wählen Sie Änderungen speichern.
5. (Optional) Wenn Sie in jeder Region dieselben Einstellungen verwenden möchten, aktualisieren Sie Ihre Einstellungen in jeder der unterstützten Regionen separat.

   Einige der optionalen Schutzpläne sind möglicherweise nicht überall verfügbar, AWS-Regionen wo sie verfügbar GuardDuty sind. Weitere Informationen finden Sie unter Regionen und Endpunkte.

API/CLI

1. Verwenden Sie UpdateOrganizationConfigurationdie Anmeldeinformationen des delegierten GuardDuty Administratorkontos, um automatisch optionale Schutzpläne in dieser Region für Ihr Unternehmen zu konfigurieren GuardDuty . Informationen zu den verschiedenen Konfigurationen für die automatische Aktivierung finden Sie unter autoEnableOrganizationMitglieder.

   Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

   Um die Einstellungen für die automatische Aktivierung für einen der unterstützten optionalen Schutzpläne in Ihrer Region festzulegen, folgen Sie den Schritten in den entsprechenden Dokumentationsabschnitten der einzelnen Schutzpläne.

2. Sie können die Einstellungen für Ihre Organisation in der aktuellen Region überprüfen. Führen Sie describeOrganizationConfiguration. Stellen Sie sicher, dass Sie die Melder-ID des delegierten GuardDuty Administratorkontos angeben.

> **Note**
>
> Die Aktualisierung der Konfiguration aller Mitgliedskonten kann bis zu 24 Stunden dauern.

1. Führen Sie alternativ den folgenden AWS CLI Befehl aus, um die Einstellungen so festzulegen, dass GuardDuty in dieser Region automatisch neue Konten (`NEW`), die der Organisation beitreten, alle Konten (`ALL`) oder keines der Konten (`NONE`) in der Organisation aktiviert oder deaktiviert werden. Weitere Informationen finden Sie unter autoEnableOrganizationMitglieder. Je nach Ihren Einstellungen müssen Sie möglicherweise `NEW` durch `ALL` oder `NONE` ersetzen. Wenn Sie den Schutzplan mit konfigurierenALL, wird der Schutzplan auch für das delegierte GuardDuty Administratorkonto aktiviert. Stellen Sie sicher, dass Sie die Melder-ID des delegierten GuardDuty Administratorkontos angeben, das die Organisationskonfiguration verwaltet.

   Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, besuchen Sie die Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

2. Sie können die Einstellungen für Ihre Organisation in der aktuellen Region überprüfen. Führen Sie den folgenden AWS CLI Befehl aus, indem Sie die Detektor-ID des delegierten GuardDuty Administratorkontos verwenden.

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0
```

(Empfohlen) Wiederholen Sie die vorherigen Schritte in jeder Region, indem Sie die Detektor-ID für das delegierte GuardDuty Administratorkonto verwenden.

> **Note**
>
> Wenn sich ein delegiertes GuardDuty Administratorkonto von einer Opt-in-Region abmeldet, GuardDuty kann es für kein Mitgliedskonto in der Organisation aktiviert werden, das derzeit deaktiviert ist, auch wenn in Ihrer Organisation die Konfiguration für die GuardDuty automatische Aktivierung entweder auf nur neue Mitgliedskonten (`NEWALL`) oder auf alle Mitgliedskonten () eingestellt ist. GuardDuty Informationen zur Konfiguration Ihrer Mitgliedskonten finden Sie im Navigationsbereich der GuardDuty Konsole unter Konten oder verwenden Sie den. ListMembersAPI

Mitglieder zur Organisation hinzufügen

Wählen Sie eine bevorzugte Zugriffsmethode, um Mitglieder zu Ihrer Organisation hinzuzufügen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto, um sich anzumelden.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.

   In der Kontentabelle werden alle Konten angezeigt, die entweder Über Organisationen (AWS Organizations) oder Auf Einladung hinzugefügt wurden. Wenn ein Mitgliedskonto nicht mit dem GuardDuty Administratorkonto der Organisation verknüpft ist, lautet der Status dieses Mitgliedskontos Kein Mitglied.
3. Wählen Sie ein oder mehrere Konten ausIDs, die Sie als Mitglieder hinzufügen möchten. Diese Konten IDs müssen den Typ Via Organizations haben.

   Konten, die auf Einladung hinzugefügt werden, gehören nicht zu Ihrer Organisation. Sie können solche Konten einzeln verwalten. Weitere Informationen finden Sie unter Verwalten von Konten auf Einladung.
4. Wählen Sie das Drop-Down Aktionen und dann Mitglied hinzufügen aus. Nachdem Sie dieses Konto als Mitglied hinzugefügt haben, gilt die GuardDuty Konfiguration für die automatische Aktivierung. Je nach den Einstellungen in kann Aktualisierung der Einstellungen für die automatische Aktivierung der Organisation sich die GuardDuty Konfiguration dieser Konten ändern.

5. Sie können den Abwärtspfeil in der Spalte Status auswählen, um die Konten nach dem Status Kein Mitglied zu sortieren, und dann jedes Konto auswählen, das in der aktuellen Region nicht GuardDuty aktiviert wurde.

   Wenn noch keines der in der Kontentabelle aufgelisteten Konten als Mitglied hinzugefügt wurde, können Sie es GuardDuty in der aktuellen Region für alle Organisationskonten aktivieren. Wählen Sie im Banner oben auf der Seite Aktivieren aus. Durch diese Aktion wird automatisch die GuardDuty Konfiguration „Automatische Aktivierung“ aktiviert, sodass sie für jedes neue Konto aktiviert GuardDuty wird, das der Organisation beitritt.
6. Wählen Sie Bestätigen, um die Konten als Mitglieder hinzuzufügen. Diese Aktion ist auch GuardDuty für alle ausgewählten Konten aktiviert. Der Status für die eingeladenen Konten ändert sich in Aktiviert.
7. (Empfohlen) Wiederholen Sie diese Schritte in jedem Schritt AWS-Region. Dadurch wird sichergestellt, dass das delegierte GuardDuty Administratorkonto Ergebnisse und andere Konfigurationen für Mitgliedskonten in allen Regionen verwalten kann, in denen Sie die GuardDuty Aktivierung aktiviert haben.

   Die automatische Aktivierungsfunktion ist GuardDuty für alle future Mitglieder Ihrer Organisation aktiviert. Auf diese Weise kann Ihr delegiertes GuardDuty Administratorkonto alle neuen Mitglieder verwalten, die innerhalb der Organisation erstellt wurden oder der Organisation hinzugefügt werden. Wenn die Anzahl der Mitgliedskonten das Limit von 50.000 erreicht, wird die Funktion zur automatischen Aktivierung automatisch deaktiviert. Wenn Sie ein Mitgliedskonto entfernen und die Gesamtzahl der Mitglieder auf weniger als 50.000 sinkt, wird die Funktion zur automatischen Aktivierung wieder aktiviert.

API/CLI

- Verwenden Sie CreateMembersdie Anmeldeinformationen des delegierten GuardDuty Administratorkontos, das Sie im vorherigen Schritt angegeben haben.

  Sie müssen die regionale Detektor-ID des delegierten GuardDuty Administratorkontos und die Kontodetails (AWS-Konto IDsund die entsprechenden E-Mail-Adressen) der Konten angeben, die Sie als GuardDuty Mitglieder hinzufügen möchten. Mit diesem API Vorgang können Sie ein oder mehrere Mitglieder erstellen.

  Wenn Sie CreateMembers in Ihrer Organisation aktiv sind, gelten die Einstellungen für die automatische Aktivierung für neue Mitglieder, sobald neue Mitgliedskonten Ihrer Organisation

beitreten. Wenn Sie CreateMembers mit einem bestehenden Mitgliedskonto arbeiten, gilt die Organisationskonfiguration auch für die vorhandenen Mitglieder. Dies könnte die aktuelle Konfiguration der vorhandenen Mitgliedskonten ändern.

Führen Sie ListAccountsden Befehl „AWS Organizations APIReferenz“ aus, um alle Konten in der AWS Organisation anzuzeigen.

> **Important**
>
> Wenn Sie ein Konto als GuardDuty Mitglied hinzufügen, wird es automatisch in dieser Region GuardDuty aktiviert. Es gibt eine Ausnahme für das Organisationsverwaltungskonto. Bevor das Verwaltungskonto als GuardDuty Mitglied hinzugefügt werden kann, muss es GuardDuty aktiviert worden sein.

- Alternativ können Sie verwenden AWS Command Line Interface. Führen Sie den folgenden AWS CLI -Befehl aus und stellen Sie sicher, dass Sie Ihre eigene gültige Detektor-ID und die mit der AWS-Konto -ID verknüpfte E-Mail-Adresse verwenden.

  Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite Einstellungen oder führen Sie den aus ListDetectorsAPI.

  ```
  aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
   --account-details AccountId=111122223333,Email=guardduty-member-
  name@amazon.com
  ```

  Sie können eine Liste aller Organisationsmitglieder anzeigen, indem Sie den folgenden AWS CLI Befehl ausführen:

  ```
  aws organizations list-accounts
  ```

Nachdem Sie dieses Konto als Mitglied hinzugefügt haben, gilt die GuardDuty Konfiguration für die automatische Aktivierung.

(Optional) Aktivieren Sie Schutzpläne für bestehende Mitgliedskonten

Das folgende Verfahren umfasst Schritte zum Aktivieren von Schutzplänen für bestehende Mitgliedskonten mithilfe der Kontoseite. Anweisungen, wie Sie dies mithilfe von API oder tun können AWS CLI, finden Sie in den Dokumenten zu dem jeweiligen Schutzplan.

Auf der Seite Konten können Sie Schutzpläne für einzelne Konten aktivieren.

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen für das delegierte GuardDuty Administratorkonto.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie das Konto aus, für das Sie einen Schutzplan konfigurieren möchten. Wiederholen Sie die folgenden Schritte für jeden Schutzplan, den Sie konfigurieren möchten:

   a. Wählen Sie Schutzpläne bearbeiten aus.
   b. Wählen Sie aus der Liste der Schutzpläne einen Schutzplan aus, den Sie konfigurieren möchten.
   c. Wählen Sie eine der Aktionen aus, die Sie für diesen Schutzplan ausführen möchten, und klicken Sie dann auf Bestätigen.
   d. Für das ausgewählte Konto wird in der Spalte, die dem konfigurierten Schutzplan entspricht, die aktualisierte Konfiguration als Aktiviert oder Nicht aktiviert angezeigt.

Aufrechterhaltung Ihrer Organisation innerhalb GuardDuty

Als delegiertes GuardDuty Administratorkonto sind Sie dafür verantwortlich, die Konfiguration GuardDuty und die optionalen Schutzpläne für alle Konten in Ihrer Organisation in allen unterstützten Konten aufrechtzuerhalten. AWS-Region In den folgenden Abschnitten finden Sie die Optionen zur Beibehaltung des Konfigurationsstatus der optionalen Schutzpläne GuardDuty oder der zugehörigen optionalen Schutzpläne:

Um den Konfigurationsstatus Ihrer gesamten Organisation in jeder Region aufrechtzuerhalten

- Legen Sie mithilfe der GuardDuty Konsole Einstellungen für die automatische Aktivierung für die gesamte Organisation fest — Sie können die GuardDuty automatische Aktivierung entweder für alle (`ALL`) Mitglieder der Organisation oder für neue (`NEW`) Mitglieder, die der Organisation beitreten, aktivieren oder festlegen, dass (`NONE`) keines der Mitglieder der Organisation automatisch aktiviert wird.

Sie können auch dieselben oder unterschiedliche Einstellungen für alle darin enthaltenen Schutzpläne konfigurieren. GuardDuty

Es kann bis zu 24 Stunden dauern, bis die Konfiguration für alle Mitgliedskonten in der Organisation aktualisiert ist.

- Aktualisieren Sie die Einstellungen für die automatische Aktivierung mithilfe von API — Ausführen UpdateOrganizationConfiguration, um die automatische Konfiguration GuardDuty und die zugehörigen optionalen Schutzpläne für das Unternehmen zu aktivieren. Wenn Sie ausführen CreateMembers, um neue Mitgliedskonten in Ihrer Organisation hinzuzufügen, werden die konfigurierten Einstellungen automatisch angewendet. Wenn Sie CreateMembers mit einem vorhandenen Mitgliedskonto arbeiten, gilt die Organisationskonfiguration auch für die vorhandenen Mitglieder. Dies könnte die aktuelle Konfiguration der vorhandenen Mitgliedskonten ändern.

  Um alle Konten in Ihrer Organisation anzuzeigen, führen Sie ListAccountsden Befehl AWS Organizations APIReferenz aus.

Um den Konfigurationsstatus für Mitgliedskonten in jeder Region einzeln zu verwalten

- Um alle Konten in Ihrer Organisation anzuzeigen, führen Sie ListAccountsden Befehl AWS Organizations APIReferenz aus.
- Wenn Sie möchten, dass bestimmte Mitgliedskonten einen anderen Konfigurationsstatus haben, führen Sie den Vorgang UpdateMemberDetectorsfür jedes Mitgliedskonto einzeln aus.

  Sie können dieselbe Aufgabe mit der GuardDuty Konsole ausführen, indem Sie in der GuardDuty Konsole zur Seite Konten navigieren.

  Informationen zur Aktivierung von Schutzplänen für einzelne Konten mithilfe der Konsole oder API finden Sie auf der Konfigurationsseite für den entsprechenden Schutzplan.

Ändern des delegierten GuardDuty Administratorkontos

Sie können das delegierte GuardDuty Administratorkonto für Ihre Organisation in jeder Region ändern und dann in jeder Region einen neuen Administrator delegieren. Um die Sicherheit der Mitgliedskonten Ihrer Organisation in einer Region aufrechtzuerhalten, benötigen Sie in dieser Region ein delegiertes GuardDuty Administratorkonto.

Bestehendes delegiertes GuardDuty Administratorkonto wird entfernt

Schritt 1 — Um ein vorhandenes delegiertes GuardDuty Administratorkonto in jeder Region zu entfernen

1. Führen Sie als vorhandenes delegiertes GuardDuty Administratorkonto alle Mitgliedskonten auf, die Ihrem Administratorkonto zugeordnet sind. Führen Sie ListMembersmit`OnlyAssociated=false`.
2. Wenn die Einstellung Automatische Aktivierung für GuardDuty oder einen der optionalen Schutzpläne auf gesetzt ist, führen Sie den Befehl aus`ALL`, UpdateOrganizationConfigurationum die Organisationskonfiguration entweder auf `NEW` oder `NONE` zu aktualisieren. Diese Aktion verhindert, dass ein Fehler auftritt, wenn Sie im nächsten Schritt die Verknüpfung aller Mitgliedskonten aufheben.
3. Führen Sie aus DisassociateMembers, um die Zuordnung aller Mitgliedskonten aufzuheben, die dem Administratorkonto zugeordnet sind.
4. Ausführen DeleteMembers, um die Verknüpfungen zwischen dem Administratorkonto und den Mitgliedskonten zu löschen.
5. Führen Sie als Organisationsverwaltungskonto aus, DisableOrganizationAdminAccountum das vorhandene delegierte GuardDuty Administratorkonto zu entfernen.
6. Wiederholen Sie diese Schritte in allen Bereichen, in AWS-Region denen Sie über dieses delegierte GuardDuty Administratorkonto verfügen.

Schritt 2 — So heben Sie die Registrierung eines bestehenden delegierten GuardDuty Administratorkontos in AWS Organizations (Einmalige globale Aktion) auf

- Führen Sie DeregisterDelegatedAdministratorden Befehl AWS Organizations APIReferenz aus, um das bestehende delegierte GuardDuty Administratorkonto in abzumelden. AWS Organizations

  Alternativ können Sie den folgenden AWS CLI Befehl ausführen:

  ```
  aws organizations deregister-delegated-administrator --account-id 111122223333 --
  service-principal guardduty.amazonaws.com
  ```

  Stellen Sie sicher, dass Sie es ersetzen *111122223333* mit dem vorhandenen delegierten GuardDuty Administratorkonto.

Nachdem Sie das alte delegierte GuardDuty Administratorkonto abgemeldet haben, können Sie es dem neuen delegierten GuardDuty Administratorkonto als Mitgliedskonto hinzufügen.

Benennen eines neuen delegierten GuardDuty Administratorkontos in jeder Region

1. Weisen Sie in jeder Region ein neues delegiertes GuardDuty Administratorkonto zu, indem Sie Ihre bevorzugte Zugriffsmethode verwenden: GuardDuty Konsole oder oder. API AWS CLI Weitere Informationen finden Sie unter Benennen eines delegierten Administratorkontos GuardDuty .
2. Führen Sie den DescribeOrganizationConfigurationBefehl aus, um die aktuelle Konfiguration für die automatische Aktivierung für Ihre Organisation anzuzeigen.

> **Important**
>
> Bevor Sie dem neuen delegierten GuardDuty Administratorkonto Mitglieder hinzufügen, müssen Sie die Konfiguration für die automatische Aktivierung für Ihre Organisation überprüfen. Diese Konfiguration ist spezifisch für das neue delegierte GuardDuty Administratorkonto und die ausgewählte Region und bezieht sich nicht auf. AWS Organizations Wenn Sie (ein neues oder ein vorhandenes) Mitgliedskonto einer Organisation unter dem neuen delegierten GuardDuty Administratorkonto hinzufügen, gilt die automatische Aktivierungskonfiguration des neuen delegierten GuardDuty Administratorkontos zum Zeitpunkt der Aktivierung GuardDuty oder eines seiner optionalen Schutzpläne.

Ändern Sie die Organisationskonfiguration für das neue delegierte GuardDuty Administratorkonto, indem Sie Ihre bevorzugte Zugriffsmethode verwenden: GuardDuty Konsole oder oder. API AWS CLI Weitere Informationen finden Sie unter Aktualisierung der Einstellungen für die automatische Aktivierung der Organisation.

GuardDuty Konten auf Einladung verwalten

Um Konten außerhalb Ihrer Organisation zu verwalten, können Sie die Legacy-Einladungsmethode verwenden. Wenn Sie diese Methode verwenden, wird Ihr Konto als Administratorkonto designiert, wenn ein anderes Konto Ihre Einladung annimmt, ein Mitgliedskonto zu werden.

Wenn es sich bei Ihrem Konto nicht um ein Administratorkonto handelt, können Sie eine Einladung von einem anderen Konto annehmen. In diesem Fall wird Ihr Konto ein Mitgliedskonto. Ein AWS Konto kann nicht gleichzeitig GuardDuty Administratorkonto und Mitgliedskonto sein.

Wenn Sie eine Einladung von einem Konto annehmen, können Sie keine Einladung von einem anderen Konto annehmen. Um eine Einladung von einem anderen Konto anzunehmen, müssen Sie zunächst die Verbindung zwischen Ihrem Konto und dem vorhandenen Administratorkonto trennen. Alternativ kann das Administratorkonto auch die Zuordnung Ihres Kontos zu seiner Organisation aufheben und es daraus entfernen.

Konten, die per Einladung verknüpft sind, haben dieselbe allgemeine account-to-member Administratorbeziehung wie Konten, die von verknüpft sind AWS Organizations, wie unter beschriebenDie Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten verstehen. Benutzer mit Administratorkonten für Einladungen können jedoch nicht GuardDuty im Namen der zugehörigen Mitgliedskonten aktivieren oder andere Konten innerhalb ihrer AWS Organizations Organisation einsehen, die keine Mitglieder sind.

> **Important**
>
> Bei der Erstellung von Mitgliedskonten mit dieser Methode kann es GuardDuty zu einer überregionalen Datenübertragung kommen. GuardDuty verwendet zur Überprüfung der E-Mail-Adressen von Mitgliedskonten einen E-Mail-Bestätigungsdienst, der nur in der Region USA Ost (Nord-Virginia) verfügbar ist.

Hinzufügen und verwalten von Konten auf Einladung

Wählen Sie eine der Zugriffsmethoden, um Konten hinzuzufügen und einzuladen, GuardDuty Mitgliedskonten als GuardDuty Administratorkonto zu werden.

Console

Schritt 1: Konto hinzufügen

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie im oberen Bereich Konten auf Einladung hinzufügen aus.

4. Geben Sie auf der Seite Mitgliedskonten hinzufügen unter Kontodetails eingeben die AWS-Konto ID und E-Mail-Adresse ein, die mit dem Konto verknüpft sind, das Sie hinzufügen möchten.
5. Um eine weitere Zeile hinzuzufügen, in der die Kontodetails nacheinander eingegeben werden können, wählen Sie Weiteres Konto hinzufügen. Sie können auch CSV-Datei mit Kontodetails hochladen wählen, um mehrere Konten gleichzeitig hinzuzufügen.

   > **Important**
   >
   > Die erste Zeile Ihrer CSV-Datei muss wie im folgenden Beispiel den folgenden Header enthalten – `Account ID,Email`. Jede nachfolgende Zeile muss eine einzige gültige AWS-Konto ID und die zugehörige E-Mail-Adresse enthalten. Das Format einer Zeile ist gültig, wenn sie nur eine AWS-Konto ID und die zugehörige E-Mail-Adresse enthält, die durch ein Komma getrennt sind.
   >
   > ```
   > Account ID,Email
   > 555555555555,user@example.com
   > ```

6. Nachdem Sie alle Kontodetails hinzugefügt haben, wählen Sie Weiter. Sie können die neu hinzugefügten Konten in der Tabelle Konten einsehen. Der Status dieser Konten lautet Einladung nicht gesendet. Informationen zum Senden einer Einladung an ein oder mehrere hinzugefügte Konten finden Sie unter Step 2 - Invite an account.

Schritt 2: Ein Konto einladen

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
2. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
3. Wählen Sie ein oder mehrere Konten aus, die Sie zu Amazon einladen möchten GuardDuty.
4. Wählen Sie im Drop-down-Menü Aktionen und dann Einladen aus.
5. Geben Sie im GuardDuty Dialogfeld „Einladung zu“ eine (optionale) Einladungsnachricht ein.

   Wenn das eingeladene Konto nicht über E-Mail-Zugang verfügt, aktivieren Sie das Kontrollkästchen Auch eine E-Mail-Benachrichtigung an den Root-Benutzer auf dem AWS-Konto des Eingeladenen senden und eine Warnmeldung im AWS Health Dashboard des Eingeladenen erzeugen.

6. Wählen Sie Send invitation (Einladung senden) aus. Wenn die eingeladenen Personen Zugriff auf die angegebene E-Mail-Adresse haben, können sie sich die Einladung ansehen, indem sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/öffnen.
7. Wenn ein Eingeladener die Einladung annimmt, ändert sich der Wert in der Spalte Status in Eingeladen. Weitere Informationen zur Annahme einer Einladung finden Sie unter Step 3 - Accept an invitation.

Schritt 3: Eine Einladung annehmen

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   > **Important**
   >
   > Sie müssen sie aktivieren, GuardDuty bevor Sie eine Mitgliedschaftseinladung anzeigen oder annehmen können.

2. Gehen Sie nur dann wie folgt vor, wenn Sie es GuardDuty noch nicht aktiviert haben. Andernfalls können Sie diesen Schritt überspringen und mit dem nächsten Schritt fortfahren.

   Wenn Sie es noch nicht aktiviert haben GuardDuty, wählen Sie auf der GuardDuty Amazon-Seite Erste Schritte aus.

   Wählen Sie auf der GuardDuty Seite Willkommen bei die Option Aktivieren aus GuardDuty.
3. Gehen Sie nach der Aktivierung GuardDuty für Ihr Konto wie folgt vor, um die Einladung zur Mitgliedschaft anzunehmen:

   a. Wählen Sie im Navigationsbereich Settings (Einstellungen).
   b. Wählen Sie -Accounts (Konten).
   c. Stellen Sie sicher, dass Sie bei den Konten den Inhaber des Kontos verifizieren, von dem Sie die Einladung annehmen. Aktivieren Sie Annehmen, um die Einladung zur Mitgliedschaft anzunehmen.
4. Nachdem Sie die Einladung angenommen haben, wird Ihr Konto zu einem GuardDuty Mitgliedskonto. Das Konto, dessen Besitzer die Einladung gesendet hat, wird zum GuardDuty Administratorkonto. Das Administratorkonto wird wissen, dass Sie die Einladung angenommen haben. Die Kontentabelle in ihrem GuardDuty Konto wird aktualisiert. Der Wert in der Spalte Status, der Ihrer Mitgliedskonto-ID entspricht, wird auf Aktiviert geändert. Der Inhaber des Administratorkontos kann jetzt die Konfigurationen GuardDuty und

Schutzpläne für Ihr Konto einsehen und verwalten. Das Administratorkonto kann auch die für Ihr Mitgliedskonto generierten GuardDuty Ergebnisse einsehen und verwalten.

API/CLI

Sie können im Rahmen der API Vorgänge ein GuardDuty Administratorkonto festlegen und auf Einladung GuardDuty Mitgliedskonten erstellen oder hinzufügen. Führen Sie die folgenden GuardDuty API Vorgänge aus, um Administratorkonten und Mitgliedskonten in festzulegen. GuardDuty

Führen Sie das folgende Verfahren mit den Anmeldeinformationen des Kontos aus AWS-Konto , das Sie als GuardDuty Administratorkonto festlegen möchten.

Mitgliedskonten erstellen oder hinzufügen

1. Führen Sie den CreateMembersAPIVorgang mit den Anmeldeinformationen des AWS Kontos aus, das GuardDuty aktiviert wurde. Dies ist das Konto, das Sie als GuardDuty Administratorkonto verwenden möchten.

   Sie müssen die Melder-ID des AWS Girokontos sowie die Konto-ID und E-Mail-Adresse der Konten angeben, denen Sie GuardDuty beitreten möchten. Mit diesem API Vorgang können Sie ein oder mehrere Mitglieder erstellen.

   Sie können auch die AWS Befehlszeilentools verwenden, um ein Administratorkonto festzulegen, indem Sie den folgenden CLI Befehl ausführen. Stellen Sie sicher, dass Sie Ihre eigene gültige Detektor-ID, Konto-ID und E-Mail verwenden.

   Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite Einstellungen oder führen Sie den ListDetectorsAPIaus.

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. Verwenden Sie für die Ausführung InviteMembersdie Anmeldeinformationen des AWS Kontos, das GuardDuty aktiviert wurde. Dies ist das Konto, das Sie als GuardDuty Administratorkonto verwenden möchten.

Sie müssen die Melder-ID des AWS Girokontos und das Konto IDs der Konten angeben, denen Sie GuardDuty beitreten möchten. Mit diesem API Vorgang können Sie ein oder mehrere Mitglieder einladen.

> **Note**
>
> Sie können mit dem `message`-Anfrageparameter auch eine optionale Einladungsbenachrichtigung erstellen.

Sie können es auch verwenden AWS Command Line Interface , um Mitgliedskonten festzulegen, indem Sie den folgenden Befehl ausführen. Stellen Sie sicher, dass Sie Ihre eigene gültige Melder-ID und ein gültiges Konto IDs für die Konten verwenden, die Sie einladen möchten.

Um das `detectorId` für dein Konto und deine aktuelle Region zu finden, besuche die Einstellungsseite in der https://console.aws.amazon.com/guardduty/Konsole oder führe den aus ListDetectorsAPI.

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

Einladungen annehmen

Führen Sie das folgende Verfahren mit den Anmeldeinformationen jedes AWS Kontos aus, das Sie als GuardDuty Mitgliedskonto festlegen möchten.

1. Führen Sie den CreateDetectorAPIVorgang für jedes AWS Konto aus, das als GuardDuty Mitgliedskonto eingeladen wurde und das Sie annehmen möchten.

   Sie müssen angeben, ob die Detektorressource mithilfe des GuardDuty Dienstes aktiviert werden soll. Ein Detektor muss erstellt und aktiviert werden, damit er GuardDuty betriebsbereit ist. Sie müssen die Aktivierung zuerst aktivieren, GuardDuty bevor Sie eine Einladung annehmen können.

   Sie können dies auch mithilfe der AWS Befehlszeilentools mit dem folgenden CLI Befehl tun.

```
aws guardduty create-detector --enable
```

2. Führen Sie den AcceptAdministratorInvitationAPIVorgang für jedes AWS Konto aus, für das Sie die Einladung zur Mitgliedschaft annehmen möchten, und verwenden Sie dabei die Anmeldeinformationen dieses Kontos.

   Sie müssen die Melder-ID dieses AWS Kontos für das Mitgliedskonto, die Konto-ID des Administratorkontos, das die Einladung gesendet hat, und die Einladungs-ID der Einladung, die Sie annehmen, angeben. Sie finden die Konto-ID des Administratorkontos in der Einladungs-E-Mail oder mithilfe der ListInvitationsBedienung vonAPI.

   Sie können eine Einladung auch mithilfe der AWS Befehlszeilentools annehmen, indem Sie den folgenden CLI Befehl ausführen. Stellen Sie sicher, dass Sie eine gültige Detektor-ID, Administratorkonto-ID und Einladungs-ID verwenden.

   Den `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

   ```
   aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --administrator-id 444455556666 --invitation-
   id 84b097800250d17d1872b34c4daadcf5
   ```

Konsolidierung von GuardDuty Administratorkonten unter einem einzigen delegierten GuardDuty Administratorkonto der Organisation

GuardDuty empfiehlt die Verwendung von Assoziation bis AWS Organizations zur Verwaltung von Mitgliedskonten unter einem delegierten GuardDuty Administratorkonto. Sie können das unten beschriebene Beispielverfahren verwenden, um das Administratorkonto und das per Einladung zugeordnete Mitglied in einer Organisation unter einem einzigen GuardDuty delegierten GuardDuty Administratorkonto zu konsolidieren.

> **Note**
>
> Konten, die bereits von einem delegierten GuardDuty Administratorkonto verwaltet werden, oder aktive Mitgliedskonten, die einem delegierten GuardDuty Administratorkonto zugeordnet sind, können keinem anderen delegierten GuardDuty Administratorkonto hinzugefügt

werden. Jede Organisation kann nur über ein delegiertes GuardDuty Administratorkonto pro Region verfügen, und jedes Mitgliedskonto kann nur über ein delegiertes Administratorkonto verfügen. GuardDuty

Wählen Sie eine der Zugriffsmethoden, um GuardDuty Administratorkonten unter einem einzigen delegierten GuardDuty Administratorkonto zu konsolidieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/

   Verwenden Sie die Anmeldeinformationen des Verwaltungskontos der Organisation, um sich anzumelden.
2. Alle Konten, die Sie verwalten möchten, GuardDuty müssen Teil Ihrer Organisation sein. Informationen zum Hinzufügen eines Kontos zu Ihrer Organisation finden Sie unter Einen AWS-Konto einladen, Ihrer Organisation beizutreten.
3. Stellen Sie sicher, dass alle Mitgliedskonten dem Konto zugeordnet sind, das Sie als einziges delegiertes GuardDuty Administratorkonto festlegen möchten. Trennen Sie alle Mitgliedskonten, die noch mit den bereits vorhandenen Administratorkonten verknüpft sind.

   Die folgenden Schritte helfen Ihnen dabei, Mitgliedskonten vom bereits vorhandenen Administratorkonto zu trennen:

   a. Öffnen Sie die GuardDuty Konsole unter. https://console.aws.amazon.com/guardduty/
   b. Um sich anzumelden, verwenden Sie die Anmeldeinformationen des bereits vorhandenen Administratorkontos.
   c. Wählen Sie im Navigationsbereich Accounts (Konten) aus.
   d. Wählen Sie auf der Seite Konten ein oder mehrere Konten aus, die Sie vom Administratorkonto trennen möchten.
   e. Wählen Sie Aktionen und dann Konto trennen.
   f. Wählen Sie Bestätigen, um den Schritt abzuschließen.
4. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

   Verwenden Sie die Anmeldeinformationen des Verwaltungskontos, um sich anzumelden.
5. Wählen Sie im Navigationsbereich Settings (Einstellungen). Geben Sie auf der Seite Einstellungen das delegierte GuardDuty Administratorkonto für die Organisation an.

6. Melden Sie sich mit dem angegebenen delegierten Administratorkonto an. GuardDuty
7. Fügen Sie Mitglieder der Organisation hinzu. Weitere Informationen finden Sie unter GuardDuty Konten verwalten mit AWS Organizations.

API/CLI

1. Alle Konten, die Sie verwalten möchten, GuardDuty müssen Teil Ihrer Organisation sein. Informationen zum Hinzufügen eines Kontos zu Ihrer Organisation finden Sie unter Einen AWS-Konto einladen, Ihrer Organisation beizutreten.
2. Stellen Sie sicher, dass alle Mitgliedskonten dem Konto zugeordnet sind, das Sie als einziges delegiertes GuardDuty Administratorkonto festlegen möchten.

   a. Führen Sie DisassociateMembersden Befehl aus, um die Zuordnung aller Mitgliedskonten aufzuheben, die noch mit den bereits vorhandenen Administratorkonten verknüpft sind.

   b. Alternativ können Sie verwenden, AWS Command Line Interface um den folgenden Befehl auszuführen und zu ersetzen *777777777777* mit der Melder-ID des bereits vorhandenen Administratorkontos, von dem Sie die Verknüpfung mit dem Mitgliedskonto trennen möchten. Ersetzen *666666666666* mit der AWS-Konto ID des Mitgliedskontos, das Sie trennen möchten.

   ```
   aws guardduty disassociate-members --detector-id 777777777777 --account-
   ids 666666666666
   ```

3. Führen Sie EnableOrganizationAdminAccountden Befehl aus, um ein AWS-Konto als delegiertes Administratorkonto zu delegieren. GuardDuty

   Alternativ können Sie den folgenden Befehl ausführen AWS Command Line Interface , um ein delegiertes Administratorkonto zu delegieren: GuardDuty

   ```
   aws guardduty enable-organization-admin-account --admin-account-id 777777777777
   ```

4. Fügen Sie Mitglieder der Organisation hinzu. Weitere Informationen finden Sie unter Create or add member member accounts using API.

> **Important**
>
> Um die Effektivität eines GuardDuty regionalen Dienstes zu maximieren, empfehlen wir Ihnen, Ihr delegiertes GuardDuty Administratorkonto festzulegen und alle Mitgliedskonten in jeder Region hinzuzufügen.

GuardDuty In mehreren Konten gleichzeitig aktivieren

Verwenden Sie die folgende Methode, um die Aktivierung GuardDuty in mehreren Konten gleichzeitig durchzuführen.

Verwenden Sie Python-Skripte, um sie GuardDuty in mehreren Konten gleichzeitig zu aktivieren

Sie können die Aktivierung oder Deaktivierung von GuardDuty für mehrere Konten automatisieren, indem Sie die Skripts aus dem Beispiel-Repository bei Amazon GuardDuty Multiaccount Scripts verwenden. Gehen Sie wie in diesem Abschnitt beschrieben vor, GuardDuty um eine Liste von Mitgliedskonten bei Amazon zu aktivierenEC2. Informationen zur Verwendung des Deaktivierungsskripts oder zur lokalen Einrichtung des Skripts finden Sie in den Anweisungen im geteilten Link.

Das `enableguardduty.py` Skript aktiviert GuardDuty, sendet Einladungen vom Administratorkonto aus und akzeptiert Einladungen in allen Mitgliedskonten. Das Ergebnis ist ein GuardDuty Administratorkonto, das alle Sicherheitsergebnisse für alle Mitgliedskonten enthält. Da GuardDuty es nach Regionen isoliert ist, werden die Ergebnisse für jedes Mitgliedskonto auf die entsprechende Region im Administratorkonto übertragen. Beispielsweise enthält die Region us-east-1 in Ihrem GuardDuty Administratorkonto die Sicherheitsergebnisse für alle us-east-1-Ergebnisse aller zugehörigen Mitgliedskonten.

Diese Skripts hängen von einer gemeinsamen IAM Rolle mit der verwalteten Richtlinie ab —AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess. Diese Richtlinie gewährt Entitäten Zugriff auf das Administratorkonto GuardDuty und muss in jedem Konto, für das Sie die Aktivierung aktivieren möchten, vorhanden sein GuardDuty.

Der folgende Prozess ist standardmäßig GuardDuty in allen verfügbaren Regionen aktiviert. Sie können die Aktivierung nur GuardDuty in bestimmten Regionen durchführen, indem Sie das optionale `--enabled_regions` Argument verwenden und eine durch Kommas getrennte Liste von Regionen

angeben. Sie können die Einladungsnachricht, die an Mitgliedskonten gesendet wird, optional auch anpassen, indem Sie `enableguardduty.py` öffnen und die Zeichenfolge `gd_invite_message` bearbeiten.

1. Erstellen Sie eine IAM Rolle im GuardDuty Administratorkonto und fügen Sie die zu aktivierende AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess Richtlinie an. GuardDuty
2. Erstellen Sie für jedes Mitgliedskonto, das Sie von Ihrem GuardDuty Administratorkonto verwalten möchten, eine IAM Rolle. Diese Rolle muss denselben Namen haben wie die in Schritt 1 erstellte Rolle, sie sollte das Administratorkonto als vertrauenswürdige Entität zulassen und sie sollte dieselbe AmazonGuardDutyFullAccess verwaltete Richtlinie haben, die zuvor beschrieben wurde.
3. Starten Sie eine neue Amazon Linux-Instance mit einer zugeordneten Rolle mit der folgenden Vertrauensstellung, die es der Instance ermöglicht, eine Servicerolle anzunehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Melden Sie sich bei der neuen Instance an und führen Sie die folgenden Befehle aus, um sie einzurichten.

```
sudo yum install git python
sudo yum install python-pip
pip install boto3
aws configure
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git
cd amazon-guardduty-multiaccount-scripts
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. Erstellen Sie eine CSV Datei mit einer Liste von Konten IDs und E-Mails der Mitgliedskonten, denen Sie in Schritt 2 eine Rolle hinzugefügt haben. Konten müssen eines pro Zeile angezeigt

werden, und die Konto-ID und die E-Mail-Adresse müssen wie im folgenden Beispiel durch ein Komma voneinander getrennt sein.

```
111122223333,guardduty-member@organization.com
```

> **Note**
>
> Die CSV Datei muss sich am selben Speicherort wie Ihr `enableguardduty.py` Skript befinden. Sie können eine vorhandene CSV Datei mit der folgenden Methode von Amazon S3 in Ihr aktuelles Verzeichnis kopieren.
>
> ```
> aws s3 cp s3://my-bucket/my_key_name example.csv
> ```

6. Führen Sie das Python-Skript aus. Stellen Sie sicher, dass Sie Ihre GuardDuty Administratorkonto-ID, den Namen der in den ersten Schritten erstellten Rolle und den Namen Ihrer CSV Datei als Argumente angeben.

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

Die GuardDuty Ergebnisse von Amazon verstehen

Ein GuardDuty Ergebnis steht für ein potenzielles Sicherheitsproblem, das in Ihrem Netzwerk erkannt wurde. GuardDutygeneriert immer dann einen Befund, wenn unerwartete und potenziell bösartige Aktivitäten in Ihrer AWS Umgebung entdeckt werden.

Sie können Ihre GuardDuty Ergebnisse auf der Seite Ergebnisse in der GuardDuty Konsole oder mithilfe der API Operationen AWS CLI oder anzeigen und verwalten. Einen Überblick über die Möglichkeiten zur Verwaltung von Erkenntnissen finden Sie unter Verwaltung der GuardDuty Amazon-Ergebnisse.

Themen:

GuardDuty-Erkenntnisformat

Machen Sie sich mit dem Format der GuardDuty Suchtypen und den verschiedenen Bedrohungszwecken vertraut, die von verfolgt werden GuardDuty.

Beispielergebnisse

Versuchen Sie, Stichprobenergebnisse zu generieren, um die GuardDuty Ergebnisse und die zugehörigen Details zu testen und zu verstehen. Diese Ergebnisse sind mit einem Präfix [SAMPLE] gekennzeichnet.

GuardDuty Testergebnisse in speziellen Konten

Führen Sie ein `guardduty-tester` Skript in einem speziellen Nicht-Produktionsumfeld aus AWS-Konto , um ausgewählte GuardDuty Ergebnisse in Ihrer AWS Umgebung zu generieren.

Erkenntnisdetails

Erfahren Sie mehr über die Details zu den GuardDuty Ergebnissen, die in Ihrem Konto generiert werden.

Erkenntnistypen

Alle verfügbaren GuardDuty Ergebnisse nach Typ anzeigen und durchsuchen. Jeder Erkenntnistypeintrag enthält eine Erläuterung der betreffenden Erkenntnis sowie Tipps und Vorschläge für die Behebung.

GuardDuty-Erkenntnisformat

Wenn GuardDuty eine verdächtige oder unerwartete Aktivität in Ihrer AWS-Umgebung erkennt, erstellt der Service eine Erkenntnis. Eine Erkenntnis ist eine Benachrichtigung, die Details zu einem von GuardDuty festgestellten potenziellen Sicherheitsrisiko enthält. Die Erkenntnisdetails enthalten Informationen darüber, was geschehen ist, welche AWS-Ressourcen an der verdächtigen Aktivität beteiligt waren und wann diese Aktivität stattfand, sowie weitere Informationen.

Eine der wichtigsten Informationen in den Ergebnisdetails ist der Ergebnistyp. Der Zweck des Ergebnistyps ist eine kurze und dennoch aussagekräftige Beschreibung des potenziellen Sicherheitsrisikos. So informiert Sie beispielsweise der GuardDuty-Ergebnistyp Recon:EC2/PortProbeUnprotectedPort darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung einen ungeschützten Port aufweist, der von einem potenziellen Angreifer untersucht wird.

GuardDuty verwendet das folgende Format für die verschiedenen Erkenntnistypen, die generiert werden:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism!Artifact

Jeder Teil dieses Formats steht für einen Aspekt eines Erkenntnistyps. Für diese Aspekte gibt es die folgenden Erklärungen:

- ThreatPurpose – Eine Beschreibung des Hauptzwecks einer Bedrohung oder eines potentiellen Angriffs. Im folgenden Abschnitt finden Sie eine vollständige Liste der Bedrohungszwecke von GuardDuty.
- ResourceTypeAffected – Dieser Wert gibt an, welche AWS-Ressource in diesem Ergebnis als potenzielles Ziel eines Angriffs ermittelt wurde. Derzeit kann GuardDuty Erkenntnisse für EC2-, S3-, IAM- und EKS-Ressourcen generieren.
- ThreatFamilyName – Eine Beschreibung der allgemeinen Bedrohung oder potenziell böswilliger Aktivitäten, die GuardDuty erkennt. Der Wert NetworkPortUnusual gibt beispielsweise an, dass eine EC2-Instance, die in der GuardDuty-Erkenntnis erkannt wurde, zuvor noch nicht über einen bestimmten Remote-Port kommuniziert hat, der ebenfalls in der Erkenntnis erkannt wurde.
- DetectionMechanism – beschreibt die Methode, mit der GuardDuty die Erkenntnis erkannt hat. Dies kann verwendet werden, um auf eine Variation eines gängigen Erkenntnistyps oder auf eine Erkenntnis hinzuweisen, für deren Erkennung GuardDuty einen bestimmten Mechanismus verwendet hat. Beispielsweise weist Backdoor:EC2/DenialOfService.Tcp darauf hin, dass eine Serviceverweigerung (DoS) über TCP erkannt wurde. Die UDP-Variante ist Backdoor:EC2/DenialOfService.Udp.

Der Wert .Custom gibt an, dass GuardDuty die Erkenntnis anhand Ihrer benutzerdefinierten Bedrohungslisten erkannt hat, wohingegen .Reputation angibt, dass GuardDuty die Erkenntnis anhand eines Domain-Reputations-Punkte-Modells erkannt hat.

- Artefakt – Eine Beschreibung einer bestimmten Ressource eines Tools, das beim Angriff verwendet wird. So gibt beispielsweise DNS im Ergebnistyp CryptoCurrency:EC2/BitcoinTool.B!DNS an, dass eine EC2-Instance mit einer Domain kommuniziert, die mit Bitcoin in Verbindung steht.

Bedrohungszwecke

In GuardDuty beschreibt ein Bedrohungszweck den Hauptzweck einer Bedrohung, einen Angriffstyp oder ein Stadium eines potenziellen Angriffs. Beispielsweise deuten einige Bedrohungszwecke, wie Backdoor, auf einen Typ von Angriff hin. Einige Bedrohungszwecke, wie etwa Impact, stimmen jedoch mit den Taktiken von MITRE ATT&CK überein. Die MITRE-ATT&CK-Taktiken deuten auf verschiedene Phasen im Angriffszyklus eines Gegners hin. In der aktuellen Version von GuardDuty kann ThreatPurpose die folgenden Werte annehmen:

Backdoor

Dieser Wert gibt an, dass der Angriff eine AWS-Ressource kompromittiert hat und seinen eigenen Command-and-Control-Server (C&C-Server) kontaktieren kann, um weitere Anweisungen für schädigende Aktivitäten zu erhalten.

Verhalten

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkennt, die sich vom normalen Verhalten einer bestimmten AWS-Ressource unterscheiden.

CredentialAccess

Dieser Wert gibt an, dass GuardDuty Aktivitätsmuster erkannt hat, anhand derer ein Angreifer Anmeldeinformationen wie Konto-IDs oder Passwörter aus Ihrer Umgebung stehlen kann. Dieser Bedrohungszweck basiert auf den MITRE-ATT&CK-Taktiken

Kryptowährung

Dieser Wert gibt an, dass GuardDuty erkannt hat, dass eine AWS-Ressource in Ihrer Umgebung Software hostet, die mit Kryptowährungen in Verbindung steht (z. B. Bitcoin).

DefenseEvasion

Dieser Wert zeigt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster entdeckt hat, die ein Angreifer nutzen könnte, um sich beim Eindringen in Ihre Umgebung der Entdeckung zu entziehen. Dieser Bedrohungszweck basiert auf den MITRE-ATT&CK-Taktiken

Erkennung

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkannt hat, anhand derer ein Angreifer sein Wissen über Ihre Systeme und internen Netzwerke erweitern kann. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Ausführung

Dieser Wert gibt an, dass GuardDuty erkannt hat, dass ein Angreifer möglicherweise versucht, bösartigen Code auszuführen, um das Netzwerk zu durchsuchen oder Daten zu stehlen. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Exfiltration

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkannt hat, die ein Angreifer verwenden könnte, wenn er versucht, Daten aus Ihrem Netzwerk zu stehlen. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Auswirkung

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkannt hat, die darauf hindeuten, dass ein Angreifer versucht, Ihre Systeme und Daten zu manipulieren, zu unterbrechen oder zu zerstören. Dieser Bedrohungszweck basiert auf den MITRE-ATT&CK-Taktiken

InitialAccess

Dieser Bedrohungszweck basiert auf den MITRE-ATT&CK-Taktiken

Penetrationstest

Manchmal führen die Eigentümer von AWS-Ressourcen oder ihre bevollmächtigten Vertreter absichtlich Tests mit AWS-Anwendungen durch, um Schwachstellen zu finden, z. B. offene Sicherheitsgruppen oder Zugriffsschlüssel, die zu viele Berechtigungen enthalten. Bei diesen Penetrationstests wird versucht, gefährdete Ressourcen zu erkennen und zu sperren, bevor sie von Angreifern entdeckt werden. Einige der von autorisierten Penetrationstestern verwendeten Tools sind jedoch kostenlos verfügbar und können daher auch von nicht autorisierten Benutzern oder Angreifern verwendet werden, um Analysetests durchzuführen. Obwohl GuardDuty den wahren Zweck einer solchen Aktivität nicht erkennen kann, zeigt der Pentest-Wert an, dass GuardDuty eine solche Aktivität erkennt, dass sie der Aktivität ähnelt, die von bekannten

Penetrationstest-Tools erzeugt wird, und dass sie auf ein böswilliges Sondieren Ihres Netzwerks hindeuten könnte.

Persistenz

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkannt hat, anhand derer ein Angreifer versuchen könnte, den Zugriff auf Ihre Systeme aufrechtzuerhalten, auch wenn der ursprüngliche Zugriffsweg unterbrochen ist. Dies könnte beispielsweise das Erstellen eines neuen IAM-Benutzers beinhalten, nachdem er über die kompromittierten Anmeldeinformationen eines vorhandenen Benutzers Zugriff erhalten hat. Wenn die Anmeldeinformationen des vorhandenen Benutzers gelöscht werden, behält der Angreifer den Zugriff auf den neuen Benutzer, der beim ursprünglichen Ereignis nicht erkannt wurde. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Richtlinie

Dieser Wert gibt an, dass Ihr AWS-Konto ein Verhalten zeigt, das den empfohlenen bewährten Sicherheitsmethoden widerspricht.

PrivilegeEscalation

Dieser Wert informiert Sie darüber, dass der betroffene Prinzipal in Ihrer AWS-Umgebung ein Verhalten an den Tag legt, das ein Angreifer nutzen könnte, um sich Zugriff auf Ihr Netzwerk auf höherer Ebene zu verschaffen. Dieser Bedrohungszweck basiert auf der MITRE-ATT&CK-Taktiken.

Recon

Dieser Wert gibt an, dass GuardDuty Aktivitäten oder Aktivitätsmuster erkannt hat, anhand derer ein Angreifer Ihr Netzwerk auskundschaften kann, um festzustellen, wie er seinen Zugriff erweitern oder Ihre Ressourcen nutzen kann. Diese Aktivität kann beispielsweise das Aufspüren von Schwachstellen in Ihrer AWS-Umgebung umfassen, indem Ports untersucht, Benutzer und Datenbanktabellen aufgelistet werden usw.

Stealth

Dieser Wert gibt an, dass ein Angreifer aktiv versucht, seine Aktionen zu verbergen. Beispielsweise könnten sie einen anonymisierenden Proxyserver verwenden, was es extrem schwierig macht, die wahre Art der Aktivität einzuschätzen.

Trojan

Dieser Wert gibt an, dass der Angriff über Trojaner-Programme erfolgt, die im Hintergrund schädliche Aktivitäten durchführen. Es kann vorkommen, dass diese Software das

Erscheinungsbild eines seriösen Programms annimmt. Es kann vorkommen, dass Benutzer diese Software versehentlich ausführen. Die Software kann auch automatisch durch Ausnutzung einer Schwachstelle ausgeführt werden.

UnauthorizedAccess

Dieser Wert gibt an, dass GuardDuty verdächtige Aktivitäten oder Aktivitätsmuster einer unbefugten Person erkennt.

GuardDuty Scan-Engine zur Malware-Erkennung

Amazon GuardDuty hat eine intern entwickelte und verwaltete Scan-Engine und einen Drittanbieter. Beide verwenden Kompromittierungsindikatoren (IoCs), die aus verschiedenen internen Feeds stammen und Aufschluss über verschiedene Arten von Schadsoftware geben, auf die möglicherweise zugegriffen werden kann AWS. GuardDuty verfügt außerdem über Erkennungsdefinitionen, die auf YARA Regeln basieren, die von unseren Sicherheitsingenieuren hinzugefügt wurden, sowie Erkennungen, die auf heuristischen Modellen und Modellen für maschinelles Lernen (ML) basieren. Die signaturbasierte Erkennung umfasst nicht nur den Abgleich von Bytes, sondern auch einen Codeausschnitt, der potenziell komplex ist, und der Scanner kann Inhalte analysieren und Entscheidungen treffen.

Die Malware-Scan-Engine führt keine Live-Verhaltensanalyse durch, bei der die Malware-Detonation die Probe überwacht, während sie in einem realen System ausgeführt wird. Die GuardDuty Lösung besteht in erster Linie in einer dateibasierten Erkennung. GuardDuty Bietet eine agentenbasierte Lösung zur Erkennung dateiloser Malware, z. B. Laufzeit-Überwachung für AmazonEKS, Amazon und Amazon EC2 ECS (einschließlich). AWS Fargate

Die verwendeten Scan-Engines sind in der Lage, verschiedene Arten von Malware wie Cryptominer, Ransomware und Webshells zu erkennen, da es keine Beschränkung der Dateiformate gibt, mit denen nach Malware GuardDuty gescannt wird. Die vollständig verwaltete GuardDuty Scan-Engine aktualisiert die Liste der Malware-Signaturen kontinuierlich alle 15 Minuten.

Die Scan-Engine ist Teil eines GuardDuty Threat Intelligence-Systems, das eine interne Komponente zur Detonation von Malware verwendet. Dadurch werden neue Bedrohungsinformationen generiert, indem unabhängig voneinander Malware und harmlose Proben aus verschiedenen Quellen gesammelt werden. Der IoC-Typ Datei-Hash aus dem Threat Intelligence System wird außerdem in die Malware-Scan-Engine eingespeist, um Malware auf der Grundlage bekannter bösartiger Datei-Hashes zu erkennen.

Generierung von Stichprobenbefunden in GuardDuty

Sie können mit Amazon Stichprobenergebnisse generieren GuardDuty , um die verschiedenen Befunde, die generiert werden GuardDuty können, zu visualisieren und zu verstehen. Wenn Sie Stichprobenergebnisse generieren, wird Ihre aktuelle Ergebnisliste mit einem Stichprobenergebnis für jeden unterstützten Befundtyp GuardDuty aufgefüllt.

Bei den generierten Beispielen handelt es sich um Näherungen, die mit Platzhalterwerten gefüllt sind. Diese Beispiele sehen möglicherweise anders aus als die tatsächlichen Ergebnisse für Ihre Umgebung, aber Sie können sie verwenden, um verschiedene Konfigurationen zu testen GuardDuty, z. B. Ihre EventBridge Ereignisse oder Filter. Eine Liste der verfügbaren Werte für die Suche nach Typen finden Sie in der Erkenntnistypen Tabelle.

Generieren von Stichprobenergebnissen über die GuardDuty Konsole oder API

Wählen Sie Ihre bevorzugte Zugriffsmethode, um Beispiel-Erkenntnisse zu generieren.

> **Note**
>
> Die Konsolenmethode generiert jeweils einen Erkenntnistyp. Ergebnisse einzelner Stichproben können nur über die generiert werdenAPI.

Console

Gehen Sie wie folgt vor, um Beispielergebnisse zu erzeugen. Dieser Prozess generiert einen Stichprobenbefund für jeden GuardDuty Befundtyp.

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Klicken Sie auf der Seite Settings unter Sample findings auf Generate sample findings.
4. Wählen Sie im Navigationsbereich Findings aus. Die Ergebnisse der Stichprobe werden auf der Seite Aktuelle Ergebnisse mit dem Präfix [SAMPLE] angezeigt.

API/CLI

Mithilfe von können Sie ein einzelnes Stichprobenergebnis generieren CreateSampleFindingsAPI, das einem beliebigen GuardDuty Befundtyp entspricht. Die verfügbaren Werte für die Befundtypen sind in der Erkenntnistypen Tabelle aufgeführt.

Dies ist nützlich für das Testen von CloudWatch Ereignisregeln oder für die Automatisierung auf der Grundlage von Ergebnissen. Das folgende Beispiel zeigt, wie Sie ein einzelnes Beispiel-Erkenntnis des `Backdoor:EC2/DenialOfService.Tcp`-Typs mithilfe der AWS CLI generieren können.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

Der Titel der mit diesen Methoden generierten Beispielergebnisse beginnt in der Konsole immer mit [SAMPLE]. Stichprobenergebnisse haben `"sample": true` im additionalInfoAbschnitt mit den JSON Ergebnisdetails den Wert von.

Informationen zur Generierung einiger allgemeiner Ergebnisse auf der Grundlage einer simulierten Aktivität in einer speziellen und isolierten AWS-Konto Umgebung finden Sie unter GuardDuty Testergebnisse in speziellen Konten.

GuardDuty Testergebnisse in speziellen Konten

Verwenden Sie dieses Dokument, um ein Tester-Skript auszuführen, das GuardDuty Ergebnisse in einem generiert AWS-Konto , das Sie speziell für diesen Zweck verwenden. Sie können diese Schritte ausführen, wenn Sie bestimmte GuardDuty Arten von Ergebnissen verstehen und mehr über sie erfahren möchten. Diese Erfahrung unterscheidet sich von der GenerierungBeispielergebnisse. Weitere Informationen zu den Erfahrungen beim Testen von GuardDuty Ergebnissen finden Sie unterÜberlegungen.

Inhalt

- Schritt 1 — Voraussetzungen
- Schritt 2 — Ressourcen bereitstellen AWS
- Schritt 3 — Tester-Skripte ausführen
- Schritt 4 — Testressourcen AWS bereinigen
- Behebung häufiger Probleme

Überlegungen

Bevor Sie fortfahren, sollten Sie die folgenden Überlegungen berücksichtigen:

- GuardDuty empfiehlt, das Tester-Skript in einer dedizierten Nicht-Produktionsumgebung AWS-Konto oder einer isolierten Umgebung bereitzustellen. Durch die Ausführung des Tester-Skripts GuardDuty werden bestimmte AWS Ressourcen in diesem Konto bereitgestellt. Dies hilft Ihnen auch dabei, diese simulierten Ergebnisse zu identifizieren.
- Das Tester-Skript generiert über 100 GuardDuty Ergebnisse mit unterschiedlichen AWS Ressourcenkombinationen. Derzeit beinhaltet dies nicht alle. Erkenntnistypen Eine Liste der Suchtypen, die Sie mit diesem Tester-Skript generieren können, finden Sie unter. GuardDuty Ergebnisse, die das Tester-Skript generieren kann
- Das Tester-Skript validiert den GuardDuty Konfigurationsstatus in Ihrem speziellen Konto. Wenn dieses Konto nicht GuardDuty aktiviert ist, werden Sie beim Ausführen Schritt 3 — Tester-Skripte ausführen des Skripts aufgefordert, es zu aktivieren. Das Test-Skript bittet Sie um Ihre Zustimmung zur Aktivierung bestimmter Schutzpläne, die zur Generierung der Ergebnisse erforderlich sind.

  GuardDuty Zum ersten Mal aktivieren

  Wenn GuardDuty es in Ihrem speziellen Konto zum ersten Mal in einer bestimmten Region aktiviert wird, wird Ihr Konto automatisch für eine kostenlose 30-Tage-Testversion registriert.

  GuardDuty bietet optionale Schutzpläne. Zum Zeitpunkt der Aktivierung GuardDuty werden auch bestimmte Schutzpläne aktiviert und sind in der kostenlosen GuardDuty 30-Tage-Testversion enthalten. Weitere Informationen finden Sie unter Verwenden Sie die kostenlose GuardDuty 30-Tage-Testversion.

  GuardDuty ist in Ihrem Konto bereits aktiviert, bevor Sie das Tester-Skript ausführen

  Wenn GuardDuty es bereits aktiviert ist, überprüft das Tester-Skript anhand der Parameter den Konfigurationsstatus bestimmter Schutzpläne und anderer Einstellungen auf Kontoebene, die zur Generierung der Ergebnisse erforderlich sind.

Durch die Ausführung dieses Testerskripts können bestimmte Schutzpläne in Ihrem speziellen Konto in einer Region zum ersten Mal aktiviert werden. Dadurch wird die kostenlose 30-Tage-Testversion für diesen Schutzplan gestartet. Informationen zur kostenlosen Testversion der einzelnen Schutzpläne finden Sie unterVerwenden Sie die kostenlose GuardDuty 30-Tage-Testversion.

- Nach Abschluss des Testerskripts werden die ursprünglichen Schutzplankonfigurationen und -einstellungen für Ihr dediziertes Konto wiederhergestellt.

GuardDuty Ergebnisse, die das Tester-Skript generieren kann

Derzeit generiert das Tester-Skript die folgenden Findetypen, die sich auf AmazonEC2, AmazonEKS, Amazon S3 und EKS Audit-Logs beziehen: IAM

- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Udp
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- PenTest:IAMUser/KaliLinux

- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- PenTest:S3/KaliLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller
- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- DefenseEvasion:Runtime/ProcessInjection.Ptrace

- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS

Schritt 1 — Voraussetzungen

Um Ihre Testumgebung vorzubereiten, benötigen Sie die folgenden Elemente:

- Git — Installieren Sie das Git-Befehlszeilentool basierend auf dem von Ihnen verwendeten Betriebssystem. Dies ist erforderlich, um das `amazon-guardduty-tester`Repository zu klonen.
- AWS Command Line Interface— Ein Open-Source-Tool, mit dem Sie mithilfe AWS -Services von Befehlen in Ihrer Befehlszeilen-Shell interagieren können. Weitere Informationen finden Sie unter Erste Schritte mit AWS CLI im AWS Command Line Interface Benutzerhandbuch.
- AWS Systems Manager— Um Session Manager-Sitzungen mit Ihren verwalteten Knoten zu initiieren, müssen AWS CLI Sie das Session Manager-Plug-In auf Ihrem lokalen Computer installieren. Weitere Informationen finden Sie unter Installieren des Session Manager-Plug-ins für AWS CLI im AWS Systems Manager Benutzerhandbuch.
- Node Package Manager (NPM) — InstallierenNPM, um alle Abhängigkeiten zu installieren.
- Docker — Sie müssen Docker installiert haben. Installationsanweisungen finden Sie auf der Docker-Website.

  Um zu überprüfen, ob Docker installiert wurde, führen Sie den folgenden Befehl aus und vergewissern Sie sich, dass eine Ausgabe vorliegt, die der folgenden Ausgabe ähnelt:

```
$ docker --version
Docker version 19.03.1
```

- Abonnieren Sie das Kali Linux-Image im. AWS Marketplace

Schritt 2 — Ressourcen bereitstellen AWS

Dieser Abschnitt enthält eine Liste der wichtigsten Konzepte und der Schritte zur Bereitstellung bestimmter AWS Ressourcen in Ihrem speziellen Konto.

Konzepte

Die folgende Liste enthält wichtige Konzepte zu den Befehlen, mit denen Sie die Ressourcen bereitstellen können:

- AWS Cloud Development Kit (AWS CDK)— CDK ist ein Open-Source-Framework für die Softwareentwicklung, mit dem Cloud-Infrastruktur im Code definiert und bereitgestellt werden kann. AWS CloudFormation CDKunterstützt eine Reihe von Programmiersprachen, um wiederverwendbare Cloud-Komponenten, sogenannte Konstrukte, zu definieren. Sie können diese zu Stacks und Apps zusammenstellen. Anschließend können Sie Ihre CDK Anwendungen bereitstellen, AWS CloudFormation um Ihre Ressourcen bereitzustellen oder zu aktualisieren. Weitere Informationen finden Sie unter Was ist der AWS CDK? im AWS Cloud Development Kit (AWS CDK) Entwicklerhandbuch.
- Bootstrapping — Dies ist der Prozess, bei dem Ihre AWS Umgebung für die Verwendung mit vorbereitet wird. AWS CDK Bevor Sie einen CDK Stack in einer AWS Umgebung bereitstellen, muss die Umgebung zunächst gebootet werden. Dieser Prozess der Bereitstellung bestimmter AWS Ressourcen in Ihrer Umgebung, die von verwendet werden, AWS CDK ist Teil der Schritte, die Sie im nächsten Abschnitt ausführen werden -. Schritte zur Bereitstellung von Ressourcen AWS

  Weitere Informationen zur Funktionsweise von Bootstrapping finden Sie unter Bootstrapping im Entwicklerhandbuch.AWS Cloud Development Kit (AWS CDK)

Schritte zur Bereitstellung von Ressourcen AWS

Führen Sie die folgenden Schritte aus, um mit der Bereitstellung der Ressourcen zu beginnen:

1. Richten Sie Ihr AWS CLI Standardkonto und Ihre Region ein, sofern die Regionsvariablen für das Konto nicht manuell in der `bin/cdk-gd-tester.ts` Datei festgelegt wurden. Weitere Informationen finden Sie im AWS Cloud Development Kit (AWS CDK) Entwicklerhandbuch unter Umgebungen.
2. Führen Sie die folgenden Befehle aus, um die Ressourcen bereitzustellen:

```
git clone https://github.com/awslabs/amazon-guardduty-tester && cd amazon-guardduty-tester
npm install
cdk bootstrap
cdk deploy
```

Der letzte Befehl (`cdk deploy`) erstellt in Ihrem Namen einen AWS CloudFormation Stack. Der Name dieses Stacks ist GuardDutyTesterStack.

GuardDuty Erstellt im Rahmen dieses Skripts neue Ressourcen, um GuardDuty Ergebnisse in Ihrem Konto zu generieren. Außerdem wird den EC2 Amazon-Instances das folgende Tag-Schlüssel:Wert-Paar hinzugefügt:

`CreatedBy:GuardDuty Test Script`

Zu den EC2 Amazon-Instances gehören auch die EC2 Instances, die EKS Knoten und ECS Cluster hosten.

> **Instance-Typen**
>
> GuardDuty erstellt `t3.micro` für alle Ressourcen mit Ausnahme der EKS Amazon-Knotengruppe. Da mindestens 2 Kerne EKS erforderlich sind, hat der EKS Knoten den `t3.medium` Instance-Typ. Weitere Informationen zu Instance-Typen finden Sie unter Verfügbare Größen im Amazon EC2 Instances Types Guide.

Schritt 3 — Tester-Skripte ausführen

Dies ist ein zweistufiger Prozess, bei dem Sie zuerst eine Sitzung mit dem Testtreiber starten und dann Skripts ausführen müssen, um GuardDuty Ergebnisse mit bestimmten Ressourcenkombinationen zu generieren.

Teil A — Starten Sie die Sitzung mit dem Testfahrer

1. Nachdem Ihre Ressourcen bereitgestellt wurden, speichern Sie den Regionalcode in einer Variablen in Ihrer aktuellen Terminalsitzung. Verwenden Sie den folgenden Befehl und ersetzen Sie *us-east-1* mit dem Regionalcode, in dem Sie die Ressourcen bereitgestellt haben:

   ```
   $ REGION=us-east-1
   ```

2. Das Tester-Skript ist nur über AWS Systems Manager (SSM) verfügbar. Um eine interaktive Shell auf der Tester-Host-Instanz zu starten, fragen Sie den Host ab InstanceId.
3. Verwenden Sie den folgenden Befehl, um Ihre Sitzung für das Tester-Skript zu beginnen:

   ```
   aws ssm start-session
     --region $REGION
     --document-name AWS-StartInteractiveCommand
     --parameters command="cd /home/ssm-user/py_tester && bash -l"
     --target $(aws ec2 describe-instances
       --region $REGION
       --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
       --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
       --output text)
   ```

Teil B — Ergebnisse generieren

Das Tester-Skript ist ein Python-basiertes Programm, das dynamisch ein Bash-Skript erstellt, um Ergebnisse auf der Grundlage Ihrer Eingabe zu generieren. Sie haben die Flexibilität, Ergebnisse auf der Grundlage eines oder mehrerer AWS Ressourcentypen, GuardDuty Schutzpläne, Bedrohungszwecke (Taktiken) oder zu generieren. Grundlegende Datenquellen the section called “GuardDuty Ergebnisse, die das Tester-Skript generieren kann”

Verwenden Sie die folgenden Befehlsbeispiele als Referenz und führen Sie einen oder mehrere Befehle aus, um Ergebnisse zu generieren, die Sie untersuchen möchten:

```
python3 guardduty_tester.py
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
```

```
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

Weitere Informationen zu gültigen Parametern erhalten Sie, wenn Sie den folgenden Hilfebefehl ausführen:

```
python3 guardduty_tester.py --help
```

Teil C — Überprüfung der generierten Ergebnisse

Wählen Sie eine bevorzugte Methode, um die generierten Ergebnisse in Ihrem Konto anzuzeigen.

GuardDuty console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Findings aus.
3. Wählen Sie in der Tabelle mit den Ergebnissen ein Ergebnis aus, für das Sie die Details anzeigen möchten. Dadurch wird der Bereich mit den Ergebnisdetails geöffnet. Weitere Informationen finden Sie unter Die GuardDuty Ergebnisse von Amazon verstehen.
4. Wenn Sie diese Ergebnisse filtern möchten, verwenden Sie den Ressourcen-Tag key and value. Um beispielsweise die für die EC2 Amazon-Instances generierten Ergebnisse zu filtern, verwenden Sie`CreatedBy: GuardDuty Test Script` tag key:value pair für Instance-Tag-Schlüssel und Instance-Tag-Schlüssel.

API

- Führen Sie ListFindingsden Befehl aus, um die Ergebnisse für eine bestimmte Melder-ID anzuzeigen. Sie können bestimmte Parameter angeben, um Ergebnisse zu filtern.

  Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

AWS CLI

- Führen Sie den folgenden AWS CLI Befehl aus, um die generierten Ergebnisse anzuzeigen und zu ersetzen *us-east-1* and *12abc34d567e8fa901bc2d34EXAMPLE* mit geeigneten Werten:

```
aws guardduty list-findings --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34EXAMPLE
```

  Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite „Einstellungen“ oder führen Sie den aus ListDetectorsAPI.

  Weitere Informationen zu den Parametern, mit denen Sie Ergebnisse filtern können, finden Sie in der AWS CLI Befehlsreferenz unter list-findings.

Schritt 4 — Testressourcen AWS bereinigen

Die Einstellungen auf Kontoebene und andere Aktualisierungen des Konfigurationsstatus, die während der Schritt 3 — Tester-Skripte ausführen Rückkehr zum ursprünglichen Zustand vorgenommen wurden, wenn das Tester-Skript abgeschlossen ist.

Nachdem Sie das Tester-Skript ausgeführt haben, können Sie wählen, ob Sie die AWS Testressourcen bereinigen möchten. Sie können dafür eine der folgenden Methoden verwenden:

- Führen Sie den folgenden Befehl aus:

```
cdk destroy
```

- Löschen Sie den AWS CloudFormation Stapel mit dem Namen GuardDutyTesterStack. Informationen zu den einzelnen Schritten finden Sie unter Löschen eines Stacks auf der AWS CloudFormation Konsole.

Behebung häufiger Probleme

GuardDuty hat häufig auftretende Probleme identifiziert und empfiehlt Schritte zur Fehlerbehebung:

- `Cloud assembly schema version mismatch`— Aktualisieren Sie AWS CDK CLI auf eine Version, die mit der erforderlichen Cloud-Assembly-Version kompatibel ist, oder auf die neueste verfügbare Version. Weitere Informationen finden Sie unter AWS CDK CLIKompatibilität.
- `Docker permission denied`— Fügen Sie den Benutzer des dedizierten Kontos zu den Docker-Benutzern hinzu, damit das dedizierte Konto die Befehle ausführen kann. Weitere Informationen zu den einzelnen Schritten finden Sie unter Docker-Zugriff verweigert.
- `Your requested instance type is not supported in your requested Availability Zone`— Einige Availability Zones unterstützen bestimmte Instanztypen nicht. Gehen Sie wie folgt vor, um herauszufinden, welche Availability Zones Ihren bevorzugten Instance-Typ unterstützen, und versuchen Sie erneut, AWS Ressourcen bereitzustellen:

  1. Wählen Sie eine bevorzugte Methode, um festzustellen, welche Availability Zones Ihren Instance-Typ unterstützen:

     Console

     Um Availability Zones zu identifizieren, die den bevorzugten Instance-Typ unterstützen

     1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
     2. Wählen Sie mithilfe der AWS Regionsauswahl in der oberen rechten Ecke der Seite die Region aus, in der Sie die Instance starten möchten.
     3. Wählen Sie im Navigationsbereich unter Instances die Option Instance-Typen aus.
     4. Wählen Sie aus der Tabelle mit den Instanztypen einen bevorzugten Instance-Typ aus.
     5. Sehen Sie sich unter Netzwerk die Regionen an, die unter Availability Zones aufgeführt sind.

        Auf der Grundlage dieser Informationen müssen Sie möglicherweise eine neue Region auswählen, in der Sie die Ressourcen bereitstellen können.

     AWS CLI

     Führen Sie den folgenden Befehl aus, um eine Liste der Availability Zones anzuzeigen. Stellen Sie sicher, dass Sie Ihren bevorzugten Instance-Typ und die Region angeben (*`us-east-1`*).

```
aws ec2 describe-instance-type-offerings --location-type availability-zone  --
filters Name=instance-type,Values=Preferred instance type --region us-east-1 --
output table
```

Weitere Informationen zu diesem Befehl finden Sie describe-instance-type-offeringsin der AWS CLI Befehlsreferenz.

Wenn Sie bei der Ausführung dieses Befehls eine Fehlermeldung erhalten, stellen Sie sicher, dass Sie die neueste Version von verwenden AWS CLI. Weitere Informationen finden Sie unter Fehlerbehebung im AWS Command Line Interface -Benutzerhandbuch.

2. Versuchen Sie erneut, die AWS Ressourcen bereitzustellen, und geben Sie eine Availability Zone an, die Ihren bevorzugten Instance-Typ unterstützt.

   Um erneut zu versuchen, Ressourcen bereitzustellen AWS

   1. Richten Sie die Standardregion in der `bin/cdk-gd-tester.ts` Datei ein.
   2. Um die Availability Zone anzugeben, öffnen Sie die `amazon-guardduty-tester/lib/common/network/vpc.ts` Datei.
   3. Ersetzen Sie diese Datei durch die Stelle`maxAzs: 2,`, `availabilityZones: ['us-east-1a', 'us-east-1c'],` an der Sie die Availability Zones für Ihren Instance-Typ angeben müssen.
   4. Fahren Sie mit den verbleibenden Schritten unter fortSchritte zur Bereitstellung von Ressourcen AWS.

GuardDuty Schweregrade der Ergebnisse

Jedem GuardDuty Ergebnis ist ein Schweregrad und ein Wert zugewiesen, der das von unseren Sicherheitstechnikern festgestellte potenzielle Risiko für Ihr Netzwerk widerspiegelt. Der Wert des Schweregrads kann an beliebiger Stelle im Bereich von 1,0 bis 8,9 liegen, wobei höhere Werte auf ein höheres Sicherheitsrisiko hinweisen. Um Ihnen dabei zu helfen, eine Reaktion auf ein potenzielles Sicherheitsproblem zu finden, das durch ein Ergebnis hervorgehoben GuardDuty wird, wird dieser Bereich in die Schweregrade Hoch, Mittel und Niedrig unterteilt.

> **Note**
>
> Die Werte 0 und 9,0 bis 10,0 sind für die zukünftige Verwendung reserviert.

Im Folgenden sind die derzeit definierten Schweregrade und Werte für die GuardDuty Ergebnisse sowie allgemeine Empfehlungen für die einzelnen Ergebnisse aufgeführt:

Schweregrad	Wertebereich
Hoch	7,0 — 8,9
Ein hoher Schweregrad weist darauf hin, dass die fragliche Ressource (eine EC2 Instanz oder ein Satz von IAM Benutzeranmeldedaten) gefährdet ist und aktiv für nicht autorisierte Zwecke verwendet wird. Es wird empfohlen, dass Sie Sicherheitsprobleme mit hohem Schweregrad als Priorität behandeln und sofortige Korrekturmaßnahmen ergreifen, um eine weitere unbefugte Nutzung Ihrer Ressourcen zu verhindern. Bereinigen Sie beispielsweise Ihre EC2 Instance oder beenden Sie sie oder wechseln Sie die IAM Anmeldeinformationen ab. Weitere Informationen finden Sie unter Schritte zur Abhilfe.	
Mittel	4,0 — 6,9
Ein mittlerer Schweregrad weist auf verdächtige Aktivitäten hin, die vom normalerweise beobachte ten Verhalten abweichen und je nach Anwendungsfall auf eine Ressourcenkomprimettierung hinweisen können. Wir empfehlen Ihnen, die betroffene Ressource so bald wie möglich zu untersuchen. Die Schritte zur Abhilfe variieren je nach Ressource und Ergebnisfamilie. Im Allgemeinen sollten Sie jedoch prüfen, ob die Aktivität autorisiert ist und mit Ihrem Anwendungsfall übereinstimmt. Wenn Sie die Ursache nicht identifizieren oder nicht bestätigen können, dass die Aktivität autorisiert wurde, sollten Sie die Ressource als kompromittiert betrachten und zum Sichern der Ressource die Schritte zur Abhilfe befolgen. Hier sind einige Dinge, die Sie bei der Überprüfung eines Ergebnisses mittleren Schweregrades beachten sollten:	

Schweregrad	Wertebereich
• Prüfen Sie, ob ein autorisierter Benutzer neue Software installiert hat, die das Verhalten einer Ressource ändert (z. B. mehr Datenverkehr als normal zugelassen oder die Kommunikation über einen neuen Port aktiviert hat). • Überprüfen Sie, ob ein autorisierter Benutzer die Einstellungen für die Systemsteuerung (z. B. eine Sicherheitsgruppeneinstellung) geändert hat. • Führen Sie eine Virenprüfung der betroffenen Ressource durch, um nicht autorisierte Software zu erkennen. • Überprüfen Sie die Berechtigungen, die mit der betreffenden IAM Rolle, dem Benutzer, der Gruppe oder dem Satz von Anmeldeinformationen verknüpft sind. Möglicherweise müssen diese geändert oder rotiert werden.	
Niedrig	1,0 — 3,9
Ein niedriger Schweregrad weist auf versuchte verdächtige Aktivitäten hin, die Ihr Netzwerk nicht gefährdet haben, z. B. einen Port-Scan oder einen fehlgeschlagenen Eindringungsversuch. Es gibt keine empfohlene Sofortmaßnahme, aber es lohnt sich, diesen Informationen Beachtung zu schenken, da dies möglicherweise darauf hindeutet, dass jemand nach Schwachstellen in Ihrem Netzwerk sucht.	

Überprüfung der GuardDuty Ergebnisse

Gehen Sie wie folgt vor, um Ihre GuardDuty Ergebnisse zu überprüfen und zu verstehen.

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Klicken Sie auf Ergebnisse und wählen Sie dann ein bestimmtes Ergebnis aus, um sich die Details anzeigen zu lassen.

   Die Details für jede Erkenntnis unterscheiden sich je nach Erkenntnistyp, betroffenen Ressourcen und Art der Aktivität. Weitere Informationen zu verfügbaren Ergebnisfeldern finden Sie unter Erkenntnisdetails.
3. (Optional) Wenn Sie eine Erkenntnis archivieren möchten, wählen Sie sie aus der Liste Ihrer Erkenntnisse aus und wählen Sie dann das Menü Aktionen. Wählen Sie dann Archivieren.

Archivierte Erkenntnisse können angezeigt werden, indem Sie in der Dropdownliste Aktuell die Option Archiviert auswählen.

Derzeit können GuardDuty Benutzer von GuardDuty Mitgliedskonten keine Ergebnisse archivieren.

> **Important**
>
> Wenn Sie ein Ergebnis manuell mit dem oben beschriebenen Verfahren archivieren, werden alle nachfolgenden Vorkommen dieses Ergebnisses (die nach Abschluss der Archivierung generiert werden) der Liste Ihrer aktuellen Ergebnisse hinzugefügt. Wenn dieses Ergebnis nie in Ihrer aktuellen Liste angezeigt werden soll, können Sie es automatisch archivieren. Weitere Informationen finden Sie unter Unterdrückungsregeln.

4. (Optional) Zum Herunterzuladen eines Ergebnisses wählen Sie es in der Ergebnisliste aus und öffnen dann das Menü Aktionen. Wählen Sie dann Exportieren. Wenn Sie ein Ergebnis exportieren, können Sie JSON das vollständige Dokument sehen.

> **Note**
>
> In einigen Fällen GuardDuty wird ihm bewusst, dass es sich bei bestimmten Ergebnissen um falsch positive Ergebnisse handelt, nachdem sie generiert wurden. GuardDuty stellt ein Konfidenzfeld für die Ergebnisse JSON bereit und setzt dessen Wert auf Null. Auf diese Weise GuardDuty wissen Sie, dass Sie solche Ergebnisse getrost ignorieren können.

Erkenntnisdetails

In der GuardDuty Amazon-Konsole können Sie die Details zu den Ergebnissen im Abschnitt Zusammenfassung der Ergebnisse einsehen. Die Erkenntnisdetails variieren je nach Erkenntnistyp.

Hauptsächlich bestimmen zwei Details, welche Arten von Informationen für jede Erkenntnis verfügbar sind. Der erste ist der Ressourcentyp, der`Instance`,`AccessKey`,`S3Bucket`,`S3Object`,`Kubernetes cluster`, `ECS cluster` `ContainerRDSDBInstance`, oder sein kann`Lambda`. Das zweite Detail, das die Suche nach Informationen bestimmt, ist die Ressourcenrolle. Die Ressourcenrolle kann `Target` für

Zugriffsschlüssel sein, was bedeutet, dass die Ressource das Ziel verdächtiger Aktivitäten war. Bei Feststellungen vom Typ Instance kann die Rolle der Ressource auch `Actor` sein, was bedeutet, dass Ihre Ressource der Akteur war, der die verdächtige Aktivität durchgeführt hat. In diesem Thema werden einige der allgemein verfügbaren Erkenntnisdetails beschrieben.

Überblick über Erkenntnisse

Der Abschnitt Überblick enthält die grundlegendsten Merkmale, anhand derer die Erkenntnis identifiziert werden kann, einschließlich der folgenden Informationen:

- Konto-ID — Die ID des AWS Kontos, in dem die Aktivität stattgefunden hat, die GuardDuty zur Generierung dieses Ergebnisses geführt hat.
- Anzahl — Gibt an, wie oft GuardDuty eine Aktivität, die diesem Muster entspricht, mit dieser Ergebnis-ID aggregiert wurde.
- Erstellt am – Uhrzeit und Datum des Zeitpunkts, an dem diese Erkenntnis erstmals erstellt wurde. Wenn dieser Wert von Aktualisiert am abweicht, bedeutet dies, dass die Aktivität mehrfach stattgefunden hat und ein fortlaufendes Problem darstellt.

> **Note**
>
> Zeitstempel für Ergebnisse in der GuardDuty Konsole werden in Ihrer lokalen Zeitzone angezeigt, während bei JSON Exporten und CLI Ausgaben Zeitstempel in angezeigt werden. UTC

- Erkenntnis-ID – Eine eindeutige Erkenntnis-ID für diesen Erkenntnistyp und Parametersatz. Neue Vorkommen von Aktivitäten, die diesem Muster entsprechen, werden für dieselbe ID aggregiert.
- Erkenntnistyp – Eine formatierte Zeichenfolge, die den Typ der Aktivität darstellt, durch den die Erkenntnis ausgelöst wurde. Weitere Informationen finden Sie unter GuardDuty-Erkenntnisformat.
- Region — Die AWS Region, in der das Ergebnis generiert wurde. Weitere Informationen zu unterstützten Regionen finden Sie unter Regionen und Endpunkte
- Ressourcen-ID — Die ID der AWS Ressource, für die die Aktivität stattgefunden hat, die GuardDuty zur Generierung dieses Ergebnisses geführt hat.
- Scan-ID — Gilt für Ergebnisse, bei denen GuardDuty Malware Protection for aktiviert EC2 ist. Dabei handelt es sich um eine Kennung des Malware-Scans, der auf den EBS Volumes ausgeführt wird, die der potenziell gefährdeten EC2 Instance- oder Container-Workload zugeordnet sind. Weitere Informationen finden Sie unter Malware-Schutz zum EC2 Auffinden von Details.

- Schweregrad – der einer Erkenntnis zugeordnete Schweregrad: Hoch, Mittel oder Niedrig. Weitere Informationen finden Sie unter GuardDuty Schweregrade der Ergebnisse.
- Aktualisiert am — Das letzte Mal, als dieses Ergebnis mit einer neuen Aktivität aktualisiert wurde, die dem Muster entspricht, das GuardDuty zur Generierung dieses Ergebnisses geführt hat.

Ressource

Die betroffene Ressource enthält Einzelheiten zu der AWS Ressource, auf die die auslösende Aktivität abzielte. Die verfügbaren Informationen variieren je nach Ressourcentyp und Aktionstyp.

Ressourcenrolle — Die Rolle der AWS Ressource, die den Befund ausgelöst hat. Dieser Wert kann TARGEToder sein und ACTORgibt an, ob Ihre Ressource das Ziel der verdächtigen Aktivität oder der Akteur war, der die verdächtige Aktivität ausgeführt hat.

Ressourcen-Typ – der Typ der betroffenen Ressource. Wenn mehrere Ressourcen betroffen waren, kann eine Erkenntnis mehrere Ressourcentypen umfassen. Die Ressourcentypen sind Instance AccessKey, S3Bucket, S3Object,, KubernetesClusterECSCluster, RDSDBInstanceContainer und Lambda. Je nach Ressourcentyp stehen unterschiedliche Erkenntnisdetails zur Verfügung. Wählen Sie eine Registerkarte mit Ressourcenoptionen aus, um mehr über die für diese Ressource verfügbaren Details zu erfahren.

Instance

Instance-Details:

> **Note**
>
> Einige Instanzdetails fehlen möglicherweise, wenn die Instanz bereits gestoppt wurde oder wenn der zugrunde liegende Aufruf bei einem API regionsübergreifenden Aufruf von einer EC2 Instanz in einer anderen Region stammte. API

- Instanz-ID — Die ID der EC2 Instanz, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Instanztyp — Der Typ der EC2 Instanz, die an der Entdeckung beteiligt war.
- Startzeit – Das Datum und die Uhrzeit, zu der die Instance gestartet wurde.
- Outpost ARN — Der Amazon-Ressourcenname (ARN) von AWS Outposts. Gilt nur für AWS Outposts Instances. Weitere Informationen finden Sie unter Was ist AWS Outposts?

- Name der Sicherheitsgruppe – Der Name der Sicherheitsgruppe, die der beteiligten Instance angefügt ist.
- Sicherheitsgruppen-ID – Die ID der Sicherheitsgruppe, die der beteiligten Instance angefügt ist.
- Instance-Status – Der aktuelle Status der Ziel-Instance.
- Availability Zone – Die Availability Zone der AWS -Region, in der sich die betroffene Instance befindet.
- Image-ID – Die ID des Amazon Machine Image, das zum Erstellen der an der Aktivität beteiligten Instance verwendet wurde.
- Image-Beschreibung – Eine Beschreibung der ID des Amazon Machine Image, das zum Erstellen der Instance verwendet wurde, die an der Aktivität beteiligt war.
- Tags – Eine Liste der Tags, die dieser Ressource angefügt sind, die im Format `key:value` aufgeführt werden.

AccessKey

Details zu Zugriffsschlüsseln:

- Zugriffsschlüssel-ID — Die Zugriffsschlüssel-ID des Benutzers, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Prinzipal-ID — Die Prinzipal-ID des Benutzers, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Benutzertyp — Der Benutzertyp, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat. Weitere Informationen finden Sie unter CloudTrail userIdentity Element.
- Benutzername — Der Name des Benutzers, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.

S3Bucket

Details zum Amazon-S3-Bucket:

- Name – Der Name des Buckets, der an der Erkenntnis beteiligt war.
- ARN— Der Bucket, ARN der an der Entdeckung beteiligt war.

- Eigentümer – Die kanonische Benutzer-ID des Benutzers, dem der Bucket gehört, der an der Erkenntnis beteiligt war. Weitere Informationen zu kanonischen Benutzern finden IDs Sie unter AWS Konto-Identifikatoren.
- Typ – Der Typ der Bucket-Erkenntnis. Mögliche Werte sind Ziel oder Quelle.
- Standardmäßige serverseitige Verschlüsselung – Verschlüsselungsdetails für den Bucket.
- Bucket-Tags – Eine Liste der Tags, die dieser Ressource zugeordnet sind und im Format `key:value` aufgeführt werden.
- Effektive Berechtigungen – Eine Auswertung aller effektiven Berechtigungen und Richtlinien für den Bucket, die angibt, ob der betreffende Bucket öffentlich verfügbar ist. Werte können Öffentlich oder Nicht öffentlich sein.

S3Object

- S3-Objektdetails — Enthält die folgenden Informationen über das gescannte S3-Objekt:
  - ARN— Amazon-Ressourcenname (ARN) des gescannten S3-Objekts.
  - Schlüssel — Der Name, der der Datei zugewiesen wurde, als sie im S3-Bucket erstellt wurde.
  - Versions-ID — Wenn Sie die Bucket-Versionierung aktiviert haben, gibt dieses Feld die Versions-ID an, die der neuesten Version des gescannten S3-Objekts zugeordnet ist. Weitere Informationen finden Sie unter Verwenden der Versionierung in S3-Buckets im Amazon S3 S3-Benutzerhandbuch.
  - eTag— Stellt die spezifische Version des gescannten S3-Objekts dar.
  - Hash — Der Hash der Bedrohung, die in diesem Ergebnis erkannt wurde.
- S3-Bucket-Details — Enthält die folgenden Informationen über den Amazon S3 S3-Bucket, der dem gescannten S3-Objekt zugeordnet ist:
  - Name — Gibt den Namen des S3-Buckets an, der das Objekt enthält.
  - ARN— Amazon-Ressourcenname (ARN) des S3-Buckets.
- Besitzer — Kanonische ID des Besitzers des S3-Buckets.

EKSCluster

Details zum Kubernetes-Cluster:

- Name – Name des Kubernetes-Clusters.
- ARN— DieARN, die den Cluster identifiziert.

- Erstellt am – Uhrzeit und Datum des Zeitpunkts, an dem dieser Cluster erstmals erstellt wurde.

  > **Note**
  >
  > Zeitstempel für Ergebnisse in der GuardDuty Konsole werden in Ihrer lokalen Zeitzone angezeigt, während bei JSON Exporten und CLI Ausgaben Zeitstempel in angezeigt werden. UTC

- VPCID — Die ID derVPC, die Ihrem Cluster zugeordnet ist.
- Status – Der aktuelle Status des Clusters.
- Tags – Die Metadaten, die Sie auf den Cluster anwenden, um die Kategorisierung und Organisation zu erleichtern. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, aufgelistet im Format `key:value`. Sie können sowohl den Schlüssel als auch den Wert definieren.

  Cluster-Tags werden nicht auf andere Ressourcen verteilt, die dem Cluster zugeordnet sind.

Details zum Kubernetes-Workload:

- Typ – Der Typ des Kubernetes-Workloads, wie Pod, Bereitstellung und Job.
- Name – Der Name des Kubernetes-Workloads.
- Uid – Die eindeutige ID des Kubernetes-Workloads.
- Erstellt am – Uhrzeit und Datum des Zeitpunkts, an dem dieser Workload erstmals erstellt wurde.
- Labels – Die Schlüssel-Wert-Paare, die dem Kubernetes-Workload angefügt wurden.
- Container – Die Details des Containers, der als Teil des Kubernetes-Workloads ausgeführt wird.
- Namespace – Der Workload gehört zu diesem Kubernetes-Namespace.
- Volumes – Die vom Kubernetes-Workload verwendeten Volumes.
  - Hostpfad – Stellt eine bereits vorhandene Datei oder ein Verzeichnis auf dem Host-Computer dar, dem das Volume zugeordnet ist.
  - Name – Der Name des Volumes.
- Pod-Sicherheitskontext – Definiert die Einstellungen für Rechte und Zugriffskontrolle für alle Container in einem Pod.
- Host-Netzwerk – Auf `true` setzen, wenn die Pods im Kubernetes-Workload enthalten sind.

Kubernetes-Benutzerdetails:

- Gruppen — Kubernetes-Gruppen RBAC (Rollenzugriffsbasierte Steuerung) des Benutzers, der an der Aktivität beteiligt war, die das Ergebnis generiert hat.
- ID – Eindeutige ID des Kubernetes-Benutzers.
- Benutzername – Name des Kubernetes-Benutzers, der an der Aktivität beteiligt war, die das Ergebnis generiert hat.
- Sitzungsname — Entität, die die IAM Rolle mit Kubernetes-Berechtigungen übernommen hat. RBAC

ECSCluster

ECSClusterdetails:

- ARN— DerARN, der den Cluster identifiziert.
- Name – Der Name des Clusters.
- Status – Der aktuelle Status des Clusters.
- Anzahl der aktiven Services – Die Anzahl der Services, die in einem `ACTIVE`-Status auf dem Cluster ausgeführt werden. Sie können diese Dienste mit anzeigen ListServices
- Anzahl registrierter Container-Instances – Die Anzahl der Container-Instances, die im Cluster registriert sind. Dazu gehören Container-Instances sowohl im Status `ACTIVE` als auch im Status `DRAINING`.
- Anzahl der laufenden Aufgaben – Die Anzahl der Aufgaben im Cluster, die sich im `RUNNING`-Status befinden.
- Tags – Die Metadaten, die Sie auf den Cluster anwenden, um die Kategorisierung und Organisation zu erleichtern. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, aufgelistet im Format `key:value`. Sie können sowohl den Schlüssel als auch den Wert definieren.
- Container – Die Details zu dem Container, der der Aufgabe zugeordnet ist:
  - Containername – Der Name des Containers.
  - Container-Image – Das Image des Containers.
- Aufgabendetails – Die Details einer Aufgabe in einem Cluster.
  - ARN— Der Amazon-Ressourcenname (ARN) der Aufgabe.

- Definition ARN — Der Amazon-Ressourcenname (ARN) der Aufgabendefinition, die die Aufgabe erstellt.
- Version – Der Versionszähler für die Aufgabe.
- Aufgabe erstellt am – Der Unix-Zeitstempel für den Erstellungszeitpunkt der Aufgabe.
- Aufgabe gestartet am – Der Unix-Zeitstempel für den Startzeitpunkt der Aufgabe.
- Aufgabe gestartet von – Das Tag, das beim Starten einer Aufgabe angegeben wurde.

Container

Details zum Container:

- Container-Laufzeit – Die Container-Laufzeit (wie z. B. `docker` oder `containerd`), die zum Ausführen des Containers verwendet wurde.
- ID — Die Container-Instance-ID oder vollständige ARN Einträge für die Container-Instance.
- Name – Der Name des Containers.

  Falls verfügbar, zeigt dieses Feld den Wert des Labels `io.kubenetes.container.name` an.
- Image – Das Image der Container-Instance.
- Volume-Mounts – Liste der Volume-Mounts von Containern. Ein Container kann ein Volume unter seinem Dateisystem mounten.
- Sicherheitskontext – Der Sicherheitskontext des Containers definiert Einstellungen für Rechte und Zugriffskontrolle für einen Container.
- Prozessdetails – Beschreibt die Details des Prozesses, der mit der Erkenntnis verknüpft ist.

RDSDBInstance

RDSDBInstanceEinzelheiten:

> **Note**
>
> Diese Ressource ist unter RDS Schutzergebnisse im Zusammenhang mit der Datenbankinstanz verfügbar.

- Datenbank-Instance-ID — Der Identifier, der der Datenbank-Instance zugeordnet ist, die an der GuardDuty Entdeckung beteiligt war.

- Engine – Der Name der Datenbank-Engine der Datenbank-Instance, die an der Erkenntnis beteiligt war. Mögliche Werte sind Aurora My SQL -Compatible oder Aurora Postgre SQL -Compatible.
- Engine-Version — Die Version der Datenbank-Engine, die an der Entdeckung beteiligt war. GuardDuty
- Datenbank-Cluster-ID — Der Bezeichner des Datenbank-Clusters, der die Datenbank-Instance-ID enthält, die an der GuardDuty Suche beteiligt war.
- Datenbankinstanz ARN — DieARN, die die Datenbankinstanz identifiziert, die an der GuardDuty Suche beteiligt war.

Lambda

Details zur Lambda-Funktion

- Funktionsname – Der Name der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- Funktionsversion – Die Version der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- Funktionsbeschreibung – Eine Beschreibung der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- Funktion ARN — Der Amazon-Ressourcenname (ARN) der Lambda-Funktion, die an der Suche beteiligt war.
- Revisions-ID – Die Revisions-ID der Lambda-Funktionsversion.
- Rolle – Die Ausführungsrolle der Lambda-Funktion, die an der Erkenntnis beteiligt ist.
- VPCKonfiguration — Die VPC Amazon-Konfiguration, einschließlich der VPC ID, Sicherheitsgruppe und des Subnetzes, die mit Ihrer Lambda-Funktion IDs verknüpft sind.
- VPCID — Die Amazon-IDVPC, die der Lambda-Funktion zugeordnet ist, die an der Entdeckung beteiligt war.
- Subnetz IDs — Die ID der Subnetze, die Ihrer Lambda-Funktion zugeordnet sind.
- Sicherheitsgruppe – Die Sicherheitsgruppe, die der betroffenen Lambda-Funktion angefügt ist. Dazu gehören der Name und die Gruppen-ID der Sicherheitsgruppe.
- Tags – Eine Liste der Tags, die dieser Ressource angefügt sind, die im Format `key:value` aufgeführt werden.

RDSBenutzerdetails für die Datenbank (DB)

> **Note**
>
> Dieser Abschnitt bezieht sich auf Ergebnisse, die sich ergeben, wenn Sie die RDS Schutzfunktion in aktivieren GuardDuty. Weitere Informationen finden Sie unter GuardDuty RDSSchutz.

Das GuardDuty Ergebnis liefert die folgenden Benutzer- und Authentifizierungsdetails der potenziell gefährdeten Datenbank.

- Benutzer – Der Benutzername, der für den anomalen Anmeldeversuch verwendet wurde.
- Anwendung – Der Anwendungsname, der für den anomalen Anmeldeversuch verwendet wurde.
- Datenbank – Der Name der Datenbank-Instance, die an dem anomalen Anmeldeversuch beteiligt war.
- SSL— Die für das Netzwerk verwendete Version von Secure Socket Layer (SSL).
- Authentifizierungsmethode – Die Authentifizierungsmethode, die von dem Benutzer verwendet wurde, der an der Erkenntnis beteiligt war.

Einzelheiten zur Laufzeitüberwachung

> **Note**
>
> Diese Details sind möglicherweise nur verfügbar, wenn eines der GuardDuty generiert wirdRuntime Monitoring: Typen finden.

Dieser Abschnitt enthält die Laufzeitdetails wie Prozessdetails und den erforderlichen Kontext. Prozessdetails beschreiben Informationen über den beobachteten Prozess und der Laufzeitkontext beschreibt alle zusätzlichen Informationen über die potenziell verdächtige Aktivität.

Details zum Prozess

- Name – Der Name des Prozesses.
- Ausführbarer Pfad – Absoluter Pfad der ausführbaren Zieldatei des Prozesses.

- Executable SHA -256 — Der `SHA256` Hash der ausführbaren Datei des Prozesses.
- Namespace PID — Die Prozess-ID des Prozesses in einem anderen sekundären PID Namespace als dem Namespace auf Host-Ebene. PID Bei Prozessen innerhalb eines Containers ist dies die Prozess-ID, die innerhalb des Containers beobachtet wird.
- Derzeitiges Arbeitsverzeichnis – Das aktuelle Arbeitsverzeichnis des Prozesses.
- Prozess-ID – Die ID, die dem Prozess vom Betriebssystem zugewiesen wurde.
- startTime— Die Uhrzeit, zu der der Prozess gestartet wurde. Dies ist im UTC Datumszeichenfolgenformat (`2023-03-22T19:37:20.168Z`).
- UUID— Die eindeutige ID, die dem Prozess von zugewiesen wurde GuardDuty.
- Parent UUID — Die eindeutige ID des übergeordneten Prozesses. Diese ID wird dem übergeordneten Prozess von zugewiesen GuardDuty.
- Benutzername – Der Benutzername, der den Prozess ausgeführt hat.
- Benutzer-ID – Die Benutzer-ID des Benutzers, der den Prozess ausgeführt hat.
- Effektive Benutzer-ID – Die effektive Benutzer-ID des Prozesses zum Zeitpunkt des Ereignisses.
- Herkunft – Informationen über die Vorfahren des Prozesses.
  - Prozess-ID – Die ID, die dem Prozess vom Betriebssystem zugewiesen wurde.
  - UUID— Die eindeutige ID, die dem Prozess von zugewiesen wurde GuardDuty.
  - Ausführbarer Pfad – Absoluter Pfad der ausführbaren Zieldatei des Prozesses.
  - Effektive Benutzer-ID – Die effektive Benutzer-ID des Prozesses zum Zeitpunkt des Ereignisses.
  - Parent UUID — Die eindeutige ID des übergeordneten Prozesses. Diese ID wird dem übergeordneten Prozess von zugewiesen GuardDuty.
  - Startzeit – Die Uhrzeit, zu der der Prozess gestartet wurde.
  - Namespace PID — Die Prozess-ID des Prozesses in einem anderen sekundären PID Namespace als dem Namespace auf Host-EbenePID. Bei Prozessen innerhalb eines Containers ist dies die Prozess-ID, die innerhalb des Containers beobachtet wird.
  - Benutzer-ID – Die Benutzer-ID des Benutzers, der den Prozess ausgeführt hat.
  - Name – Der Name des Prozesses.

Laufzeitkontext

Aus den folgenden Feldern kann eine generierte Erkenntnis nur die Felder enthalten, die für den Erkenntnistyp relevant sind.

- Mount-Quelle – Der Pfad auf dem Host, der vom Container bereitgestellt wird.
- Mount-Ziel – Der Pfad im Container, der dem Host-Verzeichnis zugeordnet ist.
- Dateisystem-Typ – Stellt den Typ des eingehängten Dateisystems dar.
- Flags – Stellt Optionen dar, die das Verhalten des Ereignisses steuern, das an dieser Erkenntnis beteiligt ist.
- Verändernder Prozess – Informationen über den Prozess, der zur Laufzeit eine Binärdatei, ein Skript oder eine Bibliothek in einem Container erstellt oder geändert hat.
- Geändert am – Der Zeitstempel, zu dem der Prozess zur Laufzeit eine Binärdatei, ein Skript oder eine Bibliothek in einem Container erstellt oder geändert hat. Dieses Feld hat das Format einer UTC Datumszeichenfolge (). `2023-03-22T19:37:20.168Z`
- Bibliothekspfad – Der Pfad zur neuen Bibliothek, die geladen wurde.
- LD-Vorladungs-Wert – Der Wert der `LD_PRELOAD`-Umgebungsvariable.
- Socket-Pfad – Der Pfad zum Docker-Socket, auf den zugegriffen wurde.
- Runc-Binär-Pfad – Der Pfad zur `runc`-Binärdatei.
- Release-Agent-Pfad – Der Pfad zur `cgroup`-Release-Agent-Datei.
- Beispiel für eine Befehlszeile — Das Beispiel der Befehlszeile, die an der potenziell verdächtigen Aktivität beteiligt war.
- Werkzeugkategorie — Kategorie, zu der das Tool gehört. Einige der Beispiele sind Backdoor Tool, Pentest Tool, Network Scanner und Network Sniffer.
- Toolname — Der Name des potenziell gefährlichen Tools.
- Skriptpfad — Der Pfad zu dem ausgeführten Skript, das den Befund generiert hat.
- Pfad der Bedrohungsdatei — Der verdächtige Pfad, für den die Bedrohungsinformationen gefunden wurden.
- Dienstname — Der Name des Sicherheitsdienstes, der deaktiviert wurde.

EBSEinzelheiten zum Scannen von Volumes

> **Note**
>
> Dieser Abschnitt bezieht sich auf Ergebnisse, die sich ergeben, wenn Sie den GuardDuty -initiierten Malware-Scan in Malware-Schutz für EC2 aktivieren.

Der EBS Volumescan liefert Informationen über das EBS Volume, das der potenziell gefährdeten EC2 Instance- oder Container-Workload zugeordnet ist.

- Scan-ID – Die Kennung des Malware-Scans.
- Scan gestartet am – Das Datum und die Uhrzeit, zu der der Malware-Scan gestartet wurde.
- Scan abgeschlossen am – Das Datum und die Uhrzeit, zu der der Malware-Scan abgeschlossen wurde.
- Trigger Finding ID — Die Finde-ID des GuardDuty Fundes, der diesen Malware-Scan ausgelöst hat.
- Quellen — Die möglichen Werte sind `Bitdefender` und`Amazon`.
- Scan-Erkennungen – Die vollständige Ansicht der Details und Ergebnisse jedes Malware-Scans.
  - Anzahl gescannter Objekte – Die Gesamtzahl der gescannten Dateien. Liefert Details wie `totalGb`, `files` und `volumes`.
  - Anzahl der entdeckten Bedrohungen – Die Gesamtzahl der während des Scans erkannten schädlichen `files`.
  - Bedrohungsdetails mit dem höchsten Schweregrad – Die Details der Bedrohung mit dem höchsten Schweregrad, die während des Scans erkannt wurde, und die Anzahl der schädlichen Dateien. Liefert Details wie `severity`, `threatName` und `count`.
  - Nach Namen erkannte Bedrohungen – Das Container-Element, in dem Bedrohungen aller Schweregrade gruppiert werden. Liefert Details wie `itemCount`, `uniqueThreatNameCount`, `shortened` und `threatNames`.

Malware-Schutz zum EC2 Auffinden von Details

> **Note**
>
> Dieser Abschnitt bezieht sich auf Ergebnisse, die sich ergeben, wenn Sie den GuardDuty -initiierten Malware-Scan in Malware-Schutz für EC2 aktivieren.

Wenn der Malware-Schutz für den EC2 Scan Malware erkennt, können Sie die Scandetails anzeigen, indem Sie auf der Seite Ergebnisse in der https://console.aws.amazon.com/guardduty/Konsole den entsprechenden Befund auswählen. Der Schweregrad Ihres EC2 Malware-Schutzes bei der Entdeckung hängt vom Schweregrad des GuardDuty Fundes ab.

> **Note**
>
> Das `GuardDutyFindingDetected`-Tag gibt an, dass die Snapshots Malware enthalten.

Die folgenden Informationen sind im Abschnitt Entdeckte Bedrohungen im Detailbereich verfügbar.

- Name – Der Name der Bedrohung, der durch Gruppierung der Dateien nach Entdeckung ermittelt wurde.
- Schweregrad – Der Schweregrad der erkannten Bedrohung.
- Hash — Der SHA -256 der Datei.
- Dateipfad — Der Speicherort der schädlichen Datei im EBS Volume.
- Dateiname – Der Name der Datei, in der die Bedrohung erkannt wurde.
- Volumen ARN — Das ARN der gescannten EBS Volumes.

Die folgenden Informationen sind im Abschnitt Malware-Scan-Details im Detailbereich verfügbar.

- Scan-ID – Die Kennung des Malware-Scans.
- Scan gestartet am – Das Datum und die Uhrzeit, zu der der Malware-Scan gestartet wurde.
- Scan abgeschlossen am – Das Datum und die Uhrzeit, zu der der Scan abgeschlossen wurde.
- Gescannte Dateien – Die Gesamtzahl der gescannten Dateien und Verzeichnisse.
- Gescannte GB insgesamt – Die Menge an Speicherplatz, die während des Vorgangs gescannt wurde.
- Erkennungs-ID des Auslösers — Die Finde-ID des GuardDuty Fundes, das diesen Malware-Scan ausgelöst hat.
- Die folgenden Informationen sind im Abschnitt Volume-Details im Detailbereich verfügbar.
  - Volume ARN — Der Amazon-Ressourcenname (ARN) des Volumes.
  - Snapshot ARN — Der ARN Snapshot des EBS Volumes.
  - Status – Der Scan-Status des Volumes, z. B. `Running`, `Skipped` und `Completed`.
  - Verschlüsselungstyp – Der Verschlüsselungstyp, der zur Verschlüsselung des Volumes verwendet wird. Beispiel, `CMCMK`.
  - Gerätename – Der Name des Geräts. Beispiel, `/dev/xvda`.

Informationen zum Malware-Schutz für S3

Die folgenden Informationen zum Malware-Scan sind verfügbar, wenn Sie GuardDuty sowohl als auch Malware Protection for S3 in Ihrem aktivieren AWS-Konto:

- Bedrohungen — Eine Liste der Bedrohungen, die während des Malware-Scans erkannt wurden.

  Informationen zur Anzahl der Bedrohungen, die das Ergebnis enthalten kann, finden Sie unterKontingente im Malware-Schutz für S3.
- Elementpfad — Eine Liste mit verschachtelten Elementpfaden und Hash-Details des gescannten S3-Objekts.
  - Verschachtelter Elementpfad — Elementpfad des gescannten S3-Objekts, in dem die Bedrohung erkannt wurde.

    Der Wert dieses Felds ist nur verfügbar, wenn es sich bei dem Objekt der obersten Ebene um ein Archiv handelt und wenn in einem Archiv eine Bedrohung erkannt wurde.
  - Hash — Hash der Bedrohung, die in diesem Ergebnis erkannt wurde.
- Quellen — Die möglichen Werte sind `Bitdefender` und`Amazon`.

Aktion

Die Aktion einer Erkenntnis gibt Details über die Art der Aktivität, durch die das Ergebnis ausgelöst wurde. Die verfügbaren Informationen variieren je nach Aktionstyp.

Aktionstyp – Der Aktivitätstyp der Erkenntnis. Dieser Wert kann NETWORK_ CONNECTION, PORT_ PROBE, DNS_ REQUEST, AWS_ API _ CALL oder RDS_ LOGIN _ seinATTEMPT. Die verfügbaren Informationen variieren je nach Aktionstyp:

- NETWORK_ CONNECTION — Zeigt an, dass Netzwerkverkehr zwischen der identifizierten EC2 Instance und dem Remote-Host ausgetauscht wurde. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - Verbindungsrichtung — Die Netzwerkverbindungsrichtung, die bei der Aktivität beobachtet wurde, die GuardDuty zur Generierung des Ergebnisses geführt hat. Bei ihnen kann es sich um einen der folgenden Werte handeln:
    - INBOUND— Zeigt an, dass ein Remote-Host eine Verbindung zu einem lokalen Port auf der identifizierten EC2 Instanz in Ihrem Konto initiiert hat.

    - OUTBOUND— Zeigt an, dass die identifizierte EC2 Instanz eine Verbindung zu einem Remote-Host initiiert hat.
    - UNKNOWN— Zeigt an, dass die Richtung der Verbindung nicht bestimmt werden GuardDuty konnte.
  - Protokoll — Das Netzwerkverbindungsprotokoll, das bei der Aktivität beobachtet wurde, die GuardDuty zur Generierung des Ergebnisses geführt hat.
  - Lokale IP – Die ursprüngliche Quell-IP-Adresse des Datenverkehrs, der die Erkenntnis ausgelöst hat. Diese Informationen können verwendet werden, um zwischen der IP-Adresse einer Zwischenebene, durch die Datenverkehr fließt, und der ursprünglichen Quell-IP-Adresse des Datenverkehrs , der die Suche ausgelöst hat, zu unterscheiden. Zum Beispiel die IP-Adresse eines EKS Pods im Gegensatz zur IP-Adresse der Instanz, auf der der EKS Pod ausgeführt wird.
  - Blockiert – Gibt an, ob der Ziel-Port blockiert ist.
- PORT_ PROBE — Zeigt an, dass ein Remote-Host die identifizierte EC2 Instanz an mehreren offenen Ports getestet hat. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - Lokale IP – Die ursprüngliche Quell-IP-Adresse des Datenverkehrs, der die Erkenntnis ausgelöst hat. Diese Informationen können verwendet werden, um zwischen der IP-Adresse einer Zwischenebene, durch die Datenverkehr fließt, und der ursprünglichen Quell-IP-Adresse des Datenverkehrs , der die Suche ausgelöst hat, zu unterscheiden. Zum Beispiel die IP-Adresse eines EKS Pods im Gegensatz zur IP-Adresse der Instance, auf der der EKS Pod ausgeführt wird.
  - Blockiert – Gibt an, ob der Ziel-Port blockiert ist.
- DNS_ REQUEST — Zeigt an, dass die identifizierte EC2 Instanz einen Domainnamen abgefragt hat. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - Protokoll — Das Netzwerkverbindungsprotokoll, das bei der Aktivität beobachtet wurde, die GuardDuty zur Generierung des Ergebnisses führte.
  - Blockiert – Gibt an, ob der Ziel-Port blockiert ist.
- AWS_ API _ CALL — Zeigt an, dass ein aufgerufen AWS API wurde. Dieser Aktionstyp enthält die folgenden zusätzlichen Informationen:
  - API— Der Name der API Operation, die aufgerufen und somit GuardDuty zur Generierung dieses Ergebnisses aufgefordert wurde.

> **Note**
>
> Diese Operationen können auch API Ereignisse umfassen, die nicht von AWS CloudTrail erfasst wurden. Weitere Informationen finden Sie unter Nicht- API Ereignisse erfasst von CloudTrail.

  - Benutzeragent — Der Benutzeragent, der die API Anfrage gestellt hat. Dieser Wert gibt an, ob der Anruf von AWS Management Console, einem AWS Dienst AWS SDKs, dem oder dem getätigt wurde AWS CLI.
  - ERRORCODE— Wenn das Ergebnis durch einen fehlgeschlagenen API Anruf ausgelöst wurde, wird der Fehlercode für diesen Anruf angezeigt.
  - Dienstname — Der DNS Name des Dienstes, der versucht hat, den API Anruf zu tätigen, der den Befund ausgelöst hat.
- RDS_ LOGIN _ ATTEMPT — Zeigt an, dass von einer Remote-IP-Adresse aus ein Anmeldeversuch bei der potenziell gefährdeten Datenbank unternommen wurde.
  - IP-Adresse – Die Remote-IP-Adresse, die für den potenziell verdächtigen Anmeldeversuch verwendet wurde.

Akteur oder Ziel

Eine Erkenntnis verfügt über den Abschnitt Actor, wenn die Ressourcenrolle `TARGET` war. Dies zeigt an, dass verdächtige Aktivitäten auf Ihre Ressource ausgerichtet waren, und der Abschnitt Actor enthält Details zur Entität, von der diese auf Ihre Ressource ausgerichtet wurden.

Eine Erkenntnis hat einen Ziel-Abschnitt, wenn die Ressourcenrolle `ACTOR` lautete. Dies zeigt an, dass Ihre Ressource an verdächtigen Aktivitäten gegen einen Remote-Host beteiligt war. Dieser Abschnitt enthält Informationen zur IP-Adresse und/oder Domain, auf die Ihre Ressource ausgerichtet ist.

Im Abschnitt Actor oder Ziel können folgende Informationen verfügbar sein:

- Verbunden — Gibt an, ob das AWS Konto des API Remote-Anrufers mit Ihrer GuardDuty Umgebung in Verbindung steht. Wenn dieser Wert ist`true`, ist der API Anrufer in irgendeiner Weise mit Ihrem Konto verbunden. Falls `false` der API Anrufer von außerhalb Ihrer Umgebung stammt.

- Remote-Konto-ID — Die Konto-ID, der die ausgehende IP-Adresse gehört, die für den Zugriff auf die Ressource im endgültigen Netzwerk verwendet wurde.
- IP-Adresse — Die IP-Adresse, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Standort — Standortinformationen für die IP-Adresse, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Organisation — Informationen zur ISP Organisation der IP-Adresse, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Port — Die Portnummer, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Domain — Die Domain, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Domain mit Suffix — Die Domain der zweiten und obersten Ebene, die an einer Aktivität beteiligt war, die möglicherweise GuardDuty zur Generierung des Ergebnisses geführt hat. Eine Liste der Domänen der obersten und zweiten Ebene finden Sie in der Liste der öffentlichen Suffixe.

Zusätzliche Informationen

Alle Erkenntnisse verfügen über einen Abschnitt Zusätzliche Informationen, der die folgenden Informationen enthalten kann:

- Name der Bedrohungsliste — Der Name der Bedrohungsliste, die die IP-Adresse oder den Domainnamen enthält, der an der Aktivität beteiligt war, die GuardDuty zur Generierung des Fundes geführt hat.
- Beispiel – Der Wert Wahr oder Falsch, gibt an, ob es sich um ein Beispiel-Erkenntnis handelt.
- Archiviert – Der Wert Wahr oder Falsch, gibt an, ob diese Erkenntnis archiviert wurde.
- Ungewöhnlich – Aktivitätsdetails, die zuvor noch nicht beobachtet wurden. Dazu können ein ungewöhnlicher (zuvor nicht beobachteter) Benutzer, ein ungewöhnlicher Ort, eine Uhrzeit, ein Bucket, ein Anmeldeverhalten oder eine ASN Organisation gehören.
- Ungewöhnliches Protokoll — Das Netzwerkverbindungsprotokoll, das an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.
- Agentendetails — Details über den Security Agent, der derzeit auf dem EKS Cluster in Ihrem installiert ist AWS-Konto. Dies gilt nur für Findetypen von EKS Runtime Monitoring.
  - Agent-Version — Die Version des GuardDuty Security Agents.

- Agenten-ID — Die eindeutige Kennung des GuardDuty Security Agents.

Beweise

Erkenntnisse, die auf Bedrohungsinformationen basieren, haben einen Abschnitt Beweise, der die folgenden Informationen enthält:

- Informationen zur Bedrohungsinformation — Der Name der Bedrohungsliste, auf der die erkannte Bedrohung `Threat name` erscheint.
- Name der Bedrohung — Der Name der Malware-Familie oder eine andere Kennung, die mit der Bedrohung verknüpft ist.
- Bedrohungsdatei SHA256 — SHA256 der Datei, die den Befund generiert hat.

Anormales Verhalten

Arten von Ergebnissen, die AnomalousBehaviorauf Folgendes enden, weisen darauf hin, dass der Befund durch das ML-Modell (Machine Learning) zur Erkennung von GuardDuty Anomalien generiert wurde. Das ML-Modell bewertet alle API Anfragen an Ihr Konto und identifiziert ungewöhnliche Ereignisse, die im Zusammenhang mit den Taktiken der Gegner stehen. Das ML-Modell verfolgt verschiedene Faktoren der API Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und den spezifischen Typ, der angefordert wurde. API

Einzelheiten darüber, welche Faktoren der API Anfrage für die CloudTrail Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails. Die Identitäten werden durch das CloudTrail userIdentity Element definiert, und die möglichen Werte sind:`Root`,,`IAMUser`, `AssumedRole` `FederatedUser``AWSAccount`, oder. `AWSService`

Zusätzlich zu den verfügbaren Informationen zu allen GuardDuty Ergebnissen, die mit API Aktivitäten in Verbindung stehen, enthalten die AnomalousBehaviorErgebnisse zusätzliche Details, die im folgenden Abschnitt beschrieben werden. Diese Details können in der Konsole eingesehen werden und sind auch in den Ergebnissen verfügbarJSON.

- Anomal APIs — Eine Liste von API Anfragen, die von der Benutzeridentität in der Nähe der primären API Anfrage aufgerufen wurden, die mit dem Ergebnis verknüpft ist. In diesem Bereich werden die Details des API Ereignisses wie folgt weiter aufgeschlüsselt.

- Bei der ersten API Liste handelt es sich um die primäre API AnfrageAPI, die mit der beobachteten Aktivität mit dem höchsten Risiko verknüpft ist. Dies ist diejenigeAPI, die den Befund ausgelöst hat und mit der Angriffsphase des Befundtyps korreliert. Dies ist auch API das, was im Abschnitt Aktion in der Konsole und in den Ergebnissen detailliert beschrieben wird. JSON
- Bei allen anderen APIs aufgelisteten Benutzern handelt es sich um weitere Anomalien APIs im Vergleich zur aufgelisteten Benutzeridentität, die in der Nähe des primären Benutzers beobachtet wurden. API Wenn nur eine Benutzeridentität API auf der Liste steht, hat das ML-Modell keine zusätzlichen API Anfragen von dieser Benutzeridentität als anomal identifiziert.
- Die Liste von APIs ist danach unterteilt, ob eine erfolgreich aufgerufen API wurde oder ob eine nicht erfolgreich aufgerufen API wurde, was bedeutet, dass eine Fehlerantwort empfangen wurde. Die Art der empfangenen Fehlerantwort ist über jeder erfolglos aufgerufenen Antwort aufgeführt. API Mögliche Fehlerantworttypen sind: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` und `operation not permitted`.
- APIswerden nach dem zugehörigen Dienst kategorisiert.
- Wenn Sie mehr Kontext benötigen, wählen Sie „Historisch“ aus, APIs um die wichtigsten Informationen zu sehenAPIs, bis zu einem Maximum von 20, die in der Regel sowohl für die Benutzeridentität als auch für alle Benutzer innerhalb des Kontos angezeigt werden. Sie APIs sind als Selten (weniger als einmal pro Monat), Selten (einige Male im Monat) oder Häufig (täglich bis wöchentlich) gekennzeichnet, je nachdem, wie oft sie in Ihrem Konto verwendet werden.

- Ungewöhnliches Verhalten (Konto) – In diesem Abschnitt finden Sie zusätzliche Informationen zum profilierten Verhalten Ihres Kontos.

> **Profiliertes Verhalten**
>
> GuardDuty erfährt anhand der bereitgestellten Ereignisse kontinuierlich mehr über die Aktivitäten in Ihrem Konto. Diese Aktivitäten und ihre beobachtete Häufigkeit werden als profiliertes Verhalten bezeichnet.

Zu den in diesem Bereich erfassten Informationen gehören:

- ASNOrg — Die ASN Organisation, von der aus der anomale API Anruf getätigt wurde.
- Benutzername — Der Name des Benutzers, der den ungewöhnlichen Anruf getätigt hat. API

  - Benutzeragent — Der Benutzeragent, der für den anomalen API Anruf verwendet wurde. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `aws-cli` oder `Botocore`.
  - Benutzertyp — Der Benutzertyp, der den anomalen API Anruf getätigt hat. Mögliche Werte sind `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` oder `ROLE`.
  - Bucket – Der Name des S3-Buckets, auf den zugegriffen wurde.
- Ungewöhnliches Verhalten (Benutzeridentität) – Dieser Abschnitt enthält zusätzliche Informationen zum profilierten Verhalten der Benutzeridentität, die an der Erkenntnis beteiligt war. Wenn ein Verhalten nicht als historisch identifiziert wurde, bedeutet dies, dass das GuardDuty ML-Modell diese Benutzeridentität während des Trainingszeitraums noch nicht auf diese Weise API aufgerufen hat. Die folgenden zusätzlichen Details zur Benutzeridentität sind verfügbar:
  - ASNOrg — Die ASN Organisation, von der aus der anomale API Aufruf getätigt wurde.
  - Benutzeragent — Der Benutzeragent, mit dem der anomale API Anruf getätigt wurde. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `aws-cli` oder `Botocore`.
  - Bucket – Der Name des S3-Buckets, auf den zugegriffen wurde.
- Ungewöhnliches Verhalten (Bucket) – Dieser Abschnitt enthält zusätzliche Informationen zum profilierten Verhalten des S3-Buckets, der mit der Erkenntnis verknüpft ist. Wenn ein Verhalten nicht als historisch identifiziert wurde, bedeutet dies, dass das GuardDuty ML-Modell innerhalb des Trainingszeitraums noch keine API Aufrufe an diesen Bucket auf diese Weise gesehen hat. Zu den in diesem Bereich erfassten Informationen gehören:
  - ASNOrg — Die ASN Organisation, von der aus der anomale API Anruf getätigt wurde.
  - Benutzername — Der Name des Benutzers, der den ungewöhnlichen Anruf getätigt hat. API
  - Benutzeragent — Der Benutzeragent, der für den anomalen API Anruf verwendet wurde. Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `aws-cli` oder `Botocore`.
  - Benutzertyp — Der Benutzertyp, der den anomalen API Anruf getätigt hat. Mögliche Werte sind `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` oder `ROLE`.

> **Note**
>
> Weitere Informationen zu historischen Verhaltensweisen finden Sie unter Historisches Verhalten in den Abschnitten Ungewöhnliches Verhalten (Konto), Benutzer-ID oder Bucket, wo Sie Details zum erwarteten Verhalten in Ihrem Konto für jede der folgenden Kategorien

anzeigen können: Selten (weniger als einmal pro Monat), Gelegentlich (einige Male pro Monat) oder Häufig (täglich bis wöchentlich), je nachdem, wie oft sie in Ihrem Konto verwendet werden.

- Ungewöhnliches Verhalten (Datenbank) – Dieser Abschnitt enthält zusätzliche Informationen zum profilierten Verhalten der Datenbank-Instance, das mit der Erkenntnis verknüpft ist. Wenn ein Verhalten nicht als historisch identifiziert wird, bedeutet dies, dass das GuardDuty ML-Modell innerhalb des Trainingszeitraums noch keinen Anmeldeversuch auf diese Weise bei dieser Datenbankinstanz festgestellt hat. Zu den Informationen, die für diesen Abschnitt im Erkenntnisbereich verfolgt werden, gehören:
  - Benutzer – Der Benutzername, der für den anomalen Anmeldeversuch verwendet wurde.
  - ASNOrganisation — Die ASN Organisation, von der aus der ungewöhnliche Anmeldeversuch unternommen wurde.
  - Anwendung – Der Anwendungsname, der für den anomalen Anmeldeversuch verwendet wurde.
  - Datenbank – Der Name der Datenbank-Instance, die an dem anomalen Anmeldeversuch beteiligt war.

  Der Abschnitt Historisches Verhalten bietet mehr Kontext zu den zuvor beobachteten Benutzernamen, ASNOrganisationen, Anwendungsnamen und Datenbanknamen für die zugehörige Datenbank. Jedem Einzelwert ist eine Anzahl zugeordnet, die angibt, wie oft dieser Wert bei einer erfolgreichen Anmeldung beobachtet wurde.
- Ungewöhnliches Verhalten (Konto-Kubernetes-Cluster, Kubernetes-Namespace und Kubernetes-Benutzername) – In diesem Abschnitt finden Sie zusätzliche Informationen zum profilierten Verhalten des Kubernetes-Clusters und des mit der Erkenntnis verbundenen Namespaces. Wenn ein Verhalten nicht als historisch identifiziert wird, bedeutet dies, dass das GuardDuty ML-Modell dieses Konto, diesen Cluster, diesen Namespace oder diesen Benutzernamen zuvor nicht auf diese Weise beobachtet hat. Zu den Informationen, die für diesen Abschnitt im Erkenntnisbereich verfolgt werden, gehören:
  - Benutzername — Der Benutzer, der das mit dem Ergebnis API verknüpfte Kubernetes aufgerufen hat.
  - Impersonierter Nutzername – Der Benutzer, für den sich `username` ausgibt.
  - Namespace — Der Kubernetes-Namespace innerhalb des EKS Amazon-Clusters, in dem die Aktion stattgefunden hat.
  - User Agent — Der Benutzeragent, der dem Kubernetes-Aufruf zugeordnet ist. API Der Benutzeragent ist die Methode, mit der der Aufruf ausgeführt wird, z. B. `kubectl`.

- API— Die Kubernetes, die `username` innerhalb des EKS Amazon-Clusters API aufgerufen wurden.
- ASNInformationen — Die ASN Informationen, wie Organisation undISP, die mit der IP-Adresse des Benutzers verknüpft sind, der diesen Anruf tätigt.
- Wochentag — Der Wochentag, an dem der API Kubernetes-Anruf getätigt wurde.
- Erlaubnis — Das Kubernetes-Verb und die Ressource, die auf Zugriff geprüft werden, um anzugeben, ob sie Kubernetes verwenden `username` können oder nicht. API
- Dienstkontoname — Das dem Kubernetes-Workload zugeordnete Dienstkonto, das dem Workload eine Identität verleiht.
- Registrierung — Die Container-Registry, die dem Container-Image zugeordnet ist, das im Kubernetes-Workload bereitgestellt wird.
- Image — Das Container-Image ohne die zugehörigen Tags und Digest, das im Kubernetes-Workload bereitgestellt wird.
- Image-Präfix-Konfiguration — Das Image-Präfix mit aktivierter Container- und Workload-Sicherheitskonfiguration, z. B. `hostNetwork` oder`privileged`, für den Container, der das Image verwendet.
- Betreffname — Die Subjekte, wie z. B. a `usergroup`, oder, `serviceAccountName` die an eine Referenzrolle in einem `RoleBinding` oder gebunden sind`ClusterRoleBinding`.
- Rollenname — Der Name der Rolle, die an der Erstellung oder Änderung von Rollen beteiligt ist, oder `roleBinding` API

Volumenbezogene S3-Anomalien

In diesem Abschnitt werden die Kontextinformationen für volumenbasierte S3-Anomalien detailliert beschrieben. Das volumenbasierte Ergebnis (Exfiltration:S3/AnomalousBehavior) sucht nach ungewöhnlich vielen API S3-Aufrufen von Benutzern an die S3-Buckets, was auf eine mögliche Datenexfiltration hindeutet. Die folgenden API S3-Aufrufe werden im Hinblick auf die volumenabhängige Erkennung von Anomalien überwacht.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Die folgenden Metriken würden dabei helfen, eine Grundlage für das übliche Verhalten zu schaffen, wenn eine IAM Entität auf einen S3-Bucket zugreift. Um Datenexfiltration zu erkennen, werden bei der volumenbasierten Erkennung von Anomalien alle Aktivitäten anhand der üblichen Verhaltensgrundlagen bewertet. Wählen Sie die Option Historisches Verhalten in den Abschnitten Ungewöhnliches Verhalten (Benutzeridentität), Beobachtetes Volumen (Benutzeridentität) und Beobachtetes Volumen (Bucket) aus, um jeweils die folgenden Metriken anzuzeigen.

- Anzahl der vom IAM Benutzer oder der IAM Rolle aufgerufenen `s3-api-name` API Aufrufe (hängt davon ab, welcher ausgelöst wurde), die mit dem betroffenen S3-Bucket in den letzten 24 Stunden verknüpft sind.
- Anzahl der vom IAM Benutzer oder der IAM Rolle aufgerufenen `s3-api-name` API Aufrufe (hängt davon ab, welcher ausgelöst wurde), die allen S3-Buckets in den letzten 24 Stunden zugeordnet wurden.
- Anzahl der `s3-api-name` API Aufrufe für alle IAM Benutzer oder IAM Rollen (hängt davon ab, welcher ausgelöst wurde), die mit dem betroffenen S3-Bucket in den letzten 24 Stunden verknüpft waren.

RDSAnomalien aufgrund von Anmeldeaktivitäten

In diesem Abschnitt wird die Anzahl der Anmeldeversuche des ungewöhnlichen Akteurs detailliert beschrieben und nach den Ergebnissen der Anmeldeversuche gruppiert. Die Erkenntnistypen für RDS Protection identifizieren anomales Verhalten, indem sie die Anmeldeereignisse auf ungewöhnliche Muster von `successfulLoginCount`, `failedLoginCount` und `incompleteConnectionCount` überwachen.

- successfulLoginCount— Dieser Zähler stellt die Summe der erfolgreichen Verbindungen (richtige Kombination von Anmeldeattributen) dar, die der ungewöhnliche Akteur mit der Datenbankinstanz hergestellt hat. Zu den Anmeldeattributen gehören Benutzername, Passwort und Datenbankname.
- failedLoginCount— Dieser Zähler stellt die Summe der fehlgeschlagenen (erfolglosen) Anmeldeversuche dar, die unternommen wurden, um eine Verbindung zur Datenbankinstanz herzustellen. Dies weist darauf hin, dass ein oder mehrere Attribute der Anmeldekombination, wie Benutzername, Passwort oder Datenbankname, falsch waren.
- incompleteConnectionCount— Dieser Zähler stellt die Anzahl der Verbindungsversuche dar, die nicht als erfolgreich oder gescheitert eingestuft werden können. Diese Verbindungen werden geschlossen, bevor die Datenbank eine Antwort liefert. Beispielsweise Port-Scanning, bei dem der Datenbank-Port zwar verbunden ist, aber keine Information an die Datenbank gesendet wird,

oder die Verbindung vor Abschluss der Anmeldung entweder erfolgreich oder fehlgeschlagen abgebrochen wurde.

GuardDuty Aggregation finden

Alle Ergebnisse sind dynamisch, d. h., wenn eine neue Aktivität im Zusammenhang mit demselben Sicherheitsproblem GuardDuty erkannt wird, wird das ursprüngliche Ergebnis mit den neuen Informationen aktualisiert, anstatt ein neues Ergebnis zu generieren. Dieses Verhalten ermöglicht es Ihnen, laufende Probleme zu identifizieren, ohne mehrere ähnliche Berichte durchsehen zu müssen, und reduziert insgesamt das ausgelöste Rauschen durch Sicherheitsprobleme, die Ihnen bereits bekannt sind.

Zum Beispiel werden bei einer `UnauthorizedAccess:EC2/SSHBruteForce`-Erkenntnis mehrere Zugriffsversuche auf Ihre Instance unter derselben Erkenntnis-ID zusammengefasst, wodurch sich die Anzahl in den Details der Erkenntnis erhöht. Dies liegt daran, dass es sich bei diesem Ergebnis um ein einzelnes Sicherheitsproblem handelt, bei dem die Instance darauf hinweist, dass der SSH Port auf der Instance nicht ordnungsgemäß gegen diese Art von Aktivität geschützt ist. Wenn jedoch eine SSH Zugriffsaktivität GuardDuty erkannt wird, die auf eine neue Instance in Ihrer Umgebung abzielt, wird ein neues Ergebnis mit einer eindeutigen Finde-ID erstellt, um Sie darauf aufmerksam zu machen, dass mit der neuen Ressource ein Sicherheitsproblem verbunden ist.

Wenn eine Erkenntnis aggregiert wird, wird sie mit Informationen aus dem letzten Ereignis dieser Aktivität aktualisiert. Das bedeutet, dass im obigen Beispiel, wenn Ihre Instance das Ziel eines Brute-Force-Versuchs von einem neuen Akteur ist, die Erkenntnisdetails aktualisiert werden, um die Remote-IP der jüngsten Quelle wiederzugeben, und ältere Informationen ersetzt werden. Vollständige Informationen zu einzelnen Aktivitätsversuchen sind weiterhin in Ihren Logs CloudTrail oder VPC Flow Logs verfügbar.

Die Kriterien, GuardDuty nach denen ein neues Ergebnis generiert wird, anstatt ein vorhandenes zu aggregieren, hängen vom Befundtyp ab. Die Aggregationskriterien für jeden Ergebnistyp werden von unseren Sicherheitstechnikern festgelegt, um Ihnen den besten Überblick über verschiedene Sicherheitsprobleme in Ihrem Konto zu geben.

Erkenntnistypen

Informationen zu wichtigen Änderungen an den GuardDuty Befundtypen, einschließlich neu hinzugefügter oder zurückgezogener Befundtypen, finden Sie unterDokumentenverlauf für Amazon GuardDuty.

Hinweise zu Erkenntnis-Typen, die nun außer Betrieb genommen wurden, finden Sie unter Nicht mehr aktive Erkenntnistypen.

ECGuardDuty EC2Erkenntnistypen

Die folgenden Erkenntnisse sind spezifisch für Amazon-EC2-Ressourcen und haben immer einen Ressourcentyp von `Instance`. Der Schweregrad und die Details der Erkenntnisse unterscheiden sich je nach Ressourcenrolle, die angibt, ob die EC2-Instance das Ziel verdächtiger Aktivitäten war oder der Akteur, der die Aktivitäten durchführte.

Die hier aufgeführten Erkenntnisse beinhalten die Datenquellen und Modelle, die zur Generierung dieses Erkenntnistyps verwendet wurden. Weitere Informationen zu Datenquellen und Modellen finden Sie unter GuardDuty grundlegende Datenquellen.

> **Note**
>
> Bei einigen EC2-Erkenntnissen fehlen möglicherweise Instance-Details, wenn die Instance bereits beendet wurde oder wenn der zugrunde liegende API-Aufruf Teil eines regionenübergreifenden API-Aufrufs war, der von einer EC2-Instance in einer anderen Region ausging.

Für alle EC2-Erkenntnisse wird empfohlen, die betreffende Ressource zu untersuchen, um festzustellen, ob sie sich erwartungsgemäß verhält. Wenn die Aktivität autorisiert ist, können Sie Unterdrückungsregeln oder Listen vertrauenswürdiger IP-Adressen verwenden, um Falschmeldungen für diese Ressource zu verhindern. Wenn die Aktivität unerwartet auftritt, besteht die bewährte Sicherheitsmethode darin, davon auszugehen, dass die Instance kompromittiert wurde, und die unter Behebung einer potenziell gefährdeten Amazon-Instance EC2 beschriebenen Aktionen auszuführen.

Themen

- Backdoor:EC2/C&CActivity.B

- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS

- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

Eine EC2-Instance fragt eine IP-Adresse ab, die einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Instance in Ihrer AWS-Umgebung eine IP-Adresse abfragt, der einem bekannten Command-and-Control (C&C)-Server zugeordnet ist. Die aufgeführte Instance ist möglicherweise kompromittiert. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen DDoS (Distributed Denial of Service)-Angriff zu starten.

> **Note**
>
> Wenn die abgefragte IP log4j-bezogen ist, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:

- service.additionalInfo .threatListName = Amazon
- service.additionalInfo.ThreatName = Log4j-bezogen

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Backdoor:EC2/C&CActivity.B!DNS

Eine EC2-Instance fragt einen Domainnamen ab, der einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Instance in Ihrer AWS-Umgebung einen Domainnamen abfragt, der einem bekannten Command-and-Control (C&C)-Server zugeordnet ist. Die aufgeführte Instance ist möglicherweise kompromittiert. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen DDoS (Distributed Denial of Service)-Angriff zu starten.

> **Note**
>
> Wenn der abgefragte Domainname mit log4j zu tun hat, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:
>
> - service.additionalInfo .threatListName = Amazon

- service.additionalInfo.ThreatName = Log4j-bezogen

> **Note**
>
> Um zu testen, wie diesen Erkenntnistyp GuardDuty generiert, können Sie eine DNS-Anfrage von Ihrer Instance (mit `dig` für Linux oder `nslookup` für Windows) gegen eine Testdomäne stellen`guarddutyc2activityb.com`.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Backdoor:EC2/DenialOfService.Dns

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des DNS-Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine große Menge ausgehenden DNS-Datenverkehrs generiert. Dies kann darauf hinweisen, dass die aufgeführte Instance kompromittiert ist und mithilfe des DNS-Protokolls zur Durchführung von denial-of-service (DoS-)Angriffen verwendet wird.

> **Note**
>
> Dieses Ergebnis erkennt nur DoS-Angriffe gegen öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Backdoor:EC2/DenialOfService.Tcp

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des TCP-Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine große Menge ausgehenden TCP-Datenverkehrs generiert. Dies kann darauf hinweisen, dass die Instance kompromittiert ist und mithilfe des TCP-Protokolls zur Durchführung von denial-of-service (DoS-)Angriffen verwendet wird.

> **Note**
>
> Dieses Ergebnis erkennt nur DoS-Angriffe gegen öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Backdoor:EC2/DenialOfService.Udp

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des UDP-Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine große Menge ausgehenden UDP-Datenverkehrs generiert. Dies kann darauf hinweisen, dass die aufgeführte Instance kompromittiert ist und mithilfe des UDP-Protokolls zur Durchführung von denial-of-service (DoS-)Angriffen verwendet wird.

> **Note**
>
> Dieses Ergebnis erkennt nur DoS-Angriffe gegen öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe des UDP-Protokolls auf einem TCP-Port genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine große Menge ausgehenden UDP-Datenverkehrs generiert, der auf einen Port zielt, der normalerweise für die TCP-Kommunikation verwendet wird. Dies kann darauf hinweisen, dass die aufgeführte Instance kompromittiert ist und verwendet wird, um einen denial-of-service (DoS)-Angriff mit dem UDP-Protokoll auf einem TCP-Port durchzuführen.

> **Note**
>
> Dieses Ergebnis erkennt nur DoS-Angriffe gegen öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Backdoor:EC2/DenialOfService.UnusualProtocol

Das Verhalten einer EC2-Instance weist darauf hin, dass sie möglicherweise gerade für die Ausführung eines Denial-of-Service (DoS)-Angriffs mithilfe eines ungewöhnlichen Protokolls genutzt wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine große Menge ausgehenden Datenverkehrs eines ungewöhnlichen Protokolltyps generiert, der normalerweise nicht von EC2-Instances verwendet wird (beispielsweise ein Internet Group Management Protocol). Dies kann darauf hinweisen, dass die Instance kompromittiert ist und verwendet wird, um denial-of-service (DoS)-Angriffe mit einem ungewöhnlichen Protokoll durchzuführen. Dieses Ergebnis erkennt nur DoS-Angriffe gegen öffentlich routingfähige IP-Adressen, die das primäre Ziel von DoS-Angriffen sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Backdoor:EC2/Spambot

Eine EC2-Instance zeigt ungewöhnliches Verhalten, indem sie mit einem Remote-Host auf Port 25 kommuniziert.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung mit einem Remote-Host auf Port 25 kommuniziert. Dieses Verhalten ist ungewöhnlich, da die betreffende EC2-Instance zuvor nicht über Port 25 kommuniziert hat. Port 25 wird in der Regel von Mailservern für die SMTP-Kommunikation verwendet. Dieses Ergebnis weist darauf hin, dass Ihre EC2-Instance für den Einsatz beim Versenden von Spam möglicherweise kompromittiert ist.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Behavior:EC2/NetworkPortUnusual

Eine EC2-Instance kommuniziert auf einem unüblichen Serverport mit einem Remote-Host.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat früher nicht auf diesem Remote-Port kommuniziert.

> **Note**
>
> Wenn die EC2-Instance über Port 389 oder Port 1389 kommuniziert hat, wird der zugehörige Erkenntnis-Schweregrad auf Hoch geändert, und die Erkenntnisfelder enthalten den folgenden Wert:
>
> - service.additionalInfo.context = Möglicher log4j-Rückruf

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Behavior:EC2/TrafficVolumeUnusual

Eine EC2-Instance generiert ungewöhnlich große Mengen an Netzwerkdatenverkehr zu einem Remote-Host.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat bisher nicht derart viel Datenverkehr an diesen Remote-Host gesendet.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

CryptoCurrency:EC2/BitcoinTool.B

Eine EC2-Instance fragt eine IP-Adresse ab, die mit einer Aktivität in Zusammenhang mit einer Kryptowährung steht.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung eine IP-Adresse abfragt, die mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bitcoin ist ein weltweites Kryptowährungs- und digitales Zahlungssystem, das gegen andere Währungen, Produkte und Services eingetauscht werden kann. Bitcoin ist eine Belohnung für das Bitcoin-Mining und bei Bedrohungsakteuren sehr gefragt.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `CryptoCurrency:EC2/BitcoinTool.B` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

CryptoCurrency:EC2/BitcoinTool.B!DNS

Eine EC2-Instance fragt einen Domainnamen ab, der mit einer Aktivität in Zusammenhang mit einer Kryptowährung steht.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen abfragt, die mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bitcoin ist ein weltweites Kryptowährungs- und digitales Zahlungssystem, das gegen andere Währungen, Produkte und Services eingetauscht werden kann. Bitcoin ist eine Belohnung für das Bitcoin-Mining und bei Bedrohungsakteuren sehr gefragt.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `CryptoCurrency:EC2/BitcoinTool.B!DNS` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

DefenseEvasion:EC2/UnusualDNSResolver

Eine Amazon-EC2-Instance kommuniziert mit einem ungewöhnlichen öffentlichen DNS-Resolver.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat in letzter Zeit nicht mit diesem öffentlichen DNS-Resolver kommuniziert. Das Feld Unüblich im Bereich mit den Erkenntnisdetails in der GuardDuty Konsole kann Informationen über den abgefragten DNS-Resolver bereitstellen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

DefenseEvasion:EC2/UnusualDoHActivity

Eine Amazon-EC2-Instance führt eine ungewöhnliche DNS-über-HTTPS-Kommunikation (DoH) durch.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat in letzter Zeit keine DNS-über-HTTPS-Kommunikation (DoH) mit diesem öffentlichen DoH-Server durchgeführt. Das Feld Ungewöhnlich in den Erkenntnisdetails kann Informationen über den abgefragten DoH-Server enthalten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

DefenseEvasion:EC2/UnusualDoTActivity

Eine Amazon-EC2-Instance führt eine ungewöhnliche DNS-über-TLS-Kommunikation (DoT) durch.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung ein Verhalten zeigt, das von ihrem normalen Verhalten abweicht. Diese EC2-Instance hat in letzter Zeit keine DNS-über-TLS-Kommunikation (DoT) mit diesem öffentlichen DoT-Server durchgeführt. Das Feld Ungewöhnlich in den Erkenntnisdetails kann Informationen über den abgefragten DoT-Server enthalten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Impact:EC2/AbusedDomainRequest.Reputation

Eine EC2-Instance fragt einen Domainnamen mit geringer Reputation ab, der mit bekanntermaßen missbrauchten Domains in Verbindung steht.

Standard-Schweregrad: Mittel

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit bekannten missbrauchten Domains oder IP-Adressen in Verbindung steht. Beispiele für missbrauchte Domains sind Top-

Level-Domainnamen (TLDs) und Second-Level-Domainnamen (2LDs), die kostenlose Subdomain-Registrierungen bieten, sowie dynamische DNS-Anbieter. Bedrohungsakteure nutzen diese Services in der Regel, um Domains kostenlos oder zu geringen Kosten zu registrieren. Bei Domains mit geringer Reputation in dieser Kategorie kann es sich auch um abgelaufene Domains handeln, die auf die Parking-IP-Adresse eines Registrars zurückgehen und daher möglicherweise nicht mehr aktiv sind. Bei einer Parking-IP leitet ein Registrar den Verkehr für Domains weiter, die mit keinem Service verknüpft wurden. Die aufgeführte Amazon-EC2-Instance kann kompromittiert sein, da Bedrohungsakteure diese Registrare oder Services häufig für C&C und die Verbreitung von Malware nutzen.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Impact:EC2/BitcoinDomainRequest.Reputation

Eine EC2-Instance fragt einen Domainnamen ab, der mit einer Aktivität in Zusammenhang mit einer Kryptowährung steht.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Dieses Ergebnis informiert Sie, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bitcoin ist ein weltweites Kryptowährungs- und digitales Zahlungssystem, das gegen andere Währungen, Produkte und Services eingetauscht werden kann. Bitcoin ist eine Belohnung für das Bitcoin-Mining und bei Bedrohungsakteuren sehr gefragt.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2-Instance verwenden, um Kryptowährung zu minen oder zu verwalten, oder diese Instance anderweitig an der Blockchain-Aktivität beteiligt ist, könnte diese Erkenntnis erwartete Aktivitäten für Ihre Umgebung repräsentieren. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Impact:EC2/BitcoinDomainRequest.Reputation` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Impact:EC2/MaliciousDomainRequest.Reputation

Eine EC2-Instance fragt eine Domain mit niedriger Reputation ab, die mit bekannten bösartigen Domains in Verbindung stehen.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit bekannten bösartigen Domains oder IP-Adressen in Verbindung stehen. Beispielsweise können Domains mit einer bekannten Sinkhole-IP-Adresse verknüpft sein. Sinkhole-Domains sind Domains, die zuvor von einem Bedrohungsakteur kontrolliert wurden, und Anfragen an sie können darauf hinweisen, dass die Instance kompromittiert wurde. Diese Domains können auch mit bekannten böswilligen Kampagnen oder Algorithmen zur Domain-Generierung korreliert sein.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Impact:EC2/PortSweep

Eine EC2-Instance untersucht einen Port auf einer großen Anzahl von IP-Adressen.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung einen Port auf einer großen Anzahl von öffentlich routingfähige IP-Adressen untersucht. Diese Art von Aktivität wird in der Regel verwendet, um anfällige Hosts zu finden, die ausgenutzt werden können. Im Bereich mit den Erkenntnisdetails in Ihrer GuardDuty Konsole wird nur die neueste Remote-IP-Adresse angezeigt

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Impact:EC2/SuspiciousDomainRequest.Reputation

Eine EC2-Instance fragt einen Domainnamen mit geringer Reputation ab, der aufgrund seines Alters oder seiner geringen Beliebtheit verdächtig ist.

Standard-Schweregrad: Niedrig

- Datenquelle: DNS-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgeführte Amazon-EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen mit niedriger Reputation abfragt, bei dem der Verdacht besteht, dass er bösartig ist. Es wurden Merkmale dieser Domain festgestellt, die mit zuvor beobachteten bösartigen Domains übereinstimmten. Unser Reputationsmodell konnte sie jedoch nicht definitiv mit einer bekannten Bedrohung in Verbindung bringen. Diese Domains werden in der Regel neu beobachtet oder erhalten nur wenig Datenverkehr.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Impact:EC2/WinRMBruteForce

Eine EC2-Instance führt einen ausgehenden Brute-Force-Angriff für die Windows-Remoteverwaltung durch.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis ist niedrig, wenn Ihre EC2-Instance das Ziel eines Brute-Force-Angriffs war. Der Schweregrad dieser Erkenntnis ist hoch, wenn Ihre EC2-Instance der zum Ausführen eines Brute-Force-Angriffs verwendete Akteur ist.

- Datenquelle: VPC-Flow-Protokolle

Dieses Ergebnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung einen Windows Remote Management (WinRM)-Brute-Force-Angriff durchführt, der darauf abzielt, Zugriff auf den Windows-Remote-Management-Service auf Windows-basierten Systemen zu erhalten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Recon:EC2/PortProbeEMRUnprotectedPort

Eine EC2-Instance verfügt über einen ungeschützten EMR-bezogenen Port, der von einem bekannten böswilligen Host untersucht wird.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass ein EMR-bezogener sensibler Port auf der aufgelisteten EC2-Instance, der Teil eines Clusters in Ihrer AWS Umgebung ist, nicht von einer Sicherheitsgruppe, einer Zugriffskontrollliste (ACL) oder einer Host-Firewall wie Linux IPTables blockiert wird. Diese Erkenntnis informiert auch darüber, dass bekannte Kabel im Internet diesen Port aktiv untersuchen. Ports, die diese Erkenntnis auslösen können, z. B. Port 8088 (YARN Web-UI-Port), könnten potenziell für die Remote-Code-Ausführung genutzt werden.

Empfehlungen zur Abhilfe:

Sie sollten den offenen Zugang zu Ports auf Clustern aus dem Internet blockieren und den Zugang nur auf bestimmte IP-Adressen beschränken, die Zugang zu diesen Ports benötigen. Weitere Informationen finden Sie unter Sicherheitsgruppen für EMR-Cluster.

Recon:EC2/PortProbeUnprotectedPort

Eine EC2-Instance hat einen ungeschützten Port, der von einem bekannten böswilligen Host getestet wird.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Niedrig. Wenn jedoch der untersuchte Port von Elasticsearch (9200 oder 9300) verwendet wird, ist der Schweregrad der Erkenntnis Hoch.

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass ein Port auf der aufgeführten EC2-Instance in Ihrer AWS-Umgebung nicht durch eine Sicherheitsgruppe, eine Zugriffssteuerungsliste (ACL) oder eine On-

Host-Firewall wie Linux IPTables blockiert ist und derzeit aktiv von bekannten Scannern im Internet untersucht wird.

Wenn der identifizierte ungeschützte Port 22 oder 3389 ist und Sie sich über diese Ports mit Ihrer Instance verbinden, können Sie die Exposition dennoch einschränken, indem Sie den Zugriff auf diese Ports nur für die IP-Adressen aus dem IP-Adressraum Ihres Unternehmensnetzwerks zulassen. Informationen zum Einschränken des Zugriffs auf Port 22 unter Linux finden Sie unter Autorisieren von eingehendem Datenverkehr für Linux-Instances. Informationen zum Einschränken des Zugriffs auf Port 3389 unter Windows finden Sie unter Autorisieren von eingehendem Datenverkehr für Windows-Instances.

GuardDuty generiert diese Erkenntnis nicht für die Ports 443 und 80.

Empfehlungen zur Abhilfe:

In einigen Fällen werden Instances absichtlich exponiert, weil sie beispielsweise Web-Server hosten. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Recon:EC2/PortProbeUnprotectedPort` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Recon:EC2/Portscan

Eine EC2-Instance führt ausgehende Port-Scans an einem Remote-Host durch.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung an einem möglichen Port-Scan-Angriff beteiligt ist, da sie versucht, in kurzer Zeit Verbindungen zu

mehreren Ports herzustellen. Das Ziel eines Port-Scan-Angriffs ist die Ermittlung offener Ports, um zu ermitteln, welche Services und welches Betriebssystem der Computer ausführt.

Empfehlungen zur Abhilfe:

Diese Erkenntnis kann falsch positiv sein, wenn Anwendungen zur Schwachstellenbewertung auf EC2-Instances in der Umgebung bereitgestellt werden, weil diese Anwendungen Port-Scans durchführen, um Sie über falsch konfigurierte offene Ports zu informieren. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Recon:EC2/Portscan` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die diese Tools zur Schwachstellenanalyse hosten. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivität unerwartet ist, ist Ihre Instance wahrscheinlich kompromittiert. Informationen dazu finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Trojan:EC2/BlackholeTraffic

Eine EC2-Instance versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, der ein bekanntes schwarzes Loch ist.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung möglicherweise kompromittiert wurde, da sie versucht, mit einer IP-Adresse eines schwarzen Lochs (oder eines Sinkholes) zu kommunizieren. Schwarze Löcher bezeichnen Orte im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend gelöscht wird, ohne die Quelle zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben. Die IP-Adresse eines schwarzen Lochs gibt einen Hostcomputer an, der nicht ausgeführt wird, oder eine Adresse, der kein Host zugewiesen wurde.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Trojan:EC2/BlackholeTraffic!DNS

Eine EC2-Instance fragt einen Domainnamen ab, der an eine die IP-Adresse eines schwarzen Lochs weitergeleitet wird.

Standard-Schweregrad: Mittel

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung möglicherweise kompromittiert wurde, da sie einen Domainnamen abfragt, der an eine IP-Adresse eines schwarzen Lochs weitergeleitet wird. Schwarze Löcher bezeichnen Orte im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend gelöscht wird, ohne die Quelle zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Trojan:EC2/DGADomainRequest.B

Eine EC2-Instance fragt algorithmisch generierte Domänen ab. Solche Domänen werden häufig von Malware genutzt und können auf eine kompromittierte EC2-Instance hinweisen.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung versucht, DGA (Domain Generation Algorithms)-Domains abzufragen. Ihre EC2-Instance wurde möglicherweise kompromittiert.

DGAs werden verwendet, um in regelmäßigen Abständen eine große Anzahl an Domainnamen zu generieren, die als Rendezvous Points mit ihren Command-and-Control (C&C)-Servern verwendet werden können. Command-and-Control-Server sind Computer, die Befehle an die Mitglieder eines Botnets senden. Hierbei handelt es sich um eine Ansammlung von mit dem Internet verbundenen Geräten, die infiziert sind und von einer gängigen Malware kontrolliert werden. Die große Anzahl potenzieller Rendezvous Points erschwert ein effektives Stilllegen von Botnets, da infizierte Computer versuchen, einige dieser Domainnamen täglich zu kontaktieren, um Updates oder Befehle zu erhalten.

> **Note**
>
> Diese Erkenntnis basiert auf der Analyse von Domainnamen mit erweiterten Heuristiken und kann daher neue DGA-Domains identifizieren, die nicht in Bedrohungsdaten-Feeds vorhanden sind.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Trojan:EC2/DGADomainRequest.C!DNS

Eine EC2-Instance fragt algorithmisch generierte Domänen ab. Solche Domänen werden häufig von Malware genutzt und können auf eine kompromittierte EC2-Instance hinweisen.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung versucht, DGA (Domain Generation Algorithms)-Domains abzufragen. Ihre EC2-Instance wurde möglicherweise kompromittiert.

DGAs werden verwendet, um in regelmäßigen Abständen eine große Anzahl an Domainnamen zu generieren, die als Rendezvous Points mit ihren Command-and-Control (C&C)-Servern verwendet

werden können. Command-and-Control-Server sind Computer, die Befehle an die Mitglieder eines Botnets senden. Hierbei handelt es sich um eine Ansammlung von mit dem Internet verbundenen Geräten, die infiziert sind und von einer gängigen Malware kontrolliert werden. Die große Anzahl potenzieller Rendezvous Points erschwert ein effektives Stilllegen von Botnets, da infizierte Computer versuchen, einige dieser Domainnamen täglich zu kontaktieren, um Updates oder Befehle zu erhalten.

> **Note**
>
> Diese Erkenntnis basiert auf bekannten DGA-Domains aus GuardDutyden Bedrohungsinformationen-Feeds von .

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Trojan:EC2/DNSDataExfiltration

Eine EC2-Instance filtert Daten durch DNS-Abfragen heraus.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung Malware ausführt, die DNS-Abfragen für ausgehende Datenübertragungen verwendet. Diese Art der Datenübertragung weist auf eine kompromittierte Instance hin und kann zur Exfiltration von Daten führen. DNS-Datenverkehr wird in der Regel nicht durch Firewalls gesperrt. So kann beispielsweise Malware in einer kompromittierten EC2-Instance Daten verschlüsseln (z. B. Ihre Kreditkartennummer) und in einer DNS-Abfrage an einen entfernten DNS-Server senden, der von einem Angreifer gesteuert wird.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Trojan:EC2/DriveBySourceTraffic!DNS

Eine EC2-Instance fragt einen Domainnamen eines Remote-Host ab, der eine bekannte Quelle von Drive-By-Downloadangriffen ist.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie, dass die aufgeführte EC2-Instance in Ihrer AWS-Umgebung möglicherweise kompromittiert wurde, da Sie einen Domainnamen von einem Remote-Host abfragt, der eine bekannte Quelle von Drive-By-Download-Angriffen ist. Hierbei handelt es sich um unbeabsichtigte Downloads von Computersoftware aus dem Internet, die eine automatische Installation von Viren, Spyware oder Malware auslösen kann.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Trojan:EC2/DropPoint

Eine EC2-Instance versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldedaten und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie, dass eine EC2-Instance in Ihrer AWS-Umgebung versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Trojan:EC2/DropPoint!DNS

Eine EC2-Instance fragt einen Domainnamen eines Remote-Hosts ab, von dem bekannt ist, dass er Anmeldedaten und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie, dass eine EC2-Instance in Ihrer AWS-Umgebung einen Domainnamen eines Remote-Hosts abfragt, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Trojan:EC2/PhishingDomainRequest!DNS

Eine EC2-Instance fragt Domänen ab, die an Phishing-Angriffen beteiligt sind. Ihre EC2-Instance wurde möglicherweise kompromittiert.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung versucht, eine Domain abzufragen, die an Phishing-Angriffen beteiligt ist. Phishing-Domains werden von jemandem eingerichtet, der sich als rechtmäßige Institution ausgibt, um Personen dazu zu bringen, sensible Daten bereitzustellen, wie beispielsweise personenbezogene Informationen, Bank- und Kreditkartendaten oder Passwörter. Ihre EC2-Instance versucht möglicherweise, sensible Daten abzurufen, die auf einer Phishing-Website gespeichert sind, oder sie versucht möglicherweise, eine Phishing-Website einzurichten. Ihre EC2-Instance wurde möglicherweise kompromittiert.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Eine EC2-Instance stellt Verbindungen zu einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste her.

Standard-Schweregrad: Mittel

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung mit einer IP-Adresse kommuniziert, die auf einer von Ihnen hochgeladenen Bedrohungsliste steht. In GuardDuty besteht eine Bedrohungsliste aus bekannten schädlichen IP-Adressen. GuardDuty generiert Ergebnisse basierend auf hochgeladenen Bedrohungslisten. Die Bedrohungsliste, die zum Generieren dieser Suche verwendet wird, wird in den Details der Suche aufgeführt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

UnauthorizedAccess:EC2/MetadataDNSRebind

Eine EC2-Instance führt DNS-Abrufe durch, die in den Instance-Metadatenservice aufgelöst werden.

Standard-Schweregrad: Hoch

- Datenquelle: DNS-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung eine Domain abfragt, die in die IP-Adresse der EC2-Metadaten (169.254.169.254) aufgelöst wird. Eine solche DNS-Abfrage kann darauf hinweisen, dass die Instance das Ziel einer DNS-Neubindung-Technik ist. Diese Technik kann verwendet werden, um Metadaten von einer EC2-Instance abzurufen, einschließlich der mit der Instance verknüpften IAM-Anmeldeinformationen.

Bei der DNS-Neubindung wird eine Anwendung, die auf der EC2-Instance läuft, dazu gebracht, Rückgabedaten von einer URL zu laden, wobei der Domainname in der URL in die IP-Adresse der EC2-Metadaten (169.254.169.254) aufgelöst wird. Dies bewirkt, dass die Anwendung auf EC2-Metadaten zugreift und sie möglicherweise für den Angreifer verfügbar macht.

Der Zugriff auf EC2-Metadaten mit DNS-Neubindung ist nur möglich, wenn auf der EC2-Instance eine anfällige Anwendung ausgeführt wird, die das Einfügen von URLs ermöglicht, oder wenn ein menschlicher Benutzer in einem Webbrowser, der auf der EC2-Instance ausgeführt wird, auf die URL zugreift.

Empfehlungen zur Abhilfe:

Prüfen Sie als Reaktion auf diese Erkenntnis, ob auf der EC2-Instance eine anfällige Anwendung ausgeführt wird, oder ob ein menschlicher Benutzer über einen Browser auf die im Ergebnis angegebene Domain zugegriffen hat. Wenn die Ursache eine anfällige Anwendung ist, beheben Sie die Schwachstelle. Wenn ein Benutzer die identifizierte Domain aufgerufen hat, blockieren Sie die Domain oder verhindern Sie, dass Benutzer darauf zugreifen. Wenn Sie in dieser Erkenntnis einen Zusammenhang mit einem der obigen Fälle feststellen, sollten Sie die der EC2-Instance zugeordnete Sitzung widerrufen.

Einige AWS-Kunden ordnen die IP-Adresse der Metadaten absichtlich einem Domainnamen auf ihren autoritativen DNS-Servern zu. Wenn dies in Ihrer -Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `UnauthorizedAccess:EC2/MetaDataDNSRebind` verwenden. Das zweite Filterkriterium sollte die DNS-Anforderungs-Domain sein, und der Wert sollte mit der Domain übereinstimmen, die Sie der Metadaten-IP-Adresse zugeordnet haben (169.254.169.254). Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

UnauthorizedAccess:EC2/RDPBruteForce

Eine EC2-Instance war an RDP-Brute-Force-Angriffen beteiligt.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis ist niedrig, wenn Ihre EC2-Instance das Ziel eines Brute-Force-Angriffs war. Der Schweregrad dieser Erkenntnis ist hoch, wenn Ihre EC2-Instance der zum Ausführen eines Brute-Force-Angriffs verwendete Akteur ist.

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung an einem Brute-Force-Angriff beteiligt war, der auf die Beschaffung von Passwörtern für RDP-Services auf Windows-basierten Systemen ausgerichtet war. Dies kann auf einen unbefugten Zugriff auf Ihre AWS-Ressourcen hinweisen.

Empfehlungen zur Abhilfe:

Wenn die Ressourcenrolle Ihrer Instance `ACTOR` lautet, bedeutet dies, dass Ihre Instance zum Ausführen von RDP-Brute-Force-Angriffen verwendet wurde. Außer, wenn diese Instance einen legitimen Grund hat, die IP-Adresse zu kontaktieren, die als `Target` aufgeführt ist, wird empfohlen, davon auszugehen, dass Ihre Instance kompromittiert wurde, und die in Behebung einer potenziell gefährdeten Amazon-Instance EC2 aufgeführten Maßnahmen zu ergreifen.

Wenn die Ressourcenrolle Ihrer Instance `TARGET` lautet, kann dieses Problem behoben werden, indem Sie Ihren RDP-Port mit Hilfe von Sicherheitsgruppen, ACLs oder Firewalls nur für vertrauenswürdige IPs sichern. Weitere Informationen finden Sie unter Tipps zur Sicherung Ihrer EC2-Instances (Linux).

UnauthorizedAccess:EC2/SSHBruteForce

Eine EC2-Instance war an SSH-Brute-Force-Angriffen beteiligt.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis ist niedrig, wenn ein Brute-Force-Angriff auf eine Ihrer EC2-Instances abzielt. Der Schweregrad dieser Erkenntnis ist hoch, wenn Ihre EC2-Instance verwendet wird, um einen Brute-Force-Angriff durchzuführen.

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung an einem Brute-Force-Angriff beteiligt war, der auf die Beschaffung von Passwörtern für SSH-Services auf Linux-basierten Systemen ausgerichtet war. Dies kann auf einen unbefugten Zugriff auf Ihre AWS-Ressourcen hinweisen.

> **Note**
>
> Dieses Ergebnis wird nur über den -Überwachungsdatenverkehr auf Port 22 generiert. Wenn Ihre SSH-Services konfiguriert sind, um andere Ports zu verwenden, wird dieses Ergebnis nicht generiert.

Empfehlungen zur Abhilfe:

Wenn das Ziel des versuchten Brute-Force-Angriffs ein Bastion-Host ist, kann dies das erwartete Verhalten für die betreffende AWS-Umgebung darstellen. In diesem Fall sollten Sie für dieses Ergebnis eine Unterdrückungsregel einrichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `UnauthorizedAccess:EC2/SSHBruteForce` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn diese Aktivitäten für Ihre Umgebung nicht erwartet werden und die Ressourcenrolle Ihrer Instance `TARGET` lautet, kann diese Erkenntnis behoben werden, indem Sie Ihren SSH-Port mit

Hilfe von Sicherheitsgruppen, ACLs oder Firewalls nur für vertrauenswürdige IPs sichern. Weitere Informationen finden Sie unter Tipps zur Sicherung Ihrer EC2-Instances (Linux).

Wenn die Ressourcenrolle Ihrer Instance `ACTOR` lautet, bedeutet dies, dass die Instance zum Ausführen von SSH-Brute-Force-Angriffen verwendet wurde. Außer, wenn diese Instance einen legitimen Grund hat, die IP-Adresse zu kontaktieren, die als `Target` aufgeführt ist, wird empfohlen, davon auszugehen, dass Ihre Instance kompromittiert wurde, und die in Behebung einer potenziell gefährdeten Amazon-Instance EC2 aufgeführten Maßnahmen zu ergreifen.

UnauthorizedAccess:EC2/TorClient

Ihre EC2-Instance stellt Verbindungen mit einem Tor Guard oder einem Authority-Knoten her.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung Verbindungen zu einem Tor-Guard oder einem Authority-Knoten herstellt. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor Guards und Authority-Knoten fungieren als erste Gateways in ein Tor-Netzwerk. Dieser Datenverkehr kann darauf hinweisen, dass diese EC2-Instance als Client in einem Tor-Netzwerk fungiert. Diese Erkenntnis kann auf einen unbefugten Zugriff auf die AWS-Ressourcen hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

UnauthorizedAccess:EC2/TorRelay

Ihre EC2-Instance stellt Verbindungen mit einem Tor-Netzwerk als Tor-Relais her.

Standard-Schweregrad: Hoch

- Datenquelle: VPC-Flow-Protokolle

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass sie als Tor-Relay fungiert. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor-Relays erhöhen die Anonymität der Kommunikation, indem sie den möglicherweise illegalen Datenverkehr des Kunden von einem Tor-Relay zu einem anderen weiterleiten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

GuardDuty IAMTypen finden

Die folgenden Ergebnisse beziehen sich spezifisch auf IAM Entitäten und Zugriffsschlüssel und haben immer den RessourcentypAccessKey. Der Schweregrad und die Details der Erkenntnisse unterscheiden sich je nach Erkenntnistyp.

Die hier aufgeführten Erkenntnisse beinhalten die Datenquellen und Modelle, die zur Generierung dieses Erkenntnistyps verwendet wurden. Weitere Informationen finden Sie unter GuardDuty grundlegende Datenquellen.

Für alle IAM diesbezüglichen Ergebnisse empfehlen wir Ihnen, die fragliche Entität zu untersuchen und sicherzustellen, dass ihre Berechtigungen der bewährten Methode der Methode der geringsten Rechte entsprechen. Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen zur Behebung von Erkenntnissen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Themen

- CredentialAccess:IAMUser/AnomalousBehavior
- DefenseEvasion:IAMUser/AnomalousBehavior
- Discovery:IAMUser/AnomalousBehavior
- Exfiltration:IAMUser/AnomalousBehavior
- Impact:IAMUser/AnomalousBehavior
- InitialAccess:IAMUser/AnomalousBehavior
- PenTest:IAMUser/KaliLinux
- PenTest:IAMUser/ParrotLinux

- PenTest:IAMUser/PentooLinux
- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

Eine, die API verwendet wurde, um Zugriff auf eine AWS Umgebung zu erhalten, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignis CloudTrail

Diese Feststellung informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API Anfrage festgestellt wurde. Dieses Ergebnis kann eine einzelne API oder eine Reihe verwandter API Anfragen beinhalten, die in unmittelbarer Nähe von derselben Benutzeridentität gestellt wurden. Das API beobachtete Problem wird häufig mit der Phase des Zugriffs auf Anmeldeinformationen in Verbindung gebracht, wenn ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihre Umgebung zu sammeln. Zu APIs dieser Kategorie gehören`GetPasswordData`,, und`GetSecretValue`. `BatchGetSecretValue` `GenerateDbAuthToken`

Diese API Anfrage wurde vom ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal eingestuft. Das ML-Modell bewertet alle API Anfragen in Ihrem Konto und identifiziert ungewöhnliche Ereignisse, die mit den von Gegnern verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt verschiedene Faktoren der API Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und den spezifischen Typ, der angefordert wurde. API Einzelheiten darüber, welche Faktoren der API Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

DefenseEvasion:IAMUser/AnomalousBehavior

Ein API zur Umgehung von Abwehrmaßnahmen eingesetztes Mittel wurde auf anomale Weise beschworen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignis CloudTrail

Diese Feststellung informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API Anfrage festgestellt wurde. Dieses Ergebnis kann eine einzelne API oder eine Reihe verwandter API Anfragen beinhalten, die in unmittelbarer Nähe von derselben Benutzeridentität gestellt wurden. Dieses API Phänomen wird häufig mit Ausweichtaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Spuren zu verwischen und nicht entdeckt zu werden. APIsZu dieser Kategorie gehören in der Regel Lösch-, Deaktivierungs- oder Stoppvorgänge wie,`DeleteFlowLogs`, `DisableAlarmActions` oder. `StopLogging`

Diese API Anfrage wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell bewertet alle API Anfragen in Ihrem Konto und identifiziert ungewöhnliche Ereignisse, die mit den von Gegnern verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt verschiedene Faktoren der API Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und den spezifischen Typ, der angefordert wurde. API Einzelheiten darüber, welche Faktoren der API

Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Discovery:IAMUser/AnomalousBehavior

Eine API häufig zum Auffinden von Ressourcen verwendete Methode wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Niedrig

- Datenquelle: Verwaltungsereignis CloudTrail

Diese Feststellung informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API Anfrage festgestellt wurde. Dieses Ergebnis kann eine einzelne API oder eine Reihe verwandter API Anfragen beinhalten, die in unmittelbarer Nähe von derselben Benutzeridentität gestellt wurden. Das API beobachtete Phänomen wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS Umgebung für einen umfassenderen Angriff anfällig ist. APIsZu dieser Kategorie gehören in der Regel Operationen zum Abrufen, Beschreiben oder Auflisten, wie, `DescribeInstancesGetRolePolicy`, oder. `ListAccessKeys`

Diese API Anfrage wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell bewertet alle API Anfragen in Ihrem Konto und identifiziert ungewöhnliche Ereignisse, die mit den von Gegnern verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt verschiedene Faktoren der API Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und den spezifischen Typ, der angefordert wurde. API Einzelheiten darüber, welche Faktoren der API Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Exfiltration:IAMUser/AnomalousBehavior

Ein API häufig zum Sammeln von Daten aus einer AWS Umgebung verwendetes Verfahren wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: Verwaltungsereignis CloudTrail

Diese Feststellung informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API Anfrage festgestellt wurde. Dieses Ergebnis kann eine einzelne API oder eine Reihe verwandter API Anfragen beinhalten, die in unmittelbarer Nähe von derselben Benutzeridentität gestellt wurden. Dieses API Phänomen wird häufig mit Exfiltrationstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten mithilfe von Paketierung und Verschlüsselung aus Ihrem Netzwerk zu sammeln, um nicht entdeckt zu werden. APIsBei diesem Befundtyp handelt es sich ausschließlich um Verwaltungsvorgänge (Steuerungsebene). Sie beziehen sich in der Regel auf S3, Snapshots und Datenbanken wie,, oder. `PutBucketReplication` `CreateSnapshot` `RestoreDBInstanceFromDBSnapshot`

Diese API Anfrage wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell bewertet alle API Anfragen in Ihrem Konto und identifiziert ungewöhnliche Ereignisse, die mit den von Gegnern verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt verschiedene Faktoren der API Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und den spezifischen Typ, der angefordert wurde. API Einzelheiten darüber, welche Faktoren der API Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Impact:IAMUser/AnomalousBehavior

Ein API häufig zur Manipulation von Daten oder Prozessen in einer AWS Umgebung verwendetes Verfahren wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: Verwaltungsereignis CloudTrail

Diese Feststellung informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API Anfrage festgestellt wurde. Dieses Ergebnis kann eine einzelne API oder eine Reihe verwandter API Anfragen beinhalten, die in unmittelbarer Nähe von derselben Benutzeridentität gestellt wurden. Das API beobachtete Phänomen wird häufig mit Einschlagstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, den Betrieb zu unterbrechen und Daten in Ihrem Konto zu manipulieren, zu unterbrechen oder zu zerstören. APIsBei diesem Erkennungstyp handelt es sich in der Regel um Lösch-, Aktualisierungs- oder Speicheroperationen wie,, `DeleteSecurityGroup` oder. `UpdateUser` `PutBucketPolicy`

Diese API Anfrage wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell bewertet alle API Anfragen in Ihrem Konto und identifiziert ungewöhnliche Ereignisse, die mit den von Gegnern verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt verschiedene Faktoren der API Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und den spezifischen Typ, der angefordert wurde. API Einzelheiten darüber, welche Faktoren der API Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

InitialAccess:IAMUser/AnomalousBehavior

Ein API häufig verwendetes Verfahren, um sich unbefugten Zugriff auf eine AWS Umgebung zu verschaffen, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignis CloudTrail

Diese Feststellung informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API Anfrage festgestellt wurde. Dieses Ergebnis kann eine einzelne API oder eine Reihe verwandter API

Anfragen beinhalten, die in unmittelbarer Nähe von derselben Benutzeridentität gestellt wurden. Das API beobachtete Phänomen wird häufig mit der ersten Zugriffsphase eines Angriffs in Verbindung gebracht, wenn ein Angreifer versucht, Zugriff auf Ihre Umgebung zu erhalten. APIsZu dieser Kategorie gehören in der Regel Operationen zum Abrufen von Token oder Sessions, wie, `GetFederationTokenStartSession`, oder. `GetAuthorizationToken`

Diese API Anfrage wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell bewertet alle API Anfragen in Ihrem Konto und identifiziert ungewöhnliche Ereignisse, die mit den von Gegnern verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt verschiedene Faktoren der API Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und den spezifischen Typ, der angefordert wurde. API Einzelheiten darüber, welche Faktoren der API Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

PenTest:IAMUser/KaliLinux

An API wurde von einer Kali-Linux-Maschine aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignis CloudTrail

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Kali Linux ausgeführt wird, API Anrufe mit Anmeldeinformationen tätigt, die zu dem aufgelisteten AWS Konto in Ihrer Umgebung gehören. Kali Linux ist ein beliebtes Tool für Penetrationstests, mit dem Sicherheitsexperten Schwachstellen in EC2 Fällen identifizieren, die gepatcht werden müssen. Angreifer verwenden dieses Tool auch, um EC2 Konfigurationsschwächen zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

PenTest:IAMUser/ParrotLinux

An API wurde von einem Parrot Security Linux-Computer aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignis CloudTrail

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Parrot Security Linux ausgeführt wird, API Anrufe mit Anmeldeinformationen tätigt, die zu dem in Ihrer Umgebung aufgelisteten AWS Konto gehören. Parrot Security Linux ist ein beliebtes Tool für Penetrationstests, mit dem Sicherheitsexperten Schwachstellen in EC2 Instanzen identifizieren, die gepatcht werden müssen. Angreifer verwenden dieses Tool auch, um EC2 Konfigurationsschwächen zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

PenTest:IAMUser/PentooLinux

An API wurde von einem Pentoo Linux-Computer aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignis CloudTrail

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Pentoo Linux ausgeführt wird, API Anrufe mit Anmeldeinformationen tätigt, die zu dem aufgelisteten AWS Konto in Ihrer Umgebung gehören. Pentoo Linux ist ein beliebtes Tool für Penetrationstests, mit dem Sicherheitsexperten Schwachstellen in EC2 Fällen identifizieren, die gepatcht werden müssen. Angreifer verwenden dieses Tool auch, um EC2 Konfigurationsschwächen zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Persistence:IAMUser/AnomalousBehavior

Ein API häufig verwendetes Tool, um unbefugten Zugriff auf eine AWS Umgebung aufrechtzuerhalten, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignis CloudTrail

Diese Feststellung informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API Anfrage festgestellt wurde. Dieses Ergebnis kann eine einzelne API oder eine Reihe verwandter API Anfragen beinhalten, die in unmittelbarer Nähe von derselben Benutzeridentität gestellt wurden. Das API beobachtete Phänomen wird häufig mit Persistenztaktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihre Umgebung verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten. APIsZu dieser Kategorie gehören in der Regel Erstellungs-, Import- oder Änderungsvorgänge wie,`CreateAccessKey`, `ImportKeyPair` oder. `ModifyInstanceAttribute`

Diese API Anfrage wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell bewertet alle API Anfragen in Ihrem Konto und identifiziert ungewöhnliche Ereignisse, die mit den von Gegnern verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt verschiedene Faktoren der API Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und den spezifischen Typ, der angefordert wurde. API Einzelheiten darüber, welche Faktoren der API Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Policy:IAMUser/RootCredentialUsage

An API wurde mit den Anmeldedaten des Root-Benutzers aufgerufen.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse

Diese Erkenntnis informiert Sie darüber, dass die Root-Benutzer-Anmeldeinformationen des in Ihrer Umgebung angeführten AWS-Konto -Kontos verwendet werden, um Anforderungen an AWS -Services zu erstellen. Es wird empfohlen, dass Benutzer niemals die Anmeldeinformationen von Root-Benutzern verwenden, um auf AWS Dienste zuzugreifen. Stattdessen sollte der Zugriff auf AWS Dienste mit temporären Anmeldeinformationen mit den geringsten Rechten von AWS Security Token Service (STS) erfolgen. In Situationen, in denen AWS STS dies nicht unterstützt wird, werden IAM Benutzeranmeldedaten empfohlen. Weitere Informationen finden Sie unter IAMBewährte Methoden.

> **Note**
>
> Wenn die S3-Bedrohungserkennung für das Konto aktiviert ist, kann diese Erkenntnis als Reaktion auf Versuche generiert werden, S3-Datenebenenvorgänge auf S3-Ressourcen unter Verwendung der Anmeldeinformationen des Root-Benutzers der AWS-Konto auszuführen. Der verwendete API Anruf wird in den Ergebnisdetails aufgeführt. Wenn die S3-Bedrohungserkennung nicht aktiviert ist, kann diese Entdeckung nur durch das Ereignisprotokoll ausgelöst werdenAPIs. Weitere Informationen zur S3-Bedrohungserkennung finden Sie unter S3 Protection.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

PrivilegeEscalation:IAMUser/AnomalousBehavior

Eine Methode, die API häufig verwendet wird, um hochrangige Berechtigungen für eine AWS Umgebung zu erhalten, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: Verwaltungsereignisse CloudTrail

Diese Feststellung informiert Sie darüber, dass in Ihrem Konto eine ungewöhnliche API Anfrage festgestellt wurde. Dieses Ergebnis kann eine einzelne API oder eine Reihe verwandter API Anfragen beinhalten, die in unmittelbarer Nähe von derselben Benutzeridentität gestellt wurden.

Das API beobachtete Problem wird häufig mit Taktiken zur Eskalation von Rechten in Verbindung gebracht, bei denen ein Angreifer versucht, Berechtigungen auf höherer Ebene für eine Umgebung zu erlangen. APIsZu dieser Kategorie gehören in der Regel Operationen, bei denen IAM Richtlinien, Rollen und Benutzer geändert werden, z. B.,, oder. `AssociateIamInstanceProfile` `AddUserToGroup` `PutUserPolicy`

Diese API Anfrage wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal eingestuft. Das ML-Modell bewertet alle API Anfragen in Ihrem Konto und identifiziert ungewöhnliche Ereignisse, die mit den von Gegnern verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt verschiedene Faktoren der API Anfrage, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und den spezifischen Typ, der angefordert wurde. API Einzelheiten darüber, welche Faktoren der API Anfrage für die Benutzeridentität, die die Anfrage aufgerufen hat, ungewöhnlich sind, finden Sie in den Ergebnisdetails.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Recon:IAMUser/MaliciousIPCaller

An API wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang, der AWS Ressourcen in einem Konto in Ihrer Umgebung auflisten oder beschreiben kann, von einer IP-Adresse aus aufgerufen wurde, die auf einer Bedrohungsliste steht. Ein Angreifer kann gestohlene Anmeldeinformationen verwenden, um diese Art der Erkennung Ihrer AWS Ressourcen durchzuführen, um wertvollere Anmeldeinformationen zu finden oder die Fähigkeiten der Anmeldeinformationen zu ermitteln, über die er bereits verfügt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Recon:IAMUser/MaliciousIPCaller.Custom

An API wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang, der AWS Ressourcen in einem Konto in Ihrer Umgebung auflisten oder beschreiben kann, von einer IP-Adresse aus aufgerufen wurde, die in einer benutzerdefinierten Bedrohungsliste enthalten ist. Die verwendete Bedrohungsliste wird in den Ergebnisdetails aufgeführt. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um diese Art der Erkennung Ihrer AWS Ressourcen durchzuführen, um wertvollere Anmeldeinformationen zu finden oder die Fähigkeiten der Anmeldeinformationen zu ermitteln, über die er bereits verfügt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Recon:IAMUser/TorIPCaller

An API wurde von der IP-Adresse eines Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass eine API Operation, die AWS Ressourcen in einem Konto in Ihrer Umgebung auflisten oder beschreiben kann, von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen wurde. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Ein Angreifer würde Tor verwenden, um seine wahre Identität zu verschleiern.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail Die Protokollierung wurde deaktiviert.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieser Befund informiert Sie darüber, dass ein CloudTrail Trail in Ihrer AWS Umgebung deaktiviert wurde. Dabei kann es sich um den Versuch eines Angreifers handeln, die Protokollierung seiner Aktivitäten zu deaktivieren, indem er alle Spuren beseitigt, während er mit böswilliger Absicht Zugriff auf die AWS -Ressourcen erlangt. Dieses Ergebnis kann durch das erfolgreiche Löschen oder Aktualisieren eines Trails ausgelöst werden. Dieses Ergebnis kann auch durch das erfolgreiche Löschen eines S3-Buckets ausgelöst werden, in dem die Protokolle eines zugehörigen Trails gespeichert sind GuardDuty.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Stealth:IAMUser/PasswordPolicyChange

Die Passwortrichtlinie des Kontos wurde geschwächt.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Schweregrad dieser Erkenntnis kann je nach Schweregrad der an der Passwortrichtlinie vorgenommenen Änderungen Niedrig, Mittel oder Hoch sein.

- Datenquelle: CloudTrail Verwaltungsereignisse

Die AWS Kontopasswortrichtlinie wurde für das aufgelistete Konto in Ihrer AWS Umgebung geschwächt. Beispiel: Sie wurde gelöscht oder aktualisiert und erfordert jetzt weniger Zeichen, keine Sonderzeichen und Zahlen mehr, oder das Ablaufdatum des Passworts musste verlängert werden. Dieses Ergebnis kann auch durch den Versuch ausgelöst werden, die Passwortrichtlinie für Ihr AWS Konto zu aktualisieren oder zu löschen. Die AWS Kontokennwortrichtlinie definiert die Regeln, die festlegen, welche Arten von Passwörtern für Ihre IAM Benutzer festgelegt werden können. Eine schwächere Passwortrichtlinie ermöglicht das Erstellen von Passwörtern, die leicht zu merken und möglicherweise einfacher zu erraten sind. Dadurch entsteht ein Sicherheitsrisiko.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Mehrere weltweit erfolgreiche Konsolenanmeldungen wurden beobachtet.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass mehrere erfolgreiche Konsolenanmeldungen für denselben IAM Benutzer an verschiedenen geografischen Standorten etwa zur gleichen Zeit beobachtet wurden. Solche anomalen und riskanten Zugriffsorte deuten auf einen potenziellen unbefugten Zugriff auf Ihre Ressourcen hin. AWS

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Anmeldeinformationen, die ausschließlich für eine EC2 Instance über eine Instance Launch-Rolle erstellt wurden, werden von einem anderen Konto innerhalb verwendet. AWS

Standard-Schweregrad: Hoch*

> **Note**
>
> Der Standard-Schweregrad diese Erkenntnis ist Hoch. Wenn der jedoch von einem Konto aufgerufen API wurde, das mit Ihrer AWS Umgebung verknüpft ist, lautet der Schweregrad Mittel.

- Datenquelle: CloudTrail Verwaltungsereignisse oder S3-Datenereignisse

Dieses Ergebnis informiert Sie darüber, wenn Ihre EC2 Instance-Anmeldeinformationen verwendet werden, um APIs von einer IP-Adresse aus aufzurufen, die einem anderen AWS Konto gehört als dem, unter dem die zugehörige EC2 Instance ausgeführt wird.

AWS empfiehlt nicht, temporäre Anmeldeinformationen außerhalb der Entität, die sie erstellt hat, neu zu verteilen (z. EC2 B. AWS Anwendungen oder Lambda). Autorisierte Benutzer können jedoch Anmeldeinformationen aus ihren EC2 Instanzen exportieren, um legitime API Anrufe zu tätigen. Wenn das `remoteAccountDetails.Affiliated` Feld lautet`True`, API wurde es von einem Konto aufgerufen, das mit Ihrer AWS Umgebung verknüpft ist. Um einen möglichen Angriff auszuschließen und die Legitimität der Aktivität zu überprüfen, wenden Sie sich an den IAM Benutzer, dem diese Anmeldeinformationen zugewiesen wurden.

> **Note**
>
> Wenn von einem Remote-Konto aus anhaltende Aktivitäten GuardDuty beobachtet werden, identifiziert das maschinelle Lernmodell (ML) dies als erwartetes Verhalten. Daher GuardDuty wird dieses Ergebnis nicht mehr für Aktivitäten von diesem Remote-Konto generiert. GuardDuty wird weiterhin Ergebnisse für neues Verhalten anderer Remote-Konten generieren und erlernte Remote-Konten neu bewerten, wenn sich das Verhalten im Laufe der Zeit ändert.

Empfehlungen zur Abhilfe:

Als Reaktion auf diese Erkenntnis können Sie den folgenden Workflow verwenden, um eine Vorgehensweise festzulegen:

1. Identifizieren Sie das betroffene Remote-Konto im `service.action.awsApiCallAction.remoteAccountDetails.accountId`-Feld.
2. Stellen Sie als Nächstes vor `service.action.awsApiCallAction.remoteAccountDetails.affiliated` Ort fest, ob dieses Konto mit Ihrer GuardDuty Umgebung verknüpft ist.
3. Wenn das Konto verknüpft ist, wenden Sie sich an den Eigentümer des Remote-Kontos und den Besitzer der EC2 Instanzanmeldeinformationen, um dies zu überprüfen.
4. Wenn das Konto nicht verknüpft ist, überprüfen Sie zunächst, ob das Konto Ihrer Organisation zugeordnet ist, aber nicht Teil Ihrer Einrichtung für GuardDuty mehrere Konten ist, oder ob GuardDuty es für das Konto noch nicht aktiviert wurde. Wenden Sie sich andernfalls an den Inhaber der EC2 Anmeldeinformationen, um festzustellen, ob es einen Anwendungsfall für die Verwendung dieser Anmeldeinformationen für ein Remotekonto gibt.
5. Wenn der Besitzer der Anmeldeinformationen das entfernte Konto nicht erkennt, wurden die Anmeldeinformationen möglicherweise von einem Bedrohungsakteur innerhalb von AWS kompromittiert. Sie sollten die unter Behebung einer potenziell gefährdeten Amazon-Instance EC2 empfohlenen Maßnahmen zum Schutz Ihrer Umgebung ergreifen.

   Darüber hinaus können Sie einen Missbrauchsbericht an das AWS Trust and Safety Team senden, um eine Untersuchung des Remote-Kontos einzuleiten. Wenn Sie Ihre Meldung an AWS Trust and Safety einreichen, geben Sie alle JSON Einzelheiten des Befundes an.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Anmeldeinformationen, die ausschließlich für eine EC2 Instance über eine Instance Launch-Rolle erstellt wurden, werden von einer externen IP-Adresse aus verwendet.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Verwaltungsereignisse oder S3-Datenereignisse

Dieses Ergebnis informiert Sie darüber, dass ein Host außerhalb von versucht AWS hat, AWS API Operationen mit temporären AWS Anmeldeinformationen auszuführen, die auf einer EC2 Instanz in Ihrer AWS Umgebung erstellt wurden. Die aufgelistete EC2 Instanz ist möglicherweise gefährdet, und die temporären Anmeldeinformationen dieser Instanz wurden möglicherweise auf einen Remote-Host außerhalb von exfiltriert. AWS AWS empfiehlt nicht, temporäre Anmeldeinformationen außerhalb der

Entität, die sie erstellt hat, neu zu verteilen (z. EC2 B. AWS Anwendungen oder Lambda). Autorisierte Benutzer können jedoch Anmeldeinformationen aus ihren EC2 Instanzen exportieren, um legitime API Anrufe zu tätigen. Um einen potenziellen Angriff auszuschließen und die Legitimität der Aktivität zu überprüfen, überprüfen Sie, ob die Verwendung von Instance-Anmeldeinformationen von der Remote-IP in der Erkenntnis erwartet wird.

> **Note**
>
> Wenn von einem Remote-Konto aus anhaltende Aktivitäten GuardDuty beobachtet werden, identifiziert das maschinelle Lernmodell (ML) dies als erwartetes Verhalten. Daher GuardDuty wird dieses Ergebnis nicht mehr für Aktivitäten von diesem Remote-Konto generiert. GuardDuty wird weiterhin Ergebnisse für neues Verhalten anderer Remote-Konten generieren und erlernte Remote-Konten neu bewerten, wenn sich das Verhalten im Laufe der Zeit ändert.

Empfehlungen zur Abhilfe:

Dieses Ergebnis wird generiert, wenn das Netzwerk so konfiguriert ist, dass Internetverkehr so weitergeleitet wird, dass er von einem lokalen Gateway und nicht von einem VPC Internet Gateway () ausgeht. IGW Allgemeine Konfigurationen, wie z. B. die Verwendung von VPC VPN Verbindungen AWS Outposts, können dazu führen, dass der Datenverkehr auf diese Weise weitergeleitet wird. Wenn dies ein erwartetes Verhalten ist, empfiehlt es sich, Unterdrückungsregeln zu verwenden und eine Regel zu erstellen, die aus zwei Filterkriterien besteht. Das erste Kriterium ist der Ergebnistyp, der `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS` sein sollte. Das zweite Filterkriterium ist die APIIPv4Anruferadresse mit der IP-Adresse oder dem CIDR Bereich Ihres lokalen Internet-Gateways. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

> **Note**
>
> Wenn eine kontinuierliche Aktivität aus einer externen Quelle GuardDuty beobachtet wird, identifiziert das maschinelle Lernmodell dieses Verhalten als erwartetes Verhalten und beendet die Generierung dieser Ergebnisse für Aktivitäten aus dieser Quelle. GuardDuty wird weiterhin Erkenntnisse für neues Verhalten aus anderen Quellen generieren und erlernte Quellen neu bewerten, wenn sich das Verhalten im Laufe der Zeit ändert.

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

An API wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang (z. B. ein Versuch, eine EC2 Instance zu starten, einen neuen IAM Benutzer zu erstellen oder Ihre AWS Rechte zu ändern) von einer bekannten bösartigen IP-Adresse aus aufgerufen wurde. Dies kann auf einen unbefugten Zugriff auf AWS Ressourcen in Ihrer Umgebung hinweisen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Ein API wurde von einer IP-Adresse aus einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang (z. B. ein Versuch, eine EC2 Instance zu starten, einen neuen IAM Benutzer zu erstellen oder AWS Rechte zu ändern) von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. In besteht eine Bedrohungsliste aus bekannten schädlichen IP-Adressen. Dies kann auf einen unbefugten Zugriff auf AWS Ressourcen in Ihrer Umgebung hinweisen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

UnauthorizedAccess:IAMUser/TorIPCaller

An API wurde von der IP-Adresse eines Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Verwaltungsereignisse

Dieses Ergebnis informiert Sie darüber, dass eine API Operation (z. B. ein Versuch, eine EC2 Instanz zu starten, einen neuen IAM Benutzer zu erstellen oder Ihre AWS Rechte zu ändern) von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen wurde. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihre AWS -Ressourcen hinweisen, mit dem Ziel, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

GuardDuty S3-Suchttypen

Die folgenden Ergebnisse sind spezifisch für Amazon S3 S3-Ressourcen und haben den Ressourcentyp, `S3Bucket` ob es sich bei der Datenquelle um CloudTrail Datenereignisse für S3 oder `AccessKey` um CloudTrail Verwaltungsereignisse handelt. Der Schweregrad und die Details der Ergebnisse unterscheiden sich je nach Ergebnistyp und Berechtigung, die dem Bucket zugeordnet sind.

Die hier aufgeführten Erkenntnisse beinhalten die Datenquellen und Modelle, die zur Generierung dieses Erkenntnistyps verwendet wurden. Weitere Informationen zu Datenquellen und Modellen finden Sie unter GuardDuty grundlegende Datenquellen.

> **Important**
>
> Ergebnisse mit einer Datenquelle für CloudTrail Datenereignisse für S3 werden nur generiert, wenn Sie den S3-Schutz aktiviert haben GuardDuty. Der S3-Schutz ist standardmäßig für alle Konten aktiviert, die nach dem 31. Juli 2020 erstellt wurden. Weitere Informationen zur Aktivierung oder Deaktivierung von S3-Schutz finden Sie unter GuardDuty S3-Schutz

Für alle `S3Bucket`-Arten von Erkenntnissen wird empfohlen, die Berechtigungen für den betreffenden Bucket und die Berechtigungen aller Benutzer, die an dem Erkenntniss beteiligt waren, zu überprüfen. Falls die Aktivität unerwartet ist, lesen Sie die Empfehlungen zur Problembehebung unter Behebung eines potenziell gefährdeten S3-Buckets.

Themen

- Discovery:S3/AnomalousBehavior
- Discovery:S3/MaliciousIPCaller
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- Exfiltration:S3/AnomalousBehavior
- Exfiltration:S3/MaliciousIPCaller
- Impact:S3/AnomalousBehavior.Delete
- Impact:S3/AnomalousBehavior.Permission
- Impact:S3/AnomalousBehavior.Write
- Impact:S3/MaliciousIPCaller
- PenTest:S3/KaliLinux
- PenTest:S3/ParrotLinux
- PenTest:S3/PentooLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom

- UnauthorizedAccess:S3/TorIPCaller

Discovery:S3/AnomalousBehavior

Eine API, die häufig zum Auffinden von S3-Objekten verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität eine S3-API aufgerufen hat, um S3-Buckets in Ihrer Umgebung zu erkennen, z. B. `ListObjects`. Diese Art von Aktivität steht im Zusammenhang mit der Erkennungsphase eines Angriffs, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS Umgebung für einen umfassenderen Angriff anfällig ist. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Discovery:S3/MaliciousIPCaller

Eine S3-API, die häufig zur Erkennung von Ressourcen in einer AWS Umgebung verwendet wird, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein S3-API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Angreifer Informationen über Ihre AWS Umgebung sammelt. Beispiele hierfür sind `GetObjectAcl` und `ListObjects`.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Discovery:S3/MaliciousIPCaller.Custom

Eine S3-API wurde von einer IP-Adresse aufgerufen, die sich auf einer benutzerdefinierten Bedrohungsliste befindet.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine S3-API, wie z. B. `GetObjectAcl` oder `ListObjects` von einer IP-Adresse aufgerufen wurde, die auf einer von Ihnen hochgeladenen Bedrohungsliste steht. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Die beobachtete API wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS -Umgebung für einen umfassenderen Angriff anfällig ist.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Discovery:S3/TorIPCaller

Eine S3-API wurde von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine S3-API, wie `GetObjectAcl` oder`ListObjects`, von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen wurde. Diese Art von Aktivität steht im Zusammenhang mit der Erkennungsphase eines Angriffs, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS Umgebung für einen umfassenderen Angriff anfällig ist. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, um die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Exfiltration:S3/AnomalousBehavior

Eine IAM-Entität hat eine S3-API auf verdächtige Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität API-Aufrufe tätigt, die einen S3-Bucket betreffen, und dass sich diese Aktivität von der festgelegten Basisaktivität dieser Entität unterscheidet. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit der Exfiltrationsphase eines Angriffs, in der ein Angreifer versucht, Daten zu sammeln. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde anhand des ML-Modells (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Exfiltration:S3/MaliciousIPCaller

Eine S3-API, die üblicherweise zum Sammeln von Daten aus einer AWS Umgebung verwendet wird, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein S3-API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Exfiltrationstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten aus Ihrem Netzwerk zu sammeln. Beispiele hierfür sind `GetObject` und `CopyObject`.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Impact:S3/AnomalousBehavior.Delete

Eine IAM-Entität hat eine S3-API aufgerufen, die versucht, Daten auf verdächtige Weise zu löschen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS Umgebung API-Aufrufe tätigt, die einen S3-Bucket betreffen, und dass sich dieses Verhalten von der festgelegten Baseline dieser Entität unterscheidet. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit einem Angriff, bei dem versucht wird, Daten zu löschen. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Wir empfehlen eine Prüfung des Inhalts Ihres S3-Buckets, um festzustellen, ob die vorherige Objektversion wiederhergestellt werden kann oder sollte.

Impact:S3/AnomalousBehavior.Permission

Eine API, die häufig zum Festlegen der Berechtigungen für Zugriffssteuerungslisten (ACL) verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS Umgebung eine Bucket-Richtlinie oder ACL für die aufgelisteten S3-Buckets geändert hat. Durch diese Änderung können Ihre S3-Buckets allen authentifizierten Benutzern öffentlich zugänglich gemacht werden. AWS

Diese API wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Wir empfehlen eine Prüfung des Inhalts Ihres S3-Buckets, um sicherzustellen, dass kein unerwarteter öffentlicher Zugriff auf Objekte gewährt wurde.

Impact:S3/AnomalousBehavior.Write

Eine IAM-Entität hat eine S3-API aufgerufen, die versucht, Daten auf verdächtige Weise zu schreiben.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS Umgebung API-Aufrufe tätigt, die einen S3-Bucket betreffen, und dass sich dieses Verhalten von der festgelegten Baseline dieser Entität unterscheidet. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit einem Angriff, bei dem versucht wird, Daten zu schreiben. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise ruft eine IAM-Entität ohne vorherige Historie eine S3-API auf, oder eine IAM-Entität ruft eine S3-API von einem ungewöhnlichen Ort aus auf.

Diese API wurde durch das ML-Modell (Machine Learning) zur Erkennung GuardDuty von Anomalien als anomal identifiziert. Das ML-Modell wertet alle API-Anfragen an Ihr Konto aus und identifiziert anomale Ereignisse, die mit Techniken von Angreifern in Verbindung gebracht werden. Es verfolgt verschiedene Faktoren der API-Anfragen, wie z. B. den Nutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die spezifische API, die angefordert wurde, den angeforderten Bucket und die Anzahl der durchgeführten API-Aufrufe. Weitere Informationen darüber, welche Faktoren der API-Anforderung für die Benutzeridentität, die die Anforderung aufgerufen hat, ungewöhnlich sind, finden Sie in den Erkenntnisdetails.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Wir empfehlen eine Prüfung des Inhalts Ihres S3-Buckets, um sicherzustellen, dass bei diesem API-Aufruf keine schädlichen oder unautorisierten Daten geschrieben wurden.

Impact:S3/MaliciousIPCaller

Eine S3-API, die häufig zur Manipulation von Daten oder Prozessen in einer AWS Umgebung verwendet wird, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein S3-API-Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Die beobachtete API wird häufig mit Schlagtaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. AWS Beispiele hierfür sind `PutObject` und `PutObjectAcl`.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

PenTest:S3/KaliLinux

Eine S3-API wurde von einem Kali-Linux-Computer aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Kali Linux ausgeführt wird, S3-API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS Konto gehören. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert. Kali Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Angreifer verwenden dieses Tool auch, um Schwachstellen in der EC2-Konfiguration zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

PenTest:S3/ParrotLinux

Eine S3-API wurde von einem Computer mit Parrot Security Linux aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Parrot Security Linux ausgeführt wird, S3-API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS Konto gehören. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert. Parrot Security Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Dieses Tool wird allerdings auch von Angreifern verwendet, um Schwächen in der EC2-Konfiguration zu finden und nicht autorisierten Zugriff auf Ihre AWS -Umgebung zu erhalten.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

PenTest:S3/PentooLinux

Eine S3-API wurde von einem Pentoo-Linux-Computer aus aufgerufen.

Standard-Schweregrad: Mittel

- Datenquelle: CloudTrail Datenereignisse für S3

Dieses Ergebnis informiert Sie darüber, dass ein Computer, auf dem Pentoo Linux ausgeführt wird, S3-API-Aufrufe mit Anmeldeinformationen durchführt, die zu Ihrem AWS Konto gehören. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert. Pentoo Linux ist ein beliebtes Tool für Penetrationstests, das von Sicherheitsexperten verwendet wird, um Schwachstellen in EC2-Instances zu erkennen, für die Patches erforderlich sind. Angreifer verwenden dieses Tool auch, um Schwachstellen in der EC2-Konfiguration zu finden und sich unbefugten Zugriff auf Ihre AWS Umgebung zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Policy:S3/AccountBlockPublicAccessDisabled

Eine IAM-Entität hat eine API aufgerufen, die verwendet wird, um Amazon S3 Block Public Access auf einen Bucket zu deaktivieren.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass Amazon S3 Block Public Access auf Kontoebene deaktiviert wurde. Wenn S3 Block Public Access aktiviert ist, werden entsprechende Einstellungen verwendet, um die auf den Bucket angewendeten Richtlinien oder Zugriffssteuerungslisten (ACL) zu filtern, um eine unbeabsichtigte öffentliche Offenlegung von Daten zu verhindern.

In der Regel ist S3 Block Public Access deaktiviert, um den öffentlichen Zugriff auf einen Bucket oder die Objekte im Bucket zuzulassen. Wenn S3 Block Public Access für ein Konto deaktiviert ist, wird der Zugriff auf Ihre Buckets durch die Richtlinien, ACLs oder Einstellungen von Block Public Access auf Bucket-Ebene gesteuert, die für Ihre individuellen Buckets gelten. Dies bedeutet nicht, dass der Bucket öffentlich freigegeben ist. Sie sollten die auf den Bucket angewendeten Berechtigungen jedoch überprüfen, um sicherzustellen, dass die passenden Zugangsebenen angewendet werden.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Policy:S3/BucketAnonymousAccessGranted

Ein IAM-Prinzipal hat den Zugriff auf einen S3-Bucket auf das Internet gewährt, indem er Bucket-Richtlinien oder ACLs geändert hat.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass der aufgelistete S3-Bucket im Internet öffentlich zugänglich gemacht wurde, weil eine IAM-Entität eine Bucket-Richtlinie oder ACL für diesen Bucket geändert hat. Nachdem eine Änderung an der Richtlinie oder der ACL erkannt wurde, ermittelt anhand Automated Reasoning auf Basis von Zelkova, ob der Bucket öffentlich zugänglich ist.

> **Note**
>
> Wenn die ACLs oder Bucket-Richtlinien eines Buckets so konfiguriert sind, dass sie explizit oder alles verweigern, spiegelt diese Erkenntnis möglicherweise nicht den aktuellen Status des Buckets wider. Diese Erkenntnis spiegelt nicht die Einstellungen für den öffentlichen Zugriff in S3, die möglicherweise für Ihren S3-Bucket aktiviert wurden, wider. In solchen Fällen wird der `effectivePermission`-Wert im Ergebnis als `UNKNOWN` markiert.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Policy:S3/BucketBlockPublicAccessDisabled

Ein IAM-Prinzipal hat eine API aufgerufen, die verwendet wird, um S3 Block Public Access auf einen Bucket zu deaktivieren.

Standard-Schweregrad: Niedrig

- Datenquelle: CloudTrail Verwaltungsereignisse

Diese Erkenntnis informiert Sie darüber, dass Block Public Access für den S3-Bucket deaktiviert wurde. Wenn S3 Block Public Access aktiviert ist, werden entsprechende Einstellungen verwendet,

um die auf den Bucket angewendeten Richtlinien oder Zugriffssteuerungslisten (ACL) zu filtern, um eine unbeabsichtigte öffentliche Offenlegung von Daten zu verhindern.

In der Regel ist S3 Block Public Access deaktiviert, um den öffentlichen Zugriff auf einen Bucket oder die Objekte im Bucket zuzulassen. Wenn S3 Block Public Access für diesen Bucket deaktiviert ist, wird der Zugriff auf den Bucket durch Richtlinien oder ACLs, gesteuert, die auf den Bucket angewendet sind. Dies bedeutet nicht, dass der Bucket öffentlich freigegeben ist. Sie sollten die auf den Bucket angewendeten Richtlinien und ACLs jedoch überprüfen, um sicherzustellen, dass die passenden Berechtigungen angewendet werden.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Policy:S3/BucketPublicAccessGranted

Ein IAM-Prinzipal hat allen AWS Benutzern öffentlichen Zugriff auf einen S3-Bucket gewährt, indem er die Bucket-Richtlinien oder ACLs geändert hat.

Standard-Schweregrad: Hoch

- Datenquelle: Verwaltungsereignisse CloudTrail

Dieses Ergebnis informiert Sie darüber, dass der aufgelistete S3-Bucket allen authentifizierten AWS Benutzern öffentlich zugänglich gemacht wurde, weil eine IAM-Entität eine Bucket-Richtlinie oder ACL für diesen S3-Bucket geändert hat. Nachdem eine Änderung an der Richtlinie oder der ACL erkannt wurde, ermittelt anhand Automated Reasoning auf Basis von Zelkova, ob der Bucket öffentlich zugänglich ist.

> **Note**
>
> Wenn die ACLs oder Bucket-Richtlinien eines Buckets so konfiguriert sind, dass sie explizit oder alles verweigern, spiegelt diese Erkenntnis möglicherweise nicht den aktuellen Status des Buckets wider. Diese Erkenntnis spiegelt nicht die Einstellungen für den öffentlichen

Zugriff in S3, die möglicherweise für Ihren S3-Bucket aktiviert wurden, wider. In solchen Fällen wird der `effectivePermission`-Wert im Ergebnis als `UNKNOWN` markiert.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Stealth:S3/ServerAccessLoggingDisabled

S3-Server-Zugriffsprotokollierung für einen Bucket wurde deaktiviert.

Standard-Schweregrad: Niedrig

- Datenquelle: Verwaltungsereignisse CloudTrail

Dieses Ergebnis informiert Sie darüber, dass die Protokollierung des S3-Serverzugriffs für einen Bucket in Ihrer AWS Umgebung deaktiviert ist. Wenn diese Option deaktiviert ist, werden keine Webanforderungsprotokolle für Versuche erstellt, auf den identifizierten S3-Bucket zuzugreifen. Aufrufe der S3-Management-API an den Bucket, z. B. DeleteBucket, werden jedoch weiterhin verfolgt. Wenn die S3-Datenereignisprotokollierung CloudTrail für diesen Bucket aktiviert ist, werden Webanfragen für Objekte innerhalb des Buckets weiterhin verfolgt. Das Deaktivieren der Protokollierung ist eine Methode, die häufig von nicht autorisierten Benutzern verwendet wird, um ihre Spuren zu verwischen. Weitere Informationen zu S3-Protokollen finden Sie unter S3-Serverzugriffsprotokollierung und Optionen für S3-Protokollierung.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Eine S3-API wurde von einer IP-Adresse aufgerufen, die sich auf einer benutzerdefinierten Bedrohungsliste befindet.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass ein S3-API-Vorgang, z. B. `PutObject` oder`PutObjectAcl` , von einer IP-Adresse aufgerufen wurde, die auf einer von Ihnen hochgeladenen Bedrohungsliste steht. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

UnauthorizedAccess:S3/TorIPCaller

Eine S3-API wurde von einer Tor-Ausgangsknotens-IP-Adresse aufgerufen.

Standard-Schweregrad: Hoch

- Datenquelle: CloudTrail Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass ein S3-API-Vorgang, wie zum Beispiel `PutObject` oder `PutObjectAcl`, von einer IP-Adresse eines Tor-Ausgangsknotens aus aufgerufen wurde. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dieser Befund kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, um die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

EKSAuditprotokolle, Typen finden

Die folgenden Erkenntnisse beziehen sich auf Kubernetes-Ressourcen und haben einen resource_type `EKSCluster`. Der Schweregrad und die Details der Erkenntnisse unterscheiden sich je nach Erkenntnistyp.

Für alle Erkenntnisse des Kubernetes-Typs empfehlen wir, dass Sie die betreffende Ressource untersuchen, um festzustellen, ob es sich um eine erwartete oder potenziell bösartige Aktivität handelt. Hinweise zur Behebung einer gefährdeten Kubernetes-Ressource, die durch einen Befund identifiziert wurde, finden Sie unter. GuardDuty Behebung der Erkenntnisse von EKS Audit Log Monitoring

> **Note**
>
> Wenn die Aktivität, aufgrund derer diese Erkenntnisse generiert werden, erwartet wird, sollten Sie erwägen, Unterdrückungsregeln sie hinzuzufügen, um zukünftige Benachrichtigungen zu verhindern.

Themen

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess
- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess
- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom

- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom
- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> Vor Kubernetes Version 1.14 war die `system:unauthenticated` Gruppe standardmäßig mit und verknüpft. `system:discovery` `system:basic-user` ClusterRoles Diese

Zuordnung kann unbeabsichtigten Zugriff durch anonyme Benutzer ermöglichen. Durch Cluster-Updates werden diese Berechtigungen nicht aufgehoben. Auch wenn Sie Ihren Cluster auf Version 1.14 oder höher aktualisiert haben, sind diese Berechtigungen möglicherweise weiterhin aktiviert. Wir empfehlen, dass Sie die Zuordnung dieser Berechtigungen zu der `system:unauthenticated`-Gruppe aufheben. Hinweise zum Widerruf dieser Berechtigungen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im EKSAmazon-Benutzerhandbuch.

CredentialAccess:Kubernetes/MaliciousIPCaller

Eine API häufig für den Zugriff auf Anmeldeinformationen oder geheime Daten in einem Kubernetes-Cluster verwendete Methode wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Das API beobachtete Phänomen wird häufig mit Taktiken für den Zugriff auf Anmeldeinformationen in Verbindung gebracht, bei denen ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Ein API häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendeter Code wurde über eine IP-Adresse auf einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Das API beobachtete Phänomen wird häufig mit Taktiken für den Zugriff auf Anmeldeinformationen in Verbindung gebracht, bei der ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die API und aufrufen durfte, und widerrufen Sie die Berechtigungen, falls erforderlich, indem Sie die Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Ein API häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendetes Verfahren wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang vom `system:anonymous` Benutzer erfolgreich aufgerufen wurde. APIAnrufe von `system:anonymous` sind nicht authentifiziert. Das beobachtete API Phänomen wird häufig mit Taktiken für den Zugriff auf Anmeldeinformationen in Verbindung gebracht, bei der ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für Ihren Kubernetes-Cluster zu sammeln. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die im Ergebnis gemeldete API Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im EKSAmazon-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

CredentialAccess:Kubernetes/TorIPCaller

Ein API häufig für den Zugriff auf Anmeldeinformationen oder Geheimnisse in einem Kubernetes-Cluster verwendeter Code wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert dich darüber, dass eine von der IP-Adresse eines Tor-Ausgangsknotens aus aufgerufen API wurde. Das API beobachtete Phänomen wird häufig mit Taktiken für den Zugriff auf Anmeldeinformationen in Verbindung gebracht, bei der ein Angreifer versucht, Passwörter, Benutzernamen und Zugriffsschlüssel für deinen Kubernetes-Cluster zu sammeln. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-

Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die Kubernetes-Cluster-Ressourcen hinweisen, mit dem Ziel, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

DefenseEvasion:Kubernetes/MaliciousIPCaller

Eine API häufig zur Umgehung von Abwehrmaßnahmen verwendete Methode wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: EKS Audit-Protokolle

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Das API beobachtete Phänomen wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen

rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Eine API häufig zur Umgehung von Abwehrmaßnahmen verwendete Methode wurde von einer IP-Adresse aus aufgerufen, die auf einer benutzerdefinierten Bedrohungsliste steht.

Standard-Schweregrad: Hoch

- Funktion: EKS Audit-Protokolle

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Das API beobachtete Phänomen wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Eine API häufig zur Umgehung von Abwehrmaßnahmen verwendete Methode wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang vom `system:anonymous` Benutzer erfolgreich aufgerufen wurde. APIAnrufe von `system:anonymous` sind nicht authentifiziert. Das beobachtete Phänomen API wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die im Ergebnis gemeldete API Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im EKSAmazon-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

DefenseEvasion:Kubernetes/TorIPCaller

Eine API häufig verwendete Methode, um Abwehrmaßnahmen zu umgehen, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert dich darüber, dass eine von der IP-Adresse eines Tor-Ausgangsknotens aus aufgerufen API wurde. Das API beobachtete Phänomen wird häufig mit Umgehungstaktiken in Verbindung gebracht, bei denen ein Gegner versucht, seine Aktionen zu verbergen, um nicht entdeckt zu werden. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der

letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihren Kubernetes-Cluster hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Discovery:Kubernetes/MaliciousIPCaller

Ein API häufig zum Auffinden von Ressourcen in einem Kubernetes-Cluster verwendetes Programm wurde von einer IP-Adresse aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Der beobachtete API Wert wird häufig in der Erkennungsphase eines Angriffs verwendet, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihr Kubernetes-Cluster für einen umfassenderen Angriff anfällig ist.

> **Für nicht authentifizierten Zugriff**
>
> MaliciousIPCallerFür einen nicht authentifizierten Zugriff werden keine Ergebnisse generiert. SuccessfulAnonymousAccessErgebnisse werden für einen nicht authentifizierten oder anonymen Zugriff generiert.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Ein API häufig zur Erkennung von Ressourcen in einem Kubernetes-Cluster verwendetes Programm wurde von einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein von einer IP-Adresse aus aufgerufen API wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Das beobachtete API Ergebnis wird häufig in der Erkennungsphase eines Angriffs verwendet, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihr Kubernetes-Cluster für einen umfassenderen Angriff anfällig ist.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen

rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Discovery:Kubernetes/SuccessfulAnonymousAccess

Ein API häufig zum Auffinden von Ressourcen in einem Kubernetes-Cluster verwendeter Vorgang wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang vom `system:anonymous` Benutzer erfolgreich aufgerufen wurde. APIAnrufe von `system:anonymous` sind nicht authentifiziert. Das beobachtete API Phänomen wird häufig mit der Erkennungsphase eines Angriffs in Verbindung gebracht, in der ein Angreifer Informationen über Ihren Kubernetes-Cluster sammelt. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die im Ergebnis gemeldete API Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Dieser Befundtyp schließt die API Endpunkte der Integritätsprüfung wie`/healthz`,, und `/livez` aus. `/readyz` `/version`

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im EKSAmazon-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Discovery:Kubernetes/TorIPCaller

Ein API häufig zur Erkennung von Ressourcen in einem Kubernetes-Cluster verwendetes Programm wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert dich darüber, dass eine von der IP-Adresse eines Tor-Ausgangsknotens aus aufgerufen API wurde. Das beobachtete API Ergebnis wird häufig in der Erkennungsphase eines Angriffs verwendet, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihr Kubernetes-Cluster für einen umfassenderen Angriff anfällig ist. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihren Kubernetes-Cluster hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer bei Bedarf den APIand Widerruf der Berechtigungen aufrufen durfte, indem Sie die Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch befolgen. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Execution:Kubernetes/ExecInKubeSystemPod

Ein Befehl wurde in einem Pod innerhalb des **`kube-system`**-Namespace ausgeführt

Standard-Schweregrad: Mittel

- Funktion: EKS Audit-Logs

Dieses Ergebnis informiert Sie darüber, dass ein Befehl in einem Pod innerhalb des `kube-system` Namespace mithilfe von Kubernetes Exec ausgeführt wurde. API `kube-system`Namespace ist ein Standard-Namespaces, der hauptsächlich für Komponenten auf Systemebene wie und verwendet wird. `kube-dns` `kube-proxy` Es ist sehr ungewöhnlich, Befehle innerhalb von Pods oder Containern unter einem `kube-system`-Namespace auszuführen, was auf verdächtige Aktivitäten hinweisen kann.

Empfehlungen zur Abhilfe:

Wenn die Ausführung dieses Befehls unerwartet erfolgt, können die Anmeldeinformationen der Benutzeridentität, die zur Ausführung des Befehls verwendet wurde, kompromittiert sein. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Impact:Kubernetes/MaliciousIPCaller

Ein API häufig zur Manipulation von Ressourcen in einem Kubernetes-Cluster verwendeter Code wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Das beobachtete API Phänomen wird häufig mit Einschlagstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. AWS

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine

böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Impact:Kubernetes/MaliciousIPCaller.Custom

Ein API häufig zur Manipulation von Ressourcen in einem Kubernetes-Cluster verwendetes Programm wurde von einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Das beobachtete API Phänomen wird häufig mit Einschlagstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. AWS

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Impact:Kubernetes/SuccessfulAnonymousAccess

Ein API häufig zur Manipulation von Ressourcen in einem Kubernetes-Cluster verwendetes Verfahren wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang vom `system:anonymous` Benutzer erfolgreich aufgerufen wurde. APIAnrufe von `system:anonymous` sind nicht authentifiziert. Das beobachtete API Phänomen wird häufig mit der Auswirkungsphase eines Angriffs in Verbindung gebracht, wenn ein Angreifer Ressourcen in Ihrem Cluster manipuliert. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die im Ergebnis gemeldete API Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im EKSAmazon-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Impact:Kubernetes/TorIPCaller

Ein API häufig verwendetes Tool, um Ressourcen in einem Kubernetes-Cluster zu manipulieren, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert dich darüber, dass eine von der IP-Adresse eines Tor-Ausgangsknotens aus aufgerufen API wurde. Das API beobachtete Phänomen wird häufig mit Einschlagstaktiken in Verbindung gebracht, bei denen ein Angreifer versucht, Daten in Ihrer Umgebung zu manipulieren, zu unterbrechen oder zu zerstören. AWS Tor ist eine Software, die anonyme Kommunikation ermöglicht.

Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihren Kubernetes-Cluster hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Persistence:Kubernetes/ContainerWithSensitiveMount

Ein Container wurde gestartet, in dem ein sensibler externer Host-Pfad eingehängt war.

Standard-Schweregrad: Mittel

- Funktion: EKS Audit-Logs

Diese Erkenntnis informiert Sie darüber, dass ein Container mit einer Konfiguration gestartet wurde, die im Abschnitt `volumeMounts` einen sensiblen Host-Pfad mit Schreibzugriff enthielt. Dadurch ist der sensible Host-Pfad vom Container aus zugänglich und beschreibbar. Diese Technik wird häufig von Gegnern verwendet, um Zugriff auf das Dateisystem des Hosts zu erhalten.

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, können die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert sein. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Wenn dieser Container-Start erwartet wird, wird empfohlen, eine Unterdrückungsregel zu verwenden, die aus Filterkriterien besteht, die auf dem Feld `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix` basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Persistence:Kubernetes/MaliciousIPCaller

Ein API häufig verwendetes, um dauerhaften Zugriff auf einen Kubernetes-Cluster zu erhalten, wurde von einer bekannten bösartigen IP-Adresse aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang von einer IP-Adresse aus aufgerufen wurde, die mit bekannten böswilligen Aktivitäten in Verbindung steht. Das API beobachtete Phänomen wird häufig mit Persistenztaktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Kubernetes-Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Ein API häufig verwendetes Verfahren, um dauerhaften Zugriff auf einen Kubernetes-Cluster zu erhalten, wurde von einer IP-Adresse aus auf einer benutzerdefinierten Bedrohungsliste aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang von einer IP-Adresse aus aufgerufen wurde, die in einer von Ihnen hochgeladenen Bedrohungsliste enthalten ist. Die mit dieser Erkenntnis verknüpfte Bedrohungsliste ist im Abschnitt Zusätzliche Informationen der Details zu einer Erkenntnis aufgeführt. Das API beobachtete Phänomen wird häufig mit Persistenztaktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Kubernetes-Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Persistence:Kubernetes/SuccessfulAnonymousAccess

Ein API häufig verwendetes Verfahren, um allgemeine Berechtigungen für einen Kubernetes-Cluster zu erhalten, wurde von einem nicht authentifizierten Benutzer aufgerufen.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein API Vorgang vom `system:anonymous` Benutzer erfolgreich aufgerufen wurde. APIAnrufe von `system:anonymous` sind nicht authentifiziert. Das beobachtete API Phänomen wird häufig mit Persistenztaktiken in Verbindung gebracht,

bei denen sich ein Angreifer Zugriff auf Ihren Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten. Diese Aktivität weist darauf hin, dass anonymer oder nicht authentifizierter Zugriff auf die im Ergebnis gemeldete API Aktion zulässig ist und bei anderen Aktionen möglicherweise zulässig ist. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im EKSAmazon-Benutzerhandbuch.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Persistence:Kubernetes/TorIPCaller

Ein API häufig verwendetes Verfahren, um dauerhaften Zugriff auf einen Kubernetes-Cluster zu erhalten, wurde von einer IP-Adresse des Tor-Ausgangsknotens aus aufgerufen.

Standard-Schweregrad: Mittel

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert dich darüber, dass eine von der IP-Adresse eines Tor-Ausgangsknotens aus aufgerufen API wurde. Das API beobachtete Phänomen wird häufig mit Persistenztaktiken in Verbindung gebracht, bei denen sich ein Angreifer Zugriff auf Ihren Kubernetes-Cluster verschafft hat und versucht, diesen Zugriff aufrechtzuerhalten. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, mit der Absicht, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Falls es sich bei dem in den Ergebnissen unter dem `KubernetesUserDetails` Abschnitt gemeldeten Benutzer um einen handelt`system:anonymous`, untersuchen Sie, warum der anonyme Benutzer die Berechtigungen aufrufen API und gegebenenfalls widerrufen durfte. Folgen Sie dazu den Anweisungen unter Bewährte Sicherheitsmethoden für Amazon EKS im EKS Amazon-Benutzerhandbuch. Wenn es sich bei dem Benutzer um einen authentifizierten Benutzer handelt, untersuchen Sie, ob die Aktivität legitim oder böswillig war. Wenn es sich bei der Aktivität um eine böswillige Aktivität handelte, sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Dem Standard-Servicekonto wurden Administratorrechte auf einem Kubernetes-Cluster gewährt.

Standard-Schweregrad: Hoch

- Funktion: EKS Audit-Logs

Diese Erkenntnis informiert Sie darüber, dass dem Standard-Servicekonto für einen Namespace in Ihrem Kubernetes-Cluster Administratorrechte gewährt wurden. Kubernetes erstellt ein Standard-Servicekonto für alle Namespaces im Cluster. Es weist Pods, die nicht explizit einem anderen Servicekonto zugeordnet wurden, automatisch das Standard-Servicekonto als Identität zu. Wenn das Standard-Servicekonto über Administratorrechte verfügt, kann dies dazu führen, dass Pods unbeabsichtigt mit Administratorrechten gestartet werden. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten nicht das Standard-Servicekonto verwenden, um Pods Berechtigungen zu erteilen. Stattdessen sollten Sie für jeden Workload ein eigenes Servicekonto erstellen und diesem Konto je nach Bedarf Berechtigungen erteilen. Um dieses Problem zu beheben, sollten Sie spezielle Servicekonten für all Ihre Pods und Workloads erstellen und die Pods und Workloads aktualisieren, um vom Standard-Servicekonto zu ihren dedizierten Konten zu migrieren. Anschließend sollten Sie die Administratorberechtigung aus dem Standard-Servicekonto entfernen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Policy:Kubernetes/AnonymousAccessGranted

Dem **`system:anonymous`** Benutzer wurde die API Berechtigung für einen Kubernetes-Cluster erteilt.

Standard-Schweregrad: Hoch

- Funktion: Audit-Logs EKS

Diese Erkenntnis informiert Sie darüber, dass ein Benutzer in Ihrem Kubernetes-Cluster erfolgreich ein `ClusterRoleBinding` oder `RoleBinding` erstellt hat, um den Benutzer `system:anonymous` an eine Rolle zu binden. Dies ermöglicht einen nicht authentifizierten Zugriff auf die von der Rolle zugelassenen API Operationen. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem `system:anonymous`-Benutzer oder der `system:unauthenticated`-Gruppe in Ihrem Cluster gewährt wurden, und unnötigen anonymen Zugriff widerrufen. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon EKS im EKSAmazon-Benutzerhandbuch. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Policy:Kubernetes/ExposedDashboard

Das Dashboard für einen Kubernetes-Cluster war im Internet verfügbar

Standard-Schweregrad: Mittel

- Funktion: EKS Audit-Logs

Diese Erkenntnis informiert Sie darüber, dass das Kubernetes-Dashboard für Ihren Cluster über einen Load Balancer-Service dem Internet zugänglich gemacht wurde. Ein offengelegtes Dashboard ermöglicht den Zugriff auf die Verwaltungsoberfläche Ihres Clusters über das Internet und ermöglicht

es Gegnern, eventuell vorhandene Lücken in der Authentifizierungs- und Zugriffssteuerung auszunutzen.

Empfehlungen zur Abhilfe:

Sie sollten sicherstellen, dass im Kubernetes-Dashboard eine starke Authentifizierung und Autorisierung durchgesetzt wird. Sie sollten auch eine Netzwerk-Zugriffssteuerung implementieren, um den Zugriff auf das Dashboard von bestimmten IP-Adressen aus zu beschränken.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Policy:Kubernetes/KubeflowDashboardExposed

Das Kubeflow-Dashboard für einen Kubernetes-Cluster war im Internet verfügbar

Standard-Schweregrad: Mittel

- Funktion: EKS Audit-Protokolle

Diese Erkenntnis informiert Sie darüber, dass das Kubeflow-Dashboard für Ihren Cluster über einen Load Balancer-Service dem Internet zugänglich gemacht wurde. Ein offengelegtes Kubeflow-Dashboard ermöglicht den Zugriff auf die Verwaltungsoberfläche Ihrer Kubeflow-Umgebung über das Internet und ermöglicht es Gegnern, eventuell vorhandene Lücken in der Authentifizierung und Zugriffssteuerung auszunutzen.

Empfehlungen zur Abhilfe:

Sie sollten sicherstellen, dass im Kubeflow-Dashboard eine starke Authentifizierung und Autorisierung durchgesetzt wird. Sie sollten auch eine Netzwerk-Zugriffssteuerung implementieren, um den Zugriff auf das Dashboard von bestimmten IP-Adressen aus zu beschränken.

Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Ein privilegierter Container mit Zugriff auf Root-Ebene wurde auf Ihrem Kubernetes-Cluster gestartet.

Standard-Schweregrad: Mittel

- Funktion: EKS Audit-Protokolle

Diese Erkenntnis informiert Sie darüber, dass ein privilegierter Container, der auf Ihrem Kubernetes-Cluster mithilfe eines Images gestartet wurde, das noch nie zuvor verwendet wurde, um privilegierte Container in Ihrem Cluster zu starten. Ein privilegierter Container hat Zugriff auf Root-Ebene auf den Host. Angreifer können als Taktik zur Erweiterung ihrer Rechte privilegierte Container starten, um sich Zugriff auf den Host zu verschaffen und ihn dann zu kompromittieren.

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, können die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert sein. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Ein Kubernetes, das API üblicherweise für den Zugriff auf Geheimnisse verwendet wird, wurde auf ungewöhnliche Weise aufgerufen.

Standard-Schweregrad: Mittel

- FunktionEKS: Audit-Logs

Dieses Ergebnis informiert Sie darüber, dass ein Kubernetes-Benutzer in Ihrem Cluster eine ungewöhnliche API Operation zum Abrufen vertraulicher Clustergeheimnisse aufgerufen hat. Das beobachtete Phänomen API wird häufig mit Taktiken für den Zugriff auf Anmeldeinformationen in Verbindung gebracht, die zu einer privilegierten Eskalation und weiterem Zugriff innerhalb Ihres Clusters führen können. Wenn dieses Verhalten nicht erwartet wird, kann dies entweder auf einen Konfigurationsfehler hinweisen oder darauf, dass Ihre AWS Anmeldeinformationen kompromittiert wurden.

Das beobachtete Phänomen API wurde durch das Modell des maschinellen Lernens (ML) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle API Benutzeraktivitäten innerhalb Ihres EKS Clusters und identifiziert ungewöhnliche Ereignisse, die auf Techniken zurückzuführen sind, die von nicht autorisierten Benutzern verwendet werden. Das ML-Modell verfolgt mehrere Faktoren des API Vorgangs, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten und den

Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API Anfrage finden Sie im Bereich mit den Suchdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Sie sollten die Berechtigungen überprüfen, die dem Kubernetes-Benutzer in Ihrem Cluster gewährt wurden, und sicherstellen, dass all diese Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell AWS kompromittierter Anmeldedaten.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

In Ihrem RoleBinding ClusterRoleBinding Kubernetes-Cluster wurde ein oder für eine übermäßig freizügige Rolle oder einen sensiblen Namespace erstellt oder geändert.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn ein RoleBinding oder jedoch das Oder ClusterRoleBinding beinhaltet, ist der Schweregrad Hoch ClusterRoles `admin`. `cluster-admin`

- Funktion: EKS Auditprotokolle

Diese Erkenntnis informiert Sie darüber, dass ein Benutzer in Ihrem Kubernetes-Cluster ein `RoleBinding` oder `ClusterRoleBinding` erstellt hat, um einen Benutzer an eine Rolle mit Administratorberechtigungen oder sensiblen Namespaces zu binden. Wenn dieses Verhalten nicht erwartet wird, kann dies entweder auf einen Konfigurationsfehler hinweisen oder darauf, dass Ihre AWS Anmeldeinformationen kompromittiert wurden.

Das beobachtete Phänomen API wurde durch das Modell des maschinellen Lernens (ML) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet

alle API Benutzeraktivitäten innerhalb Ihres Clusters. EKS Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt auch mehrere Faktoren des API Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API Anfrage finden Sie im Bereich mit den Suchdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Untersuchen Sie die dem Kubernetes-Benutzer erteilten Berechtigungen. Diese Berechtigungen sind in der Rolle und den beteiligten Subjekten in `RoleBinding` und `ClusterRoleBinding` definiert. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell AWS kompromittierter Anmeldedaten.

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Ein Befehl wurde in einem Pod auf ungewöhnliche Weise ausgeführt.

Standard-Schweregrad: Mittel

- Funktion: EKS Audit-Logs

Dieses Ergebnis informiert Sie darüber, dass ein Befehl in einem Pod mithilfe von Kubernetes Exec ausgeführt wurde. API Der Kubernetes Exec API ermöglicht die Ausführung beliebiger Befehle in einem Pod. Wenn dieses Verhalten für den Benutzer, den Namespace oder den Pod nicht erwartet wird, kann dies entweder auf einen Konfigurationsfehler hinweisen oder darauf, dass Ihre AWS Anmeldeinformationen kompromittiert wurden.

Das beobachtete Phänomen API wurde durch das Modell des maschinellen Lernens (ML) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle API Benutzeraktivitäten innerhalb Ihres Clusters. EKS Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt auch mehrere Faktoren des API Vorgangs,

z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API Anfrage finden Sie im Bereich mit den Suchdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn die Ausführung dieses Befehls unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zur Ausführung des Befehls verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell AWS kompromittierter Anmeldedaten.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Ein Workload wurde mit einem privilegierten Container auf ungewöhnliche Weise gestartet.

Standard-Schweregrad: Hoch

- Funktion: EKS Audit-Logs

Dieses Ergebnis informiert Sie darüber, dass ein Workload mit einem privilegierten Container in Ihrem EKS Amazon-Cluster gestartet wurde. Ein privilegierter Container hat Zugriff auf Root-Ebene auf den Host. Unbefugte Benutzer können privilegierte Container als Taktik zur Rechteerweiterung starten, um sich zunächst Zugriff auf den Host zu verschaffen und ihn dann zu kompromittieren.

Die beobachtete Erstellung oder Änderung eines Containers wurde durch das Modell des maschinellen Lernens (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer API - und Container-Image-Aktivitäten innerhalb Ihres Clusters. EKS Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt auch mehrere Faktoren des API Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, die in Ihrem

Konto beobachteten Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API Anfrage finden Sie im Bereich mit den Suchdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell AWS kompromittierter Anmeldedaten.

Wenn dieser Container-Start erwartet wird, empfiehlt es sich, eine Unterdrückungsregel mit Filterkriterien zu verwenden, die auf dem `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`-Feld basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount

Ein Workload wurde auf ungewöhnliche Weise bereitgestellt, wobei ein sensibler Host-Pfad innerhalb des Workloads eingehängt wurde.

Standard-Schweregrad: Hoch

- Funktion: EKS Audit-Logs

Diese Erkenntnis informiert Sie darüber, dass ein Workload mit einem Container gestartet wurde, der im Abschnitt `volumeMounts` einen sensiblen Host-Pfad enthielt. Dadurch ist der sensible Host-Pfad potenziell vom Container aus zugänglich und beschreibbar. Diese Technik wird häufig von Gegnern verwendet, um Zugriff auf das Dateisystem des Hosts zu erhalten.

Die beobachtete Erstellung oder Änderung eines Containers wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell

bewertet alle Benutzer API - und Container-Image-Aktivitäten innerhalb Ihres Clusters. EKS Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt auch mehrere Faktoren des API Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, die in Ihrem Konto beobachteten Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API Anfrage finden Sie im Bereich mit den Suchdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell AWS kompromittierter Anmeldedaten.

Wenn dieser Container-Start erwartet wird, empfiehlt es sich, eine Unterdrückungsregel mit Filterkriterien zu verwenden, die auf dem `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`-Feld basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Ein Workload wurde auf ungewöhnliche Weise gestartet.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Der Standardschweregrad ist Niedrig. Wenn der Workload jedoch einen potenziell verdächtigen Image-Namen enthält, z. B. ein bekanntes Pentest-Tool, oder einen Container, in dem beim Start ein potenziell verdächtiger Befehl ausgeführt wird, z. B. Reverse-Shell-Befehle, wird der Schweregrad dieses Ergebnistyps als Mittel eingestuft.

- Funktion: EKS Audit-Logs

Dieses Ergebnis informiert Sie darüber, dass ein Kubernetes-Workload in Ihrem Amazon-Cluster auf ungewöhnliche Weise erstellt oder geändert wurde, z. B. durch eine API Aktivität, neue Container-Images oder eine riskante Workload-Konfiguration. EKS Unbefugte Benutzer können privilegierte Container als Taktik zur Rechteerweiterung starten, um sich zunächst Zugriff auf den Host zu verschaffen und ihn dann zu kompromittieren.

Die beobachtete Erstellung oder Änderung eines Containers wurde anhand des ML-Modells (Machine Learning) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle Benutzer API - und Container-Image-Aktivitäten innerhalb Ihres Clusters. EKS Dieses ML-Modell identifiziert auch ungewöhnliche Ereignisse, die mit den von einem nicht autorisierten Benutzer verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt auch mehrere Faktoren des API Vorgangs, z. B. den Benutzer, der die Anfrage stellt, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, die in Ihrem Konto beobachteten Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API Anfrage finden Sie im Bereich mit den Suchdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn dieser Container-Start unerwartet erfolgt, wurden möglicherweise die Anmeldeinformationen der Benutzeridentität, die zum Starten des Containers verwendet wurde, kompromittiert. Sperren Sie dem Benutzer den Zugriff und machen Sie alle Änderungen rückgängig, die von einem Angreifer an Ihrem Cluster vorgenommen wurden. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell AWS kompromittierter Anmeldedaten.

Wenn dieser Container-Start erwartet wird, empfiehlt es sich, eine Unterdrückungsregel mit Filterkriterien zu verwenden, die auf dem `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`-Feld basieren. In den Filterkriterien sollte das `imagePrefix`-Feld dem in der Erkenntnis angegebenen Feld `imagePrefix` entsprechen. Weitere Informationen finden Sie unter Unterdrückungsregeln.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Eine sehr freizügige Rolle oder ClusterRole wurde auf ungewöhnliche Weise erstellt oder geändert.

Standard-Schweregrad: Niedrig

- Funktion: Audit-Logs EKS

Dieses Ergebnis informiert Sie darüber, dass ein Kubernetes-Benutzer in Ihrem Amazon-Cluster eine ungewöhnliche API Operation zum Erstellen eines `Role` oder `ClusterRole` mit übermäßigen Berechtigungen aufgerufen hat. EKS Akteure können die Rollenerstellung mit leistungsstarken Berechtigungen verwenden, um die Verwendung integrierter Administratorrollen zu vermeiden und so zu verhindern, dass sie entdeckt werden. Die übermäßigen Berechtigungen können zur Eskalation von Rechten, zur Ausführung von Remote-Code und möglicherweise zur Kontrolle über einen Namespace oder Cluster führen. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre -Anmeldeinformationen kompromittiert wurden.

Das beobachtete Ereignis API wurde durch das Modell des maschinellen Lernens (ML) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle API Benutzeraktivitäten innerhalb Ihres EKS Amazon-Clusters und identifiziert ungewöhnliche Ereignisse, die mit den von nicht autorisierten Benutzern verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt auch mehrere Faktoren des API Vorgangs, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, den verwendeten Benutzeragenten, die in Ihrem Konto beobachteten Container-Images und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API Anfrage finden Sie im Bereich mit den Suchdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Prüfen Sie die in `Role` oder `ClusterRole` definierten Berechtigungen, um sicherzustellen, dass alle Berechtigungen benötigt werden, und halten Sie sich an die Grundsätze der geringsten Berechtigung. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell AWS kompromittierter Anmeldedaten.

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Ein Benutzer hat seine Zugriffsberechtigungen auf ungewöhnliche Weise überprüft.

Standard-Schweregrad: Niedrig

- Funktion: EKS Audit-Logs

Diese Erkenntnis informiert Sie darüber, dass ein Benutzer in Ihrem Kubernetes-Cluster erfolgreich geprüft hat, ob die bekannten mächtigen Berechtigungen, die zu privilegierter Eskalation und Remote-Codeausführung führen können, zulässig sind. Ein gängiger Befehl, der verwendet wird, um die Berechtigungen eines Benutzers zu überprüfen, ist beispielsweise `kubectl auth can-i`. Wenn dieses Verhalten nicht erwartet wird, deutet dies möglicherweise auf einen Konfigurationsfehler hin oder darauf, dass Ihre Anmeldeinformationen kompromittiert wurden.

Das beobachtete API Objekt wurde durch das Modell des maschinellen Lernens (ML) zur Erkennung von GuardDuty Anomalien als anomal identifiziert. Das ML-Modell bewertet alle API Benutzeraktivitäten innerhalb Ihres EKS Amazon-Clusters und identifiziert ungewöhnliche Ereignisse, die mit den von nicht autorisierten Benutzern verwendeten Techniken zusammenhängen. Das ML-Modell verfolgt auch mehrere Faktoren des API Vorgangs, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, die Überprüfung der Berechtigungen und den Namespace, den der Benutzer verwendet hat. Die ungewöhnlichen Details der API Anfrage finden Sie in der GuardDuty Konsole im Bereich mit den Suchdetails.

Empfehlungen zur Abhilfe:

Prüfen Sie die dem Kubernetes-Benutzer erteilten Berechtigungen, um sicherzustellen, dass alle Berechtigungen benötigt werden. Wenn die Berechtigungen irrtümlich oder böswillig erteilt wurden, sollten Sie dem Benutzer den Zugriff entziehen und alle von einem Angreifer an Ihrem Cluster vorgenommenen Änderungen rückgängig machen. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Falls Ihre AWS Anmeldeinformationen kompromittiert wurden, finden Sie weitere Informationen unterBehebung potenziell AWS kompromittierter Anmeldedaten.

Runtime Monitoring: Typen finden

Amazon GuardDuty generiert die folgenden Runtime Monitoring-Ergebnisse, um auf potenzielle Bedrohungen hinzuweisen, die auf dem Verhalten von EC2 Amazon-Hosts und Containern in Ihren EKS Amazon-Clustern, Fargate- und ECS Amazon-Workloads sowie Amazon-Instances auf Betriebssystemebene basieren. EC2

> **Note**
>
> Die Erkenntnistypen der Laufzeit-Überwachung basieren auf den Laufzeit-Protokollen, die von Hosts gesammelt wurden. Die Protokolle enthalten Felder wie Dateipfade, die möglicherweise von einem böswilligen Akteur kontrolliert werden. Diese Felder sind auch in den GuardDuty Ergebnissen enthalten, um einen Laufzeitkontext bereitzustellen. Wenn Sie die Ergebnisse von Runtime Monitoring außerhalb der GuardDuty Konsole verarbeiten, müssen Sie die Suchfelder bereinigen. Sie können beispielsweise Suchfelder HTML codieren, wenn Sie sie auf einer Webseite anzeigen.

Themen

- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution
- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted
- Execution:Runtime/SuspiciousShellCreated
- PrivilegeEscalation:Runtime/ElevationToRoot

CryptoCurrency:Runtime/BitcoinTool.B

Eine EC2 Amazon-Instance oder ein Container fragt eine IP-Adresse ab, die mit einer kryptowährungsbezogenen Aktivität verknüpft ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder ein Container in Ihrer AWS Umgebung eine IP-Adresse abfragt, die mit einer kryptowährungsbezogenen Aktivität verknüpft ist. Bedrohungsakteure können versuchen, die Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2 Instanz oder einen Container verwenden, um Kryptowährungen zu minen oder zu verwalten, oder wenn eine dieser Instanzen anderweitig an Blockchain-Aktivitäten beteiligt ist, könnte das CryptoCurrency:Runtime/BitcoinTool.B Ergebnis die erwartete Aktivität für Ihre Umgebung darstellen. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Filterkriterium sollte das Attribut Erkenntnistyp mit dem Wert `CryptoCurrency:Runtime/BitcoinTool.B` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance oder die Container-Image-ID des Containers sein, der an Aktivitäten im Zusammenhang mit Kryptowährungen oder Blockchain beteiligt ist. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B

Eine EC2 Amazon-Instance oder ein Container fragt eine IP ab, die einem bekannten Command-and-Control-Server zugeordnet ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder ein Container in Ihrer AWS Umgebung eine IP abfragt, die einem bekannten Command-and-Control-Server (C&C) zugeordnet ist. Die aufgeführte Instance oder der aufgeführte Container sind möglicherweise

gefährdet. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnetz ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen ServerPCs, mobile Geräte und Geräte für das Internet der Dinge gehören können, die mit einer gängigen Art von Malware infiziert sind und von ihr kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnetzes kann der C&C-Server auch Befehle ausgeben, um einen Distributed-Denial-of-Service () -Angriff zu starten. DDoS

> **Note**
>
> Wenn die abgefragte IP log4j-bezogen ist, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

UnauthorizedAccess:Runtime/TorRelay

Ihre EC2 Amazon-Instance oder ein Container stellt als Tor-Relay Verbindungen zu einem Tor-Netzwerk her.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine EC2 Instance oder ein Container in Ihrer AWS Umgebung Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass

sie als Tor-Relay fungiert. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor-Relays erhöhen die Anonymität der Kommunikation, indem sie den möglicherweise illegalen Datenverkehr des Kunden von einem Tor-Relay zu einem anderen weiterleiten.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Um die potenziell gefährdete Ressource zu identifizieren, sieh dir den Ressourcentyp im Ergebnisfenster der GuardDuty Konsole an.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

UnauthorizedAccess:Runtime/TorClient

Deine EC2 Amazon-Instance oder ein Container stellt Verbindungen zu einem Tor Guard- oder Authority-Knoten her.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert dich darüber, dass eine EC2 Instance oder ein Container in deiner AWS Umgebung Verbindungen zu einem Tor Guard- oder einem Authority-Knoten herstellt. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor Guards und Authority-Knoten fungieren als erste Gateways in ein Tor-Netzwerk. Dieser Verkehr kann darauf hinweisen, dass diese EC2 Instanz oder der Container potenziell kompromittiert wurde und als Client in einem Tor-Netzwerk fungiert. Dieser Befund kann auf einen unbefugten Zugriff auf Ihre AWS Ressourcen hinweisen, mit der Absicht, die wahre Identität des Angreifers zu verbergen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic

Eine EC2 Amazon-Instance oder ein Container versucht, mit der IP-Adresse eines Remote-Hosts zu kommunizieren, bei dem es sich um ein bekanntes schwarzes Loch handelt.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder ein Container in Ihrer AWS Umgebung möglicherweise kompromittiert ist, weil versucht wird, mit der IP-Adresse eines schwarzen Lochs (oder Sink Hole) zu kommunizieren. Schwarze Löcher bezeichnen Orte im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend gelöscht wird, ohne die Quelle zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben. Die IP-Adresse eines schwarzen Lochs gibt einen Hostcomputer an, der nicht ausgeführt wird, oder eine Adresse, der kein Host zugewiesen wurde.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/DropPoint

Eine EC2 Amazon-Instance oder ein Container versucht, mit der IP-Adresse eines Remote-Hosts zu kommunizieren, der bekanntermaßen Anmeldeinformationen und andere gestohlene Daten enthält, die von Malware erfasst wurden.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine EC2 Instance oder ein Container in Ihrer AWS Umgebung versucht, mit der IP-Adresse eines Remote-Hosts zu kommunizieren, auf dem sich bekanntermaßen Anmeldeinformationen und andere gestohlene Daten befinden, die von Malware erfasst wurden.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Eine EC2 Amazon-Instance oder ein Container fragt einen Domainnamen ab, der mit einer Kryptowährungsaktivität verknüpft ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder ein Container in Ihrer AWS Umgebung einen Domainnamen abfragt, der mit Bitcoin oder anderen kryptowährungsbezogenen Aktivitäten verknüpft ist. Bedrohungsakteure können versuchen, die

Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2 Instanz oder diesen Container verwenden, um Kryptowährungen zu minen oder zu verwalten, oder wenn eine dieser Instanzen anderweitig an Blockchain-Aktivitäten beteiligt ist, könnte das CryptoCurrency:Runtime/BitcoinTool.B!DNS Ergebnis eine erwartete Aktivität für Ihre Umgebung sein. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `CryptoCurrency:Runtime/BitcoinTool.B!DNS` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance oder die Container-Image-ID des Containers sein, der an Aktivitäten im Zusammenhang mit Kryptowährungen oder Blockchain beteiligt ist. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B!DNS

Eine EC2 Amazon-Instance oder ein Container fragt einen Domainnamen ab, der einem bekannten Command-and-Control-Server zugeordnet ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder der Container in Ihrer AWS Umgebung einen Domainnamen abfragt, der einem bekannten Command-and-Control-Server (C&C) zugeordnet ist. Die aufgelistete EC2 Instance oder der Container ist möglicherweise kompromittiert. Command-and-control-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnetz ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen ServerPCs, mobile Geräte und Geräte für das Internet der Dinge gehören können, die mit einer gängigen Art von Malware infiziert sind und von ihr kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnetzes kann der C&C-Server auch Befehle ausgeben, um einen Distributed-Denial-of-Service () -Angriff zu starten. DDoS

> **Note**
>
> Wenn der abgefragte Domainname mit log4j zu tun hat, enthalten die Felder der zugehörigen Erkenntnis die folgenden Werte:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> Um zu testen, wie dieser Befundtyp GuardDuty generiert wird, können Sie von Ihrer Instance aus (`dig`für Linux oder Windows) eine DNS Anfrage `nslookup` für eine Testdomäne stellen. `guarddutyc2activityb.com`

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic!DNS

Eine EC2 Amazon-Instance oder ein Container fragt einen Domainnamen ab, der an eine Black-Hole-IP-Adresse umgeleitet wird.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder der Container in Ihrer AWS Umgebung möglicherweise kompromittiert ist, weil sie einen Domainnamen abfragt, der an eine Black-Hole-IP-Adresse umgeleitet wird. Schwarze Löcher bezeichnen Orte im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend gelöscht wird, ohne die Quelle zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/DropPoint!DNS

Eine EC2 Amazon-Instance oder ein Container fragt den Domainnamen eines Remote-Hosts ab, der bekanntermaßen Anmeldeinformationen und andere gestohlene Daten enthält, die von Malware erfasst wurden.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine EC2 Instance oder ein Container in Ihrer AWS Umgebung den Domainnamen eines Remote-Hosts abfragt, der bekanntermaßen Anmeldeinformationen und andere gestohlene Daten enthält, die von Malware erfasst wurden.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/DGADomainRequest.C!DNS

Eine EC2 Amazon-Instance oder ein Container fragt algorithmisch generierte Domains ab. Solche Domains werden häufig von Malware verwendet und können ein Hinweis auf eine kompromittierte EC2 Instance oder einen Container sein.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder der Container in Ihrer AWS Umgebung versucht, Domänen des Algorithmus zur Domänengenerierung (DGA) abzufragen. Ihre Ressource wurde möglicherweise kompromittiert.

DGAswerden verwendet, um in regelmäßigen Abständen eine große Anzahl von Domainnamen zu generieren, die als Treffpunkte mit ihren Command-and-Control-Servern (C&C) verwendet werden können. Command-and-Control-Server sind Computer, die Befehle an die Mitglieder eines Botnets senden. Hierbei handelt es sich um eine Ansammlung von mit dem Internet verbundenen Geräten, die infiziert sind und von einer gängigen Malware kontrolliert werden. Die große Anzahl potenzieller Rendezvous Points erschwert ein effektives Stilllegen von Botnets, da infizierte Computer versuchen, einige dieser Domainnamen täglich zu kontaktieren, um Updates oder Befehle zu erhalten.

> **Note**
>
> Dieses Ergebnis basiert auf bekannten DGA Domänen aus Threat-Intelligence-Feeds. GuardDuty

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/DriveBySourceTraffic!DNS

Eine EC2 Amazon-Instance oder ein Container fragt den Domainnamen eines Remote-Hosts ab, der eine bekannte Quelle für Drive-By-Download-Angriffe ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder der Container in Ihrer AWS Umgebung möglicherweise gefährdet ist, weil er den Domainnamen eines Remote-Hosts abfragt, der eine bekannte Quelle für Drive-by-Download-Angriffe ist. Hierbei handelt es sich um unbeabsichtigte Downloads von Computersoftware aus dem Internet, die eine automatische Installation von Viren, Spyware oder Malware auslösen kann.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Trojan:Runtime/PhishingDomainRequest!DNS

Eine EC2 Amazon-Instance oder ein Container fragt Domains ab, die an Phishing-Angriffen beteiligt sind.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass es in Ihrer AWS Umgebung eine EC2 Instance oder einen Container gibt, der versucht, eine Domain abzufragen, die an Phishing-Angriffen beteiligt ist. Phishing-Domains werden von jemandem eingerichtet, der sich als rechtmäßige Institution ausgibt, um Personen dazu zu bringen, sensible Daten bereitzustellen, wie beispielsweise personenbezogene Informationen, Bank- und Kreditkartendaten oder Passwörter. Ihre EC2 Instance oder der Container

versucht möglicherweise, sensible Daten abzurufen, die auf einer Phishing-Website gespeichert sind, oder versucht möglicherweise, eine Phishing-Website einzurichten. Ihre EC2 Instance oder der Container ist möglicherweise kompromittiert.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Impact:Runtime/AbusedDomainRequest.Reputation

Eine EC2 Amazon-Instance oder ein Container fragt einen Domainnamen mit niedriger Reputation ab, der mit bekanntermaßen missbrauchten Domains verknüpft ist.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder der Container in Ihrer AWS Umgebung einen Domainnamen mit geringer Reputation abfragt, der mit bekanntermaßen missbrauchten Domains oder IP-Adressen verknüpft ist. Beispiele für missbräuchliche Domains sind Top-Level-Domainnamen (TLDs) und Second-Level-Domainnamen (2LDs), die kostenlose Subdomainregistrierungen bieten, sowie dynamische Anbieter. DNS Bedrohungsakteure nutzen diese Services in der Regel, um Domains kostenlos oder zu geringen Kosten zu registrieren. Bei Domains mit geringer Reputation in dieser Kategorie kann es sich auch um abgelaufene Domains handeln, die auf die Parking-IP-Adresse eines Registrars zurückgehen und daher möglicherweise nicht mehr aktiv sind. Bei einer Parking-IP leitet ein Registrar den Verkehr für Domains weiter, die mit keinem Service verknüpft wurden. Die aufgelistete EC2 Amazon-Instance oder der Container können gefährdet sein, da Bedrohungsakteure diese Registrare oder Dienste häufig für C&C und die Verbreitung von Malware nutzen.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Impact:Runtime/BitcoinDomainRequest.Reputation

Eine EC2 Amazon-Instance oder ein Container fragt einen Domainnamen mit niedriger Reputation ab, der mit kryptowährungsbezogenen Aktivitäten verknüpft ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder der Container in Ihrer AWS Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit Bitcoin oder anderen kryptowährungsbezogenen Aktivitäten in Verbindung steht. Bedrohungsakteure können versuchen, die Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn Sie diese EC2 Instance oder den Container verwenden, um Kryptowährungen zu minen oder zu verwalten, oder wenn diese Ressourcen anderweitig an Blockchain-Aktivitäten beteiligt sind, könnte dieses Ergebnis die erwartete Aktivität für Ihre Umgebung darstellen. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen.

Das erste Filterkriterium sollte das Attribut Erkenntnistyp mit dem Wert `Impact:Runtime/BitcoinDomainRequest.Reputation` verwenden. Das zweite Filterkriterium sollte die Instance-ID der Instance oder die Container-Image-ID des Containers sein, der an Aktivitäten im Zusammenhang mit Kryptowährung oder Blockchain beteiligt ist. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Impact:Runtime/MaliciousDomainRequest.Reputation

Eine EC2 Amazon-Instance oder ein Container fragt eine Domain mit niedriger Reputation ab, die mit bekannten bösartigen Domains verknüpft ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder der Container in Ihrer AWS Umgebung einen Domainnamen mit niedriger Reputation abfragt, der mit bekannten bösartigen Domains oder IP-Adressen verknüpft ist. Beispielsweise können Domains mit einer bekannten Sinkhole-IP-Adresse verknüpft sein. Sinkhole-Domains sind Domains, die zuvor von einem Bedrohungsakteur kontrolliert wurden, und Anfragen an sie können darauf hinweisen, dass die Instance kompromittiert wurde. Diese Domains können auch mit bekannten böswilligen Kampagnen oder Algorithmen zur Domain-Generierung korreliert sein.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Eine EC2 Amazon-Instance oder ein Container fragt einen Domainnamen mit geringer Reputation ab, der aufgrund seines Alters oder seiner geringen Beliebtheit verdächtig ist.

Standard-Schweregrad: Niedrig

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass die aufgelistete EC2 Instance oder der Container in Ihrer AWS Umgebung einen Domainnamen mit niedriger Reputation abfragt, bei dem der Verdacht besteht, dass er bösartig ist. Es wurden Merkmale dieser Domain festgestellt, die mit zuvor beobachteten bösartigen Domains übereinstimmten. Unser Reputationsmodell konnte sie jedoch nicht definitiv mit einer bekannten Bedrohung in Verbindung bringen. Diese Domains werden in der Regel neu beobachtet oder erhalten nur wenig Datenverkehr.

Domains mit niedriger Reputation basieren auf einem Reputations-Punkte-Modell. Dieses Modell bewertet und bewertet die Eigenschaften einer Domain, um zu ermitteln, ob es sich um eine bösartige Domain handeln könnte.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Eine EC2 Amazon-Instance oder ein Container führt DNS Suchvorgänge durch, die zum Instance-Metadaten-Service weitergeleitet werden.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

> **Note**
>
> Derzeit wird dieser Findetyp nur für AMD64 Architektur unterstützt.

Dieses Ergebnis informiert Sie darüber, dass eine EC2 Instance oder ein Container in Ihrer AWS Umgebung eine Domain abfragt, die in die EC2 Metadaten-IP-Adresse (169.254.169.254) aufgelöst wird. Eine solche DNS Abfrage kann darauf hinweisen, dass die Instance das Ziel einer Rebinding-Technik ist. DNS Diese Technik kann verwendet werden, um Metadaten von einer EC2 Instanz abzurufen, einschließlich der mit der Instanz verknüpften IAM Anmeldeinformationen.

DNSBeim erneuten Binden wird eine Anwendung, die auf der EC2 Instanz ausgeführt wird, dazu gebracht, Rückgabedaten von a zu ladenURL, wobei der Domainname in der in die EC2 Metadaten-IP-Adresse () URL aufgelöst wird. `169.254.169.254` Dadurch wird die Anwendung veranlasst, auf EC2 Metadaten zuzugreifen und sie möglicherweise dem Angreifer zur Verfügung zu stellen.

Der Zugriff auf EC2 Metadaten mithilfe von DNS Rebinding ist nur möglich, wenn auf der EC2 Instanz eine anfällige Anwendung ausgeführt wird, die die Injektion von ermöglichtURLs, oder wenn jemand URL in einem Webbrowser, der auf der EC2 Instanz läuft, auf sie zugreift.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Als Reaktion auf dieses Ergebnis sollten Sie prüfen, ob auf der EC2 Instance oder im Container eine anfällige Anwendung läuft oder ob jemand einen Browser verwendet hat, um auf die in der Entdeckung identifizierte Domain zuzugreifen. Wenn die Ursache eine anfällige Anwendung ist, beheben Sie die Schwachstelle. Wenn ein Benutzer die identifizierte Domain aufgerufen hat, blockieren Sie die Domain oder verhindern Sie, dass Benutzer darauf zugreifen. Wenn Sie feststellen, dass dieses Ergebnis mit einem der oben genannten Fälle zusammenhängt, widerrufen Sie die mit der EC2 Instanz verknüpfte Sitzung.

Manche AWS Kunden ordnen die Metadaten-IP-Adresse bewusst einem Domainnamen auf ihren autoritativen DNS Servern zu. Wenn dies in Ihrer -Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Filterkriterium sollte das Attribut Erkenntnistyp mit dem Wert

`UnauthorizedAccess:Runtime/MetaDataDNSRebind` verwenden. Das zweite Filterkriterium sollte die DNSAnforderungsdomäne oder die Container-Image-ID des Containers sein. Der Wert der DNSAnforderungsdomäne sollte mit der Domain übereinstimmen, die Sie der Metadaten-IP-Adresse (`169.254.169.254`) zugeordnet haben. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/NewBinaryExecuted

Eine neu erstellte oder kürzlich geänderte Binärdatei in einem Container wurde ausgeführt.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass eine neu erstellte oder kürzlich geänderte Binärdatei in einem Container ausgeführt wurde. Es ist eine bewährte Methode, Container zur Laufzeit unveränderlich zu halten. Binärdateien, Skripten oder Bibliotheken sollten während der Lebensdauer des Containers nicht erstellt oder geändert werden. Dieses Verhalten weist darauf hin, dass ein böswilliger Akteur, der Zugriff auf den Container erlangt hat, im Rahmen der potenziellen Bedrohung Malware oder andere Software heruntergeladen und ausgeführt hat. Diese Art von Aktivität könnte zwar ein Hinweis auf eine Gefährdung sein, ist aber auch ein übliches Nutzungsmuster. GuardDuty Verwendet daher Mechanismen zur Identifizierung verdächtiger Instanzen dieser Aktivität und generiert diesen Befundtyp nur für verdächtige Fälle.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/DockerSocketAccessed

Ein Prozess in einem Container kommuniziert über den Docker-Socket mit dem Docker-Daemon.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Der Docker-Socket ist ein Unix-Domain-Socket, den Docker-Daemon (`dockerd`) verwendet, um mit seinen Clients zu kommunizieren. Ein Client kann verschiedene Aktionen ausführen, z. B. das Erstellen von Containern, indem er über den Docker-Socket mit dem Docker-Daemon kommuniziert. Es ist verdächtig, dass ein Container-Prozess auf den Docker-Socket zugreift. Ein Container-Prozess kann den Container verlassen und Zugriff auf Host-Ebene erhalten, indem er mit dem Docket-Socket kommuniziert und einen privilegierten Container erstellt.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/RuncContainerEscape

Ein Versuch, einem Container über RunC zu entkommen, wurde festgestellt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

RunC ist die Low-Level-Container-Runtime, die Container-Laufzeiten auf hoher Ebene wie Docker und Containerd verwenden, um Container zu erzeugen und auszuführen. RunC wird immer mit Root-Rechten ausgeführt, da es die Low-Level-Aufgabe, einen Container zu erstellen, ausführen muss. Ein

Bedrohungsakteur kann sich Zugriff auf Host-Ebene verschaffen, indem er eine Sicherheitslücke in der RunC-Binärdatei entweder modifiziert oder ausnutzt.

Dieses Ergebnis deckt Änderungen an der RunC-Binärdatei und mögliche Versuche auf, die folgenden RunC-Schwachstellen auszunutzen:

- CVE-2019-5736— CVE-2019-5736 Bei der Ausnutzung von wird die RunC-Binärdatei aus einem Container heraus überschrieben. Dieses Ergebnis wird ausgelöst, wenn die RunC-Binärdatei durch einen Prozess in einem Container geändert wird.
- CVE-2024-21626— CVE-2024-21626 Bei der Ausnutzung von wird das aktuelle Arbeitsverzeichnis (CWD) oder ein Container auf einen offenen Dateideskriptor gesetzt. `/proc/self/fd/`*`FileDescriptor`* Dieser Befund wird aufgerufen, wenn ein Container-Prozess mit einem aktuellen Arbeitsverzeichnis darunter erkannt `/proc/self/fd/` wird, zum Beispiel. `/proc/self/fd/7`

Dieses Ergebnis kann darauf hindeuten, dass ein böswilliger Akteur versucht hat, einen der folgenden Containertypen auszunutzen:

- Ein neuer Container mit einem vom Angreifer kontrollierten Image.
- Ein vorhandener Container, auf den der Akteur mit Schreibberechtigungen für die RunC-Binärdatei auf Hostebene zugreifen konnte.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Ein Versuch, einem Container durch den CGroups Release-Agent zu entkommen, wurde festgestellt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass ein Versuch erkannt wurde, eine Release-Agent-Datei für eine Kontrollgruppe (Cgroup) zu ändern. Linux verwendet Kontrollgruppen (Cgroups), um die Ressourcennutzung einer Reihe von Prozessen einzuschränken, zu berücksichtigen und zu isolieren. Jede Cgroup hat eine Release-Agent-Datei (`release_agent`), ein Skript, das Linux ausführt, wenn ein Prozess innerhalb der Cgroup beendet wird. Die Release-Agent-Datei wird immer auf Host-Ebene ausgeführt. Ein Bedrohungsakteur in einem Container kann zum Host entkommen, indem er beliebige Befehle in die Release-Agent-Datei schreibt, die zu einer Cgroup gehört. Wenn ein Prozess innerhalb dieser Cgroup beendet wird, werden die vom Akteur geschriebenen Befehle ausgeführt.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Proc

In einem Container oder einer EC2 Amazon-Instance wurde eine Prozessinjektion mithilfe des proc-Dateisystems festgestellt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Bei der Prozessinjektion handelt es sich um eine Technik, mit der Bedrohungsakteure Code in Prozesse einschleusen, um Schutzmaßnahmen zu umgehen und möglicherweise Rechte zu erweitern. Das proc-Dateisystem (procfs) ist ein spezielles Dateisystem in Linux, das den virtuellen Speicher eines Prozesses als Datei darstellt. Der Pfad dieser Datei ist `/proc/PID/mem`, wobei `PID` die eindeutige ID des Prozesses ist. Ein Bedrohungsakteur kann in diese Datei schreiben, um Code in den Prozess einzuschleusen. Diese Erkenntnis identifiziert potenzielle Versuche, in diese Datei zu schreiben.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

In einem Container oder einer EC2 Amazon-Instance wurde eine Prozessinjektion mithilfe eines ptrace-Systemaufrufs festgestellt.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Bei der Prozessinjektion handelt es sich um eine Technik, mit der Bedrohungsakteure Code in Prozesse einschleusen, um Schutzmaßnahmen zu umgehen und möglicherweise Rechte zu erweitern. Ein Prozess kann den ptrace-Systemaufruf verwenden, um Code in einen anderen Prozess einzuschleusen. Diese Erkenntnis identifiziert einen möglichen Versuch, mithilfe des Systemaufrufs ptrace Code in einen Prozess einzuschleusen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

In einem Container oder einer EC2 Amazon-Instance wurde eine Prozessinjektion durch direktes Schreiben in den virtuellen Speicher erkannt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Bei der Prozessinjektion handelt es sich um eine Technik, mit der Bedrohungsakteure Code in Prozesse einschleusen, um Schutzmaßnahmen zu umgehen und möglicherweise Rechte zu erweitern. Ein Prozess kann einen Systemaufruf wie `process_vm_writev` verwenden, um Code direkt in den virtuellen Speicher eines anderen Prozesses einzuschleusen. Diese Erkenntnis identifiziert einen möglichen Versuch, mithilfe eines Systemaufrufs Code in den virtuellen Speicher eines Prozesses einzuschleusen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/ReverseShell

Ein Prozess in einem Container oder einer EC2 Amazon-Instance hat eine umgekehrte Shell erstellt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Eine Reverse-Shell ist eine Shell-Sitzung, die auf einer Verbindung erstellt wird, die vom Zielhost zum Host des Akteurs initiiert wird. Dies ist das Gegenteil einer normalen Shell, die vom Host des Akteurs zum Host des Ziels initiiert wird. Bedrohungsakteure erstellen eine Reverse-Shell, um Befehle auf dem Ziel auszuführen, nachdem sie sich den ersten Zugriff auf das Ziel verschafft haben. Diese Erkenntnis weist auf einen möglichen Versuch hin, eine Reverse-Shell zu erstellen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, wurde Ihr Ressourcentyp möglicherweise kompromittiert.

DefenseEvasion:Runtime/FilelessExecution

Ein Prozess in einem Container oder einer EC2 Amazon-Instance führt Code aus dem Speicher aus.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, wenn ein Prozess mit einer im Speicher befindlichen ausführbaren Datei auf der Festplatte ausgeführt wird. Dabei handelt es sich um eine gängige Technik zur Umgehung von Schutzmaßnahmen, bei der verhindert wird, dass die schädliche ausführbare Datei auf die Festplatte geschrieben wird, um der Erkennung durch Dateisystem-Scans zu entgehen. Diese Technik wird zwar von Schadsoftware verwendet, hat aber auch einige legitime Anwendungsfälle. Eines der Beispiele ist ein just-in-time (JIT) -Compiler, der kompilierten Code in den Speicher schreibt und ihn aus dem Speicher ausführt.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der Konsole. GuardDuty

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Impact:Runtime/CryptoMinerExecuted

Ein Container oder eine EC2 Amazon-Instance führt eine Binärdatei aus, die mit einer Cryptocurrency-Mining-Aktivität verknüpft ist.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Container oder eine EC2 Instance in Ihrer AWS Umgebung eine Binärdatei ausführt, die mit einer Mining-Aktivität für Kryptowährungen verknüpft

ist. Bedrohungsakteure können versuchen, die Kontrolle über Datenverarbeitungsressourcen zu übernehmen, um sie böswillig für das unerlaubte Mining von Kryptowährungen umzuwidmen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcentypen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp im Ergebnisfenster der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie in den Ergebnisdetails in der GuardDuty Konsole unter Ressourcentyp und dann unterBehebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/NewLibraryLoaded

Eine neu erstellte oder kürzlich geänderte Bibliothek wurde von einem Prozess in einen Container geladen.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Diese Erkenntnis informiert Sie darüber, dass eine Bibliothek während der Laufzeit in einem Container erstellt oder geändert und von einem Prozess geladen wurde, der innerhalb des Containers ausgeführt wird. Es ist eine bewährte Methode, Container zur Laufzeit unveränderlich zu halten. Binärdateien, Skripten oder Bibliotheken sollten während der Lebensdauer des Containers nicht erstellt oder geändert werden. Das Laden einer neu erstellten oder geänderten Bibliothek in einen Container kann auf verdächtige Aktivitäten hinweisen. Dieses Verhalten weist auf einen böswilligen Akteur hin, der sich Zugriff auf den Container verschafft und im Rahmen der potenziellen Sicherheitslücke Malware oder andere Software heruntergeladen und ausgeführt hat. Diese Art von Aktivität könnte zwar ein Hinweis auf eine Beeinträchtigung sein, ist aber auch ein übliches Nutzungsmuster. GuardDuty Verwendet daher Mechanismen zur Identifizierung verdächtiger Instanzen dieser Aktivität und generiert diesen Befundtyp nur für verdächtige Fälle.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Ein Prozess in einem Container hat zur Laufzeit ein Host-Dateisystem gemountet.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Bei mehreren Techniken zur Container-Escape-Methode wird zur Laufzeit ein Host-Dateisystem in einem Container gemountet. Diese Erkenntnis informiert Sie darüber, dass ein Prozess in einem Container möglicherweise versucht hat, ein Host-Dateisystem zu mounten, was auf einen Fluchtversuch zum Host hindeuten kann.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/UserfaultfdUsage

Ein Prozess verwendete **`userfaultfd`**-Systemaufrufe, um Seitenfehler im Benutzerbereich zu behandeln.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Typischerweise werden Seitenfehler vom Kernel im Kernel-Space behandelt. Ein `userfaultfd`-Systemaufruf ermöglicht es einem Prozess jedoch, Seitenfehler in einem Dateisystem in der Benutzerumgebung zu behandeln. Dies ist eine nützliches Feature, die die Implementierung von

Dateisystemen in der Benutzerumgebung ermöglicht. Andererseits kann sie auch von einem potenziell bösartigen Prozess verwendet werden, um den Kernel von der Benutzerumgebung aus zu unterbrechen. Das Unterbrechen des Kernels mithilfe eines `userfaultfd`-Systemaufrufs ist eine gängige Ausnutzungstechnik, um Race-Fenster zu verlängern, während die Kernel-Race-Bedingungen ausgenutzt werden. Die Verwendung von `userfaultfd` kann auf verdächtige Aktivitäten auf der Amazon Elastic Compute Cloud (AmazonEC2) -Instance hinweisen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/SuspiciousTool

In einem Container oder einer EC2 Amazon-Instance wird eine Binärdatei oder ein Binärskript ausgeführt, das häufig in offensiven Sicherheitsszenarien wie Pentesting verwendet wird.

Standardschweregrad: Variabel

Der Schweregrad dieser Feststellung kann entweder hoch oder niedrig sein, je nachdem, ob das erkannte verdächtige Tool als doppelter Verwendungszweck oder ausschließlich für anstößige Zwecke eingestuft wird.

- Feature: Laufzeit-Überwachung

Dieser Befund informiert Sie darüber, dass ein verdächtiges Tool auf einer EC2 Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wurde. Dazu gehören Tools, die bei Pentesting-Projekten verwendet werden, auch bekannt als Backdoor-Tools, Netzwerkscanner und Netzwerk-Sniffer. All diese Tools können in harmlosen Kontexten eingesetzt werden, werden aber auch häufig von Bedrohungsakteuren mit böswilligen Absichten eingesetzt. Die Beobachtung anstößiger Sicherheitstools könnte darauf hindeuten, dass die zugehörige EC2 Instance oder der zugehörige Container kompromittiert wurde.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieser Befund nur generiert wird, wenn die zugehörige Aktivität und der zugehörige Kontext potenziell verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/SuspiciousCommand

Ein verdächtiger Befehl wurde auf einer EC2 Amazon-Instance oder einem Container ausgeführt, der auf eine Kompromittierung hindeutet.

Standardschweregrad: Variabel

Je nach Auswirkung des beobachteten Schadmusters kann der Schweregrad dieses Erkennungstyps entweder niedrig, mittel oder hoch sein.

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein verdächtiger Befehl ausgeführt wurde, und weist darauf hin, dass eine EC2 Amazon-Instance oder ein Container in Ihrer AWS Umgebung kompromittiert wurde. Dies kann bedeuten, dass entweder eine Datei von einer verdächtigen Quelle heruntergeladen und dann ausgeführt wurde oder dass ein laufender Prozess in seiner Befehlszeile ein bekanntes bösartiges Muster anzeigt. Dies deutet weiter darauf hin, dass Malware auf dem System ausgeführt wird.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieser Befund nur dann generiert wird, wenn die zugehörige Aktivität und der zugehörige Kontext potenziell verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

DefenseEvasion:Runtime/SuspiciousCommand

Ein Befehl wurde auf der aufgelisteten EC2 Amazon-Instance oder einem Container ausgeführt. Er versucht, einen Linux-Abwehrmechanismus wie eine Firewall oder wichtige Systemdienste zu ändern oder zu deaktivieren.

Standardschweregrad: Variabel

Je nachdem, welcher Abwehrmechanismus geändert oder deaktiviert wurde, kann der Schweregrad dieses Erkennungstyps entweder hoch, mittel oder niedrig sein.

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Befehl ausgeführt wurde, der versucht, einen Angriff vor den Sicherheitsdiensten des lokalen Systems zu verbergen. Dazu gehören Aktionen wie das Deaktivieren der Unix-Firewall, das Ändern lokaler IP-Tabellen, das Entfernen von crontab Einträgen, das Deaktivieren eines lokalen Dienstes oder die Übernahme der `LDPreload` Funktion. Jede Änderung ist äußerst verdächtig und ein potenzieller Hinweis auf eine Gefährdung. Daher erkennen oder verhindern diese Mechanismen weitere Beeinträchtigungen des Systems.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieser Befund nur dann generiert wird, wenn die zugehörige Aktivität und der zugehörige Kontext potenziell verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der potenziell gefährdeten Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

DefenseEvasion:Runtime/PtraceAntiDebugging

Ein Prozess in einem Container oder einer EC2 Amazon-Instance hat mithilfe des ptrace-Systemaufrufs eine Anti-Debugging-Maßnahme ausgeführt.

Standard-Schweregrad: Niedrig

- Feature: Laufzeit-Überwachung

Dieses Ergebnis zeigt, dass ein Prozess, der auf einer EC2 Amazon-Instance oder einem Container in Ihrer AWS Umgebung läuft, den ptrace-Systemaufruf mit der `PTRACE_TRACEME` Option verwendet hat. Diese Aktivität würde dazu führen, dass sich ein angehängter Debugger vom laufenden Prozess trennt. Wenn kein Debugger angehängt ist, hat dies keine Wirkung. Die Aktivität an sich erweckt jedoch Verdacht. Dies könnte darauf hindeuten, dass Malware auf dem System ausgeführt wird. Malware verwendet häufig Anti-Debugging-Techniken, um Analysen zu umgehen. Diese Techniken können zur Laufzeit erkannt werden.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieses Ergebnis nur dann generiert wird, wenn die zugehörige Aktivität und der zugehörige Kontext potenziell verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/MaliciousFileExecuted

Eine bekannte bösartige ausführbare Datei wurde auf einer EC2 Amazon-Instance oder einem Container ausgeführt.

Standard-Schweregrad: Hoch

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass eine bekannte bösartige ausführbare Datei auf einer EC2 Amazon-Instance oder einem Container in Ihrer AWS Umgebung ausgeführt wurde. Dies ist ein starker Indikator dafür, dass die Instance oder der Container potenziell kompromittiert wurde und dass Malware ausgeführt wurde.

Malware verwendet häufig Anti-Debugging-Techniken, um Analysen zu umgehen, und diese Techniken können zur Laufzeit erkannt werden.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext, sodass dieses Ergebnis nur dann generiert wird, wenn die zugehörige Aktivität und der zugehörige Kontext potenziell verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Execution:Runtime/SuspiciousShellCreated

Ein Netzwerkdienst oder ein über das Netzwerk zugänglicher Prozess auf einer EC2 Amazon-Instance oder in einem Container hat einen interaktiven Shell-Prozess gestartet.

Standard-Schweregrad: Niedrig

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein über das Netzwerk zugänglicher Service auf einer EC2 Amazon-Instance oder in einem Container in Ihrer AWS Umgebung eine interaktive Shell gestartet hat. Unter bestimmten Umständen kann dieses Szenario auf ein Verhalten nach der Nutzung hinweisen. Interaktive Shells ermöglichen es Angreifern, beliebige Befehle auf einer kompromittierten Instance oder einem kompromittierten Container auszuführen.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in

der GuardDuty Konsole. Sie können die Prozessinformationen, auf die über das Netzwerk zugegriffen werden kann, in den Details des übergeordneten Prozesses einsehen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

PrivilegeEscalation:Runtime/ElevationToRoot

Ein Prozess, der auf der aufgelisteten EC2 Amazon-Instance oder dem aufgelisteten Amazon-Container ausgeführt wird, hat Root-Rechte übernommen.

Standard-Schweregrad: Mittel

- Feature: Laufzeit-Überwachung

Dieses Ergebnis informiert Sie darüber, dass ein Prozess, der auf dem aufgelisteten Amazon EC2 oder im aufgelisteten Container in Ihrer AWS Umgebung läuft, durch ungewöhnliche oder verdächtige `setuid` Binärausführung Root-Rechte erlangt hat. Dies deutet darauf hin, dass ein laufender Prozess potenziell kompromittiert wurde, z. EC2 B. durch einen Exploit oder durch `setuid` Ausnutzung. Mithilfe der Root-Rechte kann der Angreifer möglicherweise Befehle auf der Instance oder dem Container ausführen.

Es GuardDuty ist zwar so konzipiert, dass es diesen Erkennungstyp nicht für Aktivitäten generiert, bei denen der `sudo` Befehl regelmäßig verwendet wird, generiert dieses Ergebnis jedoch, wenn es die Aktivität als ungewöhnlich oder verdächtig identifiziert.

GuardDuty untersucht die zugehörige Laufzeitaktivität und den zugehörigen Kontext und generiert diesen Befundtyp nur, wenn die zugehörige Aktivität und der zugehörige Kontext ungewöhnlich oder verdächtig sind.

Der Laufzeit-Agent überwacht Ereignisse aus mehreren Ressourcen. Informationen zur Identifizierung der betroffenen Ressource finden Sie unter Ressourcentyp in den Ergebnisdetails in der GuardDuty Konsole.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Ressource kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Ergebnisse von Runtime Monitoring.

Malware-Schutz für EC2-Suchtypen

GuardDuty Malware Protection for EC2 bietet eine einzige Suche nach Malware Protection for EC2 für alle Bedrohungen, die beim Scan einer EC2-Instance oder eines Container-Workloads erkannt wurden. Die Erkenntnis umfasst die Gesamtzahl der während des Scans entdeckten Bedrohungen und liefert, basierend auf dem Schweregrad, Details zu den 32 am häufigsten erkannten Bedrohungen. Im Gegensatz zu anderen GuardDuty Ergebnissen werden die Ergebnisse von Malware Protection for EC2 nicht aktualisiert, wenn dieselbe EC2-Instance oder dieselbe Container-Workload erneut gescannt wird.

Für jeden Scan, bei dem Malware erkannt wird, wird ein neues Ergebnis von Malware Protection for EC2 generiert. Die Ergebnisse von Malware Protection for EC2 umfassen Informationen über den entsprechenden Scan, der zu dem Ergebnis geführt hat, sowie über das GuardDuty Ergebnis, das diesen Scan ausgelöst hat. Dadurch ist es einfacher, das verdächtige Verhalten mit der erkannten Malware zu korrelieren.

> **Note**
>
> Wenn bösartige Aktivitäten auf einem Container-Workload GuardDuty erkannt werden, generiert Malware Protection for EC2 kein Ergebnis auf EC2-Ebene.

Die folgenden Ergebnisse beziehen sich speziell auf GuardDuty Malware Protection for EC2.

Themen

- Execution:EC2/MaliciousFile
- Execution:ECS/MaliciousFile
- Execution:Kubernetes/MaliciousFile
- Execution:Container/MaliciousFile
- Execution:EC2/SuspiciousFile
- Execution:ECS/SuspiciousFile
- Execution:Kubernetes/SuspiciousFile
- Execution:Container/SuspiciousFile

Execution:EC2/MaliciousFile

Auf einer EC2-Instance wurde eine schädliche Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Merkmal: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere schädliche Dateien auf der aufgelisteten EC2-Instance in Ihrer Umgebung entdeckt hat. AWS Die aufgeführte Instance ist möglicherweise kompromittiert. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Execution:ECS/MaliciousFile

Auf einem ECS-Cluster wurde eine bösartige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere schädliche Dateien auf einem Container-Workload entdeckt hat, der zu einem ECS-Cluster gehört. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, ist Ihr Container, der zum ECS-Cluster gehört, möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten Clusters ECS.

Execution:Kubernetes/MaliciousFile

Auf einem Kubernetes-Cluster wurde eine bösartige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere schädliche Dateien auf einem Container-Workload entdeckt hat, der zu einem Kubernetes-Cluster gehört. Wenn es sich um einen von EKS verwalteten Cluster handelt, enthalten die Erkenntnisdetails zusätzliche Informationen über die betroffene EKS-Ressource. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Execution:Container/MaliciousFile

In einem eigenständigen Container wurde eine bösartige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere schädliche Dateien auf einem Container-Workload erkannt hat und keine Clusterinformationen identifiziert wurden. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten Standalone-Containers.

Execution:EC2/SuspiciousFile

Auf einer EC2-Instance wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere verdächtige Dateien auf einer EC2-Instance erkannt hat. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie davon ausgehen, dass die erkannte Datei in Ihrer AWS Umgebung angezeigt wird. Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Execution:ECS/SuspiciousFile

Auf einem ECS-Cluster wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere verdächtige Dateien in einem Container entdeckt hat, der zu einem ECS-Cluster

gehört. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie damit rechnen, die erkannte Datei in Ihrer AWS Umgebung zu sehen. Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, ist Ihr Container, der zum ECS-Cluster gehört, möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten Clusters ECS.

Execution:Kubernetes/SuspiciousFile

In einem Kubernetes-Cluster wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere verdächtige Dateien in einem Container erkannt hat, der zu einem Kubernetes-Cluster gehört. Wenn es sich um einen von EKS verwalteten Cluster handelt, enthalten die Erkenntnisdetails zusätzliche Informationen über die betroffene EKS-Ressource. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise

von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie damit rechnen, die erkannte Datei in Ihrer Umgebung zu sehen. AWS Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung der Erkenntnisse von EKS Audit Log Monitoring.

Execution:Container/SuspiciousFile

In einem eigenständigen Container wurde eine verdächtige Datei entdeckt.

Standardschweregrad: Variiert je nach erkannter Bedrohung.

- Funktion: EBS-Malware-Schutz

Dieses Ergebnis weist darauf hin, dass der Scan von GuardDuty Malware Protection for EC2 eine oder mehrere verdächtige Dateien in einem Container ohne Clusterinformationen erkannt hat. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen in den Details zu den Erkenntnissen.

Erkenntnisse vom Typ `SuspiciousFile` deuten darauf hin, dass sich auf einer betroffenen Ressource potenziell unerwünschte Programme wie Adware, Spyware oder Tools mit doppeltem Verwendungszweck befinden. Diese Programme können sich negativ auf Ihre Ressource auswirken oder von Angreifern für böswillige Zwecke verwendet werden. Netzwerktools können beispielsweise von Gegnern legitim oder böswillig als Hacking-Tools verwendet werden, um zu versuchen, Ressourcen zu kompromittieren.

Wenn eine verdächtige Datei erkannt wurde, prüfen Sie, ob Sie damit rechnen, die entdeckte Datei in Ihrer AWS Umgebung zu sehen. Falls die Datei unerwartet ist, befolgen Sie die Empfehlungen zur Problembehebung im nächsten Abschnitt.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität unerwartet ist, kann Ihr Container-Workload kompromittiert sein. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten Standalone-Containers.

Suchtyp „Malware-Schutz für S3“

GuardDuty generiert nur dann ein Ergebnis, wenn es eine potenzielle Sicherheitsbedrohung in Ihrem erkennt AWS-Konto. Ein Ergebnis von Malware Protection for S3 weist darauf hin, dass das hochgeladene Objekt, das den Malware-Scan initiiert hat, eine potenziell schädliche Datei enthält.

GuardDuty Damit Amazon ein Ergebnis in Ihrem generiert AWS-Konto, aktivieren Sie GuardDuty sowohl als auch Malware Protection for S3. Es hat sich bewährt, zuerst den Malware-Schutz für S3 zu aktivieren GuardDuty und dann. Wenn diese Reihenfolge für Sie anders ist, stellen Sie sicher, dass Sie sie aktivieren, GuardDuty bevor ein S3-Objekt in Ihren geschützten Bucket hochgeladen wird.

> **Note**
>
> GuardDuty kann kein Ergebnis für ein S3-Objekt generieren, das vor der Aktivierung gescannt wurde GuardDuty. Um ein vorhandenes S3-Objekt zu scannen, können Sie es erneut hochladen.

Object:S3/MaliciousFile

Auf einem gescannten S3-Objekt wurde eine schädliche Datei entdeckt.

Standard-Schweregrad: Hoch

- Funktion: Malware-Schutz für S3

Dieses Ergebnis weist darauf hin, dass ein Malware-Scan das aufgelistete S3-Objekt als bösartig erkannt hat. Weitere Informationen finden Sie im Abschnitt Entdeckte Bedrohungen im Bereich mit den Funddetails.

Empfehlung zur Behebung:

Wenn dieses Ergebnis unerwartet war, ist das S3-Objekt potenziell bösartig. Informationen zu empfohlenen Behebungsschritten finden Sie unterBehebung eines potenziell bösartigen S3-Objekts.

Erkenntnistypen für GuardDuty RDS Protection

GuardDuty RDS Protection erkennt ungewöhnliches Anmeldeverhalten auf Ihrer Datenbank-Instance. Die folgenden Erkenntnisse beziehen sich auf Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken und weisen immer den Ressourcentyp `RDSDBInstance` auf. Der Schweregrad und die Details der Ergebnisse unterscheiden sich je nach Erkennungstyp.

Themen

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Ein Benutzer hat sich erfolgreich auf ungewöhnliche Weise bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standardschweregrad: Variabel

> **Note**
>
> Je nach dem anomalen Verhalten, das mit diesem Ergebnis einhergeht, kann der Standardschweregrad Niedrig, Mittel und Hoch gewählt werden.
>
> - Niedrig – Wenn der mit diesem Ergebnis verknüpfte Benutzername von einer IP-Adresse aus angemeldet ist, die einem privaten Netzwerk zugeordnet ist.
> - Mittel – Wenn der mit diesem Ergebnis verknüpfte Benutzername von einer öffentlichen IP-Adresse aus angemeldet ist.

- Hoch – Wenn es ein einheitliches Muster von fehlgeschlagenen Anmeldeversuchen von öffentlichen IP-Adressen aus gibt, was auf zu freizügige Zugriffsrichtlinien hindeutet.

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Diese Erkenntnis informiert Sie darüber, dass eine ungewöhnliche erfolgreiche Anmeldung in einer RDS-Datenbank in Ihrer AWS-Umgebung beobachtet wurde. Dies kann darauf hindeuten, dass sich ein zuvor unbekannter Benutzer zum ersten Mal bei einer RDS-Datenbank angemeldet hat. Ein häufiges Szenario ist ein interner Benutzer, der sich bei einer Datenbank anmeldet, auf die programmgesteuert von Anwendungen und nicht von einzelnen Benutzern zugegriffen wird.

Diese erfolgreiche Anmeldung wurde vom GuardDuty Machine Learning (ML)-Anomalieentdeckungs-Modell als ungewöhnlich eingestuft. Das ML-Modell bewertet alle Datenbank-Anmeldeereignisse in Ihrer Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken und identifiziert anomale Ereignisse, die mit den von Gegnern verwendeten Techniken in Verbindung stehen. Das ML-Modell verfolgt verschiedene Faktoren der RDS-Anmeldeaktivität, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifischen Datenbank-Verbindungsdetails, die verwendet wurden. Informationen zu potenziell ungewöhnlichen Anmeldeereignissen finden Sie unter RDSAnomalien aufgrund von Anmeldeaktivitäten.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Audit-Logs auf Aktivitäten zu überprüfen, die von dem anomalen Benutzer ausgeführt wurden. Erkenntnisse mit mittlerem und hohem Schweregrad können darauf hindeuten, dass die Zugriffsrichtlinien für die Datenbank zu freizügig sind und die Anmeldeinformationen der Benutzer möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Ein oder mehrere ungewöhnliche fehlgeschlagene Anmeldeversuche wurden in einer RDS-Datenbank in Ihrem Konto beobachtet.

Standard-Schweregrad: Niedrig

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Diese Erkenntnis informiert Sie darüber, dass eine oder mehrere ungewöhnliche erfolgreiche Anmeldungen in einer RDS-Datenbank in Ihrer AWS-Umgebung beobachtet wurde. Fehlgeschlagene Anmeldeversuche von öffentlichen IP-Adressen aus können darauf hindeuten, dass die RDS-Datenbank in Ihrem Konto einem Brute-Force-Angriff durch einen potenziell böswilligen Akteur ausgesetzt war.

Diese erfolgreiche Anmeldung wurde vom GuardDuty Machine Learning (ML)-Anomalieentdeckungs-Modell als ungewöhnlich eingestuft. Das ML-Modell bewertet alle Datenbank-Anmeldeereignisse in Ihrer Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken und identifiziert anomale Ereignisse, die mit den von Gegnern verwendeten Techniken in Verbindung stehen. Das ML-Modell verfolgt verschiedene Faktoren der RDS-Anmeldeaktivität, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifischen Datenbank-Verbindungsdetails, die verwendet wurden. Informationen zu potenziell ungewöhnlichen RDS-Anmeldeaktivitäten finden Sie unter RDSAnomalien aufgrund von Anmeldeaktivitäten.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Ein Benutzer hat sich nach einem konsistenten Muster ungewöhnlicher fehlgeschlagener Anmeldeversuche erfolgreich von einer öffentlichen IP-Adresse aus auf ungewöhnliche Weise bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standard-Schweregrad: Hoch

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass bei einer RDS-Datenbank in Ihrer AWS-Umgebung eine ungewöhnliche Anmeldung beobachtet wurde, die auf einen erfolgreichen Brute-Force-Angriff hindeutet. Vor einer anomalen erfolgreichen Anmeldung wurde ein konsistentes Muster ungewöhnlicher fehlgeschlagener Anmeldeversuche beobachtet. Dies deutet darauf hin, dass der Benutzer und das Passwort, die mit der RDS-Datenbank in Ihrem Konto verknüpft sind, möglicherweise kompromittiert wurden und dass möglicherweise ein potenziell böswilliger Akteur auf die RDS-Datenbank zugegriffen hat.

Diese erfolgreiche Anmeldung wurde vom GuardDuty Machine Learning (ML)-Anomalieentdeckungs-Modell als ungewöhnlich eingestuft. Das ML-Modell bewertet alle Datenbank-Anmeldeereignisse in Ihrer Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken und identifiziert anomale Ereignisse, die mit den von Gegnern verwendeten Techniken in Verbindung stehen. Das ML-Modell verfolgt verschiedene Faktoren der RDS-Anmeldeaktivität, z. B. den Benutzer, der die Anfrage gestellt hat, den Standort, von dem aus die Anfrage gestellt wurde, und die spezifischen Datenbank-Verbindungsdetails, die verwendet wurden. Informationen zu potenziell ungewöhnlichen RDS-Anmeldeaktivitäten finden Sie unter RDSAnomalien aufgrund von Anmeldeaktivitäten.

Empfehlungen zur Abhilfe:

Diese Aktivität weist darauf hin, dass Datenbankanmeldeinformationen möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Prüfungsprotokolle auf Aktivitäten des potenziell kompromittierten Benutzers zu überprüfen. Ein konsistentes Muster ungewöhnlicher fehlgeschlagener Anmeldeversuche deutet auf eine zu freizügige Zugriffsrichtlinie auf die Datenbank hin, oder die Datenbank wurde möglicherweise auch öffentlich zugänglich gemacht. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Ein Benutzer hat sich erfolgreich von einer bekannten bösartigen IP-Adresse aus bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standard-Schweregrad: Hoch

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass eine erfolgreiche RDS-Anmeldeaktivität von einer IP-Adresse aus erfolgte, die mit einer bekannten bösartigen Aktivität in Ihrer AWS-Umgebung in Verbindung steht. Dies deutet darauf hin, dass der Benutzer und das Passwort, die mit der RDS-Datenbank in Ihrem Konto verknüpft sind, möglicherweise kompromittiert wurden und dass möglicherweise ein potenziell böswilliger Akteur auf die RDS-Datenbank zugegriffen hat.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Benutzeranmeldeinformationen möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Prüfungsprotokolle auf Aktivitäten des potenziell kompromittiert Benutzers zu überprüfen. Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Eine IP-Adresse, die mit einer bekannten böswilligen Aktivität verknüpft ist, hat erfolglos versucht, sich bei einer RDS-Datenbank in Ihrem Konto anzumelden.

Standard-Schweregrad: Mittel

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass eine IP-Adresse, die mit bekannten böswilligen Aktivitäten in Verbindung steht, versucht hat, sich bei einer RDS-Datenbank in Ihrer AWS-Umgebung anzumelden, dabei aber nicht den richtigen Benutzernamen oder das richtige Passwort angegeben hat. Dies deutet darauf hin, dass ein potenziell böswilliger Akteur versucht, die RDS-Datenbank in Ihrem Konto zu kompromittieren.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

Discovery:RDS/MaliciousIPCaller

Eine IP-Adresse, die mit einer bekannten böswilligen Aktivität in Verbindung steht, hat eine RDS-Datenbank in Ihrem Konto untersucht. Es wurde kein Authentifizierungsversuch unternommen.

Standard-Schweregrad: Mittel

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Diese Erkenntnis informiert Sie darüber, dass eine IP-Adresse, die mit einer bekannten bösartigen Aktivität in Verbindung steht, eine RDS-Datenbank in Ihrer AWS Umgebung untersucht hat, obwohl kein Anmeldeversuch unternommen wurde. Dies kann darauf hindeuten, dass ein potenziell böswilliger Akteur versucht, nach einer öffentlich zugänglichen Infrastruktur zu scannen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Ein Benutzer hat sich erfolgreich über eine IP-Adresse des Tor-Ausgangsknotens bei einer RDS-Datenbank in Ihrem Konto angemeldet.

Standard-Schweregrad: Hoch

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass sich ein Benutzer erfolgreich von einer IP-Adresse des Tor-Ausgangsknotens aus bei einer RDS-Datenbank in Ihrer AWS-Umgebung angemeldet hat. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die RDS-Ressourcen hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Benutzeranmeldeinformationen möglicherweise offengelegt oder kompromittiert wurden. Es wird empfohlen, das Passwort des zugehörigen Datenbankbenutzers zu ändern und die verfügbaren Prüfungsprotokolle auf Aktivitäten des potenziell kompromittiert Benutzers zu überprüfen. Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Eine Tor-IP-Adresse hat erfolglos versucht, sich bei einer RDS-Datenbank in Ihrem Konto anzumelden.

Standard-Schweregrad: Mittel

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Dieses Ergebnis informiert Sie darüber, dass die IP-Adresse eines Tor-Ausgangsknotens versucht hat, sich bei einer RDS-Datenbank in Ihrer AWS-Umgebung anzumelden, aber nicht den richtigen Benutzernamen oder das richtige Passwort angegeben hat. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet.

Dies kann auf einen unbefugten Zugriff auf die RDS-Ressourcen hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

Discovery:RDS/TorIPCaller

Eine IP-Adresse des Tor-Ausgangsknotens hat eine RDS-Datenbank in Ihrem Konto untersucht, es wurde kein Authentifizierungsversuch unternommen.

Standard-Schweregrad: Mittel

- Funktion: Überwachung der RDS-Anmeldeaktivitäten

Diese Erkenntnis informiert Sie darüber, dass die IP-Adresse eines Tor-Ausgangsknotens eine RDS-Datenbank in Ihrer AWS-Umgebung untersucht hat, obwohl kein Anmeldeversuch unternommen wurde. Dies kann darauf hindeuten, dass ein potenziell böswilliger Akteur versucht, nach einer öffentlich zugänglichen Infrastruktur zu scannen. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Dies kann auf einen unbefugten Zugriff auf die RDS-Ressourcen in Ihrem Konto hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für die zugehörige Datenbank unerwartet ist, kann dies darauf hindeuten, dass die Datenbank öffentlich zugänglich ist oder dass es eine zu freizügige Zugriffsrichtlinie für die Datenbank gibt. Es wird empfohlen, die Datenbank in einer privaten VPC zu platzieren und die Sicherheitsgruppenregeln so zu beschränken, dass nur Datenverkehr aus den erforderlichen Quellen zugelassen wird. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen.

Lambda-Protection-Erkenntnistypen

In diesem Abschnitt werden die Erkenntnistypen beschrieben, die für Ihre AWS Lambda-Ressourcen spezifisch sind und in denen die `resourceType` als `Lambda` aufgeführt sind. Für alle Lambda-Erkenntnisse wird empfohlen, die betreffende Ressource zu untersuchen, um festzustellen, ob sie sich erwartungsgemäß verhält. Wenn die Aktivität autorisiert ist, können Sie Unterdrückungsregeln oder Listen vertrauenswürdiger IP-Adressen und Bedrohungen verwenden, um Falschmeldungen für diese Ressource zu verhindern.

Wenn die Aktivität unerwartet ist, besteht die bewährte Sicherheitsmethode darin, davon auszugehen, dass Lambda potenziell kompromittiert wurde, und die Empfehlungen zur Behebung zu befolgen.

Themen

Backdoor:Lambda/C&CActivity.B

Eine Lambda-Funktion fragt eine IP-Adresse ab, die einem bekannten Command-and-Control-Server zugeordnet wird.

Standard-Schweregrad: Hoch

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine aufgeführte Lambda-Funktion in Ihrer AWS-Umgebung eine IP-Adresse abfragt, die mit einem bekannten Command and Control (C&C)-Server in Verbindung steht. Die mit der generierten Erkenntnis verknüpfte Lambda-Funktion ist möglicherweise kompromittiert. C&C-Server sind Computer, die Befehle an Mitglieder eines Botnets senden.

Ein Botnet ist eine Sammlung von mit dem Internet verbundenen Geräten, zu denen PCs, Server, mobile Geräte und Geräte des Internets der Dinge gehören können, die mit einem allgemeinen Typ von Malware infiziert sind und von dieser kontrolliert werden. Botnets dienen häufig zum Verteilen von Malware und Sammeln von sich widerrechtlich angeeigneten Informationen, wie z. B. Kreditkartennummern. Je nach Zweck und Struktur des Botnets kann der C&C-Server auch den Befehl erteilen, einen DDoS (Distributed Denial of Service)-Angriff zu starten.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

CryptoCurrency:Lambda/BitcoinTool.B

Eine Lambda-Funktion fragt eine IP-Adresse ab, die mit einer Aktivität in Zusammenhang mit einer Kryptowährung in Verbindung steht.

Standard-Schweregrad: Hoch

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie, dass die aufgeführte Lambda-Funktion in Ihrer AWS-Umgebung eine IP-Adresse abfragt, die mit einer Aktivität in Zusammenhang mit Bitcoin oder einer anderen Kryptowährung in Verbindung steht. Bedrohungsakteure versuchen möglicherweise, die Kontrolle über Lambda-Funktionen zu übernehmen, um sie böswillig für das unbefugte Mining von Kryptowährungen wiederzuverwenden.

Empfehlungen zur Abhilfe:

Wenn Sie diese Lambda-Funktion verwenden, um Kryptowährungen zu minen oder zu verwalten, oder wenn diese Funktion anderweitig an einer Blockchain-Aktivität beteiligt ist, handelt es sich möglicherweise um eine erwartete Aktivität für Ihre Umgebung. Wenn dies in Ihrer AWS-Umgebung der Fall ist, empfehlen wir, für diese Erkenntnis eine Unterdrückungsregel festzulegen. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Erkenntnistyp-Attribut mit dem Wert CryptoCurrency:Lambda/BitcoinTool.B verwenden. Das zweite Filterkriterium sollte der Lambda-Funktionsname des Features sein, die an der Blockchain-Aktivität beteiligt ist. Weitere Informationen zum Erstellen von Unterdrückungsregeln finden Sie unter Unterdrückungsregeln.

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

Trojan:Lambda/BlackholeTraffic

Die Lambda-Funktion versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, der ein bekanntes schwarzes Loch ist.

Standard-Schweregrad: Mittel

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine aufgeführte Lambda-Funktion in Ihrer AWS-Umgebung versucht, mit der IP-Adresse eines schwarzen Lochs (oder einem Sinkhole) zu kommunizieren. Schwarze Löcher bezeichnen Orte im Netzwerk, an denen eingehender oder ausgehender Datenverkehr stillschweigend gelöscht wird, ohne die Quelle zu informieren, dass die Daten den vorgesehenen Empfänger nicht erreicht haben. Die IP-Adresse eines schwarzen Lochs gibt einen Hostcomputer an, der nicht ausgeführt wird, oder eine Adresse, der kein Host zugewiesen wurde. Die aufgeführte Lambda-Funktion ist möglicherweise kompromittiert.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

Trojan:Lambda/DropPoint

Eine Lambda-Funktion versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Standard-Schweregrad: Mittel

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine aufgeführte Lambda-Funktion in Ihrer AWS-Umgebung versucht, mit einer IP-Adresse eines Remote-Hosts zu kommunizieren, von dem bekannt ist, dass er Anmeldeinformationen und andere mithilfe von Malware gestohlene Daten enthält.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Eine Lambda-Funktion stellt Verbindungen zu einer IP-Adresse auf einer benutzerdefinierten Bedrohungsliste her.

Standard-Schweregrad: Mittel

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine Lambda-Funktion in Ihrer AWS-Umgebung mit einer IP-Adresse kommuniziert, die auf einer von Ihnen hochgeladenen Bedrohungsliste steht. In GuardDuty besteht eine Bedrohungsliste aus bekannten schädlichen IP-Adressen. GuardDuty generiert Erkenntnisse basierend auf hochgeladenen Bedrohungslisten. Sie können die Details der Bedrohungsliste in den Erkenntnisdetails in der GuardDuty-Konsole einsehen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

UnauthorizedAccess:Lambda/TorClient

Eine Lambda-Funktion stellt Verbindungen zu einem Tor-Guard oder einem Authority-Knoten her.

Standard-Schweregrad: Hoch

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine Lambda-Funktion in Ihrer AWS-Umgebung Verbindungen zu einem Tor-Guard oder einem Authority-Knoten herstellt. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor-Guards und Authority-Knoten fungieren als erste Gateways

in ein Tor-Netzwerk. Dieser Datenverkehr kann darauf hinweisen, dass diese Lambda-Funktion möglicherweise kompromittiert wurde. Sie fungiert jetzt als Client in einem Tor-Netzwerk.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

UnauthorizedAccess:Lambda/TorRelay

Eine Lambda-Funktion stellt Verbindungen zu einem Tor-Netzwerk als Tor-Relay her.

Standard-Schweregrad: Hoch

- Funktion: Lambda Network Activity Monitoring

Diese Erkenntnis informiert Sie darüber, dass eine Lambda-Funktion in Ihrer AWS-Umgebung Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass sie als Tor-Relay fungiert. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Tor erhöht die Anonymität der Kommunikation, indem es den möglicherweise illegalen Datenverkehr des Kunden von einem Tor-Relay zu einem anderen weiterleitet.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, könnte Ihre Lambda-Funktion kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Lambda-Funktion.

Nicht mehr aktive Erkenntnistypen

Eine Erkenntnis ist eine Benachrichtigung, die Details zu einem von GuardDuty festgestellten potenziellen Sicherheitsrisiko enthält. Weitere Informationen über wichtige Änderungen an den GuardDuty-Ergebnistypen, einschließlich neu hinzugefügter oder nicht mehr aktiver Ergebnistypen, finden Sie unter Dokumentenverlauf für Amazon GuardDuty.

Die folgenden Erkenntnistypen wurden eingestellt und werden nicht mehr von GuardDuty generiert.

> **Important**
>
> Sie können nicht mehr aktive GuardDuty-Erkenntnistypen nicht reaktivieren.

Themen

Exfiltration:S3/ObjectRead.Unusual

Eine IAM-Entität hat eine S3-API auf verdächtige Weise aufgerufen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

- Datenquelle: CloudTrail-Datenereignisse für S3

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität in Ihrer AWS-Umgebung API-Aufrufe tätigt, die einen S3-Bucket betreffen und die sich von der festgelegten Grundlinie dieser Entität unterscheiden. Der in dieser Aktivität verwendete API-Aufruf steht im Zusammenhang mit der Exfiltrationsphase eines Angriffs, in der ein Angreifer versucht, Daten zu sammeln. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Impact:S3/PermissionsModification.Unusual

Eine IAM-Entität hat eine API aufgerufen, um die Berechtigungen für eine oder mehrere S3-Ressourcen zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität API-Aufrufe durchführt, um die Berechtigungen für einen oder mehrere Buckets oder Objekte in Ihrer AWS-Umgebung zu ändern. Diese Aktion kann von einem Angreifer ausgeführt werden, um die Weitergabe von Informationen außerhalb des Kontos zu ermöglichen. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch

nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Impact:S3/ObjectDelete.Unusual

Eine IAM-Entität rief eine API zum Löschen von Daten in einem S3-Bucket auf.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Dieses Ergebnis informiert Sie darüber, dass eine bestimmte IAM-Entität in Ihrer AWS-Umgebung API-Aufrufe durchführt, um Daten im aufgeführten S3-Bucket zu löschen, indem der Bucket selbst gelöscht wird. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Discovery:S3/BucketEnumeration.Unusual

Eine IAM-Entität hat eine S3-API aufgerufen, um S3-Buckets in Ihrem Netzwerk zu erkennen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis informiert Sie darüber, dass eine IAM-Entität eine S3-API aufgerufen hat, um S3-Buckets in Ihrer Umgebung zu erkennen, z. B. `ListBuckets`. Diese Art von Aktivität steht im Zusammenhang mit der Erkennungsphase eines Angriffs, in der ein Angreifer Informationen sammelt, um festzustellen, ob Ihre AWS-Umgebung für einen umfassenderen Angriff anfällig ist. Diese Aktivität ist verdächtig, da die Art und Weise, wie die IAM-Entität die API aufgerufen hat, ungewöhnlich war. Beispielsweise hatte diese IAM-Entität noch nie zuvor diese Art von API aufgerufen, oder die API wurde von einem ungewöhnlichen Ort aus aufgerufen.

Empfehlungen zur Abhilfe:

Wenn diese Aktivität für den zugehörigen Prinzipal unerwartet ist, kann dies darauf hindeuten, dass die Anmeldeinformationen offengelegt wurden oder dass Ihre S3-Berechtigungen nicht restriktiv genug sind. Weitere Informationen finden Sie unter Behebung eines potenziell gefährdeten S3-Buckets.

Persistence:IAMUser/NetworkPermissions

Ein IAM-Entität hat eine API aufgerufen, die üblicherweise verwendet wird, um die Netzwerkzugriffsberechtigungen für Sicherheitsgruppen, Routen und ACLs in Ihrem AWS-Konto zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis bedeutet, dass ein bestimmter Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) in Ihrer AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn Netzwerkkonfigurationseinstellungen unter verdächtigen Umständen geändert werden, z. B. wenn ein Prinzipal die `CreateSecurityGroup`-API aufruft, ohne dies jemals in der Vergangenheit getan zu haben. Angreifer versuchen häufig, Sicherheitsgruppen zu ändern, um bestimmten eingehenden Datenverkehr auf verschiedenen Ports zuzulassen und besser auf eine EC2-Instance zugreifen zu können.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Persistence:IAMUser/ResourcePermissions

Ein Prinzipal hat eine API aufgerufen, die üblicherweise verwendet wird, um Sicherheitszugriffsrichtlinien verschiedener Ressourcen in Ihrem AWS-Konto zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis bedeutet, dass ein bestimmter Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) in Ihrer AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn eine Änderung an Richtlinien oder Berechtigungen festgestellt wird, die mit AWS-Ressourcen verknüpft sind, z. B. wenn ein Prinzipal in Ihrer AWS-Umgebung die `PutBucketPolicy` API aufruft, ohne dies je in der Vergangenheit getan zu haben. Einige Services, z. B. Amazon S3, unterstützen ressourcengebundene Berechtigungen, die einem oder mehreren

Prinzipalen Zugriff auf die Ressource gewähren. Mit gestohlenen Anmeldeinformationen können Angreifer die einer Ressource zugeordneten Richtlinien ändern, um sich künftig Zugriff auf diese Ressource zu verschaffen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Persistence:IAMUser/UserPermissions

Ein Prinzipal hat eine API aufgerufen, die üblicherweise dazu verwendet wird, IAM-Benutzer, Gruppen oder Richtlinien in Ihrem AWS-Konto hinzuzufügen, zu ändern oder zu löschen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis bedeutet, dass ein bestimmter Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) in Ihrer AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird durch verdächtige Änderungen an den benutzerbezogenen Berechtigungen in Ihrer AWS Umgebung ausgelöst, z. B. wenn ein Principal in Ihrer AWS-Umgebung die `AttachUserPolicy`-API aufruft, ohne dies je in der Vergangenheit getan zu haben. Angreifer können gestohlene Anmeldeinformationen verwenden, um neue Benutzer zu erstellen, Zugriffsrichtlinien für bestehende Benutzer hinzuzufügen oder Zugriffsschlüssel zu erstellen, um ihren Zugriff auf ein Konto zu maximieren, selbst wenn ihr ursprünglicher Zugangspunkt geschlossen ist. Beispielsweise könnte der Besitzer des Kontos feststellen, dass ein bestimmter IAM-Benutzer oder ein bestimmtes IAM-Passwort gestohlen wurde, und es aus dem Konto löschen. Andere Benutzer, die von einem betrügerisch erstellten Administratorprinzipal erstellt wurden, werden jedoch möglicherweise nicht gelöscht, sodass der Angreifer auf ihr AWS-Konto zugreifen kann.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

PrivilegeEscalation:IAMUser/AdministrativePermissions

Ein Prinzipal hat versucht, sich selbst eine hochgradig weitreichende Richtlinie zuzuweisen.

Standard-Schweregrad: Niedrig*

> **Note**
>
> Wenn der Angriff auf die Berechtigungseskalation nicht erfolgreich war, ist der Schweregrad des Ergebnises „Niedrig“, wenn der Angriff erfolgreich war, ist der Schweregrad „Mittel“.

Diese Erkenntnis informiert Sie darüber, dass ein bestimmter IAM-Entität in Ihrer AWS-Umgebung ein Verhalten zeigt, das auf einen ein Rechteeskalationsangriff hinweist. Diese Erkenntnis wird ausgelöst, wenn ein IAM-Benutzer oder eine Rolle versucht, sich selbst eine hochgradig weitreichende Richtlinie zuzuweisen. Wenn der/die entsprechende Benutzer oder Rolle nicht über administrative Rechte verfügen darf, können entweder die Anmeldeinformationen des Benutzers kompromittiert sein oder die Berechtigungen der Rolle wurden nicht ordnungsgemäß konfiguriert.

Angreifer können gestohlene Anmeldeinformationen verwenden, um neue Benutzer zu erstellen, Zugriffsrichtlinien für bestehende Benutzer hinzuzufügen oder Zugriffsschlüssel zu erstellen, um ihren Zugriff auf ein Konto zu maximieren, selbst wenn ihr ursprünglicher Zugangspunkt geschlossen ist. Der Eigentümer des Kontos stellt möglicherweise fest, dass ein bestimmter IAM-Benutzer oder ein Passwort gestohlen wurden, und löscht diese aus dem Konto. Hierbei entfernt er aber möglicherweise andere Benutzer nicht, die vom betrügerisch angelegten Admin-Prinzipal angelegt wurden, sodass ihr AWS-Konto dem Angreifer weiterhin zur Verfügung steht.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Recon:IAMUser/NetworkPermissions

Ein Prinzipal hat eine API aufgerufen, die üblicherweise verwendet wird, um die Netzwerkzugriffsberechtigungen für Sicherheitsgruppen, Routen und ACLs in Ihrem AWS-Konto zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis bedeutet, dass ein bestimmter Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) in Ihrer AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn Ressourcen-Zugriffsberechtigungen in Ihrem AWS-Konto unter fragwürdigen Umständen untersucht werden. Dies trifft beispielsweise dann zu, wenn ein Prinzipal zum ersten Mal die `DescribeInstances`-API aufgerufen hat. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um in Kenntnis Ihrer AWS-Ressourcen zu gelangen, um wertvolle Informationen herauszufinden oder festzustellen, welcher Funktionsumfang den Anmeldeinformationen bereits zur Verfügung steht.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Recon:IAMUser/ResourcePermissions

Ein Prinzipal hat eine API aufgerufen, die üblicherweise verwendet wird, um Sicherheitszugriffsrichtlinien verschiedener Ressourcen in Ihrem AWS-Konto zu ändern.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis bedeutet, dass ein bestimmter Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) in Ihrer AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Diese Erkenntnis wird ausgelöst, wenn Ressourcen-Zugriffsberechtigungen in Ihrem AWS-Konto unter fragwürdigen Umständen untersucht werden. Dies trifft beispielsweise dann zu, wenn ein Prinzipal zum ersten Mal die `DescribeInstances`-API aufgerufen hat. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um in Kenntnis Ihrer AWS-Ressourcen zu gelangen, um wertvolle Informationen herauszufinden oder festzustellen, welcher Funktionsumfang den Anmeldeinformationen bereits zur Verfügung steht.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Recon:IAMUser/UserPermissions

Ein Prinzipal hat eine API aufgerufen, die üblicherweise dazu verwendet wird, IAM-Benutzer, Gruppen oder Richtlinien in Ihrem AWS-Konto hinzuzufügen, zu ändern oder zu löschen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis wird ausgelöst, wenn Benutzerberechtigungen in Ihrer AWS-Umgebung unter fragwürdigen Umständen untersucht werden. Dies trifft beispielsweise dann zu, wenn ein Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle, oder Benutzer) zum ersten Mal die `ListInstanceProfilesForRole`-API aufgerufen hat. Ein Angreifer könnte gestohlene Anmeldeinformationen verwenden, um in Kenntnis Ihrer AWS-Ressourcen zu gelangen, um wertvolle Informationen herauszufinden oder festzustellen, welcher Funktionsumfang den Anmeldeinformationen bereits zur Verfügung steht.

Diese Erkenntnis zeigt an, dass ein bestimmter Prinzipal in der AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Dieser Prinzipal hat diese API bisher nicht aufgerufen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

ResourceConsumption:IAMUser/ComputeResources

Ein Prinzipal hat eine API aufgerufen, die häufig zum Starten von Datenverarbeitungsressourcen verwendet wird, wie beispielsweise EC2-Instances.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis wird ausgelöst, wenn EC2-Instances im aufgeführten Konto in Ihrer AWS-Umgebung unter fragwürdigen Umständen gestartet werden. Diese Erkenntnis deutet darauf hin, dass ein bestimmter Prinzipal in Ihrer AWS-Umgebung ein Verhalten zeigt, das von der etablierten Grundlinie abweicht, z. B. wenn ein Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle oder IAM-Benutzer) die `RunInstances`-API aufruft, ohne dies zuvor jemals getan zu haben. Dies kann ein Anzeichen für ein Angreifer sein, der gestohlene Anmeldeinformationen nutzt, um Rechenzeit zu stehlen (beispielsweise für das Mining von Kryptowährung, oder zum Entschlüsseln von Passwörtern). Es kann auch ein Hinweis auf einen Angreifer sein, der eine EC2-Instance in Ihrer AWS-Umgebung und ihre Anmeldeinformationen nutzt, um auf Ihr Konto zuzugreifen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Stealth:IAMUser/LoggingConfigurationModified

Ein Prinzipal hat eine API aufgerufen, die üblicherweise verwendet wird, um die CloudTrail-Protokollierung zu beenden, vorhandene Protokolle zu löschen und anderweitig Aktivitätsspuren aus Ihrem AWS-Konto zu entfernen.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Diese Erkenntnis wird ausgelöst, wenn die Protokollierungskonfiguration in dem aufgeführten AWS-Konto in Ihrer Umgebung unter fragwürdigen Umständen geändert wird. Diese Erkenntnis deutet darauf hin, dass ein bestimmter Prinzipal in Ihrer AWS-Umgebung ein Verhalten zeigt, das von der etablierten Grundlinie abweicht, z. B. wenn ein Prinzipal (Root-Benutzer des AWS-Kontos, IAM-Rolle oder IAM-Benutzer) die `StopLogging`-API aufruft, ohne dies zuvor jemals getan zu haben. Dies kann darauf hinweisen, dass ein Angreifer versucht, seine Spuren zu verwischen, indem er alle Anzeichen von Aktivität entfernt.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

UnauthorizedAccess:IAMUser/ConsoleLogin

In Ihrem AWS-Konto wurde eine ungewöhnliche Konsolen-Anmeldung durch einen Prinzipal festgestellt.

Standard-Schweregrad: Mittel*

> **Note**
>
> Der Standard-Schweregrad dieser Erkenntnis ist Mittel. Wenn die API jedoch mit temporären AWS-Anmeldeinformationen aufgerufen wird, die auf einer -Instance erstellt wurden, ist der Schweregrad des Ergebnisses Hoch.

Dieses Ergebnis wird ausgelöst, wenn eine Konsolenanmeldung unter fragwürdigen Umständen erkannt wird. Dies ist beispielsweise dann der Fall, wenn ein Prinzipal die ConsoleLogin-API zum ersten Mal von einem nie zuvor verwendeten Client oder von einem ungewöhnlichen Standort aus aufgerufen hat. Dies könnte darauf hinweisen, dass gestohlene Anmeldeinformationen verwendet werden, um Zugriff auf Ihr AWS-Konto zu erlangen, oder dass ein gültiger Benutzer auf ungültige oder wenig sichere Weise auf das Konto zugreift (z. B. nicht über ein zugelassenes VPN).

Diese Erkenntnis informiert Sie darüber, dass ein bestimmter Prinzipal in der AWS-Umgebung ein Verhalten zeigt, das von seinem normalen Verhalten abweicht. Für diesen Prinzipal gibt es keinen vorherigen Verlauf von Anmeldeaktivitäten mit dieser Client-Anwendung von diesem bestimmten Standort aus.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

UnauthorizedAccess:EC2/TorIPCaller

Ihre EC2-Instance erhält eingehende Verbindungen von einem Tor-Exit-Knoten.

Standard-Schweregrad: Mittel

Diese Erkenntnis informiert Sie darüber, dass eine EC2-Instance in Ihrer AWS-Umgebung eingehende Verbindungen von einem Tor-Ausgangsknotens erhält. Tor ist eine Software, die anonyme Kommunikation ermöglicht. Sie verschlüsselt Kommunikation und leitet diese beliebig durch Relays zwischen einer Reihe von Netzwerkknoten. Der letzte Tor-Knoten wird als Exit-Knoten bezeichnet. Diese Erkenntnis kann auf einen unbefugten Zugriff auf die AWS-Ressourcen hinweisen, der das Ziel hat, die wahre Identität des Angreifers zu verbergen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Backdoor:EC2/XORDDOS

Eine EC2-Instance versucht, mit einer IP-Adresse zu kommunizieren, die mit XOR-DDoS-Malware in Verbindung steht.

Standard-Schweregrad: Hoch

Diese Erkenntnis informiert Sie, dass eine EC2-Instance in der AWS-Umgebung versucht, mit einer IP-Adresse zu kommunizieren, die mit XOR-DDoS-Malware in Verbindung steht. Diese EC2-Instance wurde möglicherweise kompromittiert. XOR DDoS ist eine Trojaner-Malware, die Linux-Systeme kapert. Um Zugriff auf das System zu erhalten, startet sie einen Brute-Force-Angriff, um das Passwort für Secure Shell (SSH)-Services auf Linux zu ermitteln. Nachdem die SSH-Anmeldeinformationen erlangt wurden und die Anmeldung erfolgreich war, wird ein Skript mit Root-Berechtigungen ausgeführt, um XOR DDoS herunterzuladen und zu installieren. Diese Malware wird dann als Teil eines Botnets verwendet, um verteilte DDoS-Angriffe (Distributed Denial-of-Service) auf andere Ziele zu durchzuführen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

Behavior:IAMUser/InstanceLaunchUnusual

Ein Benutzer hat eine EC2-Instance eines ungewöhnlichen Typs gestartet.

Standard-Schweregrad: Hoch

Diese Erkenntnis informiert Sie, dass ein bestimmter Benutzer in Ihrer AWS-Umgebung ein Verhalten zeigt, das sich von seinem normalen Verhalten unterscheidet. Dieser Benutzer hat bisher keine EC2-Instance dieses Typs gestartet. Ihre Anmeldeinformationen wurden möglicherweise kompromittiert.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

CryptoCurrency:EC2/BitcoinTool.A

Eine EC2-Instance kommuniziert mit Bitcoin-Mining-Pools.

Standard-Schweregrad: Hoch

Diese Erkenntnis informiert Sie, dass eine EC2-Instance in Ihrer AWS-Umgebung mit Bitcoin-Mining-Pools kommuniziert. Beim Mining von Kryptowährungen werden Ressourcen in einem Pool kombiniert, damit die Verarbeitungsleistung über ein Netzwerk gemeinsam genutzt werden kann. Der Gewinn wird dann nach Maßgabe der zur Lösung des Blocks beigetragenen Arbeit aufgeteilt. Wenn Sie diese EC2-Instance nicht für Bitcoin-Mining verwenden, könnte Ihre EC2-Instance kompromittiert worden sein.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, kann Ihre Instance kompromittiert sein. Weitere Informationen finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

UnauthorizedAccess:IAMUser/UnusualASNCaller

Eine API wurde von einer IP-Adresse eines unüblichen Netzwerks aufgerufen.

Standard-Schweregrad: Hoch

Dieses Ergebnis informiert Sie darüber, dass eine bestimmte Aktivität von einer IP-Adresse eines unüblichen Netzwerks aufgerufen wurde. Dieses Netzwerk wurde im gesamten AWS-Nutzungsverlauf des beschriebenen Benutzers noch nie beobachtet. Diese Aktivität kann eine Konsolen-Anmeldung, einen Versuch, eine EC2-Instance zu starten, einen neuen IAM-Benutzer anzulegen, Ihre AWS-Privilegien zu ändern usw. beinhalten. Dies kann auf einen unbefugten Zugriff auf Ihre AWS-Ressourcen hinweisen.

Empfehlungen zur Abhilfe:

Wenn solche Aktivitäten unerwartet auftreten, können Ihre Anmeldeinformationen kompromittiert sein. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.

Erkenntnisse nach Ressourcentyp

Die folgenden Seiten sind nach dem Ressourcentyp kategorisiert, der mit einem GuardDuty Ergebnis verknüpft ist:

- EC2-Erkenntnistypen
- IAMTypen finden
- S3-Erkenntnistypen
- EKSAuditprotokolle, Typen finden
- Runtime Monitoring: Typen finden
- Malware-Schutz für EC2-Suchtypen
- Suchtyp „Malware-Schutz für S3“
- Erkenntnistypen für RDS Protection
- Lambda-Protection-Erkenntnistypen

Tabelle mit den Erkenntnissen

Die folgende Tabelle zeigt alle aktiven Erkenntnistypen, sortiert nach der zugrunde liegenden Datenquelle oder das jeweiligen Feature. Einige der folgenden Erkenntnistypen können einen unterschiedlichen Schweregrad haben, der durch ein Sternchen (*) gekennzeichnet ist. Informationen zum variablen Schweregrad eines Erkenntnistyps finden Sie in der detaillierten Beschreibung dieses Erkenntnistyps.

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Discovery :S3/Anoma lousBehavior	Amazon S3	CloudTrail Datenereignisse für S3	Niedrig
Discovery:S3/ MaliciousIPCal ler	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Discovery:S3/ MaliciousIPCal ler.Custom	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Discovery:S3/ TorIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail Datenereignisse für S3	Mittelschwer
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
PenTest:S3/KaliLinux	Amazon S3	CloudTrail Datenereignisse für S3	Mittelschwer
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail Datenereignisse für S3	Mittelschwer
PenTest:S3/PentooLinux	Amazon S3	CloudTrail Datenereignisse für S3	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail Datenereignisse für S3	Hoch
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Ereignis	Mittelschwer
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Niedrig
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Hoch
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
PenTest:IAMUser/KaliLinux	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
PenTest:IAMUser/PentooLinux	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail Management-Veranstaltung	Niedrig*
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail Management-Veranstaltung	Hoch*

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail Management-Veranstaltung	Niedrig
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail Management-Veranstaltung	Hoch
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail Management-Veranstaltung	Niedrig
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail Management-Veranstaltung	Hoch
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail Management-Veranstaltung	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Recon:IAMUser/TorIPCaller	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail Management-Veranstaltung	Niedrig
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail Management-Veranstaltung	Niedrig
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail Management-Veranstaltung	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail Management-Veranstaltung	Mittelschwer
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3	Niedrig
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail Verwaltungsereignisse oder CloudTrail Datenereignisse für S3	Hoch
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	DNSLogs	Hoch
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	DNSLogs	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	DNSLogs	Mittelschwer
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	DNSLogs	Hoch
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	DNSLogs	Hoch
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	DNSLogs	Niedrig
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	DNSLogs	Mittelschwer
Trojan:EC2/DGADomainRequest.B	Amazon EC2	DNSLogs	Hoch
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	DNSLogs	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Trojan:EC2/DNSDataExfiltration	Amazon EC2	DNSLogs	Hoch
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	DNSLogs	Hoch
Trojan:EC2/DropPoint!DNS	Amazon EC2	DNSLogs	Mittelschwer
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	DNSLogs	Hoch
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	DNSLogs	Hoch
Execution:Container/MaliciousFile	Container	EBSSchutz vor Schadsoftware	Variiert je nach erkannter Bedrohung
Execution:Container/SuspiciousFile	Container	EBSSchutz vor Schadsoftware	Variiert je nach erkannter Bedrohung
Execution:EC2/MaliciousFile	EC2	EBSSchutz vor Schadsoftware	Variiert je nach erkannter Bedrohung

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Execution:EC2/SuspiciousFile	EC2	EBSSchutz vor Schadsoftware	Variiert je nach erkannter Bedrohung
Execution:ECS/MaliciousFile	ECS	EBSSchutz vor Schadsoftware	Variiert je nach erkannter Bedrohung
Execution:ECS/SuspiciousFile	ECS	EBSSchutz vor Schadsoftware	Variiert je nach erkannter Bedrohung
Execution:Kubernetes/MaliciousFile	Kubernetes	EBSSchutz vor Schadsoftware	Variiert je nach erkannter Bedrohung
Execution:Kubernetes/SuspiciousFile	Kubernetes	EBSSchutz vor Schadsoftware	Variiert je nach erkannter Bedrohung
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	EKSAudit-Protokolle	Mittelschwer
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	EKSAuditprotokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSAuditprotokolle	Hoch
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSAuditprotokolle	Hoch
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	EKSAuditprotokolle	Hoch
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	EKSAuditprotokolle	Hoch
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSAuditprotokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSAuditprotokolle	Hoch
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	EKSAuditprotokolle	Hoch
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	EKSAuditprotokolle	Niedrig
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	EKSAuditprotokolle	Mittelschwer
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSAuditprotokolle	Mittelschwer
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSAuditprotokolle	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Discovery:Kubernetes/TorIPCaller	Kubernetes	EKSAuditprotokolle	Mittelschwer
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	EKSAuditprotokolle	Mittelschwer
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	EKSAuditprotokolle	Mittelschwer
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	EKSAuditprotokolle	Niedrig
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	EKSAuditprotokolle	Hoch
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSAuditprotokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSAuditprotokolle	Hoch
Impact:Kubernetes/TorIPCaller	Kubernetes	EKSAuditprotokolle	Hoch
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	EKSAuditprotokolle	Mittelschwer
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	EKSAuditprotokolle	Mittelschwer
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSAuditprotokolle	Mittelschwer
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSAuditprotokolle	Hoch
Persistence:Kubernetes/TorIPCaller	Kubernetes	EKSAuditprotokolle	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	EKSAuditprotokolle	Hoch
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	EKSAuditprotokolle	Hoch
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	EKSAuditprotokolle	Mittelschwer
Policy:Kubernetes/ExposedDashboard	Kubernetes	EKSAuditprotokolle	Mittelschwer
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	EKSAuditprotokolle	Mittel*

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	EKSAuditprotokolle	Niedrig
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	EKSAuditprotokolle	Hoch
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	EKSAuditprotokolle	Hoch
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	EKSAuditprotokolle	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Backdoor:Lambda/C&CActivity.B	Lambda	Lambda Network Activity Monitoring	Hoch
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Lambda Network Activity Monitoring	Hoch
Trojan:Lambda/BlackholeTraffic	Lambda	Lambda Network Activity Monitoring	Mittelschwer
Trojan:Lambda/DropPoint	Lambda	Lambda Network Activity Monitoring	Mittelschwer
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Lambda Network Activity Monitoring	Mittelschwer
UnauthorizedAccess:Lambda/TorClient	Lambda	Lambda Network Activity Monitoring	Hoch
UnauthorizedAccess:Lambda/TorRelay	Lambda	Lambda Network Activity Monitoring	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken	RDSÜberwachung der Anmeldeaktivitäten	Niedrig
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken	RDSÜberwachung der Anmeldeaktivitäten	Hoch
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken	RDSÜberwachung der Anmeldeaktivitäten	Variable*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken	RDSÜberwachung der Anmeldeaktivitäten	Mittelschwer
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken	RDSÜberwachung der Anmeldeaktivitäten	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
CredentialAccess:RDS/TorIPCaller.FailedLogin	Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken	RDSÜberwachung der Anmeldeaktivitäten	Mittelschwer
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken	RDSÜberwachung der Anmeldeaktivitäten	Hoch
Discovery:RDS/MaliciousIPCaller	Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken	RDSÜberwachung der Anmeldeaktivitäten	Mittelschwer
Discovery:RDS/TorIPCaller	Unterstützte Amazon Aurora- und RDS Amazon-Datenbanken	RDSÜberwachung der Anmeldeaktivitäten	Mittelschwer
Backdoor:Runtime/C&CActivity.B	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
Backdoor:Runtime/C&CActivity.B!DNS	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
CryptoCurrency:Runtime/BitcoinTool.B	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
DefenseEvasion:Runtime/FilelessExecution	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
DefenseEvasion:Runtime/ProcessInjection.Proc	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
DefenseEvasion:Runtime/PtraceAntiDebugging	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Niedrig

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
DefenseEvasion:Runtime/SuspiciousCommand	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
Execution:Runtime/MaliciousFileExecuted	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
Execution:Runtime/NewBinaryExecuted	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Execution:Runtime/NewLibraryLoaded	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Execution:Runtime/SuspiciousCommand	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Variable
Execution:Runtime/SuspiciousShellCreated	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Niedrig
Execution:Runtime/SuspiciousTool	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Variable

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Execution:Runtime/ReverseShell	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
Impact:Runtime/AbusedDomainRequest.Reputation	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Impact:Runtime/BitcoinDomainRequest.Reputation	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
Impact:Runtime/CryptoMinerExecuted	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
Impact:Runtime/MaliciousDomainRequest.Reputation	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Niedrig

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
PrivilegeEscalation:Runtime/DockerSocketAccessed	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
PrivilegeEscalation:Runtime/ElevationToRoot	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
PrivilegeEscalation:Runtime/RuncContainerEscape	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
PrivilegeEscalation:Runtime/UserfaultfdUsage	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Object:S3/MaliciousFile	S3Objekt	Malware-Schutz für S3	Hoch
Trojan:Runtime/BlackholeTraffic	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Trojan:Runtime/BlackholeTraffic!DNS	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Trojan:Runtime/DropPoint	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Trojan:Runtime/DGADomainRequest.C!DNS	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
Trojan:Runtime/DriveBySourceTraffic!DNS	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Trojan:Runtime/DropPoint!DNS	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Mittelschwer
Trojan:Runtime/PhishingDomainRequest!DNS	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
UnauthorizedAccess:Runtime/TorClient	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
UnauthorizedAccess:Runtime/TorRelay	Instanz, EKS Cluster, ECS Cluster oder Container	Laufzeit-Überwachung	Hoch
Backdoor:EC2/C&CActivity.B	EC2	VPC-Flussprotokolle	Hoch
Backdoor:EC2/DenialOfService.Dns	EC2	VPC-Flussprotokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Backdoor:EC2/DenialOfService.Tcp	EC2	VPC-Flussprotokolle	Hoch
Backdoor:EC2/DenialOfService.Udp	EC2	VPC-Flussprotokolle	Hoch
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	VPC-Flussprotokolle	Hoch
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	VPC-Flussprotokolle	Hoch
Backdoor:EC2/Spambot	EC2	VPC-Flussprotokolle	Mittelschwer
Behavior:EC2/NetworkPortUnusual	EC2	VPC-Flussprotokolle	Mittelschwer
Behavior:EC2/TrafficVolumeUnusual	EC2	VPC-Flussprotokolle	Mittelschwer
CryptoCurrency:EC2/BitcoinTool.B	EC2	VPC-Flussprotokolle	Hoch

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
DefenseEvasion:EC2/UnusualDNSResolver	EC2	VPC-Flussprotokolle	Mittelschwer
DefenseEvasion:EC2/UnusualDoHActivity	EC2	VPC-Flussprotokolle	Mittelschwer
DefenseEvasion:EC2/UnusualDoTActivity	EC2	VPC-Flussprotokolle	Mittelschwer
Impact:EC2/PortSweep	EC2	VPC-Flussprotokolle	Hoch
Impact:EC2/WinRMBruteForce	EC2	VPC-Flussprotokolle	Niedrig*
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	VPC-Flussprotokolle	Hoch
Recon:EC2/PortProbeUnprotectedPort	EC2	VPC-Flussprotokolle	Niedrig*
Recon:EC2/Portscan	EC2	VPC-Flussprotokolle	Mittelschwer

Ergebnistyp	Ressourcentyp	Grundlegende Datenquelle/Feature	Der Schweregrad einer Erkenntnis
Trojan:EC2/BlackholeTraffic	EC2	VPC-Flussprotokolle	Mittelschwer
Trojan:EC2/DropPoint	EC2	VPC-Flussprotokolle	Mittelschwer
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	VPC-Flussprotokolle	Mittelschwer
UnauthorizedAccess:EC2/RDPBruteForce	EC2	VPC-Flussprotokolle	Niedrig*
UnauthorizedAccess:EC2/SSHBruteForce	EC2	VPC-Flussprotokolle	Niedrig*
UnauthorizedAccess:EC2/TorClient	EC2	VPC-Flussprotokolle	Hoch
UnauthorizedAccess:EC2/TorRelay	EC2	VPC-Flussprotokolle	Hoch

Verwaltung der GuardDuty Amazon-Ergebnisse

GuardDuty bietet mehrere wichtige Funktionen, mit denen Sie Ihre Ergebnisse sortieren, speichern und verwalten können. Mit diesen Funktionen können Sie Erkenntnisse an Ihre spezifische Umgebung anpassen. Dadurch können Sie erkenntnisbedingtes Rauschen niedrigen Schweregrads reduzieren und sich auf spezifische Bedrohungen für Ihre AWS -Umgebung konzentrieren. Lesen Sie sich die Themen auf dieser Seite durch, um zu erfahren, wie Sie diese Funktionen nutzen können, um den Wert Ihrer GuardDuty Ergebnisse zu steigern.

Themen:

Übersichts-Dashboard

Erfahren Sie mehr über die Komponenten des Übersichts-Dashboards, das in der GuardDuty Konsole verfügbar ist.

Filtern von Ergebnissen

Erfahren Sie, wie Sie GuardDuty Ergebnisse nach von Ihnen angegebenen Kriterien filtern können.

Unterdrückungsregeln

Erfahren Sie, wie Sie mithilfe von Unterdrückungsregeln die Ergebnisse, auf die Sie GuardDuty aufmerksam gemacht werden, automatisch filtern können. Mithilfe von Unterdrückungsregeln werden Erkenntnisse automatisch auf der Grundlage von Filtern archiviert.

Arbeiten mit vertrauenswürdigen IP- und Bedrohungslisten

Passen Sie den Umfang der GuardDuty Überwachung mithilfe von IP-Listen und Bedrohungslisten an, die auf öffentlich routingfähigen IP-Adressen basieren. Vertrauenswürdige IP-Listen verhindern, dass aus IP-Adressen, die Sie für vertrauenswürdig halten, keine DNS Ergebnisse generiert werden, während Intel-Bedrohungslisten Sie vor benutzerdefinierten Aktivitäten warnen. GuardDuty IPs

Exportieren von Erkenntnissen

Exportieren Sie die generierten Ergebnisse in einen Amazon S3 S3-Bucket, sodass Sie Aufzeichnungen über die 90-tägige Aufbewahrungsfrist für Ergebnisse hinaus verwalten können. GuardDuty Verwenden Sie diese historischen Daten, um potenzielle verdächtige Aktivitäten

in Ihrem Konto nachzuverfolgen und zu bewerten, ob die empfohlenen Abhilfemaßnahmen erfolgreich waren.

Erstellen von benutzerdefinierten Antworten auf GuardDuty Erkenntnisse mit Amazon CloudWatch Events

Richten Sie automatische Benachrichtigungen für GuardDuty Ergebnisse im Rahmen von CloudWatch Amazon-Veranstaltungen ein. Sie können auch andere Aufgaben mithilfe von CloudWatch Events automatisieren, um auf Ergebnisse zu reagieren.

Grundlegendes zu CloudWatch Protokollen und Gründen für das Überspringen von Ressourcen beim Scan von Malware Protection for EC2

Erfahren Sie, wie Sie die CloudWatch Logs for GuardDuty Malware Protection überprüfen können EC2 und aus welchen Gründen Ihre betroffenen EC2 Amazon-Instances oder EBS Amazon-Volumes während des Scanvorgangs möglicherweise übersprungen wurden.

Falschmeldungen in GuardDuty Malware Protection for EC2 melden

Erfahren Sie, wie Sie potenzielle falsch positive Bedrohungserkennungen in Malware Protection for S3 melden können.

Übersichts-Dashboard

Das Übersichts-Dashboard bietet eine aggregierte Ansicht der GuardDuty Ergebnisse, die AWS-Konto in Ihrer aktuellen Region generiert wurden. Derzeit unterstützt das Dashboard ein Volumen von bis zu 5 000 Erkenntnissen. Sie können jedoch die Details aller Ergebnisse einsehen, indem Sie entweder die Ergebnisseite in der GuardDuty Konsole oder oder GetFindingsoder ListFindingsverwenden.

> **Note**
>
> Die Zusammenfassung der Ergebnisse ist nur über die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/ verfügbar.

Die folgenden Abschnitten helfen Ihnen, auf das Dashboard zuzugreifen und dessen Komponenten zu verstehen.

Inhalt

Zugriff auf das Zusammenfassungs-Dashboard

Auf der GuardDuty Konsole zeigt das Übersichts-Dashboard eine konsolidierte Ansicht der letzten 5.000 GuardDuty Ergebnisse, die in der aktuellen Region generiert wurden.

So greifen Sie auf das Zusammenfassungs-Dashboard zu

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Zusammenfassung aus. Wenn Sie die Konsole öffnen, GuardDuty wird das Übersichts-Dashboard angezeigt.
3. Standardmäßig wird die Zusammenfassung für denselben Tag angezeigt – Heute. Die GuardDuty Konsole bietet eine Option zum Anzeigen der Zusammenfassung der letzten 2 Tage, der letzten 7 Tage und der letzten 30 Tage. Um den Standardzeitbereich zu ändern, wählen Sie eine der Optionen aus dem Drop-down-Menü über dem Übersichtsbereich.
4. Filtern der Daten

   - Die Widgets Konten mit den meisten Erkenntnissen, Ressourcen mit den meisten Erkenntnissen und Am wenigsten vorkommende Erkenntnisse können die Daten nach dem Schweregrad der Ergebnisse filtern.
   - Das Widget Ressourcen mit den meisten Erkenntnissen hilft Ihnen auch dabei, die Daten auf der Grundlage Ihres potenziell betroffenen Ressourcentyps zu filtern.

     Ein Mitgliedskonto kann die Details der potenziell betroffenen Ressource einsehen, die zu seinem eigenen Konto gehört. Wenn Sie ein GuardDuty Administratorkonto haben und die Details der potenziell betroffenen Ressource einsehen möchten, öffnen Sie die GuardDuty Konsole mit den Anmeldeinformationen des zugehörigen Mitgliedskontos.
5. Geltungsbereich der Schutzpläne

   Der Geltungsbereich der Schutzpläne gibt die Anzahl der Mitgliedskonten an, die GuardDuty in Ihrer Organisation aktiviert wurden. Die Statistiken sind nur für den delegierten GuardDuty Administrator sichtbar.

Verstehen des Zusammenfassungs-Dashboards

Das Zusammenfassungs-Dashboard zeigt die aggregierten Daten in den folgenden Abschnitten. Bevor Sie sich die Zusammenfassung ansehen und verstehen, stellen Sie sicher, dass Sie in der Regionsauswahl oben in der Konsole die gewünschte AWS-Region auswählen. Stellen Sie außerdem sicher, dass Sie den gewünschten Zeitraum aus dem Dropdownmenü über dem Übersichtsbereich auswählen. Wenn für die ausgewählten Parameter keine Erkenntnisse generiert wurden, sind in keinem der Widgets Daten verfügbar.

Aus einer Menge von bis zu 5.000 GuardDuty Ergebnissen werden im Übersichts-Dashboard mit den Konten mit den meisten Ergebnissen, Ressourcen mit den meisten Ergebnissen und den am wenigsten vorkommenden Ergebnissen die Daten angezeigt, die auf den fünf wichtigsten Ergebnissen basieren. Eine eingehendere Analyse finden Sie auf der Ergebnisseite in der GuardDuty Konsole.

Übersicht

Diese Einstellung bietet die folgenden Optionen:

- Erkenntnisse insgesamt: Gibt die Gesamtzahl von Erkenntnissen an, die in Ihrem Konto in der aktuellen Region generiert wurden.
- Ergebnisse mit hohem Schweregrad: Gibt die Anzahl der GuardDuty Ergebnisse an, die in der aktuellen Region einen hohen Schweregrad aufweisen.
- Ressourcen mit Erkenntnissen: Gibt die Anzahl der Ressourcen an, die mit einer Erkenntnis verknüpft sind und möglicherweise gefährdet wurden.
- Konten mit Erkenntnissen: Gibt die Anzahl der Konten an, in denen mindestens eine Erkenntnis generiert wurde. Wenn Sie ein eigenständiges Konto haben, ist der Wert in diesem Feld 1.

Für die Zeitbereiche Letzte 7 Tage und Letzte 30 Tage kann im Bereich Übersicht der prozentuale Unterschied zwischen den generierten Erkenntnissen von Woche zu Woche (WoW) bzw. Monat zu Monat (MoM) angezeigt werden. Wenn in der Woche oder im Monat zuvor keine Erkenntnisse generiert wurden und keine Vergleichsdaten vorliegen, ist die prozentuale Differenz möglicherweise nicht verfügbar.

Wenn Sie ein GuardDuty Administratorkonto haben, enthalten all diese Felder die zusammengefassten Daten aller Mitgliedskonten in Ihrer Organisation.

Erkenntnisse nach Schweregrad

In diesem Abschnitt wird ein Balkendiagramm mit der Gesamtzahl der Erkenntnisse im ausgewählten Zeitraum angezeigt. Sie können die Anzahl der Erkenntnisse mit niedrigem, mittlerem oder hohem Schweregrad anzeigen, die an einem bestimmten Datum innerhalb des ausgewählten Zeitraums generiert wurden.

Die häufigsten Arten von Erkenntnissen

In diesem Abschnitt werden die fünf häufigsten Ergebnisarten anhand eines Kreisdiagramms anhand einer Menge von bis zu 5.000 GuardDuty Ergebnissen dargestellt, die in der aktuellen Region generiert wurden. In diesem Kreisdiagramm werden die folgenden Daten angezeigt, wenn Sie den Mauszeiger über die einzelnen Sektoren bewegen:

- Anzahl der Erkenntnisse: Gibt an, wie oft diese Erkenntnis im ausgewählten Zeitraum generiert wurde.
- Schweregrad: Gibt den Schweregrad der Erkenntnis an, z. B. Mittel und Hoch.
- Prozentsatz: Gibt den Anteil dieses Erkenntnistyps im Kreisdiagramm an.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.

Konten mit den meisten Erkenntnissen

Diese Einstellung bietet die folgenden Optionen:

- Konto: Gibt die AWS-Konto ID an, unter der das Ergebnis generiert wurde.
- Anzahl der Erkenntnisse: Gibt an, wie oft eine Erkenntnis für diese Konto-ID generiert wurde.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.
- Hoher Schweregrad: Standardmäßig werden die Daten für die Erkenntnistypen mit hohem Schweregrad angezeigt. Mögliche Optionen für dieses Feld sind Hoher Schweregrad, Mittlerer Schweregrad und Gesamter Schweregrad.

Ressourcen mit Erkenntnissen

Diese Einstellung bietet die folgenden Optionen:

- Ressource: Gibt den potenziell betroffenen Ressourcentyp an. Wenn diese Ressource zu Ihrem Konto gehört, können Sie auf den Quicklink zugreifen, um die Ressourcendetails einzusehen. Wenn Sie ein GuardDuty Administratorkonto haben, können Sie die Details der potenziell betroffenen Ressource einsehen, indem Sie mit den Anmeldeinformationen des Mitgliedskontos, zu dem diese Ressource gehört, auf die GuardDuty Konsole zugreifen.
- Konto: Gibt die AWS-Konto ID an, zu der diese Ressource gehört.
- Anzahl der Erkenntnisse: Gibt an, wie oft diese Ressource mit einer Erkenntnis verknüpft wurde.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.
- Alle Ressourcentypen: Standardmäßig werden die Daten für alle Ressourcentypen angezeigt. Mithilfe der Dropdownliste können Sie die Daten für einen bestimmten Ressourcentyp wie Instance AccessKey, Lambda und andere anzeigen.
- Hoher Schweregrad: Standardmäßig werden die Daten für die Erkenntnistypen mit hohem Schweregrad angezeigt. Mithilfe der Dropdownliste können Sie die Daten für andere Schweregrade anzeigen. Mögliche Optionen für dieses Feld sind Hoher Schweregrad, Mittlerer Schweregrad und Gesamter Schweregrad.

Am wenigsten auftretende Erkenntnisse

Dieser Abschnitt enthält Einzelheiten zu den Suchtypen, die in Ihrer AWS Umgebung nicht häufig generiert werden. Diese Einsichten können Ihnen helfen, ein neu auftretendes Bedrohungsmuster in Ihrer Umgebung zu untersuchen und entsprechende Maßnahmen zu ergreifen. Die Tabelle enthält die folgenden Daten:

- Erkenntnistyp: Gibt den Namen des Erkenntnistyps an.
- Anzahl der Erkenntnisse: Gibt an, wie oft diese Erkenntnis im ausgewählten Zeitraum generiert wurde.
- Zuletzt generiert: Gibt an, wie viel Zeit seit der letzten Generierung dieses Erkenntnistyps vergangen ist.
- Hoher Schweregrad: Standardmäßig werden die Daten für die Erkenntnistypen mit hohem Schweregrad angezeigt. Mögliche Optionen für dieses Feld sind Hoher Schweregrad, Mittlerer Schweregrad und Gesamter Schweregrad.

Geltungsbereich der Schutzpläne

In diesem Abschnitt finden Sie die Anzahl der aktiven Mitgliedskonten, die zu Ihrer Organisation gehören und für die in der aktuellen Konfiguration eine oder mehrere Funktionen und zusätzliche Funktionen (falls zutreffend) aktiviert wurden AWS-Region.

Nur ein delegierter GuardDuty Administrator kann die Statistiken für die Mitgliedskonten innerhalb seiner Organisation einsehen. Wenn eine Funktion nicht konfiguriert ist, wählen Sie in der Spalte Aktionen die Option Konfigurieren aus.

Wenn Sie eine neue AWS Organisation erstellen, kann es bis zu 24 Stunden dauern, bis die Statistiken für die gesamte Organisation generiert sind.

Feedback zum Zusammenfassungs-Dashboard geben

GuardDuty fordert Sie auf, Feedback zur Benutzerfreundlichkeit, den Funktionen und der Leistung des Übersichts-Dashboards zu geben. Dies wird uns helfen, das Dashboard zu verbessern.

Um Feedback zum Zusammenfassungs-Dashboard zu geben

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Zusammenfassung aus. Wenn Sie die GuardDuty Konsole öffnen, wird das Übersichts-Dashboard angezeigt.
3. Wählen Sie Feedback in der oberen rechten Ecke des Dashboards. Dadurch wird ein Formular geöffnet. Nachdem Sie das Feedback gegeben haben, wählen Sie Senden.

Filtern von Ergebnissen

Mit einem Erkenntnisfilter können Sie Erkenntnisse anzeigen, die den von Ihnen angegebenen Kriterien entsprechen, und alle nicht übereinstimmenden Erkenntnisse herausfiltern. Sie können Suchfilter ganz einfach mit der GuardDuty Amazon-Konsole erstellen, oder Sie können sie mit der CreateFilterAPIVerwendung von erstellenJSON. Lesen Sie die folgenden Abschnitte, um zu erfahren, wie Sie einen Filter in der Konsole erstellen. Informationen zur Verwendung dieser Filter zur automatischen Archivierung eingehender Erkenntnisse finden Sie unter Unterdrückungsregeln.

Filter in der GuardDuty Konsole erstellen

Suchfilter können über die GuardDuty Konsole erstellt und getestet werden. Sie können über die Konsole erstellte Filter speichern, um sie in Unterdrückungsregeln oder zukünftigen Filtervorgängen

zu verwenden. Ein Filter besteht aus mindestens einem Filterkriterium, das aus einem Filterattribut in Kombination mit mindestens einem Wert besteht.

Beachten Sie beim Anlegen eines neuen Benutzers Folgendes:

- Filter akzeptieren keine Platzhalter.
- Sie können mindestens ein Attribut oder maximal 50 Attribute als Kriterien für einen bestimmten Filter angeben.
- Wenn Sie die Bedingung gleich zu oder ungleich zu verwenden, um nach einem Attributwert wie z. B. der Konto-ID zu filtern, können Sie maximal 50 Werte angeben.
- Jedes Filterkriterienattribut wird als AND-Operator ausgewertet. Mehrere Werte für dasselbe Attribut werden als AND/OR ausgewertet.

So filtern Sie Ergebnisse (Konsole)

1. Wählen Sie unter Nach Attribut filtern die Option Filterkriterien hinzufügen aus. Daraufhin wird Ihnen eine erweiterte Liste von Filterattributen angezeigt.
2. Wählen Sie aus der erweiterten Attributliste das Attribut aus, das Sie als Kriterien für Ihren Filter angeben möchten, z. B. Konto-ID oder Aktionstyp.

   Eine vollständige Liste der Attribute finden Sie unterFilterattribute.
3. Geben Sie im angezeigten Textfeld einen Wert für das ausgewählte Attribut ein und klicken Sie dann auf Anwenden.
4. Um mehr als ein Filterkriterium hinzuzufügen, wiederholen Sie die Schritte 1—3.
5. Standardmäßig werden in der Liste die Ergebnisse angezeigt, die mit dem angewendeten Filter übereinstimmen. Wenn Sie die Ergebnisse anzeigen möchten, die nicht mit dem Filterattribut übereinstimmen, wählen Sie neben dem Filter Ausschließen aus.

6. Speichern Sie die angegebenen Attribute und Werte als Filter

   a. Um die angegebenen Attribute und ihre Werte (Filterkriterien) als Filter zu speichern, wählen Sie Speichern/Bearbeiten.

   b. Geben Sie den Namen und die Beschreibung der Filterregel ein.

   c. Wählen Sie Save (Speichern) aus.

Filterattribute

Wenn Sie Filter erstellen oder Ergebnisse mithilfe der API Operationen sortieren, müssen Sie die Filterkriterien unter angebenJSON. Diese Filterkriterien korrelieren mit den Details JSON eines Ergebnisses. Die folgende Tabelle enthält eine Liste der Konsolenanzeigenamen für Filterattribute und der entsprechenden JSON Feldnamen.

Konsolen-Feldname	JSON-Feldname
Konto-ID	accountId
Die ID des Ergebnisses	id
Region	Region
Schweregrad	severity Sie können die Befundtypen nach dem Schweregrad der Befundtypen filtern. Weitere Informationen zu Schweregradwerten finden Sie unter GuardDuty Schweregrade der Ergebnisse. Wenn Sie `severity` mitAPI, oder AWS CloudFormation verwenden AWS CLI, wird ihm ein numerischer Wert zugewiesen. Weitere Informationen finden Sie findingCriteriain der GuardDuty APIAmazon-Referenz.
Ergebnistyp	Typ
Aktualisiert um	updatedAt

Konsolen-Feldname	JSON-Feldname
Access Key ID	Ressource. accessKeyDetails. accessKeyId
Haupt-ID	Ressource. accessKeyDetails. principalId
Username	Ressource. accessKeyDetails. userName
Benutzertyp	Ressource. accessKeyDetails. userType
IAMID des Instanzprofils	Ressource. instanceDetails. iamInstanceProfile .id
Instance-ID	Ressource. instanceDetails. instanceId
ID des Instance-Image	Ressource. instanceDetails. imageId
Instance-Tag-Schlüssel	Ressource. instanceDetails.tags.key
Instance-Tag-Wert	Ressource. instanceDetails.tags.value
IPv6Adresse	Ressource. instanceDetails. networkInterfaces. IPv6-Adressen
Private Adresse IPv4	Ressource. instanceDetails. networkInterfaces. privateIpAddresses. privateIpAddress
Öffentlicher DNS Name	Ressource. instanceDetails. networkInterfaces. publicDnsName
Öffentliche IP	Ressource. instanceDetails. networkInterfaces. publicIp
Sicherheitsgruppen-ID	Ressource. instanceDetails. networkInterfaces. securityGroups. groupId
Name der Sicherheitsgruppe	Ressource. instanceDetails. networkInterfaces. securityGroups. groupName
Subnetz-ID	Ressource. instanceDetails. networkInterfaces. subnetId

Konsolen-Feldname	JSON-Feldname
VPCAusweis	Ressource. instanceDetails. networkInterfaces. vpcId
Außenposten ARN	Ressource. instanceDetails. Außenposten ARN
Ressourcentyp	Ressource. resourceType
Bucket-Berechtigungen	Ressource.s3BucketDetails. publicAccess. effectivePermission
Bucket-Name	resource.s3 .name BucketDetails
Bucket-Tag-Schlüssel	resource.s3 BucketDetails .tags.key
Bucket-Tag-Wert	resource.s3 BucketDetails .tags.value
Bucket-Typ	resource.s3 BucketDetails .type
Aktionstyp	dienste.aktion. actionType
APIgenannt	service.action. awsApiCallAktion.API
APITyp des Anrufers	Service.Aktion. awsApiCallAktion. callerType
APIFehlercode	service.action. awsApiCallAktion. errorCode
APIStadt des Anrufers	Service. Aktion. awsApiCallAktion. remoteIpD etails. Stadt. cityName
APILand des Anrufers	Service. Aktion. awsApiCallAktion. remoteIpD etails. Land. countryName
APIAdresse des Anrufers IPv4	Service.Aktion. awsApiCallAktion. remoteIpD etails. ipAddressV4
APIAdresse des Anrufers IPv6	Service.Aktion. awsApiCallAktion. remoteIpD etails. ipAddressV6

Konsolen-Feldname	JSON-Feldname
APIAnrufer-ID ASN	Service.Aktion. awsApiCallAktion. remoteIpD etails.organization.asn
APIName des Anrufers ASN	dienst.aktion. awsApiCallAktion. remoteIpD etails. Organisation. asnOrg
APIName des Anruferdienstes	dienst.aktion. awsApiCallAktion. serviceName
DNSDomain anfragen	service.action. dnsRequestAction.domäne
DNSDomain-Suffix anfordern	service.action. dnsRequestAction. domainWit hSuffix
Netzwerkverbindung blockiert	Service.Aktion. networkConnectionAction. blockiert
Netzwerkverbindungsrichtung	Service.Aktion. networkConnectionAction. connectionDirection
Netzwerkverbindung lokaler Port	Service.Aktion. networkConnectionAction. localPortDetails. Hafen
Netzwerkverbindungsprotokoll	Service.Aktion. networkConnectionAction. Protokoll
Netzwerkverbindung Stadt	Service.Aktion. networkConnectionAction. remoteIpDetails. Stadt. cityName
Netzwerkverbindung Land	Service.Aktion. networkConnectionAction. remoteIpDetails. Land. countryName
IPv4Remote-Adresse der Netzwerkverbindung	service.action. networkConnectionAction. remoteIpDetails. ipAddressV4
IPv6Remote-Adresse der Netzwerkverbindung	service.action. networkConnectionAction. remoteIpDetails. ipAddressV6

Konsolen-Feldname	JSON-Feldname
ASNRemote-IP-ID der Netzwerkverbindung	service.action. networkConnectionAction. remoteIpDetails.organisation.asn
Remote-IP-Name der Netzwerkverbindung ASN	service.action. networkConnectionAction. remoteIpDetails. Organisation. asnOrg
Remote-Port der Netzwerkverbindung	Service.Aktion. networkConnectionAction. remotePortDetails. Hafen
Remote-Konto zugeordnet	Service.Aktion. awsApiCallAktion. remoteAcc ountDetails. angegliedert
Adresse des Kubernetes-Anrufers API IPv4	service.action. kubernetesApiCallAktion. remoteIpDetails. ipAddressV4
Adresse des Kubernetes-Anrufers API IPv6	service.action. kubernetesApiCallAktion. remoteIpDetails. ipAddressV6
Kubernetes-Namespace	Service. Aktion. kubernetesApiCallAktion.Nam espace
Kubernetes-Anrufer-ID API ASN	dienst.aktion. kubernetesApiCallAktion. remoteIpDetails.organization.asn
Kubernetes-Anrufanfrage API URI	service.action. kubernetesApiCallAktion. requestUri
Kubernetes-Statuscode API	service.action. kubernetesApiCallAktion. statusCode
Lokale IPv4 Adresse der Netzwerkverbindung	service.action. networkConnectionAction. localIpDetails. ipAddressV4
Lokale IPv6 Adresse der Netzwerkverbindung	service.action. networkConnectionAction. localIpDetails. ipAddressV6
Protokoll	Service. Aktion. networkConnectionAction. Protokoll

Konsolen-Feldname	JSON-Feldname
APIDienstname anrufen	dienst.aktion. awsApiCallAktion. serviceName
APIKonto-ID des Anrufers	service.action. awsApiCallAktion. remoteAcc ountDetails. accountId
Name der Bedrohungsliste	Bedienung. additionalInfo. threatListName
Ressourcenrolle	Bedienung. resourceRole
EKSClustername	Ressource. eksClusterDetails.name
Name des Kubernetes-Workloads	Ressource. kubernetesDetails. kubernete sWorkloadDetails. Name
Namespace des Kubernetes-Workloads	Ressource. kubernetesDetails. kubernete sWorkloadDetails. Namespace
Kubernetes-Benutzername	Ressource. kubernetesDetails. kubernete sUserDetails.benutzername
Kubernetes-Container-Image	Ressource. kubernetesDetails. kubernete sWorkloadDetails.containers.image
Kubernetes-Container-Image-Präfix	Ressource. kubernetesDetails. kubernete sWorkloadDetails. Behälter. imagePrefix
Scan-ID	Bedienung. ebsVolumeScanEinzelheiten. scanId
EBSName der Volumenscan-Bedrohung	Dienst. ebsVolumeScanEinzelheiten. scanDetections. threatDetectedByName. threatNames.name
Name der Bedrohung durch S3-Objektscan	Dienst. malwareScanDetails.bedrohun gen.name

Konsolen-Feldname	JSON-Feldname
Schweregrad der Bedrohung	Dienst. ebsVolumeScanEinzelheiten. scanDetections. threatDetectedByName. threatNames. Schweregrad
Datei SHA	Dienst. ebsVolumeScanEinzelheiten. scanDetections. threatDetectedByName. threatNames. filePaths. Hash
ECSClustername	Ressource. ecsClusterDetails.name
ECSContainer-Bild	Ressource. ecsClusterDetails. taskDetai ls.containers.image
ECSAufgabendefinition ARN	Ressource. ecsClusterDetails. taskDetails. definitionArn
Eigenständiges Container-Image	Ressource. containerDetails. Bild
Datenbank-Instance-ID	Ressource. rdsDbInstanceEinzelheiten. dbInstanceIdentifier
Datenbank-Cluster-ID	Ressource. rdsDbInstanceEinzelheiten. dbClusterIdentifier
Datenbank-Engine	Ressource. rdsDbInstanceEinzelheiten. Motor
Datenbankbenutzer	Ressource. rdsDbUserEinzelheiten. Benutzer
Tag-Schlüssel der Datenbank-Instance	Ressource. rdsDbInstancedetails.tags.key
Tag-Wert der Datenbank-Instance	Ressource. rdsDbInstanceDetails.Tags.Wert
Ausführbar -256 SHA	Bedienung. runtimeDetails. Prozess. executabl eSha256
Prozessname	Bedienung. runtimeDetails.prozessname

Konsolen-Feldname	JSON-Feldname
Pfad der ausführbaren Datei	Dienst. runtimeDetails. Prozess. executablePath
Lambda-Funktionsname	Ressource. lambdaDetails. functionName
Lambda-Funktion ARN	Ressource. lambdaDetails. functionArn
Lambda-Funktions-Tag-Schlüssel	Ressource. lambdaDetails.tags.key
Tag-Wert der Lambda-Funktion	Ressource. lambdaDetails.tags.value
DNSDomain anfragen	service.action. dnsRequestAction. domainWithSuffix

Unterdrückungsregeln

Eine Unterdrückungsregel ist eine Reihe von Kriterien, die zum Filtern von Erkenntnissen verwendet werden, indem neue Erkenntnisse, die den angegebenen Kriterien entsprechen, automatisch archiviert werden. Unterdrückungsregeln können verwendet werden, um Ergebnisse mit niedrigem Wert, falsch positive Ergebnisse oder Bedrohungen zu filtern, auf die Sie nicht reagieren möchten, sodass die Sicherheitsbedrohungen mit den meisten Auswirkungen auf Ihre Umgebung leichter zu erkennen sind.

Nachdem Sie eine Unterdrückungsregel erstellt haben, werden neue Ergebnisse, die den in der Regel definierten Kriterien entsprechen, automatisch archiviert, solange die Unterdrückungsregel gültig ist. Sie können einen vorhandenen Filter verwenden, um eine Unterdrückungsregel zu erstellen, oder einen neuen Filter für die Unterdrückungsregel definieren, während Sie sie erstellen. Sie können Unterdrückungsregeln so konfigurieren, dass ganze Ergebnistypen unterdrückt werden, oder detailliertere Filterkriterien definieren, damit nur bestimmte Instances eines bestimmten Ergebnistyps unterdrückt werden. Sie können die Unterdrückungsregeln jederzeit bearbeiten.

Unterdrückte Ergebnisse werden nicht an AWS Security Hub Amazon Simple Storage Service, Amazon Detective oder Amazon gesendet, wodurch der Geräuschpegel reduziert wird EventBridge, wenn Sie GuardDuty Ergebnisse über Security Hub, einen Drittanbieter SIEM oder andere Alarm- und Ticketing-Anwendungen nutzen. Wenn Sie diese Option aktiviert habenMalware-Schutz für EC2, lösen die unterdrückten GuardDuty Ergebnisse keinen Malware-Scan aus.

GuardDuty generiert weiterhin Ergebnisse, auch wenn sie Ihren Unterdrückungsregeln entsprechen. Diese Ergebnisse werden jedoch automatisch als archiviert markiert. Das archivierte Ergebnis wird 90 Tage lang gespeichert und kann in GuardDuty diesem Zeitraum jederzeit eingesehen werden. Sie können unterdrückte Ergebnisse in der GuardDuty Konsole anzeigen, indem Sie in der Tabelle mit den Ergebnissen die Option Archiviert auswählen oder indem GuardDuty API Sie das Kriterium ListFindingsAPImit dem `findingCriteria` Kriterium „Wahr`service.archived`“ verwenden.

> **Note**
>
> In einer Umgebung mit mehreren Konten kann nur der GuardDuty Administrator Unterdrückungsregeln erstellen.

Häufige Anwendungsfälle für Unterdrückungsregeln und Beispiele

Die folgenden Findetypen werden häufig für die Anwendung von Unterdrückungsregeln verwendet. Wählen Sie den Namen des Befundes aus, um mehr über dieses Ergebnis zu erfahren. Lesen Sie die Beschreibung des Anwendungsfalls, um zu entscheiden, ob Sie eine Unterdrückungsregel für diesen Befundtyp erstellen möchten.

> **Important**
>
> GuardDuty empfiehlt, dass Sie Unterdrückungsregeln reaktiv und nur für Ergebnisse erstellen, für die Sie in Ihrer Umgebung wiederholt falsch positive Ergebnisse festgestellt haben.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS— Verwenden Sie eine Unterdrückungsregel, um automatisch Ergebnisse zu archivieren, die generiert werden, wenn das VPC Netzwerk so konfiguriert ist, dass der Internetverkehr so weitergeleitet wird, dass er von einem lokalen Gateway und nicht von einem VPC Internet Gateway ausgeht.

  Dieses Ergebnis wird generiert, wenn das Netzwerk so konfiguriert ist, dass Internetverkehr so weitergeleitet wird, dass er von einem lokalen Gateway und nicht von einem VPC Internet Gateway () ausgeht. IGW Allgemeine Konfigurationen, wie z. B. die Verwendung von VPC VPN Verbindungen AWS Outposts, können dazu führen, dass der Datenverkehr auf diese Weise weitergeleitet wird. Wenn dieses Verhalten zu erwarten ist, empfiehlt es sich, Unterdrückungsregeln zu verwenden und eine Regel zu erstellen, die aus zwei Filterkriterien

besteht. Das erste Kriterium ist der Ergebnistyp, der `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS` sein sollte. Das zweite Filterkriterium ist die APIIPv4Anruferadresse mit der IP-Adresse oder dem CIDR Bereich Ihres lokalen Internet-Gateways. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Suchtyp anhand der IP-Adresse des API Anrufers zu unterdrücken.

```
Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
 API caller IPv4 address: 198.51.100.6
```

> **Note**
>
> Um mehrere API Anrufer einzubeziehen, können IPs Sie für jeden Anruferadressfilter einen neuen API IPv4 Anruferadressfilter hinzufügen.

- Recon:EC2/Portscan – Verwenden Sie eine Unterdrückungsregel, um Erkenntnisse automatisch zu aktivieren, wenn Sie eine Anwendung für Schwachstellenanalysen verwenden.

  Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Recon:EC2/Portscan` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die diese Tools zur Schwachstellenanalyse hosten. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Findetyp auf der Grundlage von Instanzen mit einem bestimmten Wert zu unterdrücken. AMI

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce – Verwenden Sie eine Unterdrückungsregel, um Erkenntnisse, die sich auf Bastion-Instances beziehen, automatisch zu archivieren.

  Wenn das Ziel des Brute-Force-Versuchs ein Bastion-Host ist, kann dies ein erwartetes Verhalten für Ihre AWS Umgebung darstellen. In diesem Fall sollten Sie für dieses Ergebnis eine Unterdrückungsregel einrichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `UnauthorizedAccess:EC2/SSHBruteForce` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Das folgende Beispiel stellt den Filter dar, den Sie verwenden

würden, um diesen Erkenntnistyp auf der Grundlage von Instances mit einem bestimmten Instance-Tag-Wert zu unterdrücken.

```
Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
```

- Recon:EC2/PortProbeUnprotectedPort – Verwenden Sie eine Unterdrückungsregel, um Erkenntnisse automatisch zu archivieren, wenn sie auf absichtlich exponierte Instances ausgerichtet ist.

  In einigen Fällen werden Instances absichtlich exponiert, weil sie beispielsweise Web-Server hosten. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für dieses Ergebnis einzurichten. Die Unterdrückungsregel sollte aus zwei Filterkriterien bestehen. Das erste Kriterium sollte das Attribut Ergebnistyp mit dem Wert `Recon:EC2/PortProbeUnprotectedPort` verwenden. Das zweite Filterkriterium sollte den Instances entsprechen, die als Bastion-Host eingesetzt werden. Sie können entweder das Attribut Instance-Image-ID oder das Attribut Tag verwenden, abhängig davon, welches Kriterium mit den Instances identifiziert werden kann, die diese Tools hosten. Das folgende Beispiel stellt den Filter dar, den Sie verwenden würden, um diesen Erkenntnistyp auf der Grundlage von Instances mit einem bestimmten Instance-Tag-Schlüssel in der Konsole zu unterdrücken.

  ```
  Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
  ```

Empfohlene Unterdrückungsregeln für Ergebnisse von Runtime Monitoring

- PrivilegeEscalation:Runtime/DockerSocketAccessed wird generiert, wenn ein Prozess in einem Container mit dem Docker-Socket kommuniziert. Möglicherweise gibt es Container in Ihrer Umgebung, die aus legitimen Gründen auf den Docker-Socket zugreifen müssen. Der Zugriff von solchen Containern generiert PrivilegeEscalation:Runtime/DockerSocketAccessed-Erkenntnisse. Wenn dies in Ihrer AWS Umgebung der Fall ist, empfehlen wir Ihnen, eine Unterdrückungsregel für diesen Befundtyp einzurichten. Das erste Kriterium sollte das Attribut Erkenntnistyp mit dem Wert `PrivilegeEscalation:Runtime/DockerSocketAccessed` verwenden. Das zweite Filterkriterium ist das Feld Ausführbarer Pfad mit einem Wert, der dem Wert des Prozesses `executablePath` in der generierten Erkenntnis entspricht. Alternativ kann das zweite Filterkriterium das Feld Executable SHA -256 verwenden, dessen Wert dem Wert des Prozesses `executableSha256` im generierten Ergebnis entspricht.
- Kubernetes-Cluster betreiben ihre eigenen DNS Server als Pods, z. B. `coredns` Daher werden bei jeder DNS Suche in einem Pod zwei DNS Ereignisse GuardDuty erfasst — eines vom Pod und das

andere vom Server-Pod. Dadurch können Duplikate für die folgenden DNS Ergebnisse generiert werden:

- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS

Die doppelten Ergebnisse umfassen Pod-, Container- und Prozessdetails, die Ihrem DNS Server-Pod entsprechen. Sie können mithilfe dieser Felder eine Unterdrückungsregel einrichten, um diese doppelten Erkenntnisse zu unterdrücken. Bei den ersten Filterkriterien sollte das Feld Suchtyp mit einem Wert verwendet werden, der einem DNS Befundtyp aus der Liste der Ergebnisse entspricht, die weiter oben in diesem Abschnitt bereitgestellt wurde. Das zweite Filterkriterium könnte entweder der Pfad der ausführbaren Datei mit einem Wert sein, der dem Wert Ihres DNS Servers entspricht, `executablePath` oder die ausführbare Datei SHA -256 mit einem Wert, der dem Wert Ihres DNS Servers `executableSHA256` in der generierten Suche entspricht. Als optionales drittes Filterkriterium können Sie das Kubernetes-Container-Image-Feld verwenden, dessen Wert dem Container-Image Ihres DNS Server-Pods im generierten Ergebnis entspricht.

Regeln zur Unterdrückung erstellen

Wählen Sie Ihre bevorzugte Zugriffsmethode, um eine Unterdrückungsregel für die GuardDuty Suche nach Typen zu erstellen.

Console

Sie können Unterdrückungsregeln mithilfe der GuardDuty Konsole visualisieren, erstellen und verwalten. Unterdrückungsregeln werden auf die gleiche Weise wie Filter generiert, und Ihre

vorhandenen gespeicherten Filter können als Unterdrückungsregeln verwendet werden. Weitere Informationen zum Erstellen von Filtern finden Sie unter Filtern von Ergebnissen.

So erstellen Sie eine Unterdrückungsregel mithilfe der Konsole:

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie auf der Seite Erkenntnisse die Option „Erkenntnisse unterdrücken“, um das Fenster mit den Unterdrückungsregeln zu öffnen.
3. Um das Menü mit den Filterkriterien zu öffnen, geben Sie **`filter criteria`** in Filterkriterien hinzufügen ein. Sie können ein Kriterium aus der Liste auswählen. Geben Sie einen gültigen Wert für das gewählte Kriterium ein.

   > **Note**
   >
   > Um den gültigen Wert zu ermitteln, sehen Sie sich die Erkenntnistabelle an und wählen Sie eine Erkenntnis aus, die Sie unterdrücken möchten. Überprüfen Sie die Einzelheiten im Ergebnisfenster.

   Sie können mehrere Filterkriterien hinzufügen und sicherstellen, dass nur die Erkenntnisse in der Tabelle erscheinen, die Sie unterdrücken möchten.
4. Geben Sie einen Namen und eine Beschreibung für die Unterdrückungsregel ein. Gültige Zeichen sind alphanumerische Zeichen, Punkt (.), Bindestrich (-), Unterstrich (_) und Leerzeichen.
5. Wählen Sie Speichern.

Sie können auch eine Unterdrückungsregel aus einem vorhandenen gespeicherten Filter erstellen. Weitere Informationen zum Erstellen von Filtern finden Sie unter Filtern von Ergebnissen.

So erstellen Sie eine Unterdrückungsregel aus einem gespeicherten Filter:

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie auf der Seite Erkenntnisse die Option Erkenntnisse unterdrücken, um das Fenster mit den Unterdrückungsregeln zu öffnen.
3. Wählen Sie in der Dropdownliste Gespeicherte Regeln einen gespeicherten Filter aus.

4. Sie können auch neue Filterkriterien hinzufügen. Wenn Sie keine zusätzlichen Filterkriterien benötigen, überspringen Sie diesen Schritt.

   Um das Menü mit den Filterkriterien zu öffnen, geben Sie **`filter criteria`** in Filterkriterien hinzufügen ein. Sie können ein Kriterium aus der Liste auswählen. Geben Sie einen gültigen Wert für das gewählte Kriterium ein.

   > **Note**
   >
   > Um den gültigen Wert zu ermitteln, sehen Sie sich die Erkenntnistabelle an und wählen Sie eine Erkenntnis aus, die Sie unterdrücken möchten. Überprüfen Sie die Einzelheiten im Ergebnisfenster.

5. Geben Sie einen Namen und eine Beschreibung für die Unterdrückungsregel ein. Gültige Zeichen sind alphanumerische Zeichen, Punkt (.), Bindestrich (-), Unterstrich (_) und Leerzeichen.
6. Wählen Sie Speichern.

API/CLI

Um eine Unterdrückungsregel zu erstellen, verwenden SieAPI:

1. Sie können Unterdrückungsregeln über den erstellen CreateFilterAPI. Geben Sie dazu die Filterkriterien in einer JSON Datei an, die dem Format des unten beschriebenen Beispiels entspricht. Im folgenden Beispiel werden alle nicht archivierten Ergebnisse mit geringem Schweregrad unterdrückt, für die eine DNS Anfrage an die Domain test.example.com gestellt wurde. Bei Erkenntnissen mit mittlerem Schweregrad ist die Eingabeliste `["4", "5", "7"]`. Bei Erkenntnissen mit hohem Schweregrad ist die Eingabeliste `["6", "7", "8"]`. Sie können auch auf der Grundlage eines beliebigen Werts in der Liste filtern.

```
{
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
```

```
                "test.example.com"
            ]
        },
        "severity": {
            "Eq": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

Eine Liste der JSON Feldnamen und ihrer entsprechenden Konsolennamen finden Sie unter. Filterattribute

Verwenden Sie zum Testen Ihrer Filterkriterien dasselbe JSON Kriterium in der ListFindingsAPIund vergewissern Sie sich, dass die richtigen Ergebnisse ausgewählt wurden. AWS CLI Folgen Sie dem Beispiel, um Ihre Filterkriterien anhand Ihrer eigenen Datei detectorId und einer.json-Datei zu testen.

Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite „Einstellungen“ oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. Laden Sie Ihren Filter zur Verwendung als Unterdrückungsregel mit CreateFilterAPIoder hoch. Verwenden Sie dazu das AWS CLI folgende Beispiel mit Ihrer eigenen Melder-ID, einem Namen für die Unterdrückungsregel und einer.json-Datei.

   Um die `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite „Einstellungen“ oder führen Sie den ListDetectorsAPIaus.

```
aws guardduty create-filter --action ARCHIVE --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
 file://criteria.json
```

Sie können eine Liste Ihrer Filter programmgesteuert mit dem anzeigen. ListFilterAPI Sie können die Details eines einzelnen Filters anzeigen, indem Sie den Filternamen in das Feld eingeben. GetFilterAPI Aktualisieren Sie Filter mit dem UpdateFilteroder löschen Sie sie mit dem DeleteFilterAPI.

Löschen von Unterdrückungsregeln

Wählen Sie Ihre bevorzugte Zugriffsmethode, um eine Unterdrückungsregel für die GuardDuty Suche nach Typen zu löschen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie auf der Seite Erkenntnisse die Option Erkenntnisse unterdrücken, um das Fenster mit den Unterdrückungsregeln zu öffnen.
3. Wählen Sie in der Dropdownliste Gespeicherte Regeln einen gespeicherten Filter aus.
4. Klicken Sie auf Delete rule (Regel löschen).

API/CLI

Führen Sie das aus DeleteFilterAPI. Geben Sie den Filternamen und die zugehörige Melder-ID für die jeweilige Region an.

Alternativ können Sie das folgende AWS CLI Beispiel verwenden, indem Sie die Werte ersetzen, die wie folgt formatiert sind *red*:

```
aws guardduty delete-filter --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite Einstellungen oder führen Sie den ListDetectorsAPIaus.

Arbeiten mit vertrauenswürdigen IP- und Bedrohungslisten

Amazon GuardDuty überwacht die Sicherheit Ihrer AWS Umgebung, indem es VPC Flow Logs, AWS CloudTrail Event Logs und Logs analysiert und DNS verarbeitet. Sie können diesen Überwachungsumfang anpassen, indem Sie so konfigurieren GuardDuty , dass Warnmeldungen für vertrauenswürdige IP-Adressen IPs aus Ihren eigenen Listen für vertrauenswürdige IP-Adressen und Warnungen bei bekannten bösartigen Bedrohungen IPs aus Ihren eigenen Bedrohungslisten gestoppt werden.

Vertrauenswürdige IP-Adressen-Listen und Bedrohungslisten gelten nur für Datenverkehr, der an öffentlich routingfähige IP-Adressen geleitet wird. Die Auswirkungen einer Liste gelten für alle VPC Flow-Protokolle und CloudTrail Ergebnisse, gelten jedoch nicht für DNS Ergebnisse.

GuardDuty kann so konfiguriert werden, dass die folgenden Listentypen verwendet werden.

Liste vertrauenswürdiger IPs

Listen vertrauenswürdiger IP-Adressen bestehen aus IP-Adressen, denen Sie für die sichere Kommunikation mit Ihrer AWS Infrastruktur und Ihren Anwendungen vertraut haben. GuardDuty generiert kein VPC Datenflussprotokoll oder keine CloudTrail Ergebnisse für IP-Adressen auf vertrauenswürdigen IP-Listen. Sie können maximal 2000 IP-Adressen und CIDR Bereiche in eine einzige Liste vertrauenswürdiger IP-Adressen aufnehmen. Es kann immer nur eine Liste vertrauenswürdiger IPs pro AWS -Konto pro Region hochgeladen werden.

Liste der bedrohlichen IP-Adressen

Bedrohungslisten enthalten bekannte schädliche IP-Adressen. Diese Liste kann von Bedrohungsdaten von Drittanbietern stammen oder speziell für Ihr Unternehmen erstellt werden. Neben der Generierung von Ergebnissen aufgrund einer potenziell verdächtigen Aktivität werden GuardDuty auch Ergebnisse generiert, die auf diesen Bedrohungslisten basieren. Sie können maximal 250.000 IP-Adressen und CIDR Bereiche in eine einzige Bedrohungsliste aufnehmen. GuardDuty generiert nur Ergebnisse auf der Grundlage einer Aktivität, die IP-Adressen und CIDR Bereiche in Ihren Bedrohungslisten einbezieht. Die Ergebnisse werden nicht auf der Grundlage der Domainnamen generiert. Zu jedem Zeitpunkt können Sie AWS-Konto pro Region bis zu sechs hochgeladene Bedrohungslisten hochladen.

> **Note**
>
> Wenn Sie dieselbe IP-Adresse sowohl in eine Liste vertrauenswürdiger IP-Adressen als auch in eine Bedrohungsliste aufnehmen, wird sie zuerst von der Liste vertrauenswürdiger IP-Adressen verarbeitet und es wird keine Erkenntnis generiert.

In Umgebungen mit mehreren Konten können nur Benutzer mit GuardDuty Administratorkonten vertrauenswürdige IP-Adressen und Bedrohungslisten hinzufügen und verwalten. Listen vertrauenswürdiger IP-Adressen und Bedrohungslisten, die vom Administratorkonto hochgeladen werden, wirken sich negativ auf die GuardDuty Funktionalität der Mitgliedskonten aus. Mit anderen Worten: Bei Mitgliedskonten werden Ergebnisse auf der Grundlage von Aktivitäten GuardDuty generiert, bei denen es sich um bekannte bösartige IP-Adressen aus den Bedrohungslisten des Administratorkontos handelt, und es werden keine Ergebnisse generiert, die auf Aktivitäten basieren, die IP-Adressen aus den vertrauenswürdigen IP-Listen des Administratorkontos betreffen. Weitere Informationen finden Sie unter Verwaltung mehrerer Konten bei Amazon GuardDuty.

Listenformate

GuardDuty akzeptiert Listen in den folgenden Formaten.

Die maximale Größe der Datei, die die Liste zuverlässiger IPs oder die Bedrohungsliste hostet, ist 35 MB. In Ihren Listen für vertrauenswürdige IP-Adressen und Bedrohungslisten müssen IP-Adressen und CIDR Bereiche jeweils eine pro Zeile erscheinen. Es werden nur IPv4 Adressen akzeptiert.

- Klartext () TXT

  Dieses Format unterstützt sowohl CIDR Block- als auch einzelne IP-Adressen. Die folgende Beispielliste verwendet das Plaintext (TXT) -Format.

  ```
  192.0.2.0/24
  198.51.100.1
  203.0.113.1
  ```

- Strukturierter Ausdruck von Bedrohungsinformationen () STIX

  Dieses Format unterstützt sowohl CIDR Block- als auch einzelne IP-Adressen. In der folgenden Beispielliste wird das STIX Format verwendet.

  ```
  <?xml version="1.0" encoding="UTF-8"?>
  ```

```
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
```

```
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

- Öffnen Sie Threat Exchange (OTX) ™ CSV

  Dieses Format unterstützt sowohl CIDR Block- als auch einzelne IP-Adressen. In der folgenden Beispielliste wird das 0TX™ CSV Format verwendet.

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEye™ steht SIGHT für Threat Intelligence CSV

  Dieses Format unterstützt sowohl CIDR Block- als auch einzelne IP-Adressen. Die folgende Beispielliste verwendet ein `FireEye`™ CSV Format.

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp,
 subject, recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier,
 md5, sha1, sha256, description, fileType, packer, userAgent, registry,
 fileCompilationDateTime, filePath, asn, cidr, domain, domainTimeOfLookup,
 networkIdentifier, ip, port, protocol, registrantEmail, registrantName, networkType,
 url, malwareFamily, malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400
```

```
01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

- Proofpoint [TM] ET Intelligence Feed CSV

  Dieses Format unterstützt ausschließlich individuelle IP-Adressen. Die folgende Beispielliste verwendet das `Proofpoint` CSV Format. Der Parameter `ports` ist optional. Wenn Sie den Port überspringen, achten Sie darauf, am Ende ein Komma (,) zu hinterlassen.

  ```
  ip, category, score, first_seen, last_seen, ports (|)
  198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
  203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
  ```

- AlienVault[TM] Reputation Feed

  Dieses Format unterstützt ausschließlich individuelle IP-Adressen. Die folgende Beispielliste verwendet das `AlienVault`-Format.

  ```
  198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
  203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
  ```

Erforderliche Berechtigungen für das Hochladen von Listen mit vertrauenswürdigen IPs und Bedrohungslisten

Verschiedene IAM Identitäten erfordern spezielle Berechtigungen, um mit vertrauenswürdigen IP-Listen und Bedrohungslisten in GuardDuty arbeiten zu können. Eine Identität, der die verwaltete Richtlinie AmazonGuardDutyFullAccess angefügt ist, kann nur hochgeladene Listen mit vertrauenswürdigen IPs und Bedrohungslisten umbenennen und deaktivieren.

Um verschiedenen Identitäten vollen Zugriff auf die Arbeit mit vertrauenswürdigen IP-Listen und Bedrohungslisten zu erteilen (dies umfasst neben dem Umbenennen und Deaktivieren auch das Hinzufügen, Aktivieren, Löschen und Aktualisieren des Speicherorts oder der Namen der Listen), stellen Sie sicher, dass die folgenden Aktionen in der einem Benutzer, einer Gruppe oder einer Rolle zugewiesenen Berechtigungsrichtlinie vorhanden sind:

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> Diese Aktionen sind nicht in der verwalteten Richtlinie `AmazonGuardDutyFullAccess` enthalten.

Verwenden der serverseitigen Verschlüsselung für Listen vertrauenswürdiger IPs und Bedrohungslisten

GuardDuty unterstützt die folgenden Verschlüsselungstypen für Listen: SSE - AES256 und SSE - KMS. SSE-C wird nicht unterstützt. Weitere Informationen zu Verschlüsselungstypen für S3 finden Sie unter Schützen von Daten mit serverseitiger Verschlüsselung.

Wenn Ihre Liste serverseitig verschlüsselt ist, müssen SSE KMS Sie der GuardDuty dienstbezogenen Rolle die AWSServiceRoleForAmazonGuardDutyBerechtigung zum Entschlüsseln der Datei erteilen, um die Liste zu aktivieren. Fügen Sie der KMS Schlüsselrichtlinie die folgende Aussage hinzu und ersetzen Sie die Konto-ID durch Ihre eigene:

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
```

```
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

Hinzufügen und Aktivieren einer vertrauenswürdigen IP-Liste oder einer Bedrohungs-IP-Liste

Wählen Sie eine der folgenden Zugriffsmethoden, um eine vertrauenswürdige IP-Liste oder eine Bedrohungs-IP-Liste hinzuzufügen und zu aktivieren.

Console

(Optional) Schritt 1: Abrufen des Speicherorts URL Ihrer Liste

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie im Navigationsbereich die Option Buckets aus.
3. Wählen Sie den Amazon-S3-Bucket-Namen, der die spezifische Liste enthält, die Sie hinzufügen möchten.
4. Wählen Sie den Namen des Objekts (Liste), um dessen Details anzuzeigen.
5. Kopieren Sie auf der Registerkarte Eigenschaften das S3 URI für dieses Objekt.

Schritt 2: Hinzufügen einer Liste vertrauenswürdiger IP-Adressen oder einer Bedrohungsliste

> **Important**
>
> Es kann immer nur eine Liste vertrauenswürdiger IPs hochgeladen werden. In ähnlicher Weise können Sie bis zu sechs Bedrohungslisten haben.

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.
3. Klicken Sie auf der Seite List management auf Add a trusted IP list oder Add a threat list.
4. Je nach Ihrer Auswahl wird ein Dialogfeld angezeigt. Gehen Sie wie folgt vor:

    a. In Name der Liste geben Sie einen Namen für Ihre Liste ein.

Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

b. Geben Sie unter Standort den Ort an, an dem Sie Ihre Liste hochgeladen haben. Falls Sie den Standort noch nicht haben, finden Sie weitere Informationen unter Step 1: Fetching location URL of your list.

   Format des Standorts URL

   - https://s3.amazonaws.com/bucket.name/file.txt
   - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
   - http://bucket.s3.amazonaws.com/file.txt
   - http://bucket.s3-aws-region.amazonaws.com/file.txt
   - s3://bucket.name/file.txt

c. Aktivieren Sie das Kontrollkästchen I agree.

d. Wählen Sie Liste hinzufügen. Standardmäßig ist der Status der hinzugefügten Liste Inaktiv. Damit die Liste gültig ist, müssen Sie sie aktivieren.

Schritt 3: Hinzufügen einer Liste vertrauenswürdiger IP-Adressen oder einer Bedrohungsliste

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.
3. Wählen Sie auf der Seite Listenverwaltung die Liste aus, die Sie aktivieren möchten.
4. Wählen Sie Aktionen und dann Aktivieren. Die Aktivierung der Liste dauert bis zu 15 Minuten.

API/CLI

Für Listen vertrauenswürdiger IPs

- Führen Sie C ausreateIPSet. Stellen Sie sicher, dass Sie die `detectorId` des Mitgliedskontos angeben, für das Sie diese Liste vertrauenswürdiger IP-Adressen erstellen möchten.

  Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.

- Sie können dies auch tun, indem Sie den folgenden AWS Command Line Interface - Befehl ausführen und sicherstellen, dass Sie die `detector-id` durch die Detektor-ID des Mitgliedskontos ersetzen, für das Sie die Liste der vertrauenswürdigen IP-Adressen aktualisieren möchten.

```
aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --format Plaintext --location https://
s3.amazonaws.com/amzn-s3-demo-bucket2/DOC-EXAMPLE-SOURCE-FILE.format --
activate
```

Für Bedrohungslisten

- Lauf. CreateThreatIntelSet Stellen Sie sicher, dass Sie die `detectorId` des Mitgliedskontos angeben, für das Sie diese Bedrohungsliste erstellen möchten.
  - Alternativ können Sie dies tun, indem Sie den folgenden AWS Command Line Interface Befehl ausführen. Stellen Sie sicher, dass Sie die `detectorId` des Mitgliedskontos angeben, für das Sie eine Bedrohungsliste erstellen möchten.

```
aws guardduty create-threat-intel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
format Plaintext --location https://s3.amazonaws.com/amzn-s3-demo-bucket2/
DOC-EXAMPLE-SOURCE-FILE.format --activate
```

> **Note**
>
> Nachdem Sie eine IP-Liste aktiviert oder aktualisiert haben, GuardDuty kann es bis zu 15 Minuten dauern, bis die Liste synchronisiert ist.

Aktualisieren von Listen zuverlässiger IPs und Bedrohungslisten

Sie können den Namen einer Liste oder die IP-Adressen aktualisieren, die einer Liste hinzugefügt wurden, die bereits hinzugefügt und aktiviert wurde. Wenn Sie eine Liste aktualisieren, müssen Sie sie erneut aktivieren, GuardDuty um die neueste Version der Liste verwenden zu können.

Wählen Sie eine der Zugriffsmethoden, um eine vertrauenswürdige IP oder Bedrohungsliste zu aktualisieren.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.
3. Wählen Sie auf der Seite Listenverwaltung den Satz vertrauenswürdiger IP-Adressen oder eine Bedrohungsliste aus, die Sie aktualisieren möchten.
4. Wählen Sie Aktionen und anschließend Bearbeiten.
5. Aktualisieren Sie die Informationen im Dialogfeld Liste aktualisieren nach Bedarf.

   Einschränkungen bei der Benennung von Listen — Der Name Ihrer Liste kann Kleinbuchstaben, Großbuchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten.
6. Aktivieren Sie das Kontrollkästchen Ich stimme zu und wählen Sie dann Liste aktualisieren. Der Wert in der Spalte Status ändert sich auf Inaktiv.
7. Reaktivierung der aktualisierten Liste

   a. Wählen Sie auf der Seite Listenverwaltung die Liste aus, die Sie aktivieren möchten.

   b. Wählen Sie Aktionen und dann Aktivieren.

API/CLI

1. Führen Sie UpdateIPSet aus, um eine Liste vertrauenswürdiger IP-Adressen zu aktualisieren.
   - Sie können dies auch tun, indem Sie den folgenden AWS CLI -Befehl ausführen und sicherstellen, dass Sie die `detector-id` durch die Detektor-ID des Mitgliedskontos ersetzen, für das Sie die Liste der vertrauenswürdigen IP-Adressen aktualisieren möchten.

     ```
     aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
      --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
     activate
     ```
2. Führen Sie UpdateThreatIntelSet aus, um eine Bedrohungsliste zu aktualisieren
   - Sie können dies auch tun, indem Sie den folgenden AWS CLI -Befehl ausführen und sicherstellen, dass Sie die `detector-id` durch die Detektor-ID des Mitgliedskontos ersetzen, für das Sie die Bedrohungsliste aktualisieren möchten.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --activate
```

Deaktivieren oder Löschen einer vertrauenswürdigen IP- oder Bedrohungsliste

Wählen Sie eine der Zugriffsmethoden, um eine Liste vertrauenswürdiger IP-Adressen oder Bedrohungen zu löschen (mithilfe der KonsoleCLI) oder zu deaktivieren (mithilfe vonAPI/).

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Listen.
3. Wählen Sie auf der Seite Listenverwaltung die Liste aus, die Sie löschen möchten.
4. Wählen Sie Aktionen und anschließend Löschen.
5. Bestätigen Sie die Aktion und wählen Sie Löschen. Die spezifische Liste ist in der Tabelle nicht mehr verfügbar.

API/CLI

1. Für eine Liste vertrauenswürdiger IPs

   Führen Sie UpdateIPSet aus, um eine Liste vertrauenswürdiger IP-Adressen zu aktualisieren.

   - Sie können dies auch tun, indem Sie den folgenden AWS CLI -Befehl ausführen und sicherstellen, dass Sie die `detector-id` durch die Detektor-ID des Mitgliedskontos ersetzen, für das Sie die Liste der vertrauenswürdigen IP-Adressen aktualisieren möchten.

     Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite Einstellungen in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
no-activate
```

2. Für eine Bedrohungsliste

   Führen Sie UpdateThreatIntelSet aus, um eine Bedrohungsliste zu aktualisieren

   - Alternativ können Sie den folgenden AWS CLI -Befehl ausführen, um eine Liste vertrauenswürdiger IPs zu aktualisieren. Achten Sie dabei darauf, die `detector-id` durch die Detektor-ID des Mitgliedskontos zu ersetzen, für das Sie die Bedrohungsliste aktualisieren möchten.

     ```
     aws guardduty update-threatintel-set --detector-
     id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
     intel-set-id d4b94fc952d6912b8f3060768example --no-activate
     ```

Exportieren von Erkenntnissen

GuardDuty bewahrt die generierten Ergebnisse für einen Zeitraum von 90 Tagen auf. GuardDuty exportiert die aktiven Ergebnisse nach Amazon EventBridge (EventBridge). Sie können die generierten Ergebnisse optional in einen Amazon Simple Storage Service (Amazon S3) -Bucket exportieren. Auf diese Weise können Sie die historischen Daten potenziell verdächtiger Aktivitäten in Ihrem Konto nachverfolgen und beurteilen, ob die empfohlenen Abhilfemaßnahmen erfolgreich waren.

Alle neuen aktiven Ergebnisse, die GuardDuty generiert werden, werden innerhalb von etwa 5 Minuten nach der Generierung des Ergebnisses automatisch exportiert. Sie können festlegen, wie oft Aktualisierungen der aktiven Ergebnisse exportiert werden EventBridge. Die Häufigkeit, die Sie auswählen, gilt für den Export neuer Vorkommen vorhandener Ergebnisse in Ihren S3-Bucket (sofern konfiguriert) und Detective (falls integriert). EventBridge Informationen darüber, wie mehrere Vorkommen vorhandener Ergebnisse GuardDuty aggregiert werden, finden Sie unter. GuardDuty Aggregation finden

Wenn Sie Einstellungen für den Export von Ergebnissen in einen Amazon S3 S3-Bucket konfigurieren, GuardDuty verwendet AWS Key Management Service (AWS KMS), um die Ergebnisdaten in Ihrem S3-Bucket zu verschlüsseln. Dazu müssen Sie Ihrem S3-Bucket und dem

AWS KMS Schlüssel Berechtigungen hinzufügen, damit Sie diese für den Export der Ergebnisse in Ihrem Konto verwenden GuardDuty können.

Inhalt

Überlegungen

Bevor Sie mit den Voraussetzungen und Schritten für den Export von Ergebnissen fortfahren, sollten Sie die folgenden wichtigen Konzepte berücksichtigen:

- Die Exporteinstellungen sind regional — Sie müssen die Exportoptionen in jeder Region, die Sie verwenden, konfigurieren GuardDuty.
- Exportieren von Ergebnissen in Amazon S3 S3-Buckets in verschiedenen AWS-Regionen (regionsübergreifenden) — GuardDuty unterstützt die folgenden Exporteinstellungen:
  - Ihr Amazon S3 S3-Bucket oder Objekt und der AWS KMS Schlüssel müssen zu demselben gehören AWS-Region.
  - Für die in einer Handelsregion generierten Ergebnisse können Sie wählen, ob Sie diese Ergebnisse in einen S3-Bucket in einer beliebigen Handelsregion exportieren möchten. Sie können diese Ergebnisse jedoch nicht in einen S3-Bucket in einer Opt-in-Region exportieren.
  - Für die Ergebnisse, die in einer Opt-in-Region generiert wurden, können Sie wählen, ob Sie diese Ergebnisse in dieselbe Opt-in-Region exportieren möchten, in der sie generiert wurden, oder in eine beliebige kommerzielle Region. Sie können jedoch keine Ergebnisse aus einer Opt-in-Region in eine andere Opt-in-Region exportieren.
- Berechtigungen zum Exportieren von Ergebnissen — Um Einstellungen für den Export aktiver Ergebnisse zu konfigurieren, muss Ihr S3-Bucket über Berechtigungen verfügen, die das Hochladen von GuardDuty Objekten ermöglichen. Sie benötigen außerdem einen AWS KMS Schlüssel, mit dem Sie die Ergebnisse verschlüsseln GuardDuty können.
- Archivierte Ergebnisse werden nicht exportiert — Standardmäßig werden die archivierten Ergebnisse, einschließlich neuer Instanzen unterdrückter Ergebnisse, nicht exportiert.

Wenn ein GuardDuty Ergebnis als archiviert generiert wird, müssen Sie es entarchivieren. Dadurch wird der Suchstatus des Filters auf Aktiv geändert. GuardDuty exportiert die Aktualisierungen der vorhandenen, nicht archivierten Ergebnisse auf der Grundlage Ihrer KonfigurationSchritt 5 — Häufigkeit für den Export von Ergebnissen.

- GuardDuty Das Administratorkonto kann Ergebnisse exportieren, die in verknüpften Mitgliedskonten generiert wurden — Wenn Sie Exportergebnisse in einem Administratorkonto konfigurieren, werden alle Ergebnisse der zugehörigen Mitgliedskonten, die in derselben Region generiert wurden, auch an den Speicherort exportiert, den Sie für das Administratorkonto konfiguriert haben. Weitere Informationen finden Sie unter Die Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten verstehen.

Schritt 1 — Zum Exportieren der Ergebnisse sind Berechtigungen erforderlich

Wenn Sie Einstellungen für den Export von Ergebnissen konfigurieren, wählen Sie einen Amazon S3 S3-Bucket aus, in dem Sie die Ergebnisse und einen AWS KMS Schlüssel für die Datenverschlüsselung speichern können. Zusätzlich zu den Berechtigungen für GuardDuty Aktionen müssen Sie auch über Berechtigungen für die folgenden Aktionen verfügen, um die Einstellungen für den Export von Ergebnissen erfolgreich konfigurieren zu können:

- `s3:GetBucketLocation`
- `s3:PutObject`
- `s3:ListBucket`

Schritt 2 — Richtlinie an Ihren KMS Schlüssel anhängen

GuardDuty verschlüsselt die Ergebnisdaten in Ihrem Bucket mithilfe von. AWS Key Management Service Um die Einstellungen erfolgreich zu konfigurieren, müssen Sie zunächst die GuardDuty Erlaubnis zur Verwendung eines KMS Schlüssels erteilen. Sie können die Berechtigungen gewähren, indem Sie die Richtlinie an Ihren KMS Schlüssel anhängen.

Wenn Sie einen KMS Schlüssel von einem anderen Konto verwenden, müssen Sie die Schlüsselrichtlinie anwenden, indem Sie sich bei dem Konto anmelden AWS-Konto , dem der Schlüssel gehört. Wenn Sie die Einstellungen für den Export von Ergebnissen konfigurieren, benötigen Sie auch den Schlüssel ARN von dem Konto, dem der Schlüssel gehört.

Um die KMS Schlüsselrichtlinie für die Verschlüsselung Ihrer exportierten Ergebnisse GuardDuty zu ändern

1. Öffnen Sie die AWS KMS Konsole unter https://console.aws.amazon.com/kms.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie einen vorhandenen KMS Schlüssel aus oder führen Sie die Schritte zum Erstellen eines neuen Schlüssels im AWS Key Management Service Entwicklerhandbuch aus, mit dem Sie die exportierten Ergebnisse verschlüsseln werden.

   > **Note**
   >
   > Der AWS-Region Ihres KMS Schlüssels und des Amazon S3 S3-Buckets müssen identisch sein.

   Sie können dasselbe S3-Bucket- und KMS key pair verwenden, um die Ergebnisse aus jeder zutreffenden Region zu exportieren. Weitere Informationen finden Sie unter Informationen Überlegungen zum Exportieren von Ergebnissen zwischen Regionen.
4. Wählen Sie im Abschnitt Key policy (Schlüsselrichtlinie) die Option Edit (Bearbeiten) aus.

   Wenn Zur Richtlinienansicht wechseln angezeigt wird, wählen Sie diese aus, um die Schlüsselrichtlinie anzuzeigen, und klicken Sie dann auf Bearbeiten.
5. Kopieren Sie den folgenden Richtlinienblock in Ihre KMS Schlüsselrichtlinie, um die GuardDuty Erlaubnis zur Verwendung Ihres Schlüssels zu erteilen.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
```

```
        }
    }
}
```

6. Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte ersetzen, die wie folgt formatiert sind *red*im Richtlinienbeispiel:

   1. Ersetzen *KMS key ARN* mit dem Amazon-Ressourcennamen (ARN) des KMS Schlüssels. Informationen zum Auffinden des ARN Schlüssels finden Sie unter Finden der Schlüssel-ID und ARN im AWS Key Management Service Entwicklerhandbuch.
   2. Ersetzen *123456789012* mit der AWS-Konto ID, der das GuardDuty Konto gehört, das die Ergebnisse exportiert.
   3. Ersetzen *Region2* mit dem AWS-Region Ort, an dem die GuardDuty Ergebnisse generiert werden.
   4. Ersetzen *SourceDetectorID* mit dem GuardDuty Konto in `detectorID` der spezifischen Region, in der die Ergebnisse generiert wurden.

      Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite „Einstellungen“ oder führen Sie den aus ListDetectorsAPI.

   > **Note**
   >
   > Wenn Sie GuardDuty in einer Opt-in-Region verwenden, ersetzen Sie den Wert für den „Service“ durch den regionalen Endpunkt für diese Region. Wenn Sie beispielsweise GuardDuty in der Region Naher Osten (Bahrain) (me-south-1) verwenden, ersetzen Sie `"Service": "guardduty.amazonaws.com"` es durch. `"Service": "guardduty.me-south-1.amazonaws.com"` Informationen zu Endpunkten für jede Opt-in-Region finden Sie unter GuardDuty Endpunkte und Kontingente.

7. Wenn Sie die Richtlinienerklärung vor der endgültigen Erklärung hinzugefügt haben, fügen Sie vor dem Hinzufügen dieser Aussage ein Komma hinzu. Stellen Sie sicher, dass die JSON Syntax Ihrer KMS wichtigsten Richtlinie gültig ist.

   Wählen Sie Save (Speichern) aus.

8. (Optional) Kopieren Sie den Schlüssel ARN auf einen Notizblock, um ihn in den späteren Schritten zu verwenden.

Schritt 3 — Richtlinie an Amazon S3 S3-Bucket anhängen

Fügen Sie dem Amazon S3 S3-Bucket, in den Sie Ergebnisse exportieren, Berechtigungen hinzu, damit Sie Objekte in diesen S3-Bucket hochladen GuardDuty können. Unabhängig davon, ob Sie einen Amazon S3 S3-Bucket verwenden, der entweder zu Ihrem Konto oder zu einem anderen gehört AWS-Konto, müssen Sie diese Berechtigungen hinzufügen.

Wenn Sie zu irgendeinem Zeitpunkt entscheiden, Ergebnisse in einen anderen S3-Bucket zu exportieren, müssen Sie, um mit dem Export der Ergebnisse fortzufahren, Berechtigungen für diesen S3-Bucket hinzufügen und die Einstellungen für den Export der Ergebnisse erneut konfigurieren.

Wenn Sie noch keinen Amazon S3 S3-Bucket haben, in den Sie diese Ergebnisse exportieren möchten, finden Sie weitere Informationen unter Erstellen eines Buckets im Amazon S3 S3-Benutzerhandbuch.

So fügen Sie Ihrer S3-Bucket-Richtlinie Berechtigungen hinzu

1. Führen Sie die Schritte unter So erstellen oder bearbeiten Sie eine Bucket-Richtlinie im Amazon S3 S3-Benutzerhandbuch aus, bis die Seite Bucket-Richtlinie bearbeiten angezeigt wird.
2. Die Beispielrichtlinie zeigt, wie Sie die GuardDuty Erlaubnis zum Exportieren von Ergebnissen in Ihren Amazon S3 S3-Bucket erteilen. Wenn Sie den Pfad ändern, nachdem Sie Exportergebnisse konfiguriert haben, müssen Sie die Richtlinie ändern, um die Erlaubnis für den neuen Speicherort zu erteilen.

   Kopieren Sie die folgende Beispielrichtlinie und fügen Sie sie in den Bucket-Richtlinieneditor ein.

   Wenn Sie die Richtlinienerklärung vor der endgültigen Aussage hinzugefügt haben, fügen Sie vor dem Hinzufügen dieser Aussage ein Komma hinzu. Stellen Sie sicher, dass die JSON Syntax Ihrer KMS wichtigsten Richtlinie gültig ist.

   Beispiel für eine S3-Bucket-Richtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGuardDutygetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
```

```
            },
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": "Amazon S3 bucket ARN",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "AllowGuardDutyPutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "DenyUnencryptedUploadsThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
```

```
            }
        },
        {
            "Sid": "DenyIncorrectHeaderThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
                }
            }
        },
        {
            "Sid": "DenyNon-HTTPS",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

3. Bearbeiten Sie die Richtlinie, indem Sie die folgenden Werte ersetzen, die wie folgt formatiert sind *red*im Richtlinienbeispiel:

   1. Ersetzen *Amazon S3 bucket ARN* mit dem Amazon-Ressourcennamen (ARN) des Amazon S3-Buckets. Sie finden den Bucket ARN auf der Seite Bucket-Richtlinie bearbeiten in der https://console.aws.amazon.com/s3/Konsole.
   2. Ersetzen *123456789012* mit der AWS-Konto ID, der das GuardDuty Konto gehört, das die Ergebnisse exportiert.
   3. Ersetzen *Region2* mit dem AWS-Region Ort, an dem die GuardDuty Ergebnisse generiert werden.

4. Ersetzen *`SourceDetectorID`* mit dem GuardDuty Konto in `detectorID` der spezifischen Region, in der die Ergebnisse generiert wurden.

   Um das `detectorId` für Ihr Konto und Ihre aktuelle Region zu finden, gehen Sie in der https://console.aws.amazon.com/guardduty/Konsole auf die Seite „Einstellungen“ oder führen Sie den aus ListDetectorsAPI.

5. Ersetzen *`[optional prefix]`* Teil des *`S3 bucket ARN/[optional prefix]`* Platzhalterwert mit einem optionalen Ordnerspeicherort, in den Sie die Ergebnisse exportieren möchten. Weitere Informationen zur Verwendung von Präfixen finden Sie unter Objekte mithilfe von Präfixen organisieren im Amazon S3 S3-Benutzerhandbuch.

   Wenn Sie einen optionalen Ordnerspeicherort angeben, der noch nicht existiert, GuardDuty wird dieser Speicherort nur erstellt, wenn das mit dem S3-Bucket verknüpfte Konto mit dem Konto identisch ist, das die Ergebnisse exportiert. Wenn Sie Ergebnisse in einen S3-Bucket exportieren, der zu einem anderen Konto gehört, muss der Speicherort des Ordners bereits vorhanden sein.

6. Ersetzen *`KMS key ARN`* mit dem Amazon-Ressourcennamen (ARN) des KMS Schlüssels, der mit der Verschlüsselung der in den S3-Bucket exportierten Ergebnisse verknüpft ist. Informationen zum Auffinden des ARN Schlüssels finden Sie unter Finden der Schlüssel-ID und ARN im AWS Key Management Service Entwicklerhandbuch.

> **Note**
>
> Wenn Sie GuardDuty in einer Opt-in-Region verwenden, ersetzen Sie den Wert für den „Service“ durch den regionalen Endpunkt für diese Region. Wenn Sie beispielsweise GuardDuty in der Region Naher Osten (Bahrain) (me-south-1) verwenden, ersetzen Sie `"Service": "guardduty.amazonaws.com"` es durch. `"Service": "guardduty.me-south-1.amazonaws.com"` Informationen zu Endpunkten für jede Opt-in-Region finden Sie unter GuardDuty Endpunkte und Kontingente.

4. Wählen Sie Save (Speichern) aus.

Schritt 4 — Ergebnisse in einen S3-Bucket (Konsole) exportieren

GuardDuty ermöglicht es Ihnen, Ergebnisse in einen vorhandenen Bucket in einem anderen zu exportieren AWS-Konto.

Wenn Sie einen neuen S3-Bucket erstellen oder einen vorhandenen Bucket in Ihrem Konto auswählen, können Sie ein optionales Präfix hinzufügen. GuardDuty Erstellt bei der Konfiguration von Exportergebnissen einen neuen Ordner im S3-Bucket für Ihre Ergebnisse. Das Präfix wird an die von Ihnen GuardDuty erstellte Standardordnerstruktur angehängt. Zum Beispiel das Format des optionalen Präfixes`AWSLogs/`*`123456789012`*`/GuardDuty/`*`Region`*.

Der gesamte Pfad des S3-Objekts wird sein*`amzn-s3-demo-bucket`*`/`*`prefix-name`*`/UUID`*`.jsonl.gz`*. Das `UUID` wird zufällig generiert und stellt weder die Melder-ID noch die Befund-ID dar.

> **Important**
>
> Der KMS Schlüssel und der S3-Bucket müssen sich in derselben Region befinden.

Bevor Sie diese Schritte ausführen, stellen Sie sicher, dass Sie Ihrem KMS Schlüssel und dem vorhandenen S3-Bucket die entsprechenden Richtlinien angehängt haben.

Um Exportergebnisse zu konfigurieren

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie auf der Seite Einstellungen unter Exportoptionen für Ergebnisse für den S3-Bucket die Option Jetzt konfigurieren (oder je nach Bedarf Bearbeiten) aus.
4. Geben Sie für den S3-Bucket ARN den ein**`bucket ARN`**. Informationen zum Finden des Buckets ARN finden Sie unter Eigenschaften für einen S3-Bucket anzeigen im Amazon S3 S3-Benutzerhandbuch. Auf der Eigenschaftenseite des zugehörigen Buckets in der https://console.aws.amazon.com/guardduty/Konsole auf der Registerkarte „Berechtigungen“.
5. Geben Sie als KMSSchlüssel ARN den ein **`key ARN`**. Informationen zum Auffinden des ARN Schlüssels finden Sie unter Finden der Schlüssel-ID und ARN im AWS Key Management Service Entwicklerhandbuch.
6. Richtlinien anhängen
   - Führen Sie die Schritte aus, um die S3-Bucket-Richtlinie anzuhängen. Weitere Informationen finden Sie unter Schritt 3 — Richtlinie an Amazon S3 S3-Bucket anhängen.

- Führen Sie die Schritte aus, um die KMS Schlüsselrichtlinie anzuhängen. Weitere Informationen finden Sie unter Schritt 2 — Richtlinie an Ihren KMS Schlüssel anhängen.

7. Wählen Sie Save (Speichern) aus.

Schritt 5 — Einstellung der Häufigkeit für den Export aktualisierter aktiver Ergebnisse

Konfigurieren Sie die Häufigkeit für den Export aktualisierter aktiver Ergebnisse entsprechend Ihrer Umgebung. Standardmäßig werden aktualisierte Ergebnisse alle 6 Stunden exportiert. Dies bedeutet, dass alle Ergebnisse in den nächsten Export aufgenommen werden, die nach dem letzten Export aktualisiert wurden. Wenn aktualisierte Ergebnisse alle 6 Stunden exportiert werden und dieser Export um 12:00 Uhr erfolgt, wird jedes nach 12:00 Uhr aktualisierte Ergebnis um 18:00 Uhr exportiert.

So stellen Sie die Häufigkeit ein

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie im Bereich Exportoptionen für Erkenntnisse die Option Häufigkeit für aktualisierte Erkenntnisse aus. Dadurch wird die Häufigkeit für den Export aktualisierter Active-Ergebnisse EventBridge sowohl nach Amazon S3 als auch nach Amazon S3 festgelegt. Sie können aus den folgenden Optionen auswählen:
   - Update EventBridge und S3 alle 15 Minuten
   - Update EventBridge und S3 alle 1 Stunde
   - Update CWE und S3 alle 6 Stunden (Standard)
4. Wählen Sie Änderungen speichern.

Erstellen von benutzerdefinierten Antworten auf GuardDuty Erkenntnisse mit Amazon CloudWatch Events

GuardDuty erstellt ein Ereignis für Amazon CloudWatch Events, wenn eine Änderung der Ergebnisse stattfindet. Zu den Erkenntnissen, die ein CloudWatch Ereignis erstellen, gehören neu generierte

Erkenntnisse oder neu aggregierte Erkenntnisse. Ereignisse werden auf bestmögliche Weise ausgegeben.

Jedem GuardDuty Ergebnis wird eine Erkenntnis-ID zugewiesen. GuardDuty erstellt ein CloudWatch Ereignis für jedes Ergebnis mit einer eindeutigen Erkenntnis-ID. Jegliches nachfolgendes Vorkommen eines vorhandenen Ergebnisses wird zu den ursprünglichen Ergebnissen aggregiert. Weitere Informationen finden Sie unter GuardDuty Aggregation finden.

> **Note**
>
> Wenn Ihr Konto ein GuardDuty delegierter Administrator ist, werden die CloudWatch Ereignisse in Ihrem Konto sowie in dem Mitgliedskonto veröffentlicht, in dem die Erkenntnis generiert wurde.

Durch die Verwendung von CloudWatch Ereignissen mit können Sie Aufgaben automatisieren GuardDuty, um auf Sicherheitsprobleme zu reagieren, die durch GuardDuty Erkenntnisse aufgedeckt werden.

Um Benachrichtigungen über GuardDuty Erkenntnisse basierend auf CloudWatch Ereignissen zu erhalten, müssen Sie eine CloudWatch Ereignisregel und ein Ziel für erstellen GuardDuty. Diese Regel ermöglicht CloudWatch es , Benachrichtigungen für Erkenntnisse zu senden, die an das in der Regel angegebene Ziel GuardDuty generiert. Weitere Informationen finden Sie unter Erstellen einer CloudWatch Ereignisregel und eines Ziels für GuardDuty (CLI).

Themen

- CloudWatch Häufigkeit der Ereignisbenachrichtigung für GuardDuty
- CloudWatch Ereignisformat für GuardDuty
- Erstellen einer CloudWatch Ereignisregel, um Sie über GuardDuty Ergebnisse zu informieren (Konsole)
- Erstellen einer CloudWatch Ereignisregel und eines Ziels für GuardDuty (CLI)
- CloudWatch Ereignisse für Umgebungen mit GuardDuty mehreren Konten

CloudWatch Häufigkeit der Ereignisbenachrichtigung für GuardDuty

Benachrichtigungen für neu generierte Erkenntnisse mit einer eindeutigen Erkenntnis-ID

GuardDuty sendet innerhalb von 5 Minuten nach dem Ergebnis eine Benachrichtigung basierend auf seinem CloudWatch Ereignis. Dieses Ereignis (und diese Benachrichtigung) beinhalten auch alle nachfolgenden Vorkommen dieses Ergebnisses, die innerhalb der ersten 5 Minuten seit der Generierung dieses Ergebnisses mit einer eindeutigen ID stattfinden.

> **Note**
>
> Die Häufigkeit der Benachrichtigungen über neu erstellte Erkenntnisse beträgt standardmäßig 5 Minuten. Diese Frequenz kann nicht aktualisiert werden.

Benachrichtigungen für nachfolgende Erkenntnisse

Standardmäßig GuardDuty aggregiert für jede Erkenntnis mit einer eindeutigen Erkenntnis-ID alle nachfolgenden Vorkommen eines bestimmten Erkenntnistyps, die innerhalb der 6-Stunden-Intervalle stattfinden, in einem einzigen Ereignis. GuardDuty sendet dann basierend auf diesem Ereignis eine Benachrichtigung über diese nachfolgenden Vorkommen. Standardmäßig GuardDuty sendet für die nachfolgenden Vorkommen der vorhandenen Erkenntnisse alle 6 Stunden Benachrichtigungen basierend auf CloudWatch Ereignissen.

Nur ein Administratorkonto kann die Standardhäufigkeit der Benachrichtigungen anpassen, die über die nachfolgenden Erkenntnisereignisse an CloudWatch Ereignisse gesendet werden. Benutzer von Mitgliedskonten können diesen Häufigkeitswert nicht anpassen. Der vom Administratorkonto in seinem eigenen Konto festgelegte Häufigkeitswert wird der GuardDuty Funktionalität in allen seinen Mitgliedskonten auferlegt. Wenn ein Benutzer aus einem Administratorkonto diesen Häufigkeitswert auf 1 Stunde festlegt, haben alle Mitgliedskonten auch die Häufigkeit von 1 Stunde, mit der Benachrichtigungen über die nachfolgenden Erkenntnisereignisse empfangen werden. Weitere Informationen finden Sie unter Verwaltung mehrerer Konten bei Amazon GuardDuty.

> **Note**
>
> Als Administratorkonto können Sie die Standardhäufigkeit von Benachrichtigungen über die nachfolgenden Erkenntnisereignisse anpassen. Mögliche Werte sind 15 Minuten,

1 Stunde oder standardmäßig 6 Stunden. Weitere Informationen zum Einrichten der Häufigkeit für diese Benachrichtigungen finden Sie unter Schritt 5 — Einstellung der Häufigkeit für den Export aktualisierter aktiver Ergebnisse.

Überwachen archivierter GuardDuty Ergebnisse mit - CloudWatch Ereignissen

Für die manuell archivierten Erkenntnisse werden die ersten und alle nachfolgenden Vorkommen dieser Erkenntnisse (die nach Abschluss der Archivierung generiert wurden) mit der oben beschriebenen Häufigkeit an CloudWatch Ereignisse gesendet.

Bei den automatisch archivierten Erkenntnissen werden das anfängliche und alle nachfolgenden Vorkommen dieser Erkenntnisse (die nach Abschluss der Archivierung generiert wurden) nicht an CloudWatch Ereignisse gesendet.

CloudWatch Ereignisformat für GuardDuty

Das CloudWatch Ereignis für GuardDuty hat das folgende Format.

```
{
 "version": "0",
 "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
 "detail-type": "GuardDuty Finding",
 "source": "aws.guardduty",
 "account": "111122223333",
 "time": "1970-01-01T00:00:00Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

Note

Der Detailwert gibt die JSON-Details einer einzelnen Erkenntnis als Objekt zurück, im Gegensatz zum Wert „Erkenntnisse“, der mehrere Erkenntnisse innerhalb eines Arrays unterstützen kann.

Eine vollständige Liste aller Parameter in der `GUARDDUTY_FINDING_JSON_OBJECT` finden Sie unter GetFindings. Der `id`-Parameter, der in der `GUARDDUTY_FINDING_JSON_OBJECT` angezeigt wird, ist die zuvor beschriebene Ergebnis-ID.

Erstellen einer CloudWatch Ereignisregel, um Sie über GuardDuty Ergebnisse zu informieren (Konsole)

Sie können CloudWatch Ereignisse mit verwenden GuardDuty , um automatische Erkennungswarnungen einzurichten, indem Sie Erkenntnisereignisse an einen Messaging-Hub senden GuardDuty, um die Sichtbarkeit von GuardDuty Erkenntnissen zu erhöhen. In diesem Thema erfahren Sie, wie Sie Ergebniswarnungen an E-Mail, Slack oder Amazon Chime senden, indem Sie ein SNS-Thema einrichten und dieses Thema dann mit einer CloudWatch Ereignisregel für Ereignisse verbinden.

Einrichten eines Amazon-SNS-Themas und eines Endpunkts

Zu Beginn müssen Sie zunächst ein Thema in Amazon Simple Notification Service einrichten und einen Endpunkt hinzufügen. Weitere Informationen dazu erhalten Sie unter Erste Schritte im Entwicklerhandbuch für Amazon Simple Notification Service.

Dieses Verfahren legt fest, wohin Sie GuardDuty Erkenntnisdaten senden möchten. Das SNS-Thema kann während oder nach der Erstellung der Ereignisregel zu einer CloudWatch Ereignisereignisregel hinzugefügt werden.

Email setup

Erstellen eines SNS-Themas

1. Melden Sie sich bei der Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home an.
2. Wählen Sie im Navigationsbereich Topics (Themen) und dann Create Topic (Thema erstellen) aus.
3. Wählen Sie im Abschnitt Thema erstellen die Option Standard. Geben Sie einen Namen für das Thema ein (z. B. **`GuardDuty_to_Email`**). Weitere Angaben sind optional.
4. Wählen Sie Create Topic (Thema erstellen) aus. Die Themeneinzelheiten für Ihr neues Thema werden geöffnet.
5. Wählen Sie im Abschnitt „Subscriptions (Abonnements)“ die Option Create subscription (Abonnement erstellen) aus.

6. a. Wählen Sie im Menü Protocol (Protokoll) die Option Email (E-Mail) aus.

   b. Fügen Sie im Feld Endpoint (Endpunkt) die E-Mail-Adresse hinzu, an der Sie Benachrichtigungen erhalten möchten.

   > **Note**
   >
   > Sie werden aufgefordert, Ihr Abonnement über Ihren E-Mail-Client zu bestätigen, nachdem Sie es erstellt haben.

   c. Wählen Sie Abonnement erstellen.

7. Suchen Sie in Ihrem Posteingang nach einer Abonnementnachricht und wählen Sie Confirm Subscription (Abonnement bestätigen) aus.

Slack setup

Erstellen eines SNS-Themas

1. Melden Sie sich bei der Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home an.
2. Wählen Sie im Navigationsbereich Topics (Themen) und dann Create Topic (Thema erstellen) aus.
3. Wählen Sie im Abschnitt Thema erstellen die Option Standard. Geben Sie einen Namen für das Thema ein (z. B. **`GuardDuty_to_Slack`**). Weitere Angaben sind optional. Wählen Sie Thema erstellen, um den Vorgang abzuschließen.

Konfigurieren eines AWS Chatbot-Clients

1. Navigieren Sie zur AWS Chatbot-Konsole.
2. Wählen Sie im Bereich Konfigurierte Clients die Option Neuen Client konfigurieren.
3. Wählen Sie Slack und bestätigen Sie mit „Konfigurieren“.

> **Note**
>
> Bei der Auswahl von Slack müssen Sie die Zugriffsrechte für AWS Chatbot für Ihren Kanal bestätigen, indem Sie „Zulassen“ wählen.

4. Wählen Sie Neuen Kanal konfigurieren aus, um den Bereich mit den Konfigurationsdetails zu öffnen.

   a. Geben Sie einen Namen für den Kanal ein.

   b. Wählen Sie für den Slack-Kanal den Kanal, den Sie verwenden möchten. Um den privaten Slack-Kanal mit AWS Chatbot zu verwenden, wählen Sie „Privater Kanal“.

   c. Kopieren Sie in Slack die Kanal-ID des privaten Kanals, indem Sie mit der rechten Maustaste auf den Kanalnamen klicken und „Link kopieren“ wählen.

   d. Fügen Sie in der AWS-Verwaltungskonsole im AWS Chatbot-Fenster die ID, die Sie aus Slack kopiert haben, in das Feld Privatkanal-ID ein.

   e. Wählen Sie unter Berechtigungen, ob Sie eine IAM-Rolle mithilfe einer Vorlage erstellen möchten, falls Sie noch keine Rolle haben.

   f. Wählen Sie in Richtlinienvorlagen die Option „Benachrichtigungs-Berechtigungen“ aus. Dies ist die IAM-Richtlinienvorlage für AWS Chatbot. Es bietet die erforderlichen Lese- und Listenberechtigungen für CloudWatch Alarme, Ereignisse und Protokolle sowie für Amazon SNS-Themen.

   g. Wählen Sie die Region aus, in der Sie zuvor Ihr SNS-Thema erstellt haben, und wählen Sie dann das Amazon-SNS-Thema aus, das Sie erstellt haben, um Benachrichtigungen an den Slack-Kanal zu senden.

5. Wählen Sie Konfigurieren.

Chime setup

Erstellen eines SNS-Themas

1. Melden Sie sich bei der Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home an.
2. Wählen Sie im Navigationsbereich Topics (Themen) und dann Create Topic (Thema erstellen) aus.
3. Wählen Sie im Abschnitt Thema erstellen die Option Standard. Geben Sie einen Namen für das Thema ein (z. B. **`GuardDuty_to_Chime`**). Weitere Angaben sind optional. Wählen Sie Thema erstellen, um den Vorgang abzuschließen.

Konfigurieren eines AWS Chatbot-Clients

1. Navigieren Sie zur AWS Chatbot-Konsole.
2. Wählen Sie im Bereich Konfigurierte Clients die Option Neuen Client konfigurieren.
3. Wählen Sie „Chime“ und bestätigen Sie mit „Konfigurieren“.
4. Geben Sie im Bereich mit den Konfigurationsdetails einen Namen für den Kanal ein.
5. Öffnen Sie in Chime den gewünschten Chatraum
   a. Wählen Sie das Zahnradsymbol rechts oben und danach Manage webhooks and bots aus.
   b. Wählen Sie URL kopieren, um die Webhook-URL in Ihre Zwischenablage zu kopieren.
6. Fügen Sie in der AWS-Verwaltungskonsole im AWS Chatbot-Fenster die URL, die Sie kopiert haben, in das Feld Webhook-URL ein.
7. Wählen Sie unter Berechtigungen, ob Sie eine IAM-Rolle mithilfe einer Vorlage erstellen möchten, falls Sie noch keine Rolle haben.
8. Wählen Sie in Richtlinienvorlagen die Option „Benachrichtigungs-Berechtigungen“ aus. Dies ist die IAM-Richtlinienvorlage für AWS Chatbot. Es bietet die erforderlichen Lese- und Listenberechtigungen für CloudWatch Alarme, Ereignisse und Protokolle sowie für Amazon SNS-Themen.
9. Wählen Sie die Region aus, in der Sie zuvor Ihr SNS-Thema erstellt haben, und wählen Sie dann das Amazon-SNS-Thema aus, das Sie erstellt haben, um Benachrichtigungen an den Chime-Raum zu senden.
10. Wählen Sie Konfigurieren.

Einrichten eines CloudWatch Ereignisses für GuardDuty Ergebnisse

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Rules (Regeln) und dann Create Rule (Regel erstellen) aus.
3. Wählen Sie im Menü Servicename die Option ausGuardDuty.
4. Wählen Sie im Menü Ereignistyp die Option GuardDuty Suchen aus.
5. Wählen Sie neben Event Pattern Preview (Vorversion des Ereignismusters) die Option Edit (Bearbeiten) aus.
6. Fügen Sie den folgenden JSON-Code in die Event Pattern Preview (Vorversion des Ereignismusters) ein und wählen Sie Save (Speichern) aus

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
      5.8,
      5.9,
      6,
      6.0,
      6.1,
      6.2,
      6.3,
      6.4,
      6.5,
      6.6,
      6.7,
      6.8,
      6.9,
      7,
```

```
      7.0,
      7.1,
      7.2,
      7.3,
      7.4,
      7.5,
      7.6,
      7.7,
      7.8,
      7.9,
      8,
      8.0,
      8.1,
      8.2,
      8.3,
      8.4,
      8.5,
      8.6,
      8.7,
      8.8,
      8.9
    ]
  }
}
```

> **Note**
>
> Der obige Code warnt bei jedem Ergebnis der mittleren bis hohen Stufe.

7. Klicken Sie im Abschnitt Targets (Ziele) auf Add Target (Ziel hinzufügen).
8. Wählen Sie im Menü Select Targets (Ziele auswählen) die Option SNS Topic (SNS-Thema) aus.
9. Wählen Sie unter Select Topic (Thema auswählen) den Namen des SNS-Themas aus, das Sie in Schritt 1 erstellt haben.
10. Konfigurieren Sie die Eingabe für das Ereignis.

    - Wenn Sie Benachrichtigungen für Chime oder Slack einrichten, fahren Sie mit Schritt 11 fort, denn der Eingabetyp ist standardmäßig Abgestimmtes Ereignis.
    - Wenn Sie Benachrichtigungen für E-Mails über SNS einrichten, führen Sie die folgenden Schritte aus, um die an Ihren Posteingang gesendete Nachricht anzupassen:

a. Erweitern Sie Configure input (Eingabe konfigurieren) und wählen Sie dann Input Transformer (Eingabetransformer) aus.

b. Kopieren Sie den folgenden Code und fügen Sie ihn in das Feld Input Path (Eingabepfad) ein.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

c. Kopieren Sie den folgenden Code und fügen Sie ihn in das Feld Input Template (Eingabevorlage) ein, um die E-Mail zu formatieren.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. Klicken Sie auf Configure Details (Details konfigurieren).
12. Geben Sie auf der Seite Configure rule details (Regeldetails konfigurieren) einen Name (Name) und eine Description (Beschreibung) für die Regel ein und wählen Sie dann Create Rule (Regel erstellen) aus.

Erstellen einer CloudWatch Ereignisregel und eines Ziels für GuardDuty (CLI)

Das folgende Verfahren zeigt, wie Sie -AWS CLIBefehle verwenden, um eine CloudWatch Ereignisregel und ein Ziel für zu erstellen GuardDuty. Insbesondere zeigt Ihnen das Verfahren, wie

Sie eine Regel erstellen, die es ermöglicht, Ereignisse für alle Erkenntnisse CloudWatch zu senden, die GuardDuty generiert, und eine -AWS LambdaFunktion als Ziel für die Regel hinzuzufügen.

> **Note**
>
> Zusätzlich zu den Lambda-Funktionen GuardDuty und CloudWatch unterstützen die folgenden Zieltypen: Amazon EC2-Instances, Amazon Kinesis-Streams, Amazon-ECS-Aufgaben, AWS Step Functions Zustandsautomaten, den `-run`Befehl und integrierte Ziele.

Sie können auch eine CloudWatch Ereignisregel und ein Ziel für GuardDuty über die CloudWatch Ereigniskonsole erstellen. Weitere Informationen und detaillierte Schritte finden Sie unter Erstellen einer CloudWatch Ereignisregel, die bei einem Ereignis ausgelöst wird. Wählen Sie im Abschnitt Event Source **`GuardDuty`** für Service name und **`GuardDuty Finding`** für Event Type aus.

Erstellen von Regeln und Zielen

1. Führen Sie den folgenden CloudWatch CLI-Befehl aus, um eine Regel CloudWatch zu erstellen, die GuardDuty das Senden von Ereignissen für alle von generierten Erkenntnisse ermöglicht.

   ```
   AWS events put-rule --name Test --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   > **Important**
   >
   > Sie können Ihre Regel weiter anpassen, sodass sie anweist CloudWatch , Ereignisse nur für eine Teilmenge der von generierten Erkenntnisse GuardDutyzu senden. Diese Untergruppe basiert auf dem/den in der Regel angegebenen Ergebnisattribut(en). Verwenden Sie beispielsweise den folgenden CLI-Befehl, um eine Regel zu erstellen, die es ermöglicht CloudWatch , nur Ereignisse für die GuardDuty Ergebnisse mit dem Schweregrad 5 oder 8 zu senden:
   > `AWS events put-rule --name Test --event-pattern "{\"source\": [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"], \"detail\":{\"severity\":[5,8]}}"`
   > Zu diesem Zweck können Sie jeden der Eigenschaftswerte verwenden, die im JSON für GuardDuty Ergebnisse verfügbar sind.

2. Um eine Lambda-Funktion als Ziel für die Regel anzufügen, die Sie in Schritt 1 erstellt haben, führen Sie den folgenden CloudWatch CLI-Befehl aus.

   ```
   AWS events put-targets --rule Test --targets
   Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
   ```

   > **Note**
   >
   > Stellen Sie sicher, dass Sie <your_function> im obigen Befehl durch Ihre tatsächliche Lambda-Funktion für die GuardDuty Ereignisse ersetzen.

3. Führen Sie den folgenden Lambda-CLI-Befehl aus, um die erforderlichen Berechtigungen zum Aufrufen des Ziels hinzuzufügen.

   ```
   AWS lambda add-permission --function-name <your_function> --statement-
   id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
   ```

   > **Note**
   >
   > Stellen Sie sicher, dass Sie <your_function> im obigen Befehl durch Ihre tatsächliche Lambda-Funktion für die GuardDuty Ereignisse ersetzen.

   > **Note**
   >
   > Im obigen Verfahren verwenden wir eine Lambda-Funktion als Ziel für die Regel, die CloudWatch Ereignisse auslöst. Sie können auch andere AWS Ressourcen als Ziele konfigurieren, um CloudWatch Ereignisse auszulösen. Weitere Informationen finden Sie unter PutTargets.

CloudWatch Ereignisse für Umgebungen mit GuardDuty mehreren Konten

Als GuardDuty Administrator werden CloudWatch Ereignisregeln in Ihrem Konto basierend auf den entsprechenden Erkenntnissen aus Ihren Mitgliedskonten ausgelöst. Das bedeutet, dass Sie, wenn Sie über CloudWatch Ereignisse in Ihrem Administratorkonto, wie im vorherigen Abschnitt beschrieben, eine Benachrichtigung über Erkenntnisse mit hohem und mittlerem Schweregrad einrichten, die von Ihren Mitgliedskonten zusätzlich zu Ihren eigenen generiert werden.

Sie können das Mitgliedskonto, von dem die GuardDuty Erkenntnis stammt, mit dem `accountId` Feld der JSON-Details der Erkenntnis identifizieren.

Um mit dem Schreiben einer benutzerdefinierten Ereignisregel für ein bestimmtes Mitgliedskonto in Ihrer Umgebung in der Konsole zu beginnen, erstellen Sie eine neue Regel und fügen Sie die folgende Vorlage in die Ereignismustervorschau ein. Fügen Sie dabei die Konto-ID des Mitgliedskontos hinzu, das das Ereignis auslösen soll.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> Dieses Beispiel wird bei allen Erkenntnissen für die angegebene Konto-ID ausgelöst. Gemäß der JSON-Syntax können mehrere IDs hinzugefügt werden, die durch ein Komma getrennt sind.

Grundlegendes zu CloudWatch Protokollen und Gründen für das Überspringen von Ressourcen beim Scan von Malware Protection for EC2

GuardDuty Malware Protection for EC2 veröffentlicht Ereignisse in Ihrer CloudWatch Amazon-Protokollgruppe /aws/guardduty/ malware-scan-events. Für jedes Ereignis im Zusammenhang mit dem Malware-Scan können Sie den Status und das Scanergebnis Ihrer betroffenen Ressourcen

überwachen. Bestimmte Amazon EC2 EC2-Ressourcen und Amazon EBS-Volumes wurden möglicherweise während des Malware Protection for EC2-Scans übersprungen.

CloudWatch Protokolle in Malware Protection for EC2 GuardDuty prüfen

In der Protokollgruppe /aws/guardduty/ malware-scan-events CloudWatch werden drei Arten von Scanereignissen unterstützt.

Name des Scanereignisses „Malware-Schutz für EC2“	Erklärung
`EC2_SCAN_STARTED`	Wird erstellt, wenn ein GuardDuty Malware Protection for EC2 den Prozess des Malware-Scans einleitet, z. B. die Vorbereitung der Erstellung eines Snapshots eines EBS-Volumes.
`EC2_SCAN_COMPLETED`	Wird erstellt, wenn der GuardDuty Malware Protection for EC2-Scan für mindestens eines der EBS-Volumes der betroffenen Ressource abgeschlossen ist. Dieses Ereignis umfasst auch das `snapshotId` , das zum gescannten EBS-Volume gehört. Nach Abschluss des Scans lautet das Scanergebnis entweder `CLEAN`, `THREATS_FOUND` oder `NOT_SCANNED` .
`EC2_SCAN_SKIPPED`	Wird erstellt, wenn der GuardDuty Malware Protection for EC2-Scan alle EBS-Volumes der betroffenen Ressource überspringt. Um den Grund für das Überspringen zu ermitteln, wählen Sie das entsprechende Ereignis aus und sehen Sie sich die Details an. Weitere Informationen zu den Gründen für das Überspringen finden Sie unter Gründe für das Überspringen von Ressourcen beim Malware-Scan weiter unten.

> **Note**
>
> Wenn Sie eine verwenden AWS Organizations, werden CloudWatch Protokollereignisse von Mitgliedskonten in Organizations sowohl im Administratorkonto als auch in der Protokollgruppe des Mitgliedskontos veröffentlicht.

Wählen Sie Ihre bevorzugte Zugriffsmethode, um CloudWatch Ereignisse anzuzeigen und abzufragen.

Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Protokolle die Option Protokollgruppen. Wählen Sie die malware-scan-events Protokollgruppe /aws/guardduty/, um die Scanereignisse für Malware Protection for EC2 anzuzeigen. GuardDuty

   Um eine Abfrage auszuführen, wählen Sie Log Insights.

   Informationen zum Ausführen einer Abfrage finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights im CloudWatch Amazon-Benutzerhandbuch.
3. Wählen Sie Scan-ID, um die Details der betroffenen Ressourcen und Malware-Erkenntnisse zu überwachen. Sie können beispielsweise die folgende Abfrage ausführen, um die CloudWatch Protokollereignisse zu filtern, indem Sie`scanId`. Stellen Sie sicher, dass Sie Ihre eigene gültige *`Scan-ID`* verwenden.

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- Informationen zur Arbeit mit Protokollgruppen finden Sie unter Suchen nach Protokolleinträgen mithilfe von AWS CLI im CloudWatch Amazon-Benutzerhandbuch.

  Wählen Sie die malware-scan-events Protokollgruppe /aws/guardduty/, um die Scan-Ereignisse für Malware Protection for EC2 anzuzeigen. GuardDuty

- Informationen zum Anzeigen und Filtern von Protokollereignissen finden Sie unter GetLogEventsbzw. in der Amazon CloudWatch API-Referenz. FilterLogEvents

GuardDuty Malware-Schutz für die Aufbewahrung von EC2-Protokollen

Die Standarddauer für die Aufbewahrung von Protokollen für die Protokollgruppe /aws/guardduty/ beträgt 90 Tage. Danach werden die malware-scan-events Protokollereignisse automatisch gelöscht. Informationen zum Ändern der Protokollaufbewahrungsrichtlinie für Ihre CloudWatch Protokollgruppe finden Sie unter Ändern der Aufbewahrung von Protokolldaten in CloudWatch Logs im CloudWatch Amazon-Benutzerhandbuch oder PutRetentionPolicyin der CloudWatch Amazon-API-Referenz.

Gründe für das Überspringen von Ressourcen beim Malware-Scan

Bei Ereignissen im Zusammenhang mit dem Malware-Scan wurden möglicherweise bestimmte EC2-Ressourcen und EBS-Volumes während des Scanvorgangs übersprungen. In der folgenden Tabelle sind die Gründe aufgeführt, warum GuardDuty Malware Protection for EC2 die Ressourcen möglicherweise nicht scannt. Verwenden Sie gegebenenfalls die vorgeschlagenen Schritte, um diese Probleme zu beheben, und scannen Sie diese Ressourcen, wenn GuardDuty Malware Protection for EC2 das nächste Mal einen Malware-Scan initiiert. Die anderen Probleme dienen dazu, Sie über den Verlauf der Ereignisse zu informieren, und sind nicht umsetzbar.

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
`RESOURCE_NOT_FOUND`	Der `resourceArn` zur Initiierung des On-Demand-Malware-Scans bereitgestellte Schadsoftware-Scan wurde in Ihrer AWS Umgebung nicht gefunden.	Überprüfen Sie den `resourceArn` Ihres Amazon-EC 2-Instance- oder Container-Workloads und versuchen Sie es erneut.	
`ACCOUNT_INELIGIBLE`	Die AWS Konto-ID, von der aus Sie versucht haben, einen On-Demand-Malware-	Stellen Sie sicher, dass GuardDuty es für dieses AWS Konto aktiviert ist.	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
	Scan zu starten, wurde nicht aktiviert GuardDuty.	Wenn Sie ein neues Konto aktivieren GuardDuty AWS-Region , kann die Synchronisierung bis zu 20 Minuten dauern.	
`UNSUPPORTED_KEY_ENCRYPTION`	GuardDuty Malware Protection for EC2 unterstützt Volumes, die sowohl unverschlüsselt als auch mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind. Das Scannen von EBS-Volumes, die mit der Amazon-EBS-Verschlüsselung verschlüsselt wurden, wird nicht unterstützt. Derzeit gibt es einen regionalen Unterschied, bei dem dieser Grund für das Überspringen nicht zutrifft. Weitere Informationen zu diesen finden Sie AWS-Regionen unter Verfügbarkeit regionsspezifischer Feature.	Ersetzen Sie Ihren Verschlüsselungsschlüssel durch einen vom Kunden verwalteten Schlüssel. Weitere Informationen zu den GuardDuty unterstützten Verschlüsselungsarten finden Sie unter Unterstützte EBS Amazon-Volumes für Malware-Scans.	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
`EXCLUDED_BY_SCAN_SETTINGS`	Die EC2-Instance oder das EBS-Volume wurde beim Malware-Scan ausgeschlossen. Es gibt zwei Möglichkeiten: Entweder wurde das Tag zur Einschließen-Liste hinzugefügt, aber die Ressource ist nicht mit diesem Tag verknüpft, das Tag wurde der Ausschließen-Liste hinzugefügt und die Ressource ist mit diesem Tag verknüpft, oder das `GuardDuty Excluded` -Tag ist für diese Ressource auf `true` gesetzt.	Aktualisieren Sie Ihre Scan-Optionen oder die Ihrer Amazon-EC2-Ressource zugeordneten Tags. Weitere Informationen finden Sie unter Scan-Optionen mit benutzerdefinierten Tags.	
`UNSUPPORTED_VOLUME_SIZE`	Das Volumen ist größer als 2048 GB.	Nicht umsetzbar.	
`NO_VOLUMES_ATTACHED`	GuardDuty Malware Protection for EC2 hat die Instance in Ihrem Konto gefunden, aber es wurde kein EBS-Volume an diese Instance angehängt, um mit dem Scan fortzufahren.	Nicht umsetzbar.	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
UNABLE_TO_SCAN	Es ist ein interner Servicefehler.	Nicht umsetzbar.	
SNAPSHOT_NOT_FOUND	Die von den EBS-Volumes erstellten und mit dem Dienstkonto geteilten Snapshots wurden nicht gefunden, und GuardDuty Malware Protection for EC2 konnte den Scan nicht fortsetzen.	Stellen Sie sicher CloudTrail , dass die Snapshots nicht absichtlich entfernt wurden.	
SNAPSHOT_QUOTA_REACHED	Sie haben das maximale Volumen erreicht, das für Snapshots für jede Region zulässig ist. Dadurch wird verhindert, dass Snapshots nicht nur gespeichert, sondern auch neue erstellt werden.	Sie können entweder alte Snapshots entfernen oder eine Erhöhung des Kontingents beantragen. Das Standardlimit für Snapshots pro Region und wie Sie eine Erhöhung des Kontingents beantragen können, finden Sie unter Service Quotas im Allgemeinen Referenzhandbuch von AWS .	

Gründe für das Überspringen	Erklärung	Vorgeschlagene Schritte	
`MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED`	Mehr als 11 EBS-Volumes wurden an eine EC2-Instance angehängt. GuardDuty Malware Protection for EC2 scannte die ersten 11 EBS-Volumes, die durch alphabetische Sortierung ermittelt wurden. `deviceName`	Nicht umsetzbar.	
`UNSUPPORTED_PRODUCT_CODE_TYPE`	GuardDuty unterstützt das Scannen von Instances mit as nicht. `productCode marketplace` Weitere Informationen finden Sie unter Bezahlte AMIs im Amazon EC2 EC2-Benutzerhandbuch. Weitere Informationen zu `productCode` finden Sie unter ProductCode in der Amazon-EC2-API-Referenz.	Nicht umsetzbar.	

Falschmeldungen in GuardDuty Malware Protection for EC2 melden

GuardDuty Malware Protection for EC2-Scans können eine harmlose Datei in Ihrer Amazon EC2 EC2-Instance oder Ihrem Container-Workload als bösartig oder schädlich identifizieren. Um Ihre Erfahrung mit Malware Protection for EC2 und dem GuardDuty Service zu verbessern, können Sie falsch positive Ergebnisse melden, wenn Sie der Meinung sind, dass eine bei einem Scan als bösartig oder schädlich identifizierte Datei in Wirklichkeit keine Malware enthält.

Falsch positive Dateiübermittlung

1. Melden Sie sich in der https://console.aws.amazon.com/guardduty/-Konsole an.
2. Wenn Sie feststellen, dass es sich um ein scheinbar falsch positives Ergebnis handelt, wenden Sie sich an uns, AWS Support um den Prozess der Einreichung einer falsch positiven Datei einzuleiten.
3. Wählen Sie Malware-Scans.
4. Wählen Sie einen Scan aus, um die zugehörige Erkenntnis-ID anzuzeigen.
5. Geben Sie die Erkenntnis-ID ein. Sie müssen auch den SHA-256-Hashwert der Datei angeben. Dies ist erforderlich, um sicherzustellen, dass GuardDuty Malware Protection for EC2 die richtige Datei erhalten hat.
6. Das AWS Support Team stellt Ihnen eine Amazon Simple Storage Service (S3) -URL zur Verfügung, mit der Sie die Datei und den SHA-256-Hash hochladen können. Informieren Sie das AWS Support Team, nachdem Sie die Datei erfolgreich hochgeladen haben.

   > **Warning**
   >
   > Übergeben Sie die Datei oder den SHA-256-Hash nicht direkt an AWS Support. Sie sollten die Datei und den Hash nur über die angegebene URL auf Amazon S3 hochladen. Wenn Sie die Datei und den Hash nicht innerhalb von sieben Tagen nach Erhalt der URL hochladen, werden sie ungültig. Wenn die URL ungültig wird, müssen Sie sich an uns wenden, AWS Support um eine neue URL zu erhalten.

   GuardDuty bewahrt Ihre Datei nicht länger als 30 Tage auf. GuardDuty Die Teammitglieder werden Ihre Einreichung analysieren und geeignete Maßnahmen ergreifen, um Ihre Erfahrung mit Malware Protection for EC2 und dem GuardDuty Service zu verbessern.

Behebung von Sicherheitsproblemen, die entdeckt wurden von GuardDuty

Amazon GuardDuty generiert Ergebnisse, die auf potenzielle Sicherheitsprobleme hinweisen. In dieser Version von GuardDuty deuten die potenziellen Sicherheitsprobleme entweder auf eine gefährdete EC2 Instance- oder Container-Arbeitslast oder auf eine Reihe kompromittierter Anmeldeinformationen in Ihrer AWS Umgebung hin. In den folgenden Abschnitten werden die empfohlenen Schritte zur Behebung für alle Szenarien beschrieben. Falls es alternative Behebungsszenarien gibt, werden diese im Eintrag für diesen spezifischen Erkenntnistyp beschrieben. Sie können auf die vollständigen Informationen zu einem Erkenntnistyp zugreifen, indem Sie ihn aus der Tabelle für aktive Erkenntnistypen auswählen.

Inhalt

Behebung einer potenziell gefährdeten Amazon-Instance EC2

Folgen Sie diesen empfohlenen Schritten, um eine potenziell gefährdete EC2 Instance in Ihrer Umgebung zu reparieren: AWS

1. Identifizieren Sie die potenziell gefährdete Amazon-Instance EC2

   Untersuchen Sie die potenziell kompromittierte Instance auf Malware und entfernen Sie sämtliche gefundene Malware. Sie können Malware-Scan auf Abruf sie verwenden, um Malware in der

potenziell gefährdeten EC2 Instance zu identifizieren oder AWS Marketplacezu überprüfen, ob es hilfreiche Partnerprodukte zur Identifizierung und Entfernung von Malware gibt.

2. Isolieren Sie die potenziell gefährdete Amazon-Instance EC2

   Gehen Sie nach Möglichkeit wie folgt vor, um die potenziell gefährdete Instance zu isolieren:

   1. Erstellen Sie eine dedizierte Isolations-Sicherheitsgruppe. Eine isolierte Sicherheitsgruppe sollte nur eingehenden und ausgehenden Zugriff von bestimmten IP-Adressen aus haben. Stellen Sie sicher, dass es keine Regel für eingehenden oder ausgehenden Datenverkehr gibt, die Datenverkehr für zulässt. `0.0.0.0/0 (0-65535)`
   2. Ordnen Sie die Isolations-Sicherheitsgruppe dieser Instanz zu.
   3. Entfernen Sie alle Sicherheitsgruppenzuordnungen mit Ausnahme der neu erstellten Isolations-Sicherheitsgruppe aus der potenziell gefährdeten Instance.

   > **Note**
   >
   > Die bestehenden verfolgten Verbindungen werden nicht aufgrund wechselnder Sicherheitsgruppen beendet — nur future Datenverkehr wird von der neuen Sicherheitsgruppe effektiv blockiert.
   > Informationen zu verfolgten und nicht verfolgten Verbindungen finden Sie unter Amazon EC2 Security Group Connection Tracking im EC2Amazon-Benutzerhandbuch.
   > Informationen zum Blockieren weiteren Datenverkehrs von verdächtigen bestehenden Verbindungen finden Sie im Incident Response Playbook unter NACLsNetzwerkbasiert durchsetzen, IoCs um weiteren Datenverkehr zu verhindern.

3. Identifizieren Sie die Quelle der verdächtigen Aktivität.

   Wenn Malware erkannt wird, können Sie anhand der Art des Fundes in Ihrem Konto die potenziell unautorisierten Aktivitäten auf Ihrer EC2 Instance identifizieren und beenden. Dies kann Aktionen wie das Schließen aller offenen Ports, das Ändern von Zugriffsrichtlinien und das Aktualisieren von Anwendungen zur Behebung von Schwachstellen erfordern.

   Wenn Sie nicht in der Lage sind, unbefugte Aktivitäten auf Ihrer potenziell gefährdeten EC2 Instance zu identifizieren und zu stoppen, empfehlen wir Ihnen, die gefährdete EC2 Instance zu beenden und sie bei Bedarf durch eine neue Instance zu ersetzen. Im Folgenden finden Sie zusätzliche Ressourcen zum Schutz Ihrer EC2 Instances:

- Abschnitte zu Sicherheit und Netzwerk in Best Practices für Amazon EC2
- EC2Amazon-Sicherheitsgruppen für Linux-Instances und EC2Amazon-Sicherheitsgruppen für Windows-Instances
- Sicherheit bei Amazon EC2
- Tipps zur Sicherung Ihrer EC2 Instances (Linux).
- AWS Bewährte Sicherheitsmethoden
- Vorfälle in der Infrastrukturdomäne am AWS

4. Durchsuchen AWS re:Post

   AWS re:PostSuchen Sie nach weiterer Unterstützung.

5. Reichen Sie eine Anfrage für technischen Support ein

   Wenn Sie ein Premium-Support-Paket abonniert haben, können Sie eine Anfrage für den technischen Support senden.

Behebung eines potenziell gefährdeten S3-Buckets

Folgen Sie diesen empfohlenen Schritten, um einen potenziell gefährdeten Amazon S3 S3-Bucket in Ihrer AWS Umgebung zu beheben:

1. Identifizieren Sie die potenziell gefährdete S3-Ressource.

   Ein GuardDuty Ergebnis für S3 listet den zugehörigen S3-Bucket, seinen Amazon-Ressourcennamen (ARN) und seinen Besitzer in den Ergebnisdetails auf.

2. Identifizieren Sie die Quelle der verdächtigen Aktivität und den verwendeten API Anruf.

   Der verwendete API Anruf wird wie `API` in den Befunddetails aufgeführt. Bei der Quelle handelt es sich um einen IAM Principal (entweder eine IAM Rolle, ein Benutzer oder ein Konto), und identifizierende Details werden in den Ergebnissen aufgeführt. Je nach Quelltyp sind Informationen zur Remote-IP-Adresse oder zur Quelldomain verfügbar, anhand derer Sie beurteilen können, ob die Quelle autorisiert wurde. Wenn es sich bei der Suche um Anmeldeinformationen von einer EC2 Amazon-Instance handelte, sind die Details für diese Ressource ebenfalls enthalten.

3. Stellen Sie fest, ob die Anrufquelle autorisiert war, auf die identifizierte Ressource zuzugreifen.

   Denken Sie zum Beispiel an Folgendes:

- Wenn ein IAM Benutzer beteiligt war, ist es möglich, dass seine Anmeldeinformationen möglicherweise kompromittiert wurden? Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.
- Wenn ein von einem Prinzipal aufgerufen API wurde, der noch nie zuvor diesen Typ aufgerufen hatAPI, benötigt diese Quelle dann Zugriffsberechtigungen für diesen Vorgang? Können die Bucket-Berechtigungen weiter eingeschränkt werden?
- Wenn der Zugriff anhand des Benutzernamens `ANONYMOUS_PRINCIPAL` mit dem Benutzertyp `AWSAccount` erkannt wurde, bedeutet dies, dass der Bucket öffentlich ist und darauf zugegriffen wurde. Sollte dieser Bucket öffentlich sein? Falls nicht, finden Sie in den folgenden Sicherheitsempfehlungen alternative Lösungen für die gemeinsame Nutzung von S3-Ressourcen.
- Wenn der Zugriff ein erfolgreicher `PreflightRequest` Aufruf war, lässt sich anhand des Benutzernamens **`ANONYMOUS_PRINCIPAL`** mit dem Benutzertyp „`AWSAccount`Dies“ erkennen, dass für den Bucket eine ursprungsübergreifende Richtlinie für die gemeinsame Nutzung von Ressourcen (CORS) festgelegt wurde. Sollte dieser Bucket eine CORS Richtlinie haben? Falls nicht, stellen Sie sicher, dass der Bucket nicht versehentlich öffentlich ist, und finden Sie in den folgenden Sicherheitsempfehlungen alternative Lösungen für die gemeinsame Nutzung von S3-Ressourcen. Weitere Informationen zu Using Cross-Origin Resource Sharing (CORS) im S3-Benutzerhandbuch CORS finden Sie unter Using Cross-Origin Resource Sharing ().

4. Stellen Sie fest, ob der S3-Bucket sensible Daten enthält.

   Verwenden Sie Amazon Macie, um zu ermitteln, ob der S3-Bucket vertrauliche Daten wie personenbezogene Daten (PII), Finanzdaten oder Anmeldeinformationen enthält. Wenn die automatische Erkennung sensibler Daten für Ihr Macie-Konto aktiviert ist, überprüfen Sie die Details des S3-Buckets, um den Inhalt Ihres S3-Buckets besser zu verstehen. Wenn dieses Feature für Ihr Macie-Konto deaktiviert ist, empfehlen wir, es zu aktivieren, um Ihre Bewertung zu beschleunigen. Alternativ können Sie einen Discovery-Job für sensible Daten erstellen und ausführen, um die Objekte des S3-Buckets auf sensible Daten zu untersuchen. Weitere Informationen finden Sie unter Aufspüren sensibler Daten mit Macie.

Wenn der Zugriff autorisiert wurde, können Sie die Erkenntnis ignorieren. In der https://console.aws.amazon.com/guardduty/Konsole können Sie Regeln einrichten, um einzelne Ergebnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn Sie feststellen, dass Ihre S3-Daten offengelegt wurden oder von Unbefugten darauf zugegriffen wurde, lesen Sie sich die folgenden S3-Sicherheitsempfehlungen durch, um die Zugriffsrechte zu verschärfen und den Zugriff einzuschränken. Welche Lösungen für die Behebung geeignet sind, hängt von den Anforderungen Ihrer spezifischen Umgebung ab.

Empfehlungen, die auf spezifischen Zugriffsanforderungen für S3-Buckets basieren

Die folgende Liste enthält Empfehlungen, die auf spezifischen Zugriffsanforderungen für Amazon S3 S3-Buckets basieren:

- Um den öffentlichen Zugriff auf Ihre S3-Datennutzung zentral einzuschränken, blockiert S3 den öffentlichen Zugriff. Die Einstellungen zum Blockieren des öffentlichen Zugriffs können für Access Points, Buckets und AWS Konten über vier verschiedene Einstellungen aktiviert werden, um die Granularität des Zugriffs zu steuern. Weitere Informationen finden Sie unter Einstellungen von S3 Block Public Access.
- AWS Mithilfe von Zugriffsrichtlinien können Sie steuern, wie IAM Benutzer auf Ihre Ressourcen oder auf Ihre Buckets zugreifen können. Weitere Informationen dazu finden Sie unter Verwendung von Bucket-Richtlinien und Benutzerrichtlinien.

  Darüber hinaus können Sie Virtual Private Cloud (VPC) -Endpunkte mit S3-Bucket-Richtlinien verwenden, um den Zugriff auf bestimmte VPC Endpunkte zu beschränken. Weitere Informationen finden Sie unter Beispiel für Bucket-Richtlinien für VPC Endgeräte für Amazon S3.
- Um vertrauenswürdigen Entitäten außerhalb Ihres Kontos vorübergehend den Zugriff auf Ihre S3-Objekte zu gewähren, können Sie eine URL über S3 vorsignierte Version erstellen. Dieser Zugriff wird mit Ihren Konto-Anmeldeinformationen erstellt und kann je nach den verwendeten Anmeldeinformationen 6 Stunden bis 7 Tage dauern. Weitere Informationen finden Sie unter URLsMit S3 vorsignierte Generierung.
- Für Anwendungsfälle, die die gemeinsame Nutzung von S3-Objekten zwischen verschiedenen Quellen erfordern, können Sie S3-Zugangspunkte verwenden, um Berechtigungssätze zu erstellen, die den Zugriff nur auf diejenigen innerhalb Ihres privaten Netzwerks beschränken. Weitere Informationen finden Sie unter Verwalten des Datenzugriffs mit Amazon S3 Access Points.
- Um anderen AWS Konten sicheren Zugriff auf Ihre S3-Ressourcen zu gewähren, können Sie eine Zugriffskontrollliste (ACL) verwenden. Weitere Informationen finden Sie unter S3-Zugriff verwalten mit ACLs.

Weitere Informationen zu den S3-Sicherheitsoptionen finden Sie unter Bewährte Methoden für S3-Sicherheit.

Behebung eines potenziell bösartigen S3-Objekts

Wenn in Ihrem Ressourcentyp ein generiert Suchtyp „Malware-Schutz für S3“ wird AWS-Konto, handelt es sich bei dem potenziell schädlichen Ressourcentyp um ein S3Object.

Verwenden Sie die folgenden empfohlenen Schritte, um das generierte Ergebnis möglicherweise zu korrigieren:

1. Identifizieren Sie das potenziell schädliche S3-Objekt, indem Sie das mit dem Ergebnis ObjectDetails verknüpfte S3 überprüfen.
2. Isolieren Sie das betroffene S3-Objekt. Wenn Sie das Tagging zum Zeitpunkt der Aktivierung von Malware Protection for S3 für den zugehörigen Amazon S3 S3-Bucket aktiviert hatten, GuardDuty müssen Sie diesem Objekt das Tag bösartig zugewiesen haben. Verwenden Sie die Tag-basierte Zugriffskontrolle (TBAC), um den Zugriff auf dieses S3-Objekt einzuschränken. Weitere Informationen finden Sie unter Verwenden der tagbasierten Zugriffskontrolle () TBAC.

   Wenn Sie dieses Objekt nicht mehr benötigen, können Sie es alternativ auch löschen oder in einen isolierten S3-Bucket verschieben. Informationen zu Überlegungen beim Löschen eines S3-Objekts finden Sie unter Löschen von Objekten im Amazon S3 S3-Benutzerhandbuch.

Behebung eines potenziell gefährdeten Clusters ECS

Folgen Sie diesen empfohlenen Schritten, um einen potenziell gefährdeten ECS Amazon-Cluster in Ihrer AWS Umgebung zu beheben:

1. Identifizieren Sie den potenziell ECS gefährdeten Cluster.

   Der GuardDuty Malware-Schutz für die EC2 Suche nach ECS enthält die ECSClusterdetails im Detailbereich des Fundes.
2. Bewerten Sie die Quelle der Malware

   Prüfen Sie, ob sich die entdeckte Malware im Image des Containers befand. Wenn das Image Schadsoftware enthielt, identifizieren Sie alle anderen Aufgaben, die mit diesem Image ausgeführt werden. Informationen zum Ausführen von Aufgaben finden Sie unter ListTasks.
3. Isolieren Sie die potenziell betroffenen Aufgaben

Isolieren Sie die betroffenen Aufgaben, indem Sie den gesamten ein- und ausgehenden Datenverkehr zu der Aufgabe verweigern. Eine Regel zum Ablehnen jeglichen Datenverkehrs kann Ihnen dabei helfen, einen Angriff zu stoppen, der bereits im Gange ist, indem alle Verbindungen zu der Aufgabe unterbrochen werden.

Wenn der Zugriff autorisiert wurde, können Sie die Erkenntnis ignorieren. In der https://console.aws.amazon.com/guardduty/Konsole können Sie Regeln einrichten, mit denen einzelne Ergebnisse vollständig unterdrückt werden, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Behebung potenziell AWS kompromittierter Anmeldedaten

Folgen Sie diesen empfohlenen Schritten, um potenziell kompromittierte Anmeldeinformationen in Ihrer Umgebung zu beheben: AWS

1. Identifizieren Sie die potenziell gefährdete IAM Entität und den API verwendeten Anruf.

   Der verwendete API Anruf wird wie `API` in den Ergebnisdetails aufgeführt. Die IAM Entität (entweder eine IAM Rolle oder ein Benutzer) und ihre identifizierenden Informationen werden im Abschnitt Ressourcen der Ergebnisdetails aufgeführt. Der Typ der beteiligten IAM Entität kann im Feld Benutzertyp bestimmt werden. Der Name der IAM Entität wird im Feld Benutzername angezeigt. Der Typ der IAM Entität, die an der Suche beteiligt war, kann auch anhand der verwendeten Zugriffsschlüssel-ID bestimmt werden.

   Für Schlüssel, die mit `AKIA` beginnen:

   Bei diesem Schlüsseltyp handelt es sich um langfristige, vom Kunden verwaltete Anmeldeinformationen, die einem IAM Benutzer oder zugeordnet sind. Root-Benutzer des AWS-Kontos Informationen zur Verwaltung von Zugriffsschlüsseln für IAM Benutzer finden Sie unter Zugriffsschlüssel für IAM Benutzer verwalten.

   Für Schlüssel, die mit `ASIA` beginnen:

   Bei dieser Art von Schlüssel handelt es sich um kurzfristige temporäre Anmeldeinformationen, die von AWS Security Token Service generiert werden. Diese Schlüssel existieren nur für kurze Zeit und können in der AWS Management Console nicht angezeigt oder verwaltet werden. IAMRollen verwenden immer AWS STS Anmeldeinformationen, sie können aber auch für IAM Benutzer generiert werden. Weitere Informationen AWS STS finden Sie unter Temporäre IAM Sicherheitsanmeldeinformationen.

Wenn eine Rolle verwendet wurde, enthält das Feld Benutzername den Namen der verwendeten Rolle. Sie können feststellen, wie der Schlüssel angefordert wurde, AWS CloudTrail indem Sie das `sessionIssuer` Element des CloudTrail Protokolleintrags untersuchen. Weitere Informationen finden Sie unter IAMund AWS STS unter CloudTrail.

2. Überprüfen Sie die Berechtigungen für die IAM Entität.

   Öffnen Sie die IAM Konsole. Wählen Sie je nach Typ der verwendeten Entität die Registerkarte Benutzer oder Rollen und suchen Sie die betroffene Entität, indem Sie den identifizierten Namen in das Suchfeld eingeben. Überprüfen Sie über die Registerkarten Berechtigung und Access Advisor effektive Berechtigungen für diese Entität.

3. Stellen Sie fest, ob die Anmeldeinformationen der IAM Entität rechtmäßig verwendet wurden.

   Wenden Sie sich an den Benutzer der Anmeldeinformationen, um festzustellen, ob die Aktivität beabsichtigt war.

   Ermitteln Sie beispielsweise, ob der Benutzer die Anmeldeinformationen zu Folgendem verwendet hat:

   - Hat den API Vorgang aufgerufen, der im Ergebnis aufgeführt war GuardDuty
   - Der API Vorgang wurde zu dem Zeitpunkt aufgerufen, der im Ergebnis aufgeführt ist GuardDuty
   - Der API Vorgang wurde von der IP-Adresse aus aufgerufen, die im Ergebnis aufgeführt ist GuardDuty

Wenn es sich bei dieser Aktivität um eine legitime Verwendung der AWS Anmeldeinformationen handelt, können Sie den GuardDuty Befund ignorieren. In der https://console.aws.amazon.com/guardduty/Konsole können Sie Regeln einrichten, um einzelne Ergebnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Wenn Sie nicht bestätigen können, ob es sich bei dieser Aktivität um eine legitime Nutzung handelt, könnte dies das Ergebnis einer Kompromittierung eines bestimmten Zugriffsschlüssels sein — der Anmeldedaten des IAM Benutzers oder möglicherweise des gesamten AWS-Konto Schlüssels. Wenn Sie vermuten, dass Ihre Anmeldeinformationen kompromittiert wurden, lesen Sie die Informationen im Artikel Meine Daten sind AWS-Konto möglicherweise kompromittiert, um dieses Problem zu beheben.

Behebung eines potenziell gefährdeten Standalone-Containers

1. Isolieren Sie den potenziell gefährdeten Container

   Mithilfe der folgenden Schritte können Sie den potenziell schädlichen Container-Workload identifizieren:

   - Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
   - Wählen Sie auf der Ergebnisseite das entsprechende Ergebnis aus, um das Ergebnisfenster aufzurufen.
   - Im Erkenntnisfenster können Sie im Abschnitt Betroffene Ressource die ID und den Namen des Containers einsehen.

   Isolieren Sie diesen Container von anderen Container-Workloads.
2. Halten Sie den Container an

   Unterbrechen Sie alle Prozesse in Ihrem Container.

   Informationen zum Einfrieren Ihres Containers finden Sie unter Einen Container pausieren.

   Stoppen Sie den Container

   Wenn der obige Schritt fehlschlägt und der Container nicht angehalten wird, beenden Sie die Ausführung des Containers. Wenn Sie die Snapshot-Beibehaltung Funktion aktiviert haben, GuardDuty werden die Snapshots Ihrer EBS Volumes, die Malware enthalten, beibehalten.

   Informationen zum Stoppen des Containers finden Sie unter Stoppen eines Containers.
3. Prüfen Sie das Vorhandensein von Malware

   Prüfen Sie, ob sich die entdeckte Malware im Image des Containers befand.

Wenn der Zugriff autorisiert wurde, können Sie die Erkenntnis ignorieren. In der https://console.aws.amazon.com/guardduty/Konsole können Sie Regeln einrichten, um einzelne Ergebnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. In der GuardDuty Konsole können Sie Regeln einrichten, um einzelne Ergebnisse vollständig zu unterdrücken, sodass sie nicht mehr angezeigt werden. Weitere Informationen finden Sie unter Unterdrückungsregeln.

Behebung der Erkenntnisse von EKS Audit Log Monitoring

Amazon GuardDuty generiert Ergebnisse, die auf potenzielle Kubernetes-Sicherheitsprobleme hinweisen, wenn EKS Audit Log Monitoring für Ihr Konto aktiviert ist. Weitere Informationen finden Sie unter EKSÜberwachung des Auditprotokolls. In den folgenden Abschnitten werden die empfohlenen Schritte zur Behebung für alle Szenarien beschrieben. Spezifische Behebungsmaßnahmen werden im Eintrag für diesen spezifischen Erkenntnistyp beschrieben. Sie können auf die vollständigen Informationen zu einem Erkenntnistyp zugreifen, indem Sie ihn aus der Tabelle für aktive Erkenntnistypen auswählen.

Wenn einer der Erkennungstypen von EKS Audit Log Monitoring erwartungsgemäß generiert wurde, können Sie erwägen, Unterdrückungsregeln hinzuzufügen, um zukünftige Warnmeldungen zu verhindern.

Verschiedene Arten von Angriffen und Konfigurationsproblemen können GuardDuty Kubernetes-Erkenntnisse auslösen. Dieser Leitfaden hilft Ihnen dabei, die Ursachen für GuardDuty Erkenntnisse in Ihrem Cluster zu identifizieren und geeignete Anleitungen zur Behebung zu finden. Im Folgenden sind die Hauptursachen aufgeführt, die zu GuardDuty Kubernetes-Ergebnissen führen:

- Mögliche Konfigurationsprobleme
- Behebung potenziell kompromittierter Kubernetes-Benutzer
- Behebung potenziell kompromittierter Kubernetes-Pods
- Behebung potenziell kompromittierter Kubernetes-Knoten
- Behebung potenziell kompromittierter Container-Images

> **Note**
>
> Vor Kubernetes Version 1.14 war die `system:unauthenticated` Gruppe `system:basic-user` ClusterRoles standardmäßig `system:discovery` und zugeordnet. Dies könnte unbeabsichtigten Zugriff durch anonyme Benutzer ermöglichen. Durch Cluster-Updates werden diese Berechtigungen nicht aufgehoben. Das bedeutet, dass diese Berechtigungen auch dann noch gültig sind, wenn Sie Ihren Cluster auf Version 1.14 oder höher aktualisiert haben. Wir empfehlen, dass Sie die Zuordnung dieser Berechtigungen zu der `system:unauthenticated`-Gruppe aufheben.
> Weitere Informationen zum Entfernen dieser Berechtigungen finden Sie unter Bewährte Methoden für die Sicherheit in Amazon EKS im Amazon-EKS-Benutzerhandbuch.

Mögliche Konfigurationsprobleme

Wenn eine Erkenntnis auf ein Konfigurationsproblem hindeutet, finden Sie im Abschnitt zur Behebung dieses Fehlers Anleitungen zur Lösung dieses speziellen Problems. Weitere Informationen finden Sie unter den folgenden Erkenntnistypen, die auf Konfigurationsprobleme hinweisen:

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- Jede Erkenntnis, die auf endet SuccessfulAnonymousAccess

Behebung potenziell kompromittierter Kubernetes-Benutzer

Eine GuardDuty Erkenntnis kann auf einen kompromittierten Kubernetes-Benutzer hinweisen, wenn ein in der Erkenntnis identifizierter Benutzer eine unerwartete API-Aktion ausgeführt hat. Sie können den Benutzer im Bereich Kubernetes-Benutzerdetails im Erkenntnisfenster der Konsole oder in der `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` der JSON-Datei mit den Erkenntnissen identifizieren. Zu diesen Benutzerdetails gehören `user name`, `uid` und die Kubernetes-Gruppen, zu denen der Benutzer gehört.

Wenn der Benutzer mit einer IAM-Entität auf den Workload zugegriffen hat, können Sie den `Access Key details`-Abschnitt verwenden, um die Details einer IAM-Rolle oder eines IAM-Benutzers zu identifizieren. Sehen Sie sich die folgenden Benutzertypen und deren Anleitungen zur Problembehebung an.

> **Note**
>
> Sie können Amazon Detective verwenden, um die in der Erkenntnis identifizierte IAM-Rolle oder den IAM-Benutzer genauer zu untersuchen. Wählen Sie beim Anzeigen der Erkenntnisdetails in der GuardDuty Konsole Untersuchen in Detective aus. Wählen Sie dann AWS Benutzer oder Rolle aus den aufgelisteten Elementen aus, um sie in Detective zu untersuchen.

Integrierter Kubernetes-Admin – Der Standardbenutzer, der von Amazon EKS der IAM-Identität zugewiesen wurde, die den Cluster erstellt hat. Dieser Benutzertyp wird durch den Benutzernamen identifiziert `kubernetes-admin`.

Wie Sie einem integrierten Kubernetes-Administrator den Zugriff entziehen:

- Identifizieren Sie den `userType` aus dem `Access Key details`-Abschnitt.
  - Wenn der `userType` Rolle ist und die Rolle zu einer EC2-Instance-Rolle gehört:
    - Identifizieren Sie diese Instance und folgen Sie dann den Anweisungen unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.
  - Wenn es sich bei `userType` um einen Benutzer handelt oder um eine Rolle, die von einem Benutzer übernommen wurde:
    1. Rotieren Sie den Zugriffsschlüssel dieses Benutzers.
    2. Rotieren Sie alle Geheimnisse, auf die der Benutzer Zugriff hatte.
    3. Weitere Informationen finden Sie unter Mein AWS Konto ist möglicherweise kompromittiert.

OIDC-authentifizierter Benutzer – Ein Benutzer, dem der Zugriff über einen OIDC-Anbieter gewährt wurde. In der Regel hat ein OIDC-Benutzer eine E-Mail-Adresse als Benutzernamen. Sie können mit den folgenden Befehl überprüfen, ob Ihr Cluster OIDC verwendet: `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`*

Um einem OIDC-authentifizierten Benutzer den Zugriff zu entziehen:

1. Rotieren Sie die Anmeldeinformationen dieses Benutzers im OIDC-Anbieter.
2. Rotieren Sie alle Geheimnisse, auf die der Benutzer Zugriff hatte.

AWS-Auth ConfigMap -definierter Benutzer – Ein IAM-Benutzer, dem über eine AWS-Auth Zugriff gewährt wurde ConfigMap. Weitere Informationen finden Sie unter Verwalten von Benutzern oder IAM-Rollen für Ihren Cluster im EKS-Benutzerhandbuch. Sie können ihre Berechtigungen überprüfen, indem Sie den folgenden Befehl verwenden: `kubectl edit configmaps aws-auth --namespace kube-system`

So widerrufen Sie den Zugriff eines AWS ConfigMap-Benutzers:

1. Verwenden Sie den folgenden Befehl, um die zu öffnen ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifizieren Sie den Rollen- oder Benutzereintrag im Abschnitt mapRoles oder mapUsers mit demselben Benutzernamen wie dem im Abschnitt Kubernetes-Benutzerdetails Ihrer GuardDuty Erkenntnis gemeldeten. Sehen Sie sich das folgende Beispiel an, in dem der Admin-Benutzer in einer Erkenntnis identifiziert wurde.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. Entfernen Sie diesen Benutzer aus der ConfigMap. Sehen Sie sich das folgende Beispiel an, in dem der Admin-Benutzer entfernt wurde.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

4. Wenn es sich bei `userType` um einen Benutzer handelt oder um eine Rolle, die von einem Benutzer übernommen wurde:
   a. Rotieren Sie den Zugriffsschlüssel dieses Benutzers.
   b. Rotieren Sie alle Geheimnisse, auf die der Benutzer Zugriff hatte.
   c. Weitere Informationen finden Sie unter Mein AWS Konto ist möglicherweise kompromittiert.

Wenn die Erkenntnis keinen `resource.accessKeyDetails`-Abschnitt enthält, handelt es sich bei dem Benutzer um ein Kubernetes-Servicekonto.

Servicekonto – Das Servicekonto stellt eine Identität für Pods bereit und kann anhand eines Benutzernamens mit dem folgenden Format identifiziert werden: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Um den Zugriff auf ein Servicekonto zu widerrufen:

1. Rotieren Sie die Anmeldeinformationen für das Servicekonto.
2. Lesen Sie die Hinweise zur Pod-Kompromittierung im folgenden Abschnitt.

Behebung potenziell kompromittierter Kubernetes-Pods

Wenn Details zu einer Pod- oder Workload-Ressource innerhalb des `resource.kubernetesDetails.kubernetesWorkloadDetails` Abschnitts GuardDuty angibt, wurde diese Pod- oder Workload-Ressource möglicherweise kompromittiert. Eine GuardDuty Erkenntnis kann darauf hinweisen, dass ein einzelner Pod kompromittiert wurde oder dass mehrere Pods über eine übergeordnete Ressource kompromittiert wurden. In den folgenden Kompromissszenarien finden Sie Anleitungen zur Identifizierung des oder der Pods, die kompromittiert wurden.

Kompromittierung einzelner Pods

Wenn es sich bei dem `type`-Feld innerhalb des `resource.kubernetesDetails.kubernetesWorkloadDetails`-Abschnitts um Pods handelt, identifiziert die Erkenntnis einzelne Pods. Das Namensfeld ist der `name` der Pods und das `namespace`-Feld ist sein Namespace.

Informationen zum Identifizieren des Worker-Knotens, auf dem die Pods ausgeführt werden, finden Sie unter Identifizieren der angegriffenen Pods und Worker-Knoten.

Pods wurden über die Workload-Ressource kompromittiert

Wenn das `type`-Feld innerhalb des `resource.kubernetesDetails.kubernetesWorkloadDetails`-Abschnitts eine Workload-Ressource identifiziert, z. B. eine `Deployment`, ist es wahrscheinlich, dass alle Pods innerhalb dieser Workload-Ressource kompromittiert wurden.

Informationen zum Identifizieren aller Pods der Workload-Ressource und der Knoten, auf denen sie ausgeführt werden, finden Sie unter Identifizieren der angegriffenen Pods und Worker-Knoten mithilfe des Workload-Namens .

Pods wurden über das Servicekonto kompromittiert

Wenn eine GuardDuty Erkenntnis ein Servicekonto im `resource.kubernetesDetails.kubernetesUserDetails` Abschnitt identifiziert, ist es wahrscheinlich, dass Pods, die das identifizierte Servicekonto verwenden, kompromittiert werden. Der durch eine Erkenntnis gemeldete Benutzername ist ein Servicekonto, wenn er das folgende Format hat: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Informationen zum Identifizieren aller Pods mithilfe des Servicekontos und der Knoten, auf denen sie ausgeführt werden, finden Sie unter Identifizieren der fehlerhaften Pods und Worker-Knoten mithilfe des Servicekontonamens .

Nachdem Sie alle kompromittierten Pods und die Knoten identifiziert haben, auf denen sie ausgeführt werden, lesen Sie den Leitfaden für bewährte Methoden von Amazon EKS, um den Pod zu isolieren, seine Anmeldeinformationen zu rotieren und Daten für forensische Analysen zu sammeln.

So beheben Sie einen potenziell kompromittierten Pod:

1. Identifizieren Sie die Schwachstelle, durch die die Pods gefährdet wurden.
2. Implementieren Sie das Update für diese Schwachstelle und starten Sie neue Ersatz-Pods.
3. Löschen Sie die anfälligen Pods.

   Weitere Informationen finden Sie unter Kompromittierte Pod- oder Workload-Ressource erneut bereitstellen.

Wenn dem Worker-Knoten eine IAM-Rolle zugewiesen wurde, die es Pods ermöglicht, Zugriff auf andere AWS Ressourcen zu erhalten, entfernen Sie diese Rollen aus der Instance, um weitere Beschädigungen durch den Angriff zu verhindern. Wenn dem Pod eine IAM-Rolle zugewiesen wurde,

sollten Sie ebenfalls prüfen, ob Sie die IAM-Richtlinien sicher aus der Rolle entfernen können, ohne andere Workloads zu beeinträchtigen.

Behebung potenziell kompromittierter Container-Images

Wenn eine GuardDuty Erkenntnis auf eine Pod-Kompromittierung hinweist, kann das zum Starten des Pods verwendete Image potenziell bösartig oder kompromittiert sein. GuardDuty Erkenntnis identifizieren das Container-Image im `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` Feld . Sie können feststellen, ob das Image bösartig ist, indem Sie es auf Malware scannen.

So beheben Sie ein potenziell kompromittiertes Container-Image:

1. Beenden Sie sofort die Verwendung des Images und entfernen Sie es aus Ihrem Image-Repository.
2. Identifizieren Sie alle Pods, die das potenziell kompromittierte Image verwenden.

   Weitere Informationen finden Sie unter Identifizieren von Pods mit potenziell anfälligen oder kompromittierten Container-Images und Worker-Knoten.
3. Isolieren Sie die potenziell gefährdeten Pods, rotieren Sie die Anmeldeinformationen und sammeln Sie Daten für die Analyse. Weitere Informationen finden Sie im Leitfaden zu bewährten Methoden für Amazon EKS.
4. Löschen Sie alle Pods mit dem potenziell kompromittierten Image.

Behebung potenziell kompromittierter Kubernetes-Knoten

Eine GuardDuty Erkenntnis kann auf eine Knotenkompromittierung hinweisen, wenn der in der Erkenntnis identifizierte Benutzer eine Knotenidentität darstellt oder wenn die Erkenntnis die Verwendung eines privilegierten Containers anzeigt.

Die Benutzeridentität ist ein Worker-Knoten, wenn das Feld für den Benutzernamen das folgende Format hat: `system:node:node name`. Beispiel: `system:node:ip-192-168-3-201.ec2.internal` Dies weist darauf hin, dass der Angreifer Zugriff auf den Knoten erhalten hat und die Anmeldeinformationen des Knotens verwendet, um mit dem Kubernetes-API-Endpunkt zu kommunizieren.

Eine Erkenntnis weist auf die Verwendung eines privilegierten Containers hin, wenn für einen oder mehrere der in der Erkenntnis aufgelisteten Container das Erkenntnisfeld

`resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` auf `True` gesetzt ist.

So beheben Sie einen potenziell kompromittierten Knoten:

1. Isolieren Sie den Pod, rotieren Sie seine Anmeldeinformationen und sammeln Sie Daten für die forensische Analyse.

   Weitere Informationen finden Sie im Leitfaden zu bewährten Methoden für Amazon EKS.
2. Identifizieren Sie die Servicekonten, die von allen Pods verwendet werden, die auf dem potenziell kompromittierten Knoten ausgeführt werden. Überprüfen Sie ihre Berechtigungen und rotieren Sie die Servicekonten bei Bedarf.
3. Beenden Sie den potenziell kompromittierten Knoten.

Behebung der Ergebnisse von Runtime Monitoring

Wenn Sie Runtime Monitoring für Ihr Konto aktivieren, generiert Amazon GuardDuty möglicherweise InformationenRuntime Monitoring: Typen finden, die auf potenzielle Sicherheitsprobleme in Ihrer AWS Umgebung hinweisen. Die potenziellen Sicherheitsprobleme deuten entweder auf eine kompromittierte Amazon EC2 EC2-Instance, einen Container-Workload, einen Amazon EKS-Cluster oder eine Reihe kompromittierter Anmeldeinformationen in Ihrer Umgebung hin. AWS Der Security Agent überwacht Runtime-Ereignisse von mehreren Ressourcentypen aus. Um die potenziell gefährdete Ressource zu identifizieren, sehen Sie sich den Ressourcentyp in den generierten Suchdetails in der GuardDuty Konsole an. Im folgenden Abschnitt werden die empfohlenen Behebungsschritte für alle Szenarien beschrieben.

Instance

Wenn der Ressourcentyp in den Erkenntnisdetails Instance lautet, deutet dies darauf hin, dass entweder eine EC2-Instance oder ein EKS-Knoten potenziell kompromittiert ist.

- Informationen zur Behebung eines kompromittierten EKS-Knotens finden Sie unter Behebung potenziell kompromittierter Kubernetes-Knoten.
- Informationen zur Behebung einer kompromittierten EC2-Instance finden Sie unter Behebung einer potenziell gefährdeten Amazon-Instance EC2.

EKSCluster

Wenn der Ressourcentyp in den Erkenntnisdetails EKSCluster lautet, deutet dies darauf hin, dass entweder ein Pod oder ein Container in einem EKS-Cluster potenziell kompromittiert ist.

- Informationen zur Behebung eines kompromittierten Pods finden Sie unter Behebung potenziell kompromittierter Kubernetes-Pods.
- Informationen zur Behebung eines kompromittierten Container-Images finden Sie unter Behebung potenziell kompromittierter Container-Images.

ECSCluster

Wenn der Ressourcentyp in den Ergebnisdetails ecsCluster lautet, bedeutet dies, dass entweder eine ECS-Task oder ein Container innerhalb einer ECS-Task potenziell gefährdet ist.

1. Identifizieren Sie den betroffenen ECS-Cluster

   Das GuardDuty Runtime Monitoring-Ergebnis enthält die ECS-Cluster-Details im Detailbereich des Ergebnisses oder im `resource.ecsClusterDetails` Abschnitt in der Ergebnis-JSON.

2. Identifizieren Sie die betroffene ECS-Aufgabe

   Das GuardDuty Runtime Monitoring-Ergebnis enthält die ECS-Aufgabendetails im Detailbereich des Ergebnisses oder im `resource.ecsClusterDetails.taskDetails` Abschnitt in der Ergebnis-JSON.

3. Isolieren Sie die betroffene Aufgabe

   Isolieren Sie die betroffene Aufgabe, indem Sie den gesamten eingehenden und ausgehenden Datenverkehr für die Aufgabe verweigern. Eine Regel zum Verweigern des gesamten Datenverkehrs kann dazu beitragen, einen Angriff zu stoppen, der bereits im Gange ist, indem alle Verbindungen zu der Aufgabe unterbrochen werden.

4. Korrigieren Sie die gefährdete Aufgabe

   a. Identifizieren Sie die Sicherheitsanfälligkeit, die die Aufgabe gefährdet hat.

   b. Implementieren Sie das Update für diese Sicherheitsanfälligkeit und starten Sie eine neue Ersatzaufgabe.

   c. Beenden Sie die anfällige Aufgabe.

Container

Wenn der Ressourcentyp in den Erkenntnisdetails Container lautet, deutet dies darauf hin, dass ein alleinstehender Container potenziell kompromittiert ist.

- Informationen zur Problembehebung finden Sie unter Behebung eines potenziell gefährdeten Standalone-Containers.
- Falls die Erkenntnis für mehrere Container mit demselben Container-Image generiert wird, finden Sie weitere Informationen unter Behebung potenziell kompromittierter Container-Images.
- Wenn der Container auf den zugrunde liegenden EC2-Host zugegriffen hat, wurden die zugehörigen Instance-Anmeldeinformationen möglicherweise kompromittiert. Weitere Informationen finden Sie unter Behebung potenziell AWS kompromittierter Anmeldedaten.
- Wenn ein potenziell böswilliger Akteur auf den zugrunde liegenden EKS-Knoten oder eine EC2-Instance zugegriffen hat, finden Sie unter den Registerkarten EKSCluster und Instance die empfohlenen Abhilfemaßnahmen.

Behebung kompromittierter Container-Images

Wenn ein GuardDuty Ergebnis darauf hindeutet, dass die Aufgabe kompromittiert wurde, könnte das zum Starten der Aufgabe verwendete Image bösartig oder beschädigt sein. GuardDuty Die Ergebnisse identifizieren das Container-Image innerhalb des `resource.ecsClusterDetails.taskDetails.containers.image` Felds. Sie können feststellen, ob das Bild bösartig ist, indem Sie es auf Malware scannen.

Um ein kompromittiertes Container-Image zu korrigieren

1. Beenden Sie sofort die Verwendung des Images und entfernen Sie es aus Ihrem Image-Repository.
2. Identifizieren Sie alle Aufgaben, die dieses Image verwenden.
3. Beenden Sie alle Aufgaben, die das kompromittierte Image verwenden. Aktualisieren Sie ihre Aufgabendefinitionen, sodass sie das kompromittierte Image nicht mehr verwenden.

Behebung einer potenziell kompromittierten Datenbank

GuardDuty generiert Erkenntnistypen für RDS Protection, die auf potenziell verdächtiges und anomales Anmeldeverhalten in Ihrem hinweisen, Unterstützte Datenbanken nachdem Sie

aktiviert habenRDSSchutz. Mithilfe der RDS-Anmeldeaktivität GuardDuty analysiert und profiliert Bedrohungen, indem ungewöhnliche Muster bei Anmeldeversuchen identifiziert werden.

> **Note**
>
> Sie können auf die vollständigen Informationen zu einem Erkenntnistyp zugreifen, indem Sie ihn aus der Tabelle mit den Erkenntnissen auswählen.

Befolgen Sie diese empfohlenen Schritte, um eine potenziell kompromittierte Amazon-Aurora-Datenbank in Ihrer AWS Umgebung zu beheben.

Themen

- Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen
- Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen
- Behebung potenziell kompromittierter Anmeldeinformationen
- Einschränken von Netzwerkzugriff

Behebung einer potenziell gefährdeten Datenbank mit erfolgreichen Anmeldeereignissen

Die folgenden empfohlenen Schritte können Ihnen helfen, eine potenziell gefährdete Aurora-Datenbank zu beheben, die im Zusammenhang mit erfolgreichen Anmeldeereignissen ungewöhnliches Verhalten zeigt.

1. Identifizieren Sie die betroffene Datenbank und den betroffenen Benutzer.

   Die generierte GuardDuty Erkenntnis enthält den Namen der betroffenen Datenbank und die entsprechenden Benutzerdetails. Weitere Informationen finden Sie unter Erkenntnisdetails.

2. Bestätigen Sie, ob dieses Verhalten erwartet oder unerwartet ist.

   In der folgenden Liste sind mögliche Szenarien aufgeführt, die dazu geführt GuardDuty haben könnten, dass ein Ergebnis generiert hat:

   - Ein Benutzer, der sich nach Ablauf einer langen Zeit bei seiner Datenbank anmeldet.
   - Ein Benutzer, der sich gelegentlich bei seiner Datenbank anmeldet, z. B. ein Finanzanalyst, der sich vierteljährlich anmeldet.

- Ein potenziell verdächtiger Akteur, der an einem erfolgreichen Anmeldeversuch beteiligt ist, gefährdet möglicherweise die Datenbank.

3. Beginnen Sie mit diesem Schritt, wenn das Verhalten unerwartet ist.

   1. Beschränken Sie den Datenbankzugriff

      Beschränken Sie den Datenbankzugriff für die verdächtigen Konten und die Quelle dieser Anmeldeaktivität. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Anmeldeinformationen und Einschränken von Netzwerkzugriff.

   2. Beurteilen Sie die Auswirkungen und stellen Sie fest, auf welche Informationen zugegriffen wurde.

      - Falls verfügbar, überprüfen Sie die Prüfungsprotokolle, um festzustellen, auf welche Informationen möglicherweise zugegriffen wurde. Weitere Informationen finden Sie unter Überwachung von Ereignissen, Protokollen und Streams in einem Amazon-Aurora-DB-Cluster im Amazon-Aurora-Benutzerhandbuch.
      - Stellen Sie fest, ob auf vertrauliche oder geschützte Informationen zugegriffen oder diese geändert wurden.

Behebung einer potenziell gefährdeten Datenbank mit erfolglosen Anmeldeereignissen

Die folgenden empfohlenen Schritte können Ihnen helfen, eine potenziell gefährdete Aurora-Datenbank zu beheben, die im Zusammenhang mit erfolglosen Anmeldeereignissen ungewöhnliches Verhalten zeigt.

1. Identifizieren Sie die betroffene Datenbank und den betroffenen Benutzer.

   Die generierte GuardDuty Erkenntnis enthält den Namen der betroffenen Datenbank und die entsprechenden Benutzerdetails. Weitere Informationen finden Sie unter Erkenntnisdetails.

2. Identifizieren Sie die Quelle der fehlgeschlagenen Anmeldeversuche.

   Die generierte GuardDuty Erkenntnis stellt die IP-Adresse und die ASN-Organisation (falls es sich um eine öffentliche Verbindung handelte) im Abschnitt Akteur des Erkenntnisbereichs bereit.

   Ein Autonomes System (AS) ist eine Gruppe von einem oder mehreren IP-Präfixen (Listen von IP-Adressen, auf die in einem Netzwerk zugegriffen werden kann), die von einem oder mehreren Netzwerkbetreibern betrieben werden und eine einzige, klar definierte Routing-Richtlinie

einhalten. Netzbetreiber benötigen autonome Systemnummern (ASNs), um das Routing in ihren Netzwerken zu kontrollieren und Routing-Informationen mit anderen Internetdienstanbietern (ISPs) auszutauschen.

3. Bestätigen Sie, dass dieses Verhalten unerwartet ist.

   Prüfen Sie wie folgt, ob diese Aktivität einen Versuch darstellt, zusätzlichen unbefugten Zugriff auf die Datenbank zu erlangen:

   - Wenn es sich um eine interne Quelle handelt, überprüfen Sie, ob eine Anwendung falsch konfiguriert ist, und wiederholt versucht, eine Verbindung herzustellen.
   - Handelt es sich um einen externen Akteur, prüfen Sie, ob die entsprechende Datenbank öffentlich zugänglich ist oder ob sie falsch konfiguriert ist, sodass potenzielle böswillige Akteure gängige Benutzernamen mit Brute-Force-Angriffen verwenden können.

4. Beginnen Sie mit diesem Schritt, wenn das Verhalten unerwartet ist.

   1. Beschränken Sie den Datenbankzugriff

      Beschränken Sie den Datenbankzugriff für die verdächtigen Konten und die Quelle dieser Anmeldeaktivität. Weitere Informationen finden Sie unter Behebung potenziell kompromittierter Anmeldeinformationen und Einschränken von Netzwerkzugriff.

   2. Führen Sie eine Ursachenanalyse durch und ermitteln Sie die Schritte, die möglicherweise zu dieser Aktivität geführt haben.

      Richten Sie eine Warnung ein, um benachrichtigt zu werden, wenn eine Aktivität eine Netzwerkrichtlinie ändert und zu einem unsicheren Zustand führt. Weitere Informationen finden Sie unter Firewall-Richtlinien in AWS Network Firewall im Entwicklerhandbuch fürAWS Network Firewall .

Behebung potenziell kompromittierter Anmeldeinformationen

Eine GuardDuty Erkenntnis kann darauf hinweisen, dass die Benutzeranmeldeinformationen für eine betroffene Datenbank kompromittiert wurden, wenn der in der Erkenntnis identifizierte Benutzer einen unerwarteten Datenbankvorgang ausgeführt hat. Sie können den Benutzer im Bereich RDS-DB-Benutzerdetails im Suchfenster der Konsole oder in der `resource.rdsDbUserDetails` der JSON-Datei mit den Erkenntnissen identifizieren. Zu diesen Benutzerdetails gehören der Benutzername, die verwendete Anwendung, die abgerufene Datenbank, die SSL-Version und die Authentifizierungsmethode.

- Informationen zum Widerrufen des Zugriffs oder zum Wechseln von Passwörtern für bestimmte Benutzer, die an der Erkenntnis beteiligt sind, finden Sie unter Sicherheit mit Amazon Aurora MySQL oder Sicherheit mit Amazon Aurora PostgreSQL im Amazon-Aurora-Benutzerhandbuch.
- Verwenden Sie AWS Secrets Manager , um die Secrets für Amazon Relational Database Service (RDS)-Datenbanken sicher zu speichern und automatisch zu rotieren. Weitere Informationen finden Sie unter AWS Secrets Manager -Konzepte im AWS Secrets Manager -Benutzerhandbuch.
- Verwenden Sie die IAM-Datenbankauthentifizierung, um den Zugriff von Datenbankbenutzern zu verwalten, ohne dass Passwörter erforderlich sind. Weitere Informationen finden Sie unter IAM-Datenbank-Authentifizierung im Amazon Aurora-Benutzerhandbuch.

  Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden für Amazon Relational Database Service im Amazon-RDS-Benutzerhandbuch.

Einschränken von Netzwerkzugriff

Eine GuardDuty Erkenntnis kann darauf hinweisen, dass über Ihre Anwendungen oder Virtual Private Cloud (VPC) hinaus auf eine Datenbank zugegriffen werden kann. Wenn es sich bei der Remote-IP-Adresse in der Erkenntnis um eine unerwartete Verbindungsquelle handelt, überprüfen Sie die Sicherheitsgruppen. Eine Liste der an die Datenbank angehängten Sicherheitsgruppen ist in der Konsole https://console.aws.amazon.com/rds/ unter Sicherheitsgruppen oder in der `resource.rdsDbInstanceDetails.dbSecurityGroups` JSON-Datei der Erkenntnisse verfügbar. Weitere Informationen zur Konfiguration von Sicherheitsgruppen finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen im Amazon-RDS-Benutzerhandbuch.

Wenn Sie eine Firewall verwenden, schränken Sie den Netzwerkzugriff auf die Datenbank ein, indem Sie die Network Access Control Lists (NACLs) neu konfigurieren. Weitere Informationen finden Sie unter Firewall-Richtlinien in AWS Network Firewall im Entwicklerhandbuch fürAWS Network Firewall .

Behebung einer potenziell gefährdeten Lambda-Funktion

Wenn ein Lambda-Protection-Ergebnis GuardDuty generiert wird und die Aktivität unerwartet ist, ist Ihre Lambda-Funktion möglicherweise beeinträchtigt. Wir empfehlen, die folgenden Schritte auszuführen, um eine kompromittierte Lambda-Funktion zu beheben.

So beheben Sie Erkenntnisse von Lambda Protection

1. Identifizieren Sie die potenziell gefährdete Lambda-Funktionsversion.

Ein GuardDuty Ergebnis für Lambda Protection enthält den Namen, den Amazon-Ressourcennamen (ARN), die Funktionsversion und die Revisions-ID, die mit der Lambda-Funktion verknüpft sind, die in den Ergebnisdetails aufgeführt sind.

2. Identifizieren Sie die Quelle der potenziell verdächtigen Aktivität.

   a. Überprüfen Sie den Code, der der Lambda-Funktionsversion zugeordnet ist, die an der Erkenntnis beteiligt war.

   b. Überprüfen Sie die importierten Bibliotheken und Ebenen der Lambda-Funktionsversion, die an der Erkenntnis beteiligt waren.

   c. Wenn Sie AWS Lambda Scanfunktionen mit Amazon Inspector aktiviert haben, überprüfen Sie die Ergebnisse von Amazon Inspector im Zusammenhang mit der Lambda-Funktion, die an dem Ergebnis beteiligt war.

   d. Überprüfen Sie die AWS CloudTrail Protokolle, um den Principal zu identifizieren, der das Funktionsupdate verursacht hat, und stellen Sie sicher, dass die Aktivität autorisiert oder erwartet wurde.

3. Korrigieren Sie die potenziell gefährdete Lambda-Funktion.

   a. Deaktivieren Sie die Ausführungsauslöser der Lambda-Funktion, die an der Erkenntnis beteiligt sind. Weitere Informationen finden Sie unter. DeleteFunctionEventInvokeConfig

   b. Überprüfen Sie den Lambda-Code und aktualisieren Sie die Bibliotheksimporte und Lambda-Funktionsschichten, um die potenziell verdächtigen Bibliotheken und Schichten zu entfernen.

   c. Mindern Sie die Ergebnisse von Amazon Inspector im Zusammenhang mit der Lambda-Funktion, die an der Erkenntnis beteiligt war.

Schätzung der Kosten GuardDuty

Während der kostenlosen 30-Tage-Testversion können Sie die GuardDuty Konsole oder den API Betrieb verwenden, um die durchschnittlichen täglichen Nutzungskosten für zu schätzen. GuardDuty Die Kostenschätzung geht davon aus, wie hoch Ihre geschätzten Kosten nach dem Testzeitraum sein werden. Um während der kostenlosen Testversion einen genauen Kostenvoranschlag zu überprüfen, GuardDuty empfiehlt es sich jedoch, AWS Billing at zu https://console.aws.amazon.com/billing/verwenden.

Wenn Sie in einer Umgebung mit mehreren Konten arbeiten, kann das GuardDuty Administratorkonto die Kostenkennzahlen für alle Mitgliedskonten überwachen.

> **Hinweis zu den Nutzungskosten von Malware Protection for S3**
>
> Die Nutzungskosten für Malware Protection for S3 sind in der GuardDuty Konsole nicht unter Nutzung enthalten. Weitere Informationen finden Sie unter Nutzung und Kosten für Malware Protection for S3 anzeigen.

Sie können die Kostenschätzung anhand der folgenden Metriken einsehen:

- Konto-ID — Listet die geschätzten Kosten für Ihr Konto oder für Ihre Mitgliedskonten auf, wenn Sie ein GuardDuty Administratorkonto verwenden.
- Datenquellen — Listet die geschätzten Kosten für jede grundlegende Datenquelle auf — AWS CloudTrail Verwaltungsereignisse, VPC Flow-Logs und Route53 DNS Resolver-Abfrageprotokolle.
- Funktionen — Listet die geschätzten Kosten für die GuardDuty Funktionen auf — CloudTrail Datenereignisse für S3, EKS Audit Log Monitoring, EBS Volumendaten, RDS Anmeldeaktivität, EKS Runtime Monitoring, Fargate Runtime Monitoring, EC2 Runtime Monitoring oder Lambda Network Activity Monitoring.
- S3-Buckets – Listet die geschätzten Kosten für S3-Datenereignisse in einem bestimmten Bucket oder die teuersten Buckets für Konten in Ihrer Umgebung auf. Diese Statistik ist nur verfügbar, wenn Sie für eine aktivierenS3-Schutz. AWS-Konto

Verstehen Sie, wie die GuardDuty Nutzungskosten berechnet werden

Die in der GuardDuty Konsole angezeigten Schätzungen können geringfügig von denen auf Ihrer AWS Billing and Cost Management Konsole abweichen. In der folgenden Liste wird erläutert, wie die Nutzungskosten GuardDuty geschätzt werden:

- Die geschätzte GuardDuty Nutzung bezieht sich nur auf die aktuelle Region.
- Die GuardDuty Nutzungskosten basieren auf den Nutzungsdaten der letzten 30 Tage.
- Die Kostenschätzung für die Nutzung der Testversion beinhaltet die Schätzung für grundlegende Datenquellen und Feature, die sich derzeit im Testzeitraum befinden. Für jede Funktion und Datenquelle GuardDuty gibt es einen eigenen Testzeitraum, der sich jedoch mit dem Testzeitraum von GuardDuty oder einer anderen Funktion, die gleichzeitig aktiviert wurde, überschneiden kann.
- Die geschätzte GuardDuty Nutzung beinhaltet GuardDuty Mengenrabatte pro Region, wie auf der GuardDuty Amazon-Preisseite detailliert beschrieben, jedoch nur für einzelne Konten, die den Volumenpreisstufen entsprechen. Mengenrabatte sind in den Schätzungen für die kombinierte Gesamtnutzung zwischen Konten innerhalb einer Organisation nicht enthalten. Informationen zu Mengenrabatten bei kombinierter Nutzung finden Sie unter AWS -Abrechnung: Mengenrabatte.
- Die Summe der Nutzungskosten für die einzelnen AWS-Konto Benutzer in Ihrer Organisation entspricht möglicherweise nicht immer den geschätzten Kosten der letzten 30 Tage für die ausgewählte Datenquelle. Die Preisstufe kann sich ändern, wenn mehr Ereignisse oder Daten GuardDuty verarbeitet werden. Weitere Informationen finden Sie unter Preisstufen im AWS Billing Benutzerhandbuch.

In diesem Szenario wird erklärt, dass Sie sowohl die Funktionen Runtime Monitoring als auch Runtime Monitoring deaktivieren müssen, damit keine Nutzungskosten für EKS Runtime Monitoring anfallen.

GuardDuty hat die Konsolenerfahrung für EKS Runtime Monitoring in Runtime Monitoring zusammengefasst. GuardDuty empfiehlt Überprüfen Sie den Konfigurationsstatus von EKS Runtime Monitoring undMigration von EKS Runtime Monitoring zu Runtime Monitoring.

Stellen Sie im Rahmen der Migration zu Runtime Monitoring sicher, dass Deaktivieren Sie die Laufzeitüberwachung EKS Dies ist wichtig, denn wenn Sie sich später dafür entscheiden, Runtime

Monitoring zu deaktivieren, aber EKS Runtime Monitoring nicht deaktivieren, fallen weiterhin Nutzungskosten für EKS Runtime Monitoring an.

Runtime Monitoring — Wie sich VPC Flow-Logs von EC2 Instances auf die Nutzungskosten auswirken

Wenn Sie den Security Agent (entweder manuell oder über GuardDuty) in EKS Runtime Monitoring oder Runtime Monitoring für EC2 Instances verwalten und derzeit auf einer EC2 Amazon-Instance bereitgestellt GuardDuty ist und diese Gesammelte Laufzeit-Ereignistypen von dieser Instance erhält, fallen GuardDuty Ihnen keine Gebühren AWS-Konto für die Analyse der VPC Flow-Logs dieser EC2 Amazon-Instance an. Dadurch werden doppelte Nutzungskosten für das Konto GuardDuty vermieden.

Wie GuardDuty schätzt man die Nutzungskosten für CloudTrail Veranstaltungen

Wenn Sie diese Option aktivieren GuardDuty, werden automatisch AWS CloudTrail Ereignisprotokolle verwendet, die für Ihr Konto im ausgewählten Bereich aufgezeichnet wurden AWS-Region. GuardDuty repliziert globale Service-Ereignisprotokolle und verarbeitet diese Ereignisse dann unabhängig voneinander in jeder Region, in der Sie sie GuardDuty aktiviert haben. Dies hilft bei der GuardDuty Verwaltung von Benutzer- und Rollenprofilen in jeder Region, um Anomalien zu identifizieren.

Ihre CloudTrail Konfiguration hat keinen Einfluss auf die GuardDuty Nutzungskosten oder die Art und Weise, wie Ihre GuardDuty Ereignisprotokolle verarbeitet werden. Ihre GuardDuty Nutzungskosten hängen davon ab AWS APIs, welches Protokoll Sie verwenden CloudTrail. Weitere Informationen finden Sie unter AWS CloudTrail Management-Ereignisse.

Überprüfung der GuardDuty Nutzungsstatistiken

Wählen Sie Ihre bevorzugte Zugriffsmethode, um die Nutzungsstatistiken für Ihr GuardDuty Konto zu überprüfen. Wenn Sie ein GuardDuty Administratorkonto haben, helfen Ihnen die folgenden Methoden dabei, die Nutzungsstatistiken für alle Mitglieder zu überprüfen.

Console

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.

Stellen Sie sicher, dass Sie das GuardDuty Administratorkonto verwenden.

2. Wählen Sie im Navigationsbereich Benutzer.
3. Auf der Seite Nutzung kann ein GuardDuty Administratorkonto mit Mitgliedskonten die geschätzten Organisationskosten der letzten 30 Tage einsehen. Dies sind die geschätzten Gesamtnutzungskosten für Ihre Organisation.
4. GuardDuty Administratorkonten mit Mitgliedern können entweder die Aufschlüsselung der Nutzungskosten nach Datenquelle oder nach Konten einsehen. Einzelne oder eigenständige Konten können die Aufschlüsselung nach Datenquelle einsehen.

   Wenn Sie Mitgliedskonten haben, können Sie die Statistiken für ein einzelnes Konto einsehen, indem Sie dieses Konto in der Tabelle Konten auswählen.

   Wenn Sie auf der Registerkarte Nach Datenquellen eine Datenquelle auswählen, der Nutzungskosten zugeordnet sind, ist die entsprechende Summe der Kostenaufschlüsselung auf Kontoebene möglicherweise nicht immer dieselbe.

API/CLI

Führen Sie den GetUsageStatisticsAPIVorgang mit den Anmeldeinformationen des GuardDuty Administratorkontos aus. Geben Sie die folgenden Informationen ein, um den Befehl auszuführen:

- (Erforderlich) Geben Sie die regionale GuardDuty Melder-ID des Kontos an, für das Sie die Statistiken abrufen möchten.
- (Erforderlich) Geben Sie eine der folgenden Arten von Statistiken an, die abgerufen werden sollen: `SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE`.

  Unterstützt derzeit `TOP_ACCOUNTS_BY_FEATURE` nicht das Abrufen von Nutzungsstatistiken für`RDS_LOGIN_EVENTS`.
- (Erforderlich) Stellen Sie eine oder mehrere Datenquellen oder Funktionen zur Abfrage Ihrer Nutzungsstatistiken bereit.
- (Optional) Geben Sie eine Liste der Konten an, IDs für die Sie Nutzungsstatistiken abrufen möchten.

Sie können auch die AWS Command Line Interface verwenden. Der folgende Befehl ist ein Beispiel für das Abrufen der Nutzungsstatistiken für alle Datenquellen und Funktionen, berechnet

nach Konten. Stellen Sie sicher, dass Sie die `detector-id` durch Ihre eigene gültige Detektor-ID ersetzen. Bei eigenständigen Konten gibt dieser Befehl die Nutzungskosten der letzten 30 Tage nur für Ihr Konto zurück. Wenn Sie ein GuardDuty Administratorkonto mit Mitgliedskonten haben, werden die Kosten für alle Mitglieder nach Konten aufgelistet.

Informationen zu den Einstellungen `detectorId` für Ihr Konto und Ihre aktuelle Region finden Sie auf der Seite „Einstellungen“ in der https://console.aws.amazon.com/guardduty/Konsole oder führen Sie den aus ListDetectorsAPI.

Ersetzen Sie es `SUM_BY_ACCOUNT` durch den Typ, mit dem Sie die Nutzungsstatistiken berechnen möchten.

Um nur die Kosten für Datenquellen zu überwachen

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
 "EC2_MALWARE_SCAN"]}'
```

Um die Kosten für Funktionen zu überwachen

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
 "EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
 "EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Sicherheit in Amazon GuardDuty

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der geteilten Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für GuardDuty gelten, finden Sie unter Im Rahmen des Compliance-Programms gültige AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, einschließlich der Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von GuardDuty einsetzen können. Es zeigt Ihnen, wie Sie GuardDuty konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren außerdem, wie Sie andere AWS-Services verwenden, um Ihre GuardDuty-Ressourcen zu überwachen und zu schützen.

Inhalt

Datenschutz bei Amazon GuardDuty

Das AWS Modell der gilt für den Datenschutz bei Amazon GuardDuty. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS -Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie im Abschnitt Datenschutz FAQ. Informationen zum Datenschutz in Europa finden Sie im AWS Shared Responsibility Model und im GDPR Blogbeitrag auf dem AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden SieSSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS -Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter Federal Information Processing Standard () 140-3. FIPS

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole arbeiten GuardDuty oder sie anderweitig AWS -Services verwenden,API, AWS CLI oder. AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen in den angebenURL, um Ihre Anfrage an diesen Server zu überprüfen.

Verschlüsselung im Ruhezustand

Alle GuardDuty Kundendaten werden im Ruhezustand mithilfe von AWS Verschlüsselungslösungen verschlüsselt.

GuardDuty Daten, wie z. B. Ergebnisse, werden im Ruhezustand mithilfe von AWS Key Management Service (AWS KMS) unter Verwendung von eigenen, vom AWS Kunden verwalteten Schlüsseln verschlüsselt.

Verschlüsselung während der Übertragung

GuardDuty analysiert Protokolldaten von anderen Diensten. Es verschlüsselt alle Daten, die von diesen Diensten übertragen werden, mit HTTPS undKMS. Sobald die GuardDuty benötigten Informationen aus den Protokollen extrahiert wurden, werden sie verworfen. Weitere Informationen darüber, wie Informationen aus anderen Diensten GuardDuty verwendet werden, finden Sie unter GuardDuty Datenquellen.

GuardDuty Daten werden bei der Übertragung zwischen Diensten verschlüsselt.

Abmeldung von der Verwendung Ihrer Daten zur Serviceverbesserung

Sie können sich dafür entscheiden, die Verwendung Ihrer Daten zur Entwicklung GuardDuty und Verbesserung anderer AWS Sicherheitsdienste abzulehnen, indem Sie die AWS Organizations Opt-Out-Richtlinie verwenden. Sie können sich dafür entscheiden, sich abzumelden, auch wenn derzeit GuardDuty keine derartigen Daten erfasst werden. Weitere Informationen zur Deaktivierung finden Sie in den Opt-Out-Richtlinien für KI-Services im Benutzerhandbuch für AWS Organizations .

> **Note**
>
> Damit Sie die Opt-Out-Richtlinie nutzen können, müssen Ihre AWS Konten zentral von verwaltet werden AWS Organizations. Wenn Sie noch keine Organisation für Ihre AWS Konten erstellt haben, finden Sie weitere Informationen unter Organisation erstellen und verwalten im AWS Organizations Benutzerhandbuch.

Opt-Out hat folgende Auswirkungen:

- GuardDuty löscht die Daten, die es vor Ihrer Abmeldung gesammelt und gespeichert hat, um den Service zu verbessern (falls vorhanden).

- Nach Ihrer Abmeldung GuardDuty werden diese Daten nicht mehr zu Zwecken der Serviceverbesserung gesammelt oder gespeichert.

In den folgenden Themen wird erklärt, wie die einzelnen Funktionen GuardDuty möglicherweise Ihre Daten zur Serviceverbesserung verarbeiten.

Inhalt

GuardDuty Überwachung der Laufzeit

GuardDuty Runtime Monitoring bietet Runtime-Bedrohungserkennung für Amazon Elastic Kubernetes Service (AmazonEKS) -Cluster, nur AWS Fargate (Fargate) Amazon Elastic Container Service (AmazonECS) und Amazon Elastic Compute Cloud (AmazonEC2) -Instances in Ihrer AWS Umgebung. Nachdem Sie Runtime Monitoring aktiviert und den GuardDuty Security Agent für Ihre Ressource bereitgestellt haben, GuardDuty beginnt es mit der Überwachung und Analyse der Runtime-Ereignisse, die mit Ihrer Ressource verknüpft sind. Zu diesen Runtime-Ereignistypen gehören Prozessereignisse, DNS Container-Ereignisse, Ereignisse und mehr. Weitere Informationen finden Sie unter Gesammelte Runtime-Ereignistypen, die verwendet GuardDuty .

Obwohl GuardDuty jetzt Befehlszeilenargumente gesammelt werden, die Sie an Ihre Workloads weiterleiten können, werden diese Argumente derzeit nicht zur Serviceverbesserung verwendet (dies könnte in future der Fall sein). In Erwartung neuer Regeln und Erkenntnisse zur Bedrohungserkennung, die bald veröffentlicht werden, haben wir damit begonnen, Befehlszeilenargumente zu sammeln. Ihr Vertrauen, Ihre Privatsphäre und die Sicherheit Ihrer Inhalte haben für uns höchste Priorität und wir stellen sicher, dass unsere Nutzung unseren Verpflichtungen Ihnen gegenüber entspricht. Weitere Informationen finden Sie unter Datenschutz. FAQ

GuardDuty Schutz vor Schadsoftware

GuardDuty Der Malware-Schutz scannt und erkennt Malware in EBS Volumes, die an Ihre potenziell gefährdeten EC2 Amazon-Instance- und Container-Workloads angehängt sind, sowie in neu hochgeladenen Dateien in Ihren ausgewählten Amazon S3-Buckets. Sammelt oder verwendet derzeit GuardDuty keine erkannte Malware zur Serviceverbesserung. Wenn GuardDuty Malware Protection jedoch in future eine EBS Volume-Datei oder eine S3-Datei als bösartig oder schädlich identifiziert, sammelt und speichert GuardDuty Malware Protection diese Datei, um die Malware-

Erkennungen und den GuardDuty Service weiterzuentwickeln und zu verbessern. Diese Datei kann auch zur Entwicklung und Verbesserung anderer AWS Sicherheitsdienste verwendet werden. Ihr Vertrauen, Ihre Privatsphäre und die Sicherheit Ihrer Inhalte haben für uns höchste Priorität und wir stellen sicher, dass unsere Nutzung unseren Verpflichtungen Ihnen gegenüber entspricht. Weitere Informationen finden Sie unter Datenschutz FAQ.

Protokollierung Amazon GuardDuty Amazon-API-Aufrufen mit AWS CloudTrail

Amazon GuardDuty ist in einen Service integriertAWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in ausgeführt wurden GuardDuty. CloudTrail erfasst alle API-Aufrufe GuardDuty als Ereignisse, einschließlich Aufrufe von der GuardDuty Konsole und von Codeaufrufen an die GuardDuty APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon Simple Storage Service (Amazon S3) -Bucket aktivieren, einschließlich Ereignissen für GuardDuty. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, an die die Anfrage gestellt wurde GuardDuty, die IP-Adresse, von der die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen dazu CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrailBenutzerhandbuch.

GuardDuty Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn unterstützte Ereignisaktivitäten in auftreten GuardDuty, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für GuardDuty, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit.

Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des IAM-Benutzers gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen föderierten Benutzer ausgeführt wurde
- Ob die Anforderung von einem anderen AWS-Service getätigt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

GuardDuty Ereignisse auf der Kontrollebene in CloudTrail

Standardmäßig CloudTrail protokolliert es alle GuardDuty API-Operationen, die in der Amazon GuardDuty API-Referenz bereitgestellt werden, als Ereignisse in CloudTrail Dateien.

GuardDuty Datenereignisse in CloudTrail

GuardDuty Überwachung der Laufzeitverwendet einen GuardDuty Sicherheitsagenten, der auf Ihren Amazon Elastic Kubernetes Service (Amazon EKS) -Clustern, Amazon Elastic Compute Cloud (Amazon EC2) -Instances und AWS Fargate (nur Amazon Elastic Container Service (Amazon ECS)) Aufgaben installiert ist, um Add-on (`aws-guardduty-agent`) zu sammeln, die Gesammelte Laufzeit-Ereignistypen für Ihre AWS Workloads gesammelt werden, und sendet sie dann zur Bedrohungserkennung und GuardDuty -analyse an.

Protokollierung und Überwachung von Datenereignissen

Sie können die AWS CloudTrail Protokolle optional so konfigurieren, dass die Datenereignisse für Ihren Security Agent angezeigt werden. GuardDuty

Informationen zum Erstellen und Konfigurieren CloudTrail finden Sie unter Datenereignisse im AWS CloudTrailBenutzerhandbuch und folgen Sie den Anweisungen zur Protokollierung von Datenereignissen mit erweiterten Ereignisauswahlmöglichkeiten in der AWS Management Console. Wenn Sie den Trail protokollieren, stellen Sie sicher, dass Sie die folgenden Änderungen vornehmen:

- Wählen Sie für den Ereignistyp „Daten“ die Option GuardDuty Detektor aus.
- Wählen Sie für die Protokollauswahlvorlage die Option Alle Ereignisse protokollieren aus.
- Erweitern Sie die JSON-Ansicht für die Konfiguration. Die Ausgabe sollte ähnlich dem folgenden JSON aussehen:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Nachdem Sie den Selektor für den Trail aktiviert haben, navigieren Sie zur Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/. Sie können die Datenereignisse aus Ihrem S3-Bucket herunterladen, den Sie bei der Konfiguration der CloudTrail Protokolle ausgewählt haben.

Beispiel: Einträge in GuardDuty Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der das Ereignis auf der Datenebene demonstriert.


```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
```

```
        "requestParameters": null,
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateIPThreatIntelSet` Aktion demonstriert (Ereignis auf der Steuerungsebene).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
```

```
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```


Aus diesem Ereignis Informationen können Sie ersehen, dass die Anfrage gestellt wurde, um eine Bedrohungsliste `Example` in GuardDuty zu erstellen. Sie können auch sehen, dass die Anfrage von einem Benutzer namens Alice am 14. Juni 2018 gemacht wurde.

Identity and Access Management für Amazon GuardDuty

AWS Identity and Access Management (IAM) hilft einem Administrator AWS -Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um GuardDuty Ressourcen zu verwenden. IAMist eine AWS -Service , die Sie ohne zusätzliche Kosten verwenden können.

Themen

- Zielgruppe

- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So GuardDuty arbeitet Amazon mit IAM
- Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty
- Verwenden von serviceverknüpften Rollen für Amazon GuardDuty
- AWS verwaltete Richtlinien für Amazon GuardDuty
- Fehlerbehebung Amazon GuardDuty Amazon-Identität und -Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie arbeiten GuardDuty.

Dienstbenutzer — Wenn Sie den GuardDuty Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr GuardDuty Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in nicht auf eine Funktion zugreifen können GuardDuty, finden Sie weitere Informationen unterFehlerbehebung Amazon GuardDuty Amazon-Identität und -Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die GuardDuty Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf GuardDuty. Es ist Ihre Aufgabe, zu bestimmen, auf welche GuardDuty Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit verwenden kann GuardDuty, finden Sie unterSo GuardDuty arbeitet Amazon mit IAM.

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff darauf zu verwalten GuardDuty. Beispiele für GuardDuty identitätsbasierte Richtlinien, die Sie in verwenden könnenIAM, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM Rolle übernehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAMIdentity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit der Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAMBenutzerhandbuch unter AWS API Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS -Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der

Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS -Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS -Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe ist eine Identität, die eine Sammlung von IAM Benutzern spezifiziert. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM Benutzerberechtigungen — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um jemandem (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS -Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

- Serviceübergreifender Zugriff — Einige AWS -Services verwenden Funktionen in anderen. AWS -Services Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der an aufruft AWS -Service, kombiniert mit der Anforderung, Anfragen AWS -Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS -Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS -Service an eine.
  - Dienstbezogene Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS -Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie unter Wann sollte eine IAM Rolle (anstelle eines Benutzers) erstellt werden? im IAMBenutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie

mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS -Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bietenACLs. Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für

eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.

- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen AWS Organizations. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Geräte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAMBenutzerhandbuch unter Bewertungslogik für Richtlinien.

So GuardDuty arbeitet Amazon mit IAM

Informieren Sie sich vor der Verwendung IAM zur Verwaltung des Zugriffs auf GuardDuty, welche IAM Funktionen zur Nutzung verfügbar sind GuardDuty.

IAMFunktionen, die Sie mit Amazon verwenden können GuardDuty

IAMFunktion	GuardDuty Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC(Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie GuardDuty und wie andere AWS Dienste mit den meisten IAM Funktionen funktionieren, finden Sie IAM im IAMBenutzerhandbuch unter AWS Dienste, die mit funktionieren.

Identitätsbasierte Richtlinien für GuardDuty

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie in der Referenz zu den IAM JSON Richtlinienelementen im IAMBenutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für GuardDuty

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Ressourcenbasierte Richtlinien finden Sie in GuardDuty

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS -Services

Um den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource gewähren. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie IAMim IAMBenutzerhandbuch unter Kontenübergreifender Ressourcenzugriff.

Politische Maßnahmen für GuardDuty

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der GuardDuty Aktionen finden Sie unter Von Amazon definierte Aktionen GuardDuty in der Service Authorization Reference.

Bei den in der Richtlinie GuardDuty verwendeten Aktionen wird vor der Aktion das folgende Präfix verwendet:

```
guardduty
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Politische Ressourcen für GuardDuty

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der GuardDuty Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von Amazon definierte Ressourcen GuardDuty in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie die ARN einzelnen Ressourcen spezifizieren können, finden Sie unter Von Amazon definierte Aktionen GuardDuty.

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Bedingungsschlüssel für Richtlinien für GuardDuty

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontext-Schlüssel für AWS globale Bedingungen im IAMBenutzerhandbuch.

Eine Liste der GuardDuty Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon GuardDuty in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon definierte Aktionen GuardDuty.

Beispiele für GuardDuty identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Zugriffskontrolllisten () ACLs in GuardDuty

UnterstütztACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle () mit ABAC GuardDuty

Unterstützt ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt vonABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Temporäre Anmeldeinformationen verwenden mit GuardDuty

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS -Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen darüber, AWS -Services wie Sie mit temporären Anmeldeinformationen arbeiten können AWS -Services , finden Sie IAM im IAMBenutzerhandbuch unter Diese Informationen.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Kennwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Rollenwechsel finden Sie unter Wechseln zu einer Rolle (Konsole) im IAMBenutzerhandbuch.

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen unter IAM.

Serviceübergreifende Prinzipalberechtigungen für GuardDuty

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in

einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS -Service, kombiniert mit der Anforderung, Anfragen AWS -Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS -Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für GuardDuty

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS -Service an eine.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann zu GuardDuty Funktionseinschränkungen führen. Bearbeiten Sie Servicerollen nur, GuardDuty wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für GuardDuty

Unterstützt dienstbezogene Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS -Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von GuardDuty dienstbezogenen Rollen finden Sie unter. Verwenden von serviceverknüpften Rollen für Amazon GuardDuty

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter AWS Dienste, die mit funktionieren. IAM Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Amazon GuardDuty

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Ressourcen zu erstellen oder zu ändern GuardDuty. Sie können auch keine Aufgaben mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen AWS API. Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter IAMRichtlinien erstellen im IAMBenutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden GuardDuty, einschließlich des Formats von ARNs für jeden der Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon GuardDuty in der Service Authorization Reference.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand GuardDuty Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst

Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.

- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS -Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.
- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Wenn Sie festlegen möchten, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Verwenden der GuardDuty Konsole

Um auf die GuardDuty Amazon-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Informationen zu den GuardDuty Ressourcen in Ihrem Verzeichnis aufzulisten und einzusehen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur Anrufe an AWS CLI oder am tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS API. Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die GuardDuty Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die GuardDuty `ConsoleAccess` oder die `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie im Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen IAM Benutzer.

Erforderliche Berechtigungen zum Aktivieren von GuardDuty

Um Berechtigungen zu gewähren, über die verschiedene IAM Identitäten (Benutzer, Gruppen und Rollen) verfügen müssen, fügen Sie die erforderliche AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess Richtlinie zur Aktivierung GuardDuty bei.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die Inline- und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
```

```
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Benutzerdefinierte IAM Richtlinie zur Gewährung von schreibgeschütztem Zugriff auf GuardDuty

Um Ihnen nur Lesezugriff zu gewähren, können GuardDuty Sie die verwaltete Richtlinie verwenden. `AmazonGuardDutyReadOnlyAccess`

Um eine benutzerdefinierte Richtlinie zu erstellen, die einer IAM Rolle, einem Benutzer oder einer Gruppe schreibgeschützten Zugriff gewährt GuardDuty, können Sie die folgende Anweisung verwenden:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
```

```
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
            ],
            "Resource": "*"
        }
    ]
}
```

Zugriff auf Ergebnisse verweigern GuardDuty

Sie können die folgende Richtlinie verwenden, um einer IAM Rolle, einem Benutzer oder einer Gruppe den Zugriff auf GuardDuty Ergebnisse zu verweigern. Benutzer können die Ergebnisse oder die Details zu den Ergebnissen nicht anzeigen, aber sie können auf alle anderen GuardDuty Operationen zugreifen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
```

```
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:ArchiveFindings",
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
```

```
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Verwendung einer benutzerdefinierten IAM Richtlinie zur Beschränkung des Zugriffs auf GuardDuty Ressourcen

Um den Zugriff eines Benutzers auf der GuardDuty Grundlage der Melder-ID zu definieren, können Sie alle GuardDutyAPIAktionen in Ihren benutzerdefinierten IAM Richtlinien verwenden, mit Ausnahme der folgenden Operationen:

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Verwenden Sie die folgenden Operationen in einer IAM Richtlinie, um den Zugriff eines Benutzers auf der GuardDuty Grundlage der IPSet ID und ThreatIntelSet ID zu definieren:

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

Die folgenden Beispiele zeigen, wie Richtlinien mithilfe einiger der vorhergehenden Vorgänge erstellt werden:

- Diese Richtlinie erlaubt einem Benutzer die Ausführung des `guardduty:UpdateDetector`-Vorgangs mithilfe der Detektor-ID 1234567 in der Region „us-east-1“:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateDetector",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
        }
    ]
}
```

- Diese Richtlinie ermöglicht es einem Benutzer, den `guardduty:UpdateIPSet` Vorgang unter Verwendung der Melder-ID 1234567 und der IPSet ID 000000 in der Region us-east-1 auszuführen:

> **Note**
>
> Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen für den Zugriff auf vertrauenswürdige IP-Adressen und Bedrohungslisten in verfügt. GuardDuty Weitere Informationen finden Sie unter Erforderliche Berechtigungen für das Hochladen von Listen mit vertrauenswürdigen IPs und Bedrohungslisten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
        }
    ]
}
```

- Diese Richtlinie ermöglicht es einem Benutzer, den `guardduty:UpdateIPSet` Vorgang mit einer beliebigen Melder-ID und der IPSet ID 000000 in der Region us-east-1 auszuführen:

> **Note**
>
> Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen für den Zugriff auf vertrauenswürdige IP-Adressen und Bedrohungslisten in verfügt. GuardDuty Weitere Informationen finden Sie unter Erforderliche Berechtigungen für das Hochladen von Listen mit vertrauenswürdigen IPs und Bedrohungslisten.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- Diese Richtlinie ermöglicht es einem Benutzer, den `guardduty:UpdateIPSet` Vorgang mit seiner Melder-ID und einer beliebigen IPSet ID in der Region us-east-1 auszuführen:

> **Note**
>
> Stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen für den Zugriff auf vertrauenswürdige IP-Adressen und Bedrohungslisten in verfügt. GuardDuty Weitere Informationen finden Sie unter Erforderliche Berechtigungen für das Hochladen von Listen mit vertrauenswürdigen IPs und Bedrohungslisten.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

Verwenden von serviceverknüpften Rollen für Amazon GuardDuty

Amazon GuardDuty verwendet dienstbezogene Rollen AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle (SLR) ist ein einzigartiger IAM Rollentyp, mit dem direkt verknüpft ist. GuardDuty Mit Diensten verknüpfte Rollen sind vordefiniert GuardDuty und enthalten alle Berechtigungen, die GuardDuty erforderlich sind, um andere AWS Dienste in Ihrem Namen aufzurufen.

Mit einer dienstverknüpften Rolle können Sie sie einrichten, GuardDuty ohne die erforderlichen Berechtigungen manuell hinzufügen zu müssen. GuardDuty definiert die Berechtigungen der dienstbezogenen Rolle. Sofern die Berechtigungen nicht anders definiert sind, GuardDuty kann Only die Rolle übernehmen. Zu den definierten Berechtigungen gehören die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen IAM Entität zugeordnet werden.

GuardDuty unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen dies verfügbar GuardDuty ist. Weitere Informationen finden Sie unter Regionen und Endpunkte.

Sie können die GuardDuty dienstverknüpfte Rolle erst löschen, nachdem Sie sie zuerst GuardDuty in allen Regionen deaktiviert haben, in denen sie aktiviert ist. Dadurch werden Ihre GuardDuty Ressourcen geschützt, da Sie die Zugriffsberechtigung nicht versehentlich entziehen können.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie im IAMBenutzerhandbuch unter AWS Services that work with. Suchen Sie IAM in der Spalte Serviceverknüpfte Rolle nach den Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Dienstbezogene Rollenberechtigungen für GuardDuty

GuardDuty verwendet die benannte dienstverknüpfte Rolle (SLR). `AWSServiceRoleForAmazonGuardDuty` Das SLR ermöglicht GuardDuty die Ausführung der folgenden Aufgaben. Es ermöglicht auch GuardDuty , die abgerufenen Metadaten, die zu der EC2 Instanz gehören, in die Erkenntnisse einzubeziehen, die GuardDuty möglicherweise über die potenzielle Bedrohung generiert werden. Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonGuardDuty` vertraut dem Service `guardduty.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die Berechtigungsrichtlinien helfen bei der GuardDuty Ausführung der folgenden Aufgaben:

- Verwenden Sie EC2 Amazon-Aktionen, um Informationen über Ihre EC2 Instances, Images und Netzwerkkomponenten wie VPCs Subnetze und Transit-Gateways zu verwalten und abzurufen.
- Verwenden Sie AWS Systems Manager Aktionen, um SSM Verknüpfungen auf EC2 Amazon-Instances zu verwalten, wenn Sie GuardDuty Runtime Monitoring mit automatisiertem Agenten für Amazon aktivierenEC2. Wenn die GuardDuty automatische Agentenkonfiguration deaktiviert ist, werden nur die EC2 Instances GuardDuty berücksichtigt, die über ein Inclusion-Tag (`GuardDutyManaged:true`) verfügen.
- Verwenden Sie AWS Organizations Aktionen, um die zugehörigen Konten und die Organisations-ID zu beschreiben.
- Verwenden Sie Amazon-S3-Aktionen, um Informationen über S3-Buckets und Objekte abzurufen.
- Verwenden Sie AWS Lambda Aktionen, um Informationen über Ihre Lambda-Funktionen und -Tags abzurufen.
- Verwenden Sie EKS Amazon-Aktionen, um Informationen zu den EKS Clustern zu verwalten und abzurufen und EKSAmazon-Add-Ons für EKS Cluster zu verwalten. Die EKS Aktionen rufen auch die Informationen über die zugehörigen Tags ab GuardDuty.
- Wird verwendetIAM, um das zu erstellen, Servicebezogene Rollenberechtigungen für Malware Protection für EC2 nachdem der Malware-Schutz für aktiviert EC2 wurde.
- Verwenden Sie ECS Amazon-Aktionen, um Informationen zu den ECS Amazon-Clustern zu verwalten und abzurufen, und verwalten Sie die ECS Amazon-Kontoeinstellungen mit`guarddutyActivate`. Die Aktionen im Zusammenhang mit Amazon rufen ECS auch die Informationen zu den zugehörigen Tags ab. GuardDuty

Die Rolle ist mit der folgenden AWS -verwalteten Richtlinie namens `AmazonGuardDutyServiceRolePolicy` konfiguriert.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GuardDutyGetDescribeListPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeTransitGatewayAttachments",
                "organizations:ListAccounts",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketTagging",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "lambda:GetFunctionConfiguration",
                "lambda:ListTags",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ecs:ListClusters",
                "ecs:DescribeClusters"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GuardDutyCreateSLRPolicy",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                },
                "StringLike": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.*.guardduty-data",
                        "com.amazonaws.*.guardduty-data-fips"
                    ]
                }
            }
        },
        {
            "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpoint",
                "ec2:DeleteVpcEndpoints"
            ],
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:ModifyVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*",
```

```
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
             "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
             "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateVpcEndpoint"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutySecurityGroupManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/GuardDutyManaged": "*"
                }
```

```
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        },
        {
            "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateEksAddonPolicy",
            "Effect": "Allow",
            "Action": "eks:CreateAddon",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEksAddonManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "eks:DeleteAddon",
                "eks:UpdateAddon",
                "eks:DescribeAddon"
            ],
            "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
        },
        {
```

```
            "Sid": "GuardDutyEksClusterTagResourcePolicy",
            "Effect": "Allow",
            "Action": "eks:TagResource",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
            "Effect": "Allow",
            "Action": "ecs:PutAccountSettingDefault",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:account-setting": [
                        "guardDutyActivate"
                    ]
                 }
            }
        },
        {
            "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:DeleteAssociation",
                "ssm:UpdateAssociation",
                "ssm:CreateAssociation",
                "ssm:StartAssociationsOnce"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmAddTagsToResourcePermission",
            "Effect": "Allow",
            "Action": [
```

```
                "ssm:AddTagsToResource"
            ],
            "Resource": "arn:aws:arn:aws:ssm:*:*:association/*",
            "Condition":{
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateAssociation",
                "ssm:UpdateAssociation"
            ],
            "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
        },
        {
            "Sid": "SsmSendCommandPermission",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
            ]
        },
        {
            "Sid": "SsmGetCommandStatus",
            "Effect": "Allow",
            "Action": "ssm:GetCommandInvocation",
            "Resource": "*"
        }
    ]
}
```

Nachfolgend wird die der serviceverknüpften Rolle `AWSServiceRoleForAmazonGuardDuty` zugeordnete Vertrauensrichtlinie gezeigt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Einzelheiten zu Aktualisierungen der `AmazonGuardDutyServiceRolePolicy` Richtlinie finden Sie unterGuardDuty Aktualisierungen der AWS verwalteten Richtlinien. Abonnieren Sie den RSS Feed auf der Dokumentverlauf Seite, um automatische Benachrichtigungen über Änderungen an dieser Richtlinie zu erhalten.

Erstellen einer dienstbezogenen Rolle für GuardDuty

Die `AWSServiceRoleForAmazonGuardDuty` dienstverknüpfte Rolle wird automatisch erstellt, wenn Sie sie GuardDuty zum ersten Mal oder GuardDuty in einer unterstützten Region aktivieren, in der sie zuvor nicht aktiviert war. Sie können die dienstverknüpfte Rolle auch manuell mithilfe der IAM Konsole, der oder der AWS CLI erstellen. IAM API

> **Important**
>
> Die dienstverknüpfte Rolle, die für das GuardDuty delegierte Administratorkonto erstellt wurde, gilt nicht für die Mitgliedskonten. GuardDuty

Sie müssen Berechtigungen konfigurieren, damit ein IAM Hauptbenutzer (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine dienstbezogene Rolle erstellen, bearbeiten oder löschen kann. Damit die `AWSServiceRoleForAmazonGuardDuty` dienstverknüpfte Rolle erfolgreich erstellt werden kann, muss der IAM Prinzipal, den Sie GuardDuty mit verwenden, über die erforderlichen Berechtigungen verfügen. Um die erforderlichen Berechtigungen zu erteilen, weisen Sie diesem -Benutzer bzw. dieser-Gruppe oder -Rolle die folgende Richtlinie zu:

> **Note**
>
> Ersetzen Sie das Beispiel *account ID* im folgenden Beispiel mit Ihrer tatsächlichen AWS Konto-ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Weitere Informationen zum manuellen Erstellen der Rolle finden Sie unter Erstellen einer serviceverknüpften Rolle im IAMBenutzerhandbuch.

Bearbeiten einer serviceverknüpften Rolle für GuardDuty

GuardDuty erlaubt es Ihnen nicht, die `AWSServiceRoleForAmazonGuardDuty` dienstbezogene Rolle zu bearbeiten. Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten auf die Rolle verweisen könnten. Sie können die Beschreibung der Rolle jedoch mit IAM bearbeiten. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Bearbeiten einer dienstbezogenen Rolle.

Löschen einer serviceverknüpften Rolle für GuardDuty

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

> **Important**
>
> Wenn Sie den Malware-Schutz für aktiviert habenEC2, wird `AWSServiceRoleForAmazonGuardDuty` das Löschen nicht automatisch gelöscht`AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Informationen zum Löschen `AWSServiceRoleForAmazonGuardDutyMalwareProtection` finden Sie unter Löschen einer serviceverknüpften Rolle für Malware Protection for EC2.

Sie müssen sie zunächst GuardDuty in allen Regionen deaktivieren, in denen sie aktiviert ist, um die `AWSServiceRoleForAmazonGuardDuty` zu löschen. Wenn der GuardDuty Dienst nicht deaktiviert ist, wenn Sie versuchen, die mit dem Dienst verknüpfte Rolle zu löschen, schlägt das Löschen fehl. Weitere Informationen finden Sie unter Aussetzen oder Deaktivieren GuardDuty.

Wenn Sie ihn deaktivieren GuardDuty, wird `AWSServiceRoleForAmazonGuardDuty` er nicht automatisch gelöscht. Wenn Sie es GuardDuty erneut aktivieren, wird das Bestehende verwendet`AWSServiceRoleForAmazonGuardDuty`.

Um die mit dem Service verknüpfte Rolle manuell zu löschen, verwenden Sie IAM

Verwenden Sie die IAM Konsole, den oder AWS CLI, IAM API um die `AWSServiceRoleForAmazonGuardDuty` dienstverknüpfte Rolle zu löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Löschen einer dienstbezogenen Rolle.

Unterstützt AWS-Regionen

Amazon GuardDuty unterstützt die Verwendung der `AWSServiceRoleForAmazonGuardDuty` serviceverknüpften Rolle überall AWS-Regionen dort, wo sie verfügbar GuardDuty ist. Eine Liste der Regionen, in denen GuardDuty das Produkt derzeit verfügbar ist, finden Sie unter GuardDuty Amazon-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz.

Servicebezogene Rollenberechtigungen für Malware Protection für EC2

Malware Protection for EC2 verwendet die mit dem Dienst verknüpfte Rolle (SLR) mit dem Namen. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` SLRDadurch kann Malware Protection for EC2 Scans ohne Agenten durchführen, um Malware in Ihrem GuardDuty Konto zu erkennen. Es ermöglicht GuardDuty Ihnen, einen EBS Volume-Snapshot in Ihrem Konto zu erstellen und diesen Snapshot mit dem GuardDuty Dienstkonto zu teilen. Nach der GuardDuty Auswertung des Snapshots werden die abgerufenen EC2 Instance- und Container-Workload-Metadaten in den Malware-Schutz aufgenommen, um die EC2 Ergebnisse zu ermitteln. Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` vertraut dem Service `malware-protection.guardduty.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die Berechtigungsrichtlinien für diese Rolle helfen Malware Protection for EC2 bei der Ausführung der folgenden Aufgaben:

- Verwenden Sie Amazon Elastic Compute Cloud (AmazonEC2) -Aktionen, um Informationen über Ihre EC2 Amazon-Instances, Volumes und Snapshots abzurufen. Malware Protection for gewährt EC2 auch die Erlaubnis, auf die Amazon EKS - und ECS Amazon-Cluster-Metadaten zuzugreifen.
- Erstellen Sie Snapshots für EBS Volumes, deren `GuardDutyExcluded` Tag nicht auf `true` gesetzt ist. Standardmäßig werden die Snapshots mit einem `GuardDutyScanId`-Tag erstellt. Entfernen Sie dieses Tag nicht, da Malware Protection for EC2 sonst keinen Zugriff auf die Snapshots hat.

> **Important**
>
> Wenn Sie das `GuardDutyExcluded` auf setzen`true`, kann der GuardDuty Dienst in future nicht mehr auf diese Snapshots zugreifen. Dies liegt daran, dass die anderen Anweisungen in dieser dienstbezogenen Rolle GuardDuty verhindern, dass Aktionen für die Snapshots ausgeführt werden, für die der Wert auf gesetzt ist. `GuardDutyExcluded` `true`

- Lassen Sie das Teilen und Löschen von Snapshots nur zu, wenn das `GuardDutyScanId`-Tag existiert und das `GuardDutyExcluded`-Tag nicht auf `true` gesetzt ist.

  > **Note**
  >
  > Lässt nicht zu, dass Malware Protection für EC2 die Snapshots veröffentlicht.

- Greifen Sie auf vom Kunden verwaltete Schlüssel zu, mit Ausnahme von Schlüsseln, für die ein `GuardDutyExcluded` Tag auf gesetzt ist`true`, `CreateGrant` um über den verschlüsselten Snapshot, der mit dem GuardDuty Servicekonto geteilt wird, ein verschlüsseltes EBS Volume zu erstellen und darauf zuzugreifen. Eine Liste der GuardDuty Dienstkonten für jede Region finden Sie unter[GuardDuty Dienstkonten von AWS-Region](#).
- Greifen Sie auf CloudWatch Kundenprotokolle zu, um die EC2 Protokollgruppe „Malware-Schutz für“ zu erstellen und die Ereignisprotokolle der Malware-Suche unter der `/aws/guardduty/malware-scan-events` Protokollgruppe abzulegen.
- Lassen Sie den Kunden entscheiden, ob er die Snapshots, auf denen Malware erkannt wurde, in seinem Konto behalten möchte. Wenn beim Scan Malware erkannt wird, ermöglicht die mit dem Dienst verknüpfte Rolle GuardDuty das Hinzufügen von zwei Tags zu Snapshots: und. `GuardDutyFindingDetected` `GuardDutyExcluded`

  > **Note**
  >
  > Das `GuardDutyFindingDetected`-Tag gibt an, dass die Snapshots Malware enthalten.

- Ermitteln Sie, ob ein Volume mit einem EBS verwalteten Schlüssel verschlüsselt ist. GuardDuty führt die `DescribeKey` Aktion zur Bestimmung `key Id` des EBS verwalteten Schlüssels in Ihrem Konto durch.
- Rufen Sie den Snapshot der mit Von AWS verwalteter Schlüssel, verschlüsselten EBS Volumes von Ihrem ab AWS-Konto und kopieren Sie ihn in den. [GuardDuty Dienstkonto](#) Zu diesem Zweck verwenden wir die Berechtigungen `GetSnapshotBlock` und`ListSnapshotBlocks`. GuardDuty scannt dann den Snapshot im Dienstkonto. Derzeit ist der Malware-Schutz zur EC2 Unterstützung des Scannens von EBS Volumes, die mit verschlüsselt sind, Von AWS verwalteter Schlüssel möglicherweise nicht in allen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter [Verfügbarkeit regionsspezifischer Feature](#).
- Erlauben EC2 Sie AWS KMS Amazon, im Namen von Malware Protection mehrere kryptografische Aktionen mit vom Kunden verwalteten Schlüsseln durchzuführen. EC2 Aktionen wie `kms:ReEncryptTo` und `kms:ReEncryptFrom` sind erforderlich, um die Snapshots zu teilen,

die mit den vom Kunden verwalteten Schlüsseln verschlüsselt sind. Es sind nur die Schlüssel zugänglich, für die das `GuardDutyExcluded`-Tag nicht auf `true` festgelegt ist.

Die Rolle ist mit der folgenden AWS -verwalteten Richtlinie namens `AmazonGuardDutyMalwareProtectionServiceRolePolicy` konfiguriert.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DescribeAndListPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ecs:ListClusters",
                "ecs:ListContainerInstances",
                "ecs:ListTasks",
                "ecs:DescribeTasks",
                "eks:DescribeCluster"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateSnapshotVolumeConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "CreateSnapshotConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyScanId"
```

```
                }
            }
        },
        {
            "Sid": "CreateTagsPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:*/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSnapshot"
                }
            }
        },
        {
            "Sid": "AddTagsToSnapshotPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyExcluded",
                        "GuardDutyFindingDetected"
                    ]
                }
            }
        },
        {
            "Sid": "DeleteAndShareSnapshotPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot",
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
```

```
                "aws:ResourceTag/GuardDutyExcluded": "true"
            }
        }
    },
    {
        "Sid": "PreventPublicAccessToSnapshotPermission",
        "Effect": "Deny",
        "Action": [
            "ec2:ModifySnapshotAttribute"
        ],
        "Resource": "arn:aws:ec2:*:*:snapshot/*",
        "Condition": {
            "StringEquals": {
                "ec2:Add/group": "all"
            }
        }
    },
    {
        "Sid": "CreateGrantPermission",
        "Effect": "Allow",
        "Action": "kms:CreateGrant",
        "Resource": "arn:aws:kms:*:*:key/*",
        "Condition": {
            "Null": {
                "aws:ResourceTag/GuardDutyExcluded": "true"
            },
            "StringLike": {
                "kms:EncryptionContext:aws:ebs:id": "snap-*"
            },
            "ForAllValues:StringEquals": {
                "kms:GrantOperations": [
                    "Decrypt",
                    "CreateGrant",
                    "GenerateDataKeyWithoutPlaintext",
                    "ReEncryptFrom",
                    "ReEncryptTo",
                    "RetireGrant",
                    "DescribeKey"
                ]
            },
            "Bool": {
                "kms:GrantIsForAWSResource": "true"
            }
        }
```

```
        },
        {
            "Sid": "ShareSnapshotKMSPermission",
            "Effect": "Allow",
            "Action": [
                "kms:ReEncryptTo",
                "kms:ReEncryptFrom"
            ],
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": "ec2.*.amazonaws.com"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "DescribeKeyPermission",
            "Effect": "Allow",
            "Action": "kms:DescribeKey",
            "Resource": "arn:aws:kms:*:*:key/*"
        },
        {
            "Sid": "GuardDutyLogGroupPermission",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:CreateLogGroup",
                "logs:PutRetentionPolicy"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
        },
        {
            "Sid": "GuardDutyLogStreamPermission",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
        },
```

```
        {
            "Sid": "EBSDirectAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "ebs:GetSnapshotBlock",
                "ebs:ListSnapshotBlocks"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        }
    ]
}
```

Nachfolgend wird die der serviceverknüpften Rolle `AWSServiceRoleForAmazonGuardDutyMalwareProtection` zugeordnete Vertrauensrichtlinie gezeigt:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Erstellen einer dienstbezogenen Rolle für den Malware-Schutz für EC2

Die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` dienstbezogene Rolle wird automatisch erstellt, wenn Sie den Malware-Schutz EC2 zum ersten Mal oder den Malware-Schutz für eine unterstützte Region aktivieren, EC2 in der er zuvor nicht aktiviert war. Sie können

die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` dienstverknüpfte Rolle auch manuell mithilfe der IAM Konsole, der oder der IAM CLI erstellen. IAM API

> **Note**
>
> Wenn Sie neu bei Amazon sind GuardDuty, EC2 ist Malware Protection for standardmäßig automatisch aktiviert.

> **Important**
>
> Die dienstbezogene Rolle, die für das delegierte GuardDuty Administratorkonto erstellt wurde, gilt nicht für die GuardDuty Mitgliedskonten.

Sie müssen Berechtigungen konfigurieren, damit ein IAM Hauptbenutzer (z. B. ein Benutzer, eine Gruppe oder eine Rolle) eine dienstbezogene Rolle erstellen, bearbeiten oder löschen kann. Damit die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` dienstverknüpfte Rolle erfolgreich erstellt werden kann, muss die IAM Identität, die Sie GuardDuty mit verwenden, über die erforderlichen Berechtigungen verfügen. Um die erforderlichen Berechtigungen zu erteilen, weisen Sie diesem -Benutzer bzw. dieser-Gruppe oder -Rolle die folgende Richtlinie zu:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

Weitere Informationen zum manuellen Erstellen der Rolle finden Sie unter Erstellen einer dienstbezogenen Rolle im IAMBenutzerhandbuch.

Bearbeiten einer dienstbezogenen Rolle für Malware Protection für EC2

Mit Malware Protection for können Sie die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` dienstverknüpfte EC2 Rolle nicht bearbeiten. Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten auf die Rolle verweisen könnten. Sie können die Beschreibung der Rolle jedoch mithilfe IAM von bearbeiten. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Bearbeiten einer dienstbezogenen Rolle.

Löschen einer dienstbezogenen Rolle für Malware Protection für EC2

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird.

> **Important**
>
> Um die zu löschen`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, müssen Sie zuerst den Malware-Schutz für EC2 in allen Regionen deaktivieren, in denen er aktiviert ist.
> Wenn der Malware-Schutz für EC2 nicht deaktiviert ist, wenn Sie versuchen, die dienstbezogene Rolle zu löschen, schlägt der Löschvorgang fehl. Weitere Informationen finden Sie unter Um den GuardDuty -initiierten Malware-Scan zu aktivieren oder zu deaktivieren.

Wenn Sie „Deaktivieren“ wählen, um den Dienst „Malware-Schutz für“ zu beenden, `AWSServiceRoleForAmazonGuardDutyMalwareProtection` wird der EC2 Dienst nicht automatisch gelöscht. Wenn Sie dann „Aktivieren“ wählen, um den EC2 Dienst „Malware-Schutz für“ erneut zu starten, GuardDuty wird der vorhandene Dienst wieder verwendet`AWSServiceRoleForAmazonGuardDutyMalwareProtection`.

Um die mit dem Dienst verknüpfte Rolle manuell zu löschen, verwenden Sie IAM

Verwenden Sie die IAM Konsole, den oder AWS CLI, IAM API um die `AWSServiceRoleForAmazonGuardDutyMalwareProtection` dienstverknüpfte Rolle zu löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Löschen einer dienstbezogenen Rolle.

Unterstützt AWS-Regionen

Amazon GuardDuty unterstützt die Verwendung der `AWSServiceRoleForAmazonGuardDutyMalwareProtection` servicebezogenen Rolle in allen Bereichen, in AWS-Regionen denen Malware Protection for verfügbar EC2 ist.

Eine Liste der Regionen, in denen GuardDuty das Produkt derzeit verfügbar ist, finden Sie unter GuardDuty Amazon-Endpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz.

> **Note**
>
> Der Malware-Schutz für EC2 ist derzeit in AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) nicht verfügbar.

AWS verwaltete Richtlinien für Amazon GuardDuty

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um vom IAMKunden verwaltete Richtlinien zu erstellen, die Ihrem Team nur die Berechtigungen gewähren, die es benötigt. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste fügen einer AWS verwalteten Richtlinie gelegentlich zusätzliche Berechtigungen hinzu, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Es ist sehr wahrscheinlich, dass Dienste eine AWS verwaltete Richtlinie aktualisieren, wenn eine neue Funktion eingeführt wird oder wenn neue Operationen verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und eine Beschreibung der Richtlinien für Jobfunktionen finden Sie im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien für Jobfunktionen.

Die `Version`-Richtlinienelemente legen die Sprachsyntaxregeln fest, die für die Verarbeitung einer Richtlinie verwendet werden sollen. Die folgenden Richtlinien beinhalten die aktuelle Version, die IAM unterstützt. Weitere Informationen finden Sie unter IAMJSONRichtlinienelemente: Version.

AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess

Sie können die `AmazonGuardDutyFullAccess` Richtlinie an Ihre IAM Identitäten anhängen.

Diese Richtlinie gewährt Administratorberechtigungen, die einem Benutzer vollen Zugriff auf alle GuardDuty Aktionen gewähren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `GuardDuty`— Ermöglicht Benutzern vollen Zugriff auf alle GuardDuty Aktionen.
- `IAM`:
  - Ermöglicht Benutzern, die GuardDuty dienstbezogene Rolle zu erstellen.
  - Ermöglicht einem Administratorkonto die Aktivierung GuardDuty für Mitgliedskonten.
  - Ermöglicht es Benutzern, eine Rolle zu übergeben GuardDuty , die diese Rolle verwendet, um die Funktion GuardDuty Malware Protection for S3 zu aktivieren. Dies ist unabhängig davon, wie Sie den Malware-Schutz für S3 aktivieren — innerhalb des GuardDuty Dienstes oder unabhängig davon.
- `Organizations`— Ermöglicht Benutzern, einen delegierten Administrator zu benennen und Mitglieder für eine GuardDuty Organisation zu verwalten.

Mit der Berechtigung zum Ausführen einer `iam:GetRole` Aktion `AWSServiceRoleForAmazonGuardDutyMalwareProtection` wird festgelegt, ob die dienstbezogene Rolle (SLR) für Malware Protection for in einem Konto EC2 vorhanden ist.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "AmazonGuardDutyFullAccessSid1",
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleSid1",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "guardduty.amazonaws.com",
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "ActionsForOrganizationsSid1",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IamGetRoleSid1",
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        },
        {
            "Sid": "AllowPassRoleToMalwareProtectionPlan",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "malware-protection-
plan.guardduty.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonGuardDutyReadOnlyAccess

Sie können die `AmazonGuardDutyReadOnlyAccess` Richtlinie an Ihre IAM Identitäten anhängen.

Diese Richtlinie gewährt nur Leseberechtigungen, die es einem Benutzer ermöglichen, GuardDuty Ergebnisse und Details Ihrer Organisation einzusehen. GuardDuty

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `GuardDuty`— Ermöglicht Benutzern das Anzeigen von GuardDuty Ergebnissen und das Ausführen von API Vorgängen, die mit `GetList`, oder beginnen. `Describe`
- `Organizations`— Ermöglicht Benutzern das Abrufen von Informationen über Ihre GuardDuty Organisationskonfiguration, einschließlich Details zum delegierten Administratorkonto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:Describe*",
                "guardduty:Get*",
                "guardduty:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinie: AmazonGuardDutyServiceRolePolicy

Sie können keine Verbindungen `AmazonGuardDutyServiceRolePolicy` zu Ihren IAM Entitäten herstellen. Diese AWS verwaltete Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es GuardDuty ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Dienstbezogene Rollenberechtigungen für GuardDuty.

GuardDuty Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die GuardDuty seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS Feed auf der Seite GuardDuty Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Die `ec2:DescribeVpcs` Erlaubnis wurde hinzugefügt. Auf diese Weise können GuardDuty VPC Aktualisierungen nachverfolgt werden, z. B. das VPC CIDR Abrufen von.	22. August 2024
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Es wurde eine Berechtigung hinzugefügt, mit der Sie eine IAM Rolle übergeben können, GuardDuty wenn Sie Malware Protection for S3 aktivieren. `{ "Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow", "Action": [`	10. Juni 2024

Änderung	Beschreibung	Datum
	"iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": "guardduty.amazonaws.com" } } }	
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Verwenden Sie AWS Systems Manager Aktionen, um SSM Verknüpfungen auf EC2 Amazon-Instances zu verwalten, wenn Sie GuardDuty Runtime Monitoring mit automatisiertem Agenten für Amazon aktivieren EC2. Wenn die GuardDuty automatische Agentenkonfiguration deaktiviert ist, werden nur die EC2 Instances GuardDuty berücksichtigt, die über ein Inclusion-Tag (`GuardDutyManaged :true`) verfügen.	26. März 2024

Änderung	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	GuardDuty hat eine neue Berechtigung hinzugefügt `organization:DescribeOrganization` , um die Organisations-ID des gemeinsamen VPC Amazon-Kontos abzurufen und die VPC Amazon-Endpunktrichtlinie mit der Organisations-ID festzulegen.	9. Februar 2024
AmazonGuardDutyMalwareProtectionServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Malware Protection for EC2 hat zwei zusätzliche Berechtigungen hinzugefügt: `GetSnapshotBlock` Sie `ListSnapshotBlocks` können den Snapshot eines EBS Volumes (verschlüsselt mit Von AWS verwalteter Schlüssel) von Ihrem Volume abrufen AWS-Konto und in das GuardDuty Dienstkonto kopieren, bevor der Malware-Scan gestartet wird.	25. Januar 2024
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Neue Berechtigungen wurden hinzugefügt, um das Hinzufügen von `guardduty Activate` ECS Amazon-Kontoeinstellungen und das Ausführen von Listen- und Beschreibungsvorgängen auf ECS Amazon-Clustern zu ermöglichen GuardDuty .	26. November 2023

Änderung	Beschreibung	Datum
AmazonGuardDutyReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty hat eine neue Richtlinie für `organizations` to hinzugefügt `ListAccounts` .	16. November 2023
AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty hat eine neue Richtlinie für `organizations` to hinzugefügt `ListAccounts` .	16. November 2023
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	GuardDuty neue Berechtigungen hinzugefügt, um die kommende GuardDuty EKS Runtime Monitoring-Funktion zu unterstützen.	08. März 2023

Änderung	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	GuardDuty hat neue Berechtigungen hinzugefügt, um die Erstellung GuardDuty einer dienstbezogenen Rolle für Malware Protection for EC2 zu ermöglichen. Dies wird dazu beitragen, den Prozess der Aktivierung von Malware Protection für zu GuardDuty rationalisieren. EC2 GuardDuty kann jetzt die folgende IAM Aktion ausführen : `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	21. Februar 2023
AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty aktualisiert ARN für `iam:GetRole` bis`*AWSServiceRoleForAmazonGuardDutyMalwareProtection` .	26. Juli 2022

Änderung	Beschreibung	Datum
AmazonGuardDutyFullAccess – Aktualisierung auf eine bestehende Richtlinie	GuardDuty Es wurde eine neue hinzugefü gt`AWSServiceName` , um die Erstellung einer dienstbez ogenen Rolle mithilfe von GuardDuty Malware Protectio n `iam:CreateServiceL inkedRole` for EC2 Service zu ermöglichen. GuardDuty kann jetzt die `iam:GetRole` Aktion ausführen, für `AWSServic eRole` die Informationen abgerufen werden sollen.	26. Juli 2022

Änderung	Beschreibung	Datum
AmazonGuardDutyServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	GuardDuty neue Berechtigungen hinzugefügt, um die Nutzung von EC2 Amazon-Netzwerkaktionen zur Verbesserung der Ergebnisse zu ermöglichen GuardDuty . GuardDuty kann jetzt die folgenden EC2 Aktionen ausführen, um Informationen darüber zu erhalten, wie Ihre EC2 Instances kommunizieren. Diese Informationen werden verwendet, um die Genauigkeit der Erkenntnisse zu verbessern. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	3. August 2021
GuardDuty hat begonnen, Änderungen zu verfolgen	GuardDuty hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	3. August 2021

Fehlerbehebung Amazon GuardDuty Amazon-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit GuardDuty und auftreten könnenIAM.

Themen

Ich bin nicht berechtigt, eine Aktion durchzuführen in GuardDuty

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einer fiktiven *`my-example-widget`* Ressource anzuzeigen, aber nicht über die fiktiven `guardduty:`*`GetWidget`* Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `guardduty:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam: PassRole auszuführen.

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an GuardDuty diese Person übergeben können.

Einige AWS -Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in GuardDuty auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine GuardDuty Ressourcen ermöglichen.

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen GuardDuty unterstützt werden, finden Sie unter. So GuardDuty arbeitet Amazon mit IAM
- Informationen darüber, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM Benutzerhandbuch unter Gewähren des Zugriffs auf einen anderen IAMBenutzer AWS-Konto , der Ihnen gehört.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

Konformitätsvalidierung für Amazon GuardDuty

Informationen darüber, ob AWS -Service ein AWS -Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS -Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS -Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

  > **Note**
  >
  > Nicht alle sind berechtigt AWS -Services . HIPAA Weitere Informationen finden Sie in der Referenz für HIPAA qualifizierte Dienste.

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS -Services und die Leitlinien für Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zusammengefasst.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.

- AWS Security Hub— Auf diese AWS -Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS -Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- AWS Audit Manager— Auf diese AWS -Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Ausfallsicherheit bei Amazon GuardDuty

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und -Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und -Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Infrastruktursicherheit bei Amazon GuardDuty

Als verwalteter Service GuardDuty ist Amazon durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API Aufrufe für den Zugriff GuardDuty über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Sicherheit auf Transportschicht (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit perfekter Vorwärtsgeheimhaltung (PFS) wie (Ephemeral Diffie-Hellman) oder DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Integration von AWS Diensten mit GuardDuty

GuardDuty kann in andere AWS Sicherheitsdienste integriert werden. Diese Dienste können Daten aufnehmen GuardDuty , sodass Sie die Ergebnisse auf neue Weise betrachten können. Sehen Sie sich die folgenden Integrationsoptionen an, um mehr darüber zu erfahren, wie dieser Dienst für die Verwendung eingerichtet ist. GuardDuty

Integration GuardDuty mit AWS Security Hub

AWS Security Hub sammelt Sicherheitsdaten aus all Ihren AWS Konten, Diensten und unterstützten Produkten von Drittanbietern, um den Sicherheitsstatus Ihrer Umgebung gemäß Industriestandards und Best Practices zu bewerten. Security Hub bewertet nicht nur Ihren Sicherheitsstatus, sondern bietet auch einen zentralen Ort für Erkenntnisse aus all Ihren integrierten AWS Services und AWS Partnerprodukten. Wenn GuardDuty Sie Security Hub mit aktivieren, können GuardDuty Befunddaten automatisch von Security Hub aufgenommen werden.

Weitere Informationen zur Verwendung von Security Hub mit GuardDuty finden Sie unterIntegrieren mit AWS Security Hub.

Integration GuardDuty mit Amazon Detective

Amazon Detective verwendet Protokolldaten aus all Ihren AWS Konten, um Datenvisualisierungen für Ihre Ressourcen und IP-Adressen zu erstellen, die mit Ihrer Umgebung interagieren. Die Visualisierungen von Detective helfen Ihnen dabei, Sicherheitsprobleme schnell und einfach zu untersuchen. Sobald beide Dienste aktiviert sind, können Sie von der GuardDuty Suche nach Details zu Informationen in der Detective-Konsole wechseln.

Weitere Informationen zur Verwendung von Detective mit GuardDuty finden Sie unterIntegration mit Amazon Detective.

Integrieren mit AWS Security Hub

AWS Security Hub liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre Umgebung anhand von Sicherheitsstandards und bewährten Methoden der Branche zu überprüfen. Security Hub sammelt Sicherheitsdaten von AWS Konten, Diensten und unterstützten Partnerprodukten von Drittanbietern und hilft Ihnen dabei, Ihre Sicherheitstrends zu analysieren und die Sicherheitsprobleme mit der höchsten Priorität zu identifizieren.

Die GuardDuty Amazon-Integration mit Security Hub ermöglicht es Ihnen, Ergebnisse von an Security Hub GuardDuty zu senden. Der Security Hub kann diese Erkenntnisse dann in die Analyse Ihres Sicherheitsniveaus einbeziehen.

Inhalt

So GuardDuty sendet Amazon Ergebnisse an AWS Security Hub

AWS Security Hub In werden Sicherheitsprobleme als Ergebnisse erfasst. Einige Ergebnisse stammen aus Problemen, die von anderen AWS Diensten oder von Drittanbietern entdeckt wurden. Security Hub verwendet ebenfalls verschiedene Regeln, um Sicherheitsprobleme zu erkennen und Ergebnisse zu generieren.

Security Hub bietet Tools zur Verwaltung von Erkenntnissen aus all diesen Quellen. Sie können Listen mit Erkenntnissen anzeigen und filtern und Details zu einer Erkenntnis anzeigen. Weitere Informationen finden Sie unter Anzeigen der Erkenntnisse im AWS Security Hub -Benutzerhandbuch. Sie können auch den Status einer Untersuchung zu einer Erkenntnis nachverfolgen. Weitere Informationen finden Sie unter Ergreifen von Maßnahmen zu Erkenntnissen im AWS Security Hub -Benutzerhandbuch.

Alle Ergebnisse in Security Hub verwenden ein JSON Standardformat namens AWS Security Finding Format (ASFF). Das ASFF beinhaltet Details zur Ursache des Problems, zu den betroffenen Ressourcen und zum aktuellen Stand der Ergebnisse. Weitere Informationen finden Sie im AWS Security Hub Benutzerhandbuch unter Format für AWS Sicherheitsbefunde (ASFF).

Amazon GuardDuty ist einer der AWS Dienste, der Ergebnisse an Security Hub sendet.

Arten von Ergebnissen, die GuardDuty an Security Hub gesendet werden

Sobald Sie Security Hub in demselben Konto innerhalb desselben aktiviert GuardDuty haben AWS-Region, GuardDuty werden alle generierten Ergebnisse an Security Hub gesendet. Diese Ergebnisse werden mit dem Security Finding Format (ASFF) an AWS Security Hub gesendet. In gibt ASFF das `Types` Feld den Befundtyp an.

Latenz beim Senden neuer Ergebnisse

Wenn ein neues Ergebnis GuardDuty erstellt wird, wird es normalerweise innerhalb von fünf Minuten an Security Hub gesendet.

Wiederholen, wenn der Security Hub nicht verfügbar ist

Wenn Security Hub nicht verfügbar ist, wird GuardDuty erneut versucht, die Ergebnisse zu senden, bis sie empfangen werden.

Aktualisieren von vorhandenen Erkenntnissen in Security Hub

Nachdem es ein Ergebnis an Security Hub gesendet hat, GuardDuty sendet es Updates, um zusätzliche Beobachtungen der Findungsaktivität widerzuspiegeln, an Security Hub. Die neuen Beobachtungen dieser Ergebnisse werden basierend auf den Schritt 5 — Häufigkeit für den Export von Ergebnissen Einstellungen in Ihrem an Security Hub gesendet AWS-Konto.

Wenn Sie einen Befund archivieren oder die Archivierung aufheben, GuardDuty wird dieser Befund nicht an Security Hub gesendet. Manuell dearchivierte Ergebnisse, die später aktiv werden, werden nicht an Security Hub gesendet. GuardDuty

GuardDuty Ergebnisse anzeigen in AWS Security Hub

Um Ihre GuardDuty Ergebnisse in Security Hub einzusehen, wählen Sie auf der Übersichtsseite die Option Ergebnisse unter Amazon anzeigen GuardDuty aus. Alternativ können Sie im Navigationsbereich die Option Ergebnisse auswählen und die Ergebnisse so filtern, dass nur GuardDuty Ergebnisse angezeigt werden, indem Sie das Feld Produktname: mit dem Wert von auswählen`GuardDuty`.

Interpretieren von GuardDuty Fundnamen in AWS Security Hub

GuardDuty sendet die Ergebnisse mithilfe des Security Finding Formats (ASFF) an AWS Security Hub. In gibt ASFF das `Types` Feld den Befundtyp an. ASFFTypen verwenden ein anderes

Benennungsschema als GuardDuty Typen. In der folgenden Tabelle sind alle GuardDuty Findetypen mit ihren ASFF Gegenstücken aufgeführt, so wie sie in Security Hub erscheinen.

> **Note**
>
> Für einige GuardDuty Ergebnisarten weist Security Hub unterschiedliche Ergebnisnamen ASFF zu, je nachdem, ob die Ressourcenrolle des Ergebnisdetails ACTORoder TARGETwar. Weitere Informationen finden Sie unter Erkenntnisdetails.

GuardDuty Findetyp	ASFFTyp finden
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual

GuardDuty Findetyp	ASFFTyp finden
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:Kubernetes/MaliciousIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess
CredentialAccess:Kubernetes/TorIPCaller	TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin

GuardDuty Findetyp	ASFFTyp finden
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity

GuardDuty Findetyp	ASFFTyp finden
DefenseEvasion:IAMUser/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Kubernetes/MaliciousIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess
DefenseEvasion:Kubernetes/TorIPCaller	TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/ProcessInjection.Proc	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Proc
DefenseEvasion:Runtime/ProcessInjection.Ptrace	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Ptrace
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.VirtualMemoryWrite
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand
Entdeckung:IAMUser/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked

GuardDuty Findetyp	ASFFTyp finden
Discovery:Kubernetes/MaliciousIPCaller	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller
Discovery:Kubernetes/MaliciousIPCaller.Custom	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom
Discovery:Kubernetes/SuccessfulAnonymousAccess	TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess
Discovery:Kubernetes/TorIPCaller	TTPs/Discovery/Discovery:Kubernetes-TorIPCaller
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Exfiltration:IAMUser/AnomalousBehavior	TTPs/Exfiltration/IAMUser-AnomalousBehavior
Execution:Kubernetes/ExecInKubeSystemPod	TTPs/Execution/Execution:Kubernetes-ExecInKubeSystemPod
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed

GuardDuty Findetyp	ASFFTyp finden
Impact:Kubernetes/MaliciousIPCaller	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller
Impact:Kubernetes/MaliciousIPCaller.Custom	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom
Impact:Kubernetes/SuccessfulAnonymousAccess	TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess
Impact:Kubernetes/TorIPCaller	TTPs/Impact/Impact:Kubernetes-TorIPCaller
Persistence:Kubernetes/ContainerWithSensitiveMount	TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Persistence:Kubernetes/MaliciousIPCaller	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller
Persistence:Kubernetes/MaliciousIPCaller.Custom	TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller.Custom
Persistence:Kubernetes/SuccessfulAnonymousAccess	TTPs/Persistence/Persistence:Kubernetes-SuccessfulAnonymousAccess
Persistence:Kubernetes/TorIPCaller	TTPs/Persistence/Persistence:Kubernetes-TorIPCaller
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile

GuardDuty Findetyp	ASFFTyp finden
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousShellCreated	TTPs/Execution/Execution:Runtime-SuspiciousShellCreated
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior

GuardDuty Findetyp	ASFFTyp finden
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Wirkung:IAMUser/AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete

GuardDuty Findetyp	ASFFTyp finden
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess:IAMUser/AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
Object:S3/MaliciousFile	TTPs/Object/Object:S3-MaliciousFile
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
Beharrlichkeit:/IAMUserAnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions

GuardDuty Findetyp	ASFFTyp finden
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AdminAccessToDefaultServiceAccount
Policy:Kubernetes/AnonymousAccessGranted	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AnonymousAccessGranted
Policy:Kubernetes/ExposedDashboard	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-ExposedDashboard
Policy:Kubernetes/KubeflowDashboardExposed	Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-KubeflowDashboardExposed
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation:IAMUser/AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions

GuardDuty Findetyp	ASFFTyp finden
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleBindingCreated
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Kubernetes/PrivilegedContainer	TTPs/PrivilegeEscalation/PrivilegeEscalation:Kubernetes-PrivilegedContainer
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/ElevationToRoot	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ElevationToRoot
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller

GuardDuty Findetyp	ASFFTyp finden
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B

GuardDuty Findetyp	ASFFTyp finden
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint

GuardDuty Findetyp	ASFFTyp finden
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/UnauthorizedAccess:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS

GuardDuty Findetyp	ASFFTyp finden
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Typische Erkenntnis von GuardDuty

GuardDuty sendet Ergebnisse mithilfe des Security Finding Formats (ASFF) an AWS Security Hub.

Hier ist ein Beispiel für ein typisches Ergebnis von GuardDuty.

```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws::securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
```

```
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws::securityhub:us-east-1::product/
aws/guardduty/arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws::ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
```

```
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```


Aktivieren und Konfigurieren der Integration

Um die Integration mit verwenden zu können AWS Security Hub, müssen Sie Security Hub aktivieren. Informationen zur Aktivierung von Security Hub finden Sie unter Einrichten von Security Hub im AWS Security Hub -Leitfaden.

Wenn Sie GuardDuty sowohl als auch Security Hub aktivieren, wird die Integration automatisch aktiviert. GuardDutybeginnt sofort, Ergebnisse an Security Hub zu senden.

Verwendung von GuardDuty Steuerelementen in Security Hub

AWS Security Hub nutzt Sicherheitskontrollen, um Ihre AWS Ressourcen zu bewerten und zu überprüfen, ob Sie die Sicherheitsstandards und bewährten Verfahren der Branche einhalten. Sie können die Kontrollen verwenden, die sich auf GuardDuty Ressourcen und ausgewählte Schutzpläne beziehen. Weitere Informationen finden Sie unter Amazon GuardDuty Controls im AWS Security Hub Benutzerhandbuch.

Eine Liste aller Kontrollen für AWS Dienste und Ressourcen finden Sie im AWS Security Hub Benutzerhandbuch unter Security Hub-Steuerungsreferenz.

Einstellung der Veröffentlichung von Erkenntnissen in Security Hub

Um das Senden von Ergebnissen an Security Hub zu beenden, können Sie entweder die Security Hub Hub-Konsole oder die verwendenAPI.

Weitere Informationen finden Sie im AWS Security Hub Benutzerhandbuch unter Den Fluss von Ergebnissen aus einer Integration deaktivieren und aktivieren (Konsole) oder Den Fluss von Ergebnissen aus einer Integration deaktivieren (Security Hub API AWS CLI).

Integration mit Amazon Detective

Amazon Detective hilft Ihnen dabei, Sicherheitsereignisse in einem oder mehreren AWS Konten schnell zu analysieren und zu untersuchen, indem es Datenvisualisierungen generiert, die das Verhalten und die Interaktion Ihrer Ressourcen im Laufe der Zeit darstellen. Detective erstellt Visualisierungen von Ergebnissen. GuardDuty

Detective nimmt Erkenntnisdetails für alle Erkenntnistypen auf und bietet Zugriff auf die Entitätsprofile, um verschiedene Entitäten zu untersuchen, die an der Erkenntnis beteiligt sind. Eine Entität kann eine AWS-Konto, eine AWS Ressource innerhalb eines Kontos oder eine externe IP-Adresse sein, die mit Ihren Ressourcen interagiert hat. Die GuardDuty Konsole unterstützt das Pivotieren von den folgenden Entitäten zu Amazon Detective, je nach Findetyp: IAM Rolle AWS-Konto, Benutzer oder Rollensitzung, Benutzeragent, Verbundbenutzer, EC2 Amazon-Instance oder IP-Adresse.

Inhalt

Aktivierung der Integration

Um Amazon Detective mit verwenden zu können, müssen GuardDuty Sie zuerst Amazon Detective aktivieren. Informationen zur Aktivierung von Detective finden Sie unter Amazon Detective einrichten in der Verwaltungsanleitung für Amazon Detective.

Wenn Sie GuardDuty sowohl als auch Detective aktivieren, wird die Integration automatisch aktiviert. Nach der Aktivierung nimmt Detective Ihre GuardDuty Ergebnisdaten sofort auf.

> **Note**
>
> GuardDuty sendet Ergebnisse auf der Grundlage der Häufigkeit des Exports der GuardDuty Ergebnisse an Detective. Standardmäßig beträgt die Exporthäufigkeit für Aktualisierungen vorhandener Erkenntnisse 6 Stunden. Um sicherzustellen, dass Detective die neuesten Aktualisierungen Ihrer Ergebnisse erhält, wird empfohlen, die Exporthäufigkeit in jeder Region, in der Sie Detective verwenden, auf 15 Minuten zu ändern GuardDuty. Weitere Informationen finden Sie unter Schritt 5 — Einstellung der Häufigkeit für den Export aktualisierter aktiver Ergebnisse.

Von einem GuardDuty Befund zu Amazon Detective wechseln

1. Loggen Sie sich in die https://console.aws.amazon.com/guardduty/Konsole ein.
2. Wählen Sie eine einzelne Erkenntnis aus Ihrer Erkenntnistabelle aus.
3. Wählen Sie im Bereich mit den Erkenntnisdetails die Option Mit Detective untersuchen.
4. Wählen Sie einen Aspekt der Erkenntnis aus, den Sie mit Amazon Detective untersuchen möchten. Dadurch wird die Detective-Konsole für diese Erkenntnis oder diese Entität geöffnet.

Wenn sich der Wechsel nicht wie erwartet verhält, finden Sie weitere Informationen unter Fehlerbehebung beim Wechsel im Amazon-Detective-Benutzerhandbuch.

> **Note**
>
> Wenn Sie ein GuardDuty Ergebnis in der Detective-Konsole archivieren, wird dieses Ergebnis auch in der GuardDuty Konsole archiviert.

Verwendung der Integration in einer Umgebung mit GuardDuty mehreren Konten

Wenn Sie eine Umgebung mit mehreren Konten in verwalten GuardDuty, müssen Sie Ihre Mitgliedskonten zu Amazon Detective hinzufügen, um Detective-Datenvisualisierungen für Ergebnisse und Entitäten in diesen Konten zu sehen.

Es wird empfohlen, dasselbe GuardDuty Administratorkonto wie das Administratorkonto für Detective zu verwenden. Weitere Informationen zum Hinzufügen von Mitgliedskonten in Detective finden Sie unter Mitgliedskonten einladen.

> **Note**
>
> Detective ist ein regionaler Service, d. h. Sie müssen Detective aktivieren und Ihre Mitgliedskonten in jeder Region hinzufügen, in der Sie die Integration verwenden möchten.

Aussetzen oder Deaktivieren GuardDuty

Sie können die GuardDuty Konsole verwenden, um den GuardDuty Service auszusetzen oder zu deaktivieren. Die Nutzung wird Ihnen nicht in Rechnung gestellt GuardDuty , wenn der Dienst gesperrt ist.

- Alle Mitgliedskonten müssen getrennt oder gelöscht werden, bevor Sie sie sperren oder deaktivieren GuardDuty können.
- Wenn Sie die GuardDuty Sperre sperren, wird die Sicherheit Ihrer AWS Umgebung nicht mehr überwacht und es werden keine neuen Erkenntnisse mehr generiert. Ihre vorhandenen Ergebnisse bleiben erhalten und sind von der GuardDuty Sperrung nicht betroffen. Sie können wählen, ob Sie es GuardDuty später wieder aktivieren möchten.
- Wenn Sie es GuardDuty in einem Konto deaktivieren, wird es nur für das aktuell ausgewählte AWS-Region Konto deaktiviert. Wenn Sie es vollständig deaktivieren möchten GuardDuty, müssen Sie es in jeder Region deaktivieren, in der es aktiviert ist.
- Wenn Sie die Option deaktivieren GuardDuty, gehen Ihre vorhandenen Ergebnisse und die GuardDuty Konfiguration verloren und können nicht wiederhergestellt werden. Wenn Sie Ihre vorhandenen Ergebnisse speichern möchten, müssen Sie sie exportieren, bevor Sie die Deaktivierung bestätigen GuardDuty. Weitere Informationen zum Exportieren von Erkenntnissen finden Sie unter Exportieren von Erkenntnissen.
- Wenn Sie Malware Protection for S3 für einen oder mehrere geschützte Buckets in Ihrem Konto aktiviert haben, wirkt sich das Sperren oder Deaktivieren GuardDuty nicht auf den Status eines geschützten Buckets unter Malware Protection for S3 aus. Auch nach der Sperrung oder Deaktivierung fallen für Ihr Konto weiterhin die Nutzungskosten an GuardDuty, die mit der Funktion „Malware-Schutz für S3“ verbunden sind. Informationen zur Deaktivierung von Malware Protection for S3 finden Sie unter. Deaktivieren Sie den Malware-Schutz für S3 für einen geschützten Bucket

So sperren oder deaktivieren GuardDuty

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie im GuardDuty Abschnitt „Sperren“ die Option „ GuardDutySperren“ oder „Deaktivieren GuardDuty“ und bestätigen Sie dann Ihre Aktion.

Um die Aktivierung nach GuardDuty dem Sperren wieder zu aktivieren

1. Öffnen Sie die GuardDuty Konsole unter https://console.aws.amazon.com/guardduty/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie Erneut aktivieren. GuardDuty

SNS GuardDuty Amazon-Ankündigungen abonnieren

Dieser Abschnitt enthält Informationen zum Abonnieren von Amazon SNS (Simple Notification Service) für GuardDuty Ankündigungen zum Erhalt von Benachrichtigungen über neu veröffentlichte Befundtypen, Aktualisierungen der vorhandenen Befundtypen und andere Funktionsänderungen. Benachrichtigungen sind in allen Formaten verfügbar, die Amazon SNS unterstützt.

Der GuardDuty SNS sendet eine Ankündigung über Aktualisierungen des GuardDuty Dienstes AWS an jedes abonnierte Konto. Informationen, um Benachrichtigungen über Erkenntnisse in Ihrem Konto zu erhalten, finden Sie unter Erstellen von benutzerdefinierten Antworten auf GuardDuty Erkenntnisse mit Amazon CloudWatch Events.

> **Note**
>
> Ihr IAM Benutzer muss über `sns::subscribe` Berechtigungen verfügen, um einen SNS zu abonnieren.

Sie können eine SQS Amazon-Warteschlange für dieses Benachrichtigungsthema abonnieren, müssen jedoch ein Thema verwendenARN, das sich in derselben Region befindet. Weitere Informationen finden Sie unter Tutorial: Abonnieren einer SQS Amazon-Warteschlange für ein SNS Amazon-Thema im Amazon Simple Queue Service-Entwicklerhandbuch.

Sie können auch eine AWS Lambda Funktion verwenden, um Ereignisse auszulösen, wenn Benachrichtigungen empfangen werden. Weitere Informationen finden Sie unter Aufrufen von Lambda-Funktionen mithilfe von SNS Amazon-Benachrichtigungen im Amazon Simple Queue Service-Entwicklerhandbuch.

Die SNS ARNs Amazon-Themen für jede Region sind unten aufgeführt.

AWS Region	SNSAmazon-Thema ARN
`us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`

AWS Region	SNSAmazon-Thema ARN
us-east-2	arn:aws:sns:us-east-2:118283430703:GuardDutyAnnouncements
us-west-1	arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements
us-west-2	arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements
ca-central-1	arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements
ca-west-1	arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements
eu-north-1	arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements
eu-west-1	arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements

AWS Region	SNSAmazon-Thema ARN
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements

AWS Region	SNSAmazon-Thema ARN
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

AWS Region	SNSAmazon-Thema ARN
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

AWS Region	SNSAmazon-Thema ARN
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements

Um die GuardDuty Update-Benachrichtigungs-E-Mail im zu abonnieren AWS Management Console

1. Öffnen Sie die SNS Amazon-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie in der Regionsliste dieselbe Region wie das Thema aus, das Sie ARN abonnieren möchten. In diesem Beispiel wird die Region `us-west-2` verwendet.
3. Wählen Sie im linken Navigationsbereich Subscriptions (Abonnements) und danach Create subscription (Abonnement erstellen) aus.
4. Fügen Sie im Dialogfeld „Abonnement erstellen“ unter Thema ARN das folgende Thema einARN:`arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus. Geben Sie unter Endpoint (Endpunkt) eine E-Mail-Adresse ein, um die Benachrichtigung zu empfangen.
6. Wählen Sie Create subscription (Abonnement erstellen) aus.
7. Öffnen Sie in Ihrer E-Mail-Anwendung die Nachricht unter AWS Benachrichtigungen und klicken Sie auf den Link, um Ihr Abonnement zu bestätigen.

   Ihr Webbrowser zeigt eine Bestätigungsantwort von Amazon anSNS.

Um die GuardDuty Update-Benachrichtigungs-E-Mail mit dem zu abonnieren AWS CLI

1. Führen Sie den folgenden Befehl mit der AWS CLI aus:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Öffnen Sie in Ihrer E-Mail-Anwendung die Nachricht unter AWS Benachrichtigungen und klicken Sie auf den Link, um Ihr Abonnement zu bestätigen.

   Ihr Webbrowser zeigt eine Bestätigungsantwort von Amazon anSNS.

SNSAmazon-Nachrichtenformat

Ein Beispiel GuardDuty für eine allgemeine Benachrichtigung:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"GENERAL\",\"message\":[{\"title
\":\"Updated AmazonGuardDutyFullAccess policy\",\"body\":\"Added permission that
 allows you to pass an IAM role to GuardDuty when you enable Malware Protection for
 S3.\",\"links\":[\"https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess\"]}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:

```
{
        "version": "1",
        "type": "GENERAL",
        "message": [
            {
                "title": "Updated AmazonGuardDutyFullAccess policy",
                "body": "Added permission that allows you to pass an IAM role to
 GuardDuty when you enable Malware Protection for S3.",
                "links": [
                    "https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-
awsmanpol.html#security-iam-awsmanpol-AmazonGuardDutyFullAccess"
                ]
             }
        ]
}
```

Im Folgenden finden Sie ein Beispiel für eine GuardDuty Aktualisierungsbenachrichtigung über neue Ergebnisse:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
```

```
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:

```
{
    "version": "1",
    "type": "NEW_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

Im Folgenden finden Sie ein Beispiel für eine GuardDuty Update-Benachrichtigung über GuardDuty Funktionsupdates:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_controlplane\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
```

```
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:

```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_controlplane"
    }]
}
```

Im Folgenden finden Sie ein Beispiel für eine GuardDuty Update-Benachrichtigung über aktualisierte Ergebnisse:

```
{
    "Type": "Notification",
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
```

```
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

Die geparste Benachrichtigung (mit entfernten Escape-Zeichen) ist nachfolgend gezeigt:

```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
}
```

GuardDuty Amazon-Kontingente

Ihr AWS-Konto Land verfügt über Standardkontingente, die früher als Limits bezeichnet wurden AWS -Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Für einige Kontingente können Sie Erhöhungen beantragen, während andere Kontingente nicht erhöht werden können.

Um die Kontingente für anzuzeigen GuardDuty, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich Amazon aus AWS -Servicesund wählen Sie es aus GuardDuty.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Ihr AWS-Konto hat die folgenden Kontingente für Amazon GuardDuty pro Region.

> **Note**
>
> - Spezifische Kontingente für GuardDuty Malware Protection for EC2 finden Sie unterMalware-Schutz für Kontingente EC2.
> - Spezifische Kontingente für Malware Protection for S3 finden Sie unterKontingente im Malware-Schutz für S3.

GuardDuty Kontingente pro Region

Ressource	Standard	Kommentare
Detektoren	1	Die maximale Anzahl an Detektorr essourcen, die Sie pro AWS -Konto und Region erstellen können. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
Filter	100	Die maximale Anzahl an gespeicherten Filtern pro AWS Konto und Region. Sie können keine Erhöhung des Kontingents beantragen.
Aufbewahrungszeitraum für Ergebnisse	90 Tage	Die maximale Anzahl von Tagen, die ein Ergebnis aufbewahrt wird. Sie können keine Erhöhung des Kontingents beantragen.
IP-Adressen und CIDR-Bereiche pro Liste vertrauenswürdiger IPs	2.000	Die maximale Anzahl von IP-Adressen und CIDR-Bere ichen, die Sie in eine einzelne Liste vertrauenswürdiger IPs aufnehmen können. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
IP-Adressen und CIDR-Bereiche pro Bedrohungsliste	250 000	Die maximale Anzahl von IP-Adress- und CIDR-Bereichen, die Sie in eine Bedrohungsliste aufnehmen können. Sie können keine Erhöhung des Kontingents beantragen.
Maximale Dateigröße	35 MB	Die maximale Größe für die Datei, die verwendet wird, um eine Liste von IP-Adressen oder CIDR-Bereichen hochzuladen, die in eine Liste vertrauenswürdiger IPs oder Bedrohungsliste aufgenommen werden sollen. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
Mitgliedskonten (nach Einladung)	5000	Die maximale Anzahl von Mitgliedskonten, die einem Administr atorkonto zugeordnet sind. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Kommentare
Mitgliedskonten	50 000	Die maximale Anzahl von Mitgliedskonten, die einem Administratorkonto zugeordnet sind AWS Organizations. Dazu gehören auch Mitgliedskonten, die der Organisation auf Einladung hinzugefügt werden. Dieser Standardwert hängt von Ihrem aktuellen Kontingent für Mitgliedskonten in ab AWS Organizations. Die Anzahl der Mitgliedskonten GuardDuty , über AWS Organizations die hinzugefügt werden, darf die Anzahl der Mitgliedskonten in Ihrer Organisation nicht überschreiten. Informationen zur Anzahl von AWS-Konten in einer Organisation finden Sie unter Höchst- und Mindestwerte im AWS Organizations Benutzerhandbuch.

Ressource	Standard	Kommentare
Threat-Intelligence-Sätze	6	Die maximale Anzahl von Threat-Intelligence-Sätzen, die Sie pro AWS -Konto und Region hinzufügen können. Sie können keine Erhöhung des Kontingents beantragen.
Vertrauenswürdige IP-Sätze	1	Die maximale Anzahl vertrauenswürdiger IP-Sets, die pro AWS Konto und Region hochgeladen und aktiviert werden können. Sie können keine Erhöhung des Kontingents beantragen.

Problembehebung bei Amazon GuardDuty

Wenn Sie Probleme im Zusammenhang mit der Durchführung einer bestimmten Aktion von haben GuardDuty, lesen Sie die Themen in diesem Abschnitt.

Themen

Allgemeine Probleme in GuardDuty

Ich erhalte beim Exportieren der GuardDuty Ergebnisse einen Zugriffsfehler. Wie kann ich das beheben?

Wenn GuardDuty Sie die Einstellungen für den Export von Ergebnissen konfiguriert haben und die Ergebnisse nicht exportiert werden können, wird auf der Seite Einstellungen in der GuardDuty Konsole eine Fehlermeldung angezeigt. Dies kann möglicherweise passieren, wenn GuardDuty Sie nicht mehr auf die Zielressource zugreifen können, z. B. wenn Ihr Amazon S3 S3-Bucket gelöscht oder die Zugriffsberechtigung für den Bucket geändert wurde. Dies kann möglicherweise auch passieren, wenn GuardDuty Sie nicht mehr auf den AWS KMS Schlüssel zugreifen können, der zur Verschlüsselung der Daten in Ihrem Amazon S3 S3-Bucket verwendet wurde. Wenn der Export nicht möglich GuardDuty ist, sendet es eine Benachrichtigung an die mit dem Konto verknüpfte E-Mail-Adresse mit Informationen zu diesem Problem.

Um das Problem zu lösen, stellen Sie sicher, dass die entsprechenden Ressourcen vorhanden sind und GuardDuty über die erforderlichen Zugriffsrechte verfügen. Wenn Sie das Problem nicht vor Ablauf der 90-tägigen Aufbewahrungsfrist für Ergebnisse lösen GuardDuty, werden Ihre Ergebnisse nicht exportiert. GuardDuty deaktiviert die Suche nach Exporteinstellungen für dieses Konto in der jeweiligen Region. Auch nach Ablauf dieses Aufbewahrungsdatums können Sie die Konfigurationseinstellungen aktualisieren, um den Export der Ergebnisse in der jeweiligen Region wieder aufzunehmen.

Weitere Informationen finden Sie unter Exportieren von Erkenntnissen.

Malware-Schutz bei EC2-Problemen

Ich initiiere einen Malware-Scan auf Abruf, der jedoch zu einem Fehler wegen fehlender erforderlicher Berechtigungen führt.

Wenn Sie eine Fehlermeldung erhalten, die darauf hindeutet, dass Sie nicht über die erforderlichen Berechtigungen verfügen, um einen Malware-Scan auf Abruf auf einer Amazon-EC2-Instance zu starten, überprüfen Sie, ob Sie Ihrer IAM-Rolle die AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess-Richtlinie angefügt haben.

Wenn Sie Mitglied einer AWS Organisation sind und immer noch dieselbe Fehlermeldung erhalten, stellen Sie eine Verbindung mit Ihrem Verwaltungskonto her. Weitere Informationen finden Sie unter AWS Organizations SCP— Zugriff verweigert.

Ich erhalte bei der Arbeit mit Malware Protection for EC2 eine **`iam:GetRole`** Fehlermeldung.

Wenn Sie diesen Fehler erhalten —`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`, bedeutet das, dass Sie nicht berechtigt sind, entweder den GuardDuty -initiierten Malware-Scan zu aktivieren oder den On-Demand-Malware-Scan zu verwenden. Stellen Sie sicher, dass Sie die AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess-Richtlinie Ihrer IAM-Rolle angehängt haben.

Ich habe ein GuardDuty Administratorkonto und muss den GuardDuty -initiierten Malware-Scan aktivieren, verwende aber keine AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess zur Verwaltung. GuardDuty

- Konfigurieren Sie die IAM-Rolle, die Sie mit verwenden, so, dass Sie über die erforderlichen Berechtigungen verfügen, GuardDuty um den GuardDuty -initiierten Malware-Scan zu aktivieren. Weitere Informationen zu den erforderlichen Berechtigungen finden Sie unter Eine serviceverknüpfte Rolle für Malware Protection for EC2 erstellen.
- Fügen Sie die AWS verwaltete Richtlinie: AmazonGuardDutyFullAccess an Ihre IAM-Rolle an. Auf diese Weise können Sie den GuardDuty -initiierten Malware-Scan für die Mitgliedskonten aktivieren.

Probleme mit der Laufzeitüberwachung

Mein AWS Step Functions Workflow schlägt unerwartet fehl

Wenn der GuardDuty Container zum Workflow-Fehler beigetragen hat, finden Sie weitere Informationen unterFehlerbehebung bei Abdeckungsproblemen. Wenn das Problem weiterhin besteht, führen Sie einen der folgenden Schritte aus, um zu verhindern, dass der Workflow aufgrund des GuardDuty Containers fehlschlägt:

- Fügen Sie das `false` Tag`GuardDutyManaged`: zum zugehörigen Amazon ECS-Cluster hinzu.
- Deaktivieren Sie die automatische Agentenkonfiguration für AWS Fargate (nur ECS) auf Kontoebene. Fügen Sie das Inclusion-Tag`GuardDutyManaged`: `true` zu dem zugehörigen Amazon ECS-Cluster hinzu, den Sie mit dem GuardDuty automatisierten Agenten weiter überwachen möchten.

Fehlerbehebung bei Speichermangel in Runtime Monitoring (nur Amazon EC2-Support)

In diesem Abschnitt werden die Schritte zur Problembehebung beschrieben, wenn der Fehler „Nicht genügend Arbeitsspeicher“ auftritt, basierend auf dem Problem, den GuardDuty Security Agent manuell CPUund Speicherlimit zu installieren.

Wenn der GuardDuty Agent aufgrund des `out-of-memory` Problems `systemd` beendet wird und Sie der Meinung sind, dass es sinnvoll ist, dem GuardDuty Agenten mehr Speicher zur Verfügung zu stellen, können Sie das Limit aktualisieren.

1. Öffnen `/lib/systemd/system/amazon-guardduty-agent.service` Sie mit der Root-Berechtigung.
2. Suchen Sie `MemoryLimit` nach und und aktualisieren Sie beide Werte. `MemoryMax`

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. Starten Sie den GuardDuty Agenten nach dem Aktualisieren der Werte neu, indem Sie den folgenden Befehl verwenden:

```
sudo systemctl daemon-reload
```

```
sudo systemctl restart amazon-guardduty-agent
```

4. Führen Sie den folgenden Befehl aus, um den Status anzuzeigen:

```
sudo systemctl status amazon-guardduty-agent
```

In der erwarteten Ausgabe wird das neue Speicherlimit angezeigt:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Probleme mit der Verwaltung mehrerer Konten

Ich möchte mehrere Konten verwalten, benötige aber keine AWS Organizations Verwaltungsberechtigung.

Wenn Sie diese Fehlermeldung erhalten —`The request failed because you do not have required AWS Organization master permission.`, bedeutet das, dass Sie nicht berechtigt sind, den GuardDuty -initiierten Malware-Scan für mehrere Konten in Ihrer Organisation zu aktivieren. Weitere Informationen zur Erteilung von Berechtigungen für das Verwaltungskonto finden Sie unterEinrichtung eines vertrauenswürdigen Zugriffs zur Aktivierung des GuardDuty -initiierten Malware-Scans.

Fehlerbehebung bei anderen Problemen

Wenn Sie kein geeignetes Szenario für Ihr Problem finden, sehen Sie sich die folgenden Optionen zur Fehlerbehebung an:

- Informationen zu allgemeinen IAM-Problemen beim Zugriff auf https://console.aws.amazon.com/guardduty/ finden Sie unter Fehlerbehebung Amazon GuardDuty Amazon-Identität und -Zugriff.
- Informationen zu Authentifizierungs- und Autorisierungsproblemen beim Zugriff AWS AWS Console Home finden Sie unter Problembehandlung bei IAM.

Regionen und Endpunkte

Informationen darüber, AWS-Regionen wo Amazon verfügbar GuardDuty ist, finden Sie unter GuardDuty Amazon-Endpunkte in der Allgemeine Amazon Web Services-Referenz.

Wir empfehlen Ihnen, alle unterstützten GuardDuty AWS-Regionen Optionen zu aktivieren. Auf diese Weise können GuardDuty auch in Regionen, die Sie nicht aktiv nutzen, Erkenntnisse über unbefugte oder ungewöhnliche Aktivitäten generiert werden. Auf diese Weise können GuardDuty auch AWS CloudTrail Ereignisse für die unterstützten Länder überwacht werden. Die Fähigkeit AWS-Regionen, Aktivitäten zu erkennen, die globale Dienste betreffen, ist eingeschränkt.

Verfügbarkeit regionsspezifischer Feature

Eine Liste mit regionalen Unterschieden zur Angabe der Verfügbarkeit von GuardDuty Funktionen.

ListFindings und GetFindingsStatistics APIs

Die ListFindingsAPIs GetFindingsStatisticsund haben ein temporäres `consoleOnly` Flag. Wenn Sie eine oder beide dieser APIs verwenden, bedeutet das `consoleOnly` Flag, dass die API Ergebnisse bis zu einer Höchstgrenze von 1000 abrufen kann.

GuardDuty Funktionen mit regionalen Unterschieden

Malware-Schutz für EC2

GuardDuty unterstützt die Funktion Malware Protection for EC2 in den AWS Dedicated Local Zones.

Allgemeine API-Unterstützung

Die folgenden APIs in der Amazon GuardDuty API-Referenz können regionale Unterschiede aufweisen, da einige der zuvor angegebenen AWS-Regionen Datenquellen oder Funktionen nicht verfügbar sind:

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector
- GetMemberDetectors

- DescribeOrganizationConfiguration

Amazon-EC2-Erkenntnistypen – DefenseEvasion:EC2/UnusualDoHActivity und DefenseEvasion:EC2/UnusualDoTActivity

Die folgende Tabelle zeigt, AWS-Regionen wo verfügbar GuardDuty ist, aber diese beiden Amazon EC2-Suchttypen werden noch nicht unterstützt.

AWS-Region	Regionscode
Asien-Pazifik (Seoul)	ap-northeast-2
Asien-Pazifik (Osaka)	ap-northeast-3
Asien-Pazifik (Jakarta)	ap-southeast-3

AWS GovCloud (US) Regionen

Aktuelle Informationen finden Sie unter Amazon GuardDuty im AWS GovCloud (US) Benutzerhandbuch.

Regionen Chinas

Aktuelle Informationen finden Sie unter Verfügbarkeit von Features und Unterschiede bei der Implementierung.

GuardDuty Legacy-Aktionen und Parameter

Amazon GuardDuty hat einige API-Aktionen und -Parameter als veraltet eingestuft, unterstützt sie aber weiterhin. Es hat sich bewährt, die neuen API-Aktionen und -Parameter zu verwenden, die die alten Optionen ersetzen. Die folgende Tabelle vergleicht die alten und neuen Aktionen und Parameter.

Ältere Aktionen/ Parameter	Ältere Aktionen/Parameter	Vergleich
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Bei derselben Implementierung in beiden Aktionen wird der Begriff `Administrator` in GuardDuty verwendet. `DisassociateFromAdministratorAccount`
`autoEnable` Parameter in DescribeOrganizationConfigurationund UpdateOrganizationConfiguration	`autoEnableOrganizationMembers`	Mit `autoEnableOrganizationMembers` kann das GuardDuty Administratorkonto GuardDuty für alle Mitgliedskonten einen der Werte prüfen und durchsetzen. Bei der Verwendung von APIs kann die Aktualisierung der Konfiguration aller Mitgliedskonten bis zu 24 Stunden dauern. Weitere Informationen zu den möglichen Werten des `autoEnableOrganizationMembers` Felds finden Sie unter autoEnableOrganizationMitglieder
`dataSources` - Parameter in den APIs, die in GuardDuty APIÄnderungen	`features`	Ab März 2023 können Sie die neuen GuardDuty Schutzpläne konfigurieren GuardDuty Malware-Schutz für EC2 und verwenden`features`. Die vor März 2023 eingeführten Schutzpläne, einschließlich Malware Protectio

Ältere Aktionen/ Parameter	Ältere Aktionen/Parameter	Vergleich
im März 2023 aufgeführt sind.		n for EC2, unterstützen weiterhin die Konfiguration mithilfe von`dataSourc es` . Wenn Sie APIs verwenden, um einen Schutzplan zu konfigurieren, kann jede API-Anfrage entweder `dataSources` oder `features` beinhalten, aber nicht beide.

Dokumentenverlauf für Amazon GuardDuty

In der folgenden Tabelle werden wichtige Änderungen an der Dokumentation seit der letzten Version des GuardDuty Amazon-Benutzerhandbuchs beschrieben. Um über Aktualisierungen dieser Dokumentation informiert zu werden, können Sie einen RSS Feed abonnieren.

Änderung	Beschreibung	Datum
Die GuardDuty serviceverknüpfte Rolle () SLR wurde aktualisiert	GuardDuty hat das aktualisiertSLR, um die `ec2:Describe:Vpcs` Erlaubnis in die EC2 Amazon-Aktionen aufzunehmen. Weitere Informationen finden Sie unter Servicebezogene Rollenberechtigungen für GuardDuty.	22. August 2024
Signifikante Ergänzung des Inhalts	GuardDuty der Funktion „Malware-Schutz für S3“ wurden wichtige Inhaltsaktualisierungen hinzugefügt. • Es wurden neue Beispiele für ein Beispielbenachrichtigungsschema hinzugefügt, um EventBridge Amazon-Regeln für den Empfang von Benachrichtigungen in Bezug auf den Ressourcenstatus des Malware-Schutzplans und das Ergebnis des S3-Objektscans einzurichten. Weitere Informationen finden Sie unter Überwachung von S3-Objektscans mit Amazon EventBridge.	20. August 2024

	• Es wurden Informationen zur Behebung von Fehlern bei S3-Objekten nach dem Scannen von Tags hinzugefügt.	
Aktualisierte Funktionen in GuardDuty Runtime Monitoring - Amazon EC2	Runtime Monitoring hat eine neue Agentenversion 1.3.0 für EC2 Amazon-Ressourcen veröffentlicht. Weitere Informationen zu den Versionshinweisen finden Sie unter GuardDuty Security Agent for Amazon EC2.	19. August 2024
Aktualisierte Funktionen in GuardDuty Runtime Monitoring - Amazon EKS	Runtime Monitoring hat eine neue Agentenversion 1.7.0 für EKS Amazon-Ressourcen veröffentlicht. Weitere Informationen zu den Versionshinweisen finden Sie unter GuardDuty Security Agent for Amazon EKS Clusters.	17. August 2024
Signifikante Ergänzung des Inhalts	GuardDuty neue Informationen zur Malware-Erkennungsmethodik und zu den Scan-Engines hinzugefügt, die für die EC2 Funktionen Malware Protection for S3 und Malware Protection for verwendet werden. Weitere Informationen finden Sie unter Scan-Engine zur GuardDuty Malware-Erkennung.	15. August 2024

Neue Funktion — Schutz von KI-Workloads	GuardDuty Die grundlegende Bedrohungserkennung und Lambda Protection helfen Ihnen dabei, Bedrohungen für KI-Workloads, auf denen aufbaut, besser zu schützen und zu erkennen. AWS Weitere Informationen finden Sie unter Schutz von KI-Workloads mit. GuardDuty	14. August 2024
Aktualisierte Funktionalität in GuardDuty Runtime Monitoring — Fargate (ECSnur Amazon)	Runtime Monitoring hat eine neue Agentenversion 1.3.0 für Ressourcen AWS Fargate (ECSnur Amazon) veröffentlicht. Weitere Informationen zu den Versionshinweisen finden Sie unter GuardDuty Security Agent for Fargate- ECS.	9. August 2024
Aktualisierte Funktionalität — Malware-Schutz für S3	GuardDuty Malware Protection for S3 erhöht das Kontingent für die maximale Anzahl von S3-Buckets von 10 auf 25 Buckets. Dieses Kontingent gilt für jeweils einen AWS-Konto . AWS-Region Weitere Informationen finden Sie unter Malware-Schutz für S3.	8. August 2024

Aktualisiert — Neue Findetypen in Runtime Monitoring	GuardDuty hat zwei neue Findetypen für Runtime Monitoring hinzugefügt, mit deren Hilfe Sie Bedrohungen erkennen können, bei denen verdächtige Shells auf der überwachten Ressource erstellt werden, sowie durch Rechteeskalation, bei der ein Prozess seine Rechte verdächtig auf Root-Rechte erhöht. • Execution:Runtime/SuspiciousShellCreated • PrivilegeEscalation:Runtime/ElevationToRoot	6. August 2024
Aktualisiert — Integration mit AWS Security Hub	AWS Security Hub bietet eine Liste von GuardDuty Sicherheitskontrollen, mit denen Sie Ihre Ressourcen bewerten und überprüfen können, ob Sie die Sicherheitsstandards und bewährten Verfahren der Branche einhalten. Weitere Informationen finden Sie unter Verwenden von GuardDuty Steuerelementen in Security Hub.	11. Juli 2024

Das GuardDuty Tester-Skript für die Ergebnisse wurde aktualisiert	GuardDuty unterstützt jetzt über 100 Ergebnisse mit unterschiedlichen AWS Ressourcen in einem speziellen Konto. Verwenden Sie das `amazon-guardduty-tester` Repository und folgen Sie den Schritten, um die Ergebnisse zu testen und zu überprüfen, um die Ergebnisse zu verstehen. Weitere Informationen finden Sie unter GuardDuty Ergebnisse in speziellen Konten testen.	28. Juni 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat einen neuen Security Agent Version 1.2.0 für die EC2 Amazon-Ressource veröffentlicht. Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für EC2 Amazon-Instance. Informationen zur manuellen Aktualisierung des Security Agents auf diese Release-Version finden Sie unter Manuelles Verwalten des Security Agents für EC2 Amazon-Instance.	13. Juni 2024

Neue Funktion — Verfügbarkeit des Malware-Schutzes für die S3-Region	GuardDuty Malware Protection for S3 ist jetzt in allen kommerziellen Regionen verfügbar, in denen GuardDuty es verfügbar ist. Mit dieser Funktion können Sie neu in Amazon S3 S3-Buckets hochgeladene Objekte auf potenzielle Malware und verdächtige Uploads überprüfen und Maßnahmen ergreifen, um sie zu isolieren, bevor sie in nachgelagerte Prozesse aufgenommen werden. Informationen zur Aktivierung von Malware Protection for S3 finden Sie unter GuardDuty Malware Protection for S3.	12. Juni 2024

Neue Funktion — Malware-Schutz für S3	GuardDuty kündigt die allgemeine Verfügbarkeit von Malware Protection for S3 an, mit dessen Hilfe Sie neu in Amazon S3 S3-Buckets hochgeladene Objekte auf potenzielle Malware und verdächtige Uploads überprüfen und Maßnahmen ergreifen können, um sie zu isolieren, bevor sie in nachgelagerte Prozesse aufgenommen werden. Diese Funktion wird vollständig verwaltet von. AWS GuardDuty veröffentlicht das Ergebnis des S3-Objekt scans in Ihrem EventBridge Standard-Event-Bus. Sie können zulassen GuardDuty , dass Ihren gescannten S3-Objekten Tags hinzugefügt werden. Sie können nachgelagerte Workflows erstellen, z. B. die Isolierung eines Quarantäne-Buckets, oder Bucket-Richtlinien mithilfe von Tags definieren, die verhindern, dass Benutzer oder Anwendungen auf bestimmte Objekte zugreifen. Weitere Informationen finden Sie unter GuardDuty Malware-Schutz für S3. Derzeit ist es in den folgenden Regionen verfügbar:	11. Juni 2024

	• USA Ost (Nord-Virginia) • USA Ost (Ohio) • USA West (Oregon) • Europa (Irland) • Europa (Frankfurt) • Europa (Stockholm) • Asien-Pazifik (Sydney) • Asien-Pazifik (Tokio) • Asien-Pazifik (Singapur)	
Aktualisierte AmazonGuardDutyFullAccess Richtlinie	Es wurde eine Berechtigung hinzugefügt, mit der Sie eine IAM Rolle übergeben können, GuardDuty wenn Sie Malware Protection for S3 aktivieren. Weitere Informationen zu diesem Richtlinienupdate finden Sie unter GuardDuty Updates für AWS verwaltete Richtlinien.	10. Juni 2024

Die Funktionalität in GuardDuty RDS Protection wurde aktualisiert	RDSProtection erweitert die Unterstützung für die Überwachung der Anmeldeaktivitäten in Ihren RDS für SQL Postgre-Datenbanken. Im Rahmen dieser Erweiterung beginnt GuardDuty automatisch die Überwachung der Anmeldedaten RDS für SQL Postgre-Datenbanken für Konten, für die Protection bereits aktiviert wurde GuardDuty RDS. Weitere Informationen finden Sie unter RDSSchutz.	6. Juni 2024
Aktualisierte Funktionalität in GuardDuty Runtime Monitoring — Fargate (ECSnur Amazon)	Runtime Monitoring hat eine neue Agentenversion 1.2.0 für Ressourcen AWS Fargate (ECSnur Amazon) veröffentlicht. Weitere Informationen zu den Versionshinweisen finden Sie unter GuardDuty Security Agent for Fargate- ECS.	31. Mai 2024

Aktualisierte Funktionalität im GuardDuty Malware-Schutz für EC2	Für jedes EBS Amazon-Volume, das an Ihre EC2 Amazon-Instances und Container-Workloads angehängt ist, EC2 hat GuardDuty Malware Protection for die Größe des zu EBS scannenden Volumes auf bis zu 2048 GB erhöht. Informationen zum Scannen von EBS Amazon-Volumes, die an Ihre Instances angehängt sind, finden Sie unter GuardDuty Malware-Schutz für EC2.	29. Mai 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring for Amazon ECS — Fargate-Ressourcen unterstützen jetzt die Erkennung potenzieller Bedrohungen für Ihre von AWS Batch und gestarteten Aufgaben. AWS CodePipeline Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring with Fargate (ECSnur Amazon).	28. Mai 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.6.1 für EKS Amazon-Ressourcen veröffentlicht. Informationen zu den Versionshinweisen finden Sie in der Versionshistorie des EKS Add-On-Agenten.	14. Mai 2024

Erweiterte Regionsunterstützung für Runtime Monitoring	GuardDuty erweitert die Unterstützung für Runtime Monitoring auf die Region Canada West (Calgary) . Informationen zu den ersten Schritten mit Runtime Monitoring finden Sie unter Runtime Monitoring aktivieren.	7. Mai 2024
Erweiterte Unterstützung für RDS Schutzmaßnahmen in der Region	GuardDuty erweitert die RDS Protection-Unterstützung auf Folgendes AWS-Regionen: • Kanada West (Calgary) • Asien-Pazifik (Hyderabad) • Europa (Spain) • Europa (Zürich) • Naher Osten (UAE) • Israel (Tel Aviv) • Asien-Pazifik (Melbourne) Informationen zur Aktivierung dieser Funktion finden Sie unter RDSSchutz.	3. Mai 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.1.0 für Ressourcen AWS Fargate (ECSnur Amazon) veröffentlicht. Weitere Informationen zu den Versionshinweisen finden Sie unter GuardDuty Security Agent for Fargate- ECS.	1. Mai 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.6.0 für EKS Amazon-Ressourcen veröffentlicht. Informationen zu den Versionshinweisen finden Sie in der Versionshistorie des EKS Add-On-Agenten.	29. April 2024
Support für IPAddressv6	GuardDuty hat IPAddressv6 Unterstützung für lokale und Remote-IP-Details hinzugefügt. Sie können die zugehörigen Filterattribute verwenden, um GuardDuty Ergebnisse zu filtern oder Unterdrückungsregeln zu erstellen.	18. April 2024
Die Konsolenoberfläche wurde aktualisiert, um den Export von Ergebnissen zu konfigurieren	GuardDuty hat die Konsolenoberfläche aktualisiert, sodass die in Ihrem AWS-Konten generierten Ergebnisse in einen Amazon S3 S3-Bucket exportiert werden. Weitere Informationen finden Sie unter GuardDuty Ergebnisse exportieren.	1. April 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat einen neuen Security Agent Version 1.1.0 für die EC2 Amazon-Ressource veröffentlicht. Diese Version unterstützt die GuardDuty automatische Agentenkonfiguration in Runtime Monitoring für EC2 Amazon-Instances. Informationen zu Versionshinweisen finden Sie unter GuardDuty Security Agent für EC2 Amazon-Instance.	28. März 2024

Allgemeine Verfügbarkeit von Runtime Monitoring für EC2 Amazon-Instances	GuardDuty kündigt die allgemeine Verfügbarkeit (GA) von Runtime Monitoring für EC2 Amazon-Instances an. Jetzt haben Sie die Möglichkeit, die automatische Agentenkonfiguration zu aktivieren, mit der GuardDuty Sie den Security Agent für Ihre EC2 Amazon-Instances in Ihrem Namen installieren und verwalten können. Mit dem GuardDuty automatisierten Agenten können Sie auch Inklusions- oder Ausschluss-Tags verwenden, um Sie darüber GuardDuty zu informieren, dass der Security Agent nur auf ausgewählten EC2 Amazon-Instances installiert und verwaltet werden soll. Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring mit EC2 Amazon-Instances. Liste der neuen Findetypen, die zusammen mit dieser GA veröffentlicht wurden • Ausführung: Runtime/SuspiciousTool • Ausführung: Runtime/SuspiciousCommand	28. März 2024

- DefenseEvasionAusführung: Runtime/ ----SEP----:Runtime/ SuspiciousCommand
- DefenseEvasion:Runtime/ ----SEP----:Runtime/ PtraceAntiDebugging
- Ausführung: Runtime/ MaliciousFileExecuted

Amazon GuardDuty hat die mit dem Service verknüpfte Rolle aktualisiert () SLR	Verwenden Sie AWS Systems Manager Aktionen, um SSM Verknüpfungen auf EC2 Amazon-Instances zu verwalten, wenn Sie GuardDuty Runtime Monitoring mit automatisiertem Agenten für Amazon aktivieren EC2. Wenn die GuardDuty automatische Agentenkonfiguration deaktiviert ist, werden nur die EC2 Instances GuardDuty berücksichtigt, die über ein Inclusion-Tag (`GuardDutyManaged :true`) verfügen. • Die folgende Liste zeigt die neuen Berechtigungen: `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	26. März 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	Mit der neuesten Version des GuardDuty Security Agents (Add-on) v1.5.0 für Amazon EKS unterstützt Runtime Monitoring jetzt die Konfiguration bestimmter Parameter Ihres GuardDuty Security Agents, wie CPU z. B. Speichereinstellungen, `PriorityClass` Einstellungen und DNS Richtlinieneinstellungen. Weitere Informationen finden Sie unter Konfiguration der Parameter des GuardDuty Security Agents (EKSAdd-on).	7. März 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.5.0 für EKS Amazon-Ressourcen veröffentlicht. Informationen zu den Versionshinweisen finden Sie in der Versionshistorie des EKS Add-On-Agenten.	7. März 2024
Support für Canada West (Calgary)	Amazon GuardDuty ist jetzt in der Region Kanada West (Calgary) verfügbar. Einige der darin enthaltenen Schutzpläne sind in dieser Region GuardDuty möglicherweise nicht verfügbar. Die neuesten Informationen finden Sie unter Regionen und Endpunkte.	6. März 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	Die GuardDuty Security Agent-Versionen 1.0.0 und 1.1.0 für EKS Amazon-Cluster werden ab dem 14. Mai 2024 nicht mehr unterstützt. Informationen darüber, welche Schritte Sie vor Ablauf des Standard-Supports ergreifen können, finden Sie unter GuardDuty Security Agent for Amazon EKS Clusters.	16. Februar 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring unterstützt die neueste Kubernetes-Version 1.29 mit der vorhandenen Security Agent-Version 1.4.1. Die Unterstützung ist seit dem Start dieser Kubernetes-Version verfügbar. Informationen zu den unterstützten Kubernetes-Versionen finden Sie unter Vom Security Agent unterstützte Kubernetes-Versionen. GuardDuty	16. Februar 2024

Aktualisierte Funktionalität in Runtime Monitoring — Regionale Verfügbarkeit	GuardDuty Runtime Monitoring unterstützt jetzt gemeinsam genutztes Amazon VPC innerhalb desselben AWS Organizations. GuardDuty Die serviceverknüpfte Rolle (SLR) hat eine neue Berechtigung — `organizations:DescribeOrganization` sie hilft beim Abrufen der Organisations-ID für das gemeinsame VPC Amazon-Konto, um die Endpunktrichtlinie festzulegen. Informationen zu den Voraussetzungen für die Verwendung eines gemeinsamen VPC Amazon-Endpunkts in Runtime Monitoring finden Sie unter Support für gemeinsam genutzten Amazon VPC. Diese Funktion ist in allen Regionen verfügbar, in denen Runtime Monitoring GuardDuty unterstützt wird.	12. Februar 2024

Aktualisierte Funktionalität in Runtime Monitoring — Regionale Verfügbarkeit	GuardDuty Runtime Monitoring unterstützt jetzt gemeinsam genutztes Amazon VPC innerhalb desselben AWS Organizations. GuardDuty Die serviceverknüpfte Rolle (SLR) hat eine neue Berechtigung — `organizations:DescribeOrganization` sie hilft beim Abrufen der Organisations-ID für das gemeinsame VPC Amazon-Konto, um die Endpunktrichtlinie festzulegen. Informationen zu den Voraussetzungen für die Verwendung eines gemeinsamen VPC Amazon-Endpunkts in Runtime Monitoring finden Sie unter Support für gemeinsam genutzten Amazon VPC. Derzeit ist diese Funktion in einigen der AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Regionen und Endpunkte.	9. Februar 2024
Aktualisierte Funktionalität mit Unterstützung für neue Funktionen AWS-Regionen — Malware-Schutz für EC2	Der Malware-Schutz unterstützt EC2 derzeit das Scannen von verschlüsselten EBS Volumes Von AWS verwaltete Schlüssel in der Region USA West (Oregon).	6. Februar 2024

Aktualisierte Funktionalität mit Unterstützung für neue Funktionen AWS-Regionen — Malware-Schutz für EC2	Der Malware-Schutz unterstützt EC2 ab sofort das Scannen von EBS Volumes, die mit folgenden Von AWS verwaltete Schlüssel Verschlüsselungen verschlüsselt wurden AWS-Regionen: • Asien-Pazifik (Singapur) (`ap-southeast-1`) • Europa (Frankfurt) (`eu-central-1`) • Asien-Pazifik (Osaka) (`ap-northeast-3`) • USA Ost (Ohio) (`us-east-2`) • Europa (Mailand) (`eu-south-1`) • Asien-Pazifik (Tokio) (`ap-northeast-1`) • Asien-Pazifik (Seoul) (`ap-northeast-2`) • Kanada (Zentral) (`ca-central-1`) • Europa (Irland) (`eu-west-1`) • USA Ost (Nord-Virginia) (`us-east-1`)	5. Februar 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	GuardDuty Runtime Monitoring hat eine neue Version des GuardDuty Security Agents (v1.0.2) für EC2 Amazon-Instances veröffentlicht. Diese Agentenversion beinhaltet Unterstützung für die neueste Version von Amazon ECSAMIs. Weitere Informationen zum Versionsverlauf von Agenten finden Sie unter GuardDuty Sicherheitsagent für EC2 Amazon-Instances.	2. Februar 2024

Aktualisierte Funktionalität mit Unterstützung für neue Funktionen AWS-Regionen — Malware-Schutz für EC2	Malware Protection unterstützt EC2 derzeit das Scannen von EBS Amazon-Volumes, die wie folgt verschlüsselt sind AWS-Regionen: Von AWS verwaltete Schlüssel • Europa (London) (`eu-west-2`) • Europa (Stockholm) (`eu-north-1`) • Asien-Pazifik (Hongkong) (`ap-east-1`) • Afrika (Kapstadt) (`af-south-1`) • Naher Osten (Bahrain) (`me-south-1`) • Asien-Pazifik (Hyderabad) (`ap-south-2`) • Europa (Spanien) (`eu-south-2`) • Asien-Pazifik (Melbourne) (`ap-southeast-4`) • Asien-Pazifik (Sydney) (`ap-southeast-2`) • Israel (Tel Aviv) (`il-central-1`)	31. Januar 2024

Die Verwaltung von Konten wurde aktualisiert mit AWS Organizations	Der Inhalt unter Konten verwalten mit AWS Organizations wurde neu organisiert. , fügte Schritte zum Ändern des delegierten GuardDuty Administratorkontos hinzu und aktualisierte Informationen zur Beziehung zwischen GuardDuty Administratorkonto und Mitgliedskonten.	30. Januar 2024
Aktualisierte Funktionalität mit Unterstützung für neue AWS-Regionen	Der Malware-Schutz unterstützt EC2 derzeit das Scannen von EBS Volumes, die wie folgt verschlüsselt sind AWS-Regionen: Von AWS verwaltete Schlüssel • Asien-Pazifik (Jakarta) (`ap-southeast-3`) • USA West (Nordkalifornien) (`us-west-1`) • Naher Osten (UAE) (`me-central-1`) • Europa (Zürich) (`eu-central-2`) • Asien-Pazifik (Mumbai) (`ap-south-1`) • Südamerika (São Paulo) (`sa-east-1`)	29. Januar 2024

Aktualisierte Funktionalität im Malware-Schutz für EC2	Der Malware-Schutz unterstützt EC2 derzeit das Scannen von EBS Volumes, die mit verschlüsselt wurden Von AWS verwaltete Schlüssel . Die Rolle „Malware-Schutz für EC2 dienstbezogene“ (SLR) verfügt über zwei neue Berechtigungen — `GetSnapshotBlock` und`ListSnapshotBlocks` . Diese Berechtigungen helfen dabei, den Snapshot eines EBS Volumes (verschlüsselt mit Von AWS verwalteter Schlüssel) von Ihrem GuardDuty abzurufen AWS-Konto und ihn in das GuardDuty Dienstkonto zu kopieren, bevor der Malware-Scan gestartet wird. Derzeit ist diese Funktion nur in Europa (Paris) (`eu-west-3`) verfügbar. Weitere Informationen finden Sie unter Unterstützte Volumes für den Malware-Scan.	25. Januar 2024

Die Funktionalität in Runtime Monitoring wurde aktualisiert	GuardDuty Runtime Monitoring hat eine neue Version des GuardDuty Security Agents (v1.0.1) mit allgemeiner Leistungsoptimierung und Verbesserungen veröffentlicht. Weitere Informationen zum Versionsverlauf von Agenten finden Sie unter GuardDuty Sicherheitsagent für EC2 Amazon-Instances.	23. Januar 2024
Die Funktionalität in Runtime Monitoring wurde aktualisiert	Runtime Monitoring hat eine neue Agentenversion 1.4.1 für EKS Amazon-Ressourcen veröffentlicht. Weitere Informationen finden Sie in der Versionshistorie des EKS Add-On-Agenten.	16. Januar 2024
Runtime Monitoring hat den neuen Agenten v1.4.0 für EKS Amazon-Ressourcen veröffentlicht	Runtime Monitoring hat eine neue Agentenversion 1.4.0 für EKS Amazon-Ressourcen veröffentlicht. Weitere Informationen finden Sie in der Versionshistorie des EKS Add-On-Agenten.	21. Dezember 2023

In Europa (Zürich), Europa (Spanien), Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne) und Israel (Tel Aviv) wurden die Befundtypen S3 und AWS CloudTrail maschinelles Lernen (ML) hinzugefügt	Die folgenden S3 und CloudTrail Ergebnisse, die das anomale Verhalten mithilfe GuardDuty des ML-Modells zur Erkennung von Anomalien identifizieren, sind jetzt in den Regionen Europa (Zürich), Europa (Spanien), Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne) und Israel (Tel Aviv) verfügbar: • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior	21. Dezember 2023

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty unterstützt 50.000 Mitgliedskonten durch AWS Organizations	Ein delegierter GuardDuty Administrator kann jetzt maximal 50.000 Mitglieds konten über AWS Organizat ions verwalten. Dazu gehören auch maximal 5000 Mitglieds konten, die dem GuardDuty Administratorkonto auf Einladung zugeordnet wurden.	20. Dezember 2023
GuardDuty Die Unterstützung für Runtime Monitoring wurde auf 19 erweitert AWS-Regio nen	Runtime Monitoring ist jetzt in Asien-Pazifik (Jakarta), Europa (Paris), Asien-Pazifik (Osaka), Asien-Pazifik (Seoul), Naher Osten (Bahrain), Europa (Spanien), Asien-Paz ifik (Hyderabad), Asien-Paz ifik (Melbourne), Israel (Tel Aviv), USA West (Nordkali fornien), Europa (London), Asien-Pazifik (Hongkong), Europa (Mailand), Naher Osten (UAE), Südamerika (São Paulo) verfügbar, Asien-Pazifik (Mumbai), Kanada (Zentral), Afrika (Kapstadt), Europa (Zürich).	6. Dezember 2023

GuardDuty erweitert die Funktionen zur Runtime-Überwachung	GuardDuty Kündigt neben der Erkennung von Bedrohungen für Ihre EKS Amazon-Cluster die allgemeine Verfügbarkeit von Runtime Monitoring zur Erkennung von Bedrohungen für Ihre ECS Amazon-Workloads und eine Vorabversion zur Erkennung von Bedrohungen für Ihre EC2 Amazon-Instances an. Weitere Informationen darüber, welche AWS-Regionen derzeit Runtime Monitoring unterstützen, finden Sie unter Regionen und Endpunkte.	26. November 2023

Amazon GuardDuty hat die mit dem Service verknüpfte Rolle aktualisiert () SLR	GuardDuty hat neue Berechtigungen hinzugefügt, um ECS Amazon-Aktionen zum Verwalten und Abrufen von Informationen über die ECS Amazon-Cluster zu verwenden und die ECS Amazon-Kontoeinstellungen mit zu verwalten`guardduty Activate` . Die Aktionen im Zusammenhang mit Amazon rufen ECS auch die Informationen zu den zugehörigen Tags ab. GuardDuty • Die folgenden Berechtigungen wurden im Rahmen der GuardDuty Erweiterung der Runtime Monitoring-Funktionen hinzugefügt: `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	26. November 2023
Die AWS verwalteten Richtlinien wurden aktualisiert	GuardDuty hat dem AmazonGuardDutyFullAccessPolicyund eine neue Berechtigung hinzugefügt AmazonGuardDutyReadOnlyAccess. `organizations:ListAccounts`	16. November 2023

GuardDuty hat neue Befundtypen veröffentlicht, die EKS Audit Log Monitoring verwenden.	EKSAudit Log Monitoring unterstützt jetzt die folgenden Befundtypen in Asien-Pazifik (Melbourne) (`ap-southeast-4`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	11. November 2023

GuardDuty veröffentlichte neue Befundtypen, die EKS Audit Log Monitoring verwenden.	EKSAudit Log Monitoring unterstützt jetzt die folgenden Befundtypen in den Regionen Asien-Pazifik (Hyderaba `dap-south-2`) (), Europa (Zürich`eu-central-2`) () und Europa (Spanien) (`eu-south-2`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	10. November 2023

- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

GuardDuty hat neue Befundtypen veröffentlicht, die EKS Audit Log Monitoring verwenden.	EKSAudit Log Monitoring unterstützt jetzt die folgenden Befundtypen. Diese Ergebnisarten sind in den Regionen Asien-Pazifik (Hyderabad) (`ap-south-2`), Europa (Zürich) (`eu-central-2`), Europa (Spanien) (`eu-south-2`) und Asien-Pazifik (Melbourne) (`ap-southeast-4`) noch nicht verfügbar. • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	8. November 2023

	• PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
EKSRuntime Monitoring hat den neuen Agenten v1.3.1 veröffentlicht	EKSRuntime Monitoring hat eine neue Agentenversion 1.3.1 veröffentlicht, die wichtige Sicherheitspatches und Updates enthält.	23. Oktober 2023
Neues Filterattribut für die Erkenntnis	GuardDuty hat ein neues Kriterium hinzugefügt, um die generierten Ergebnisse zu filtern. DNSDas Suffix für die Anfrage gibt die Domäne der zweiten und obersten Ebene an, die an der Aktivität beteiligt war, die GuardDuty zur Generierung des Ergebnisses geführt hat.	17. Oktober 2023
EKSRuntime Monitoring hat den neuen Agenten v1.3.0 veröffentlicht, der Kubernetes Version 1.28 unterstützt	EKSRuntime Monitoring hat eine neue Agentenversion 1.3.0 veröffentlicht, die Kubernetes Version 1.28 unterstützt. Unterstützung für Ubuntu hinzugefügt. Weitere Informationen finden Sie in der Versionshistorie des EKSAdd-on-Agenten.	05. Oktober 2023

Für die Regionen Asien-Pazifik (Jakarta) und Naher Osten () wurden S3 und auf AWS CloudTrail maschinel lem Lernen (ML) basierende Befundtypen hinzugefügt UAE	Die folgenden S3 und CloudTrail Ergebnisse, die das anomale Verhalten mithilfe des ML-Modells zur Erkennung GuardDuty von Anomalien identifizieren, sind jetzt in den Regionen Asien-Pazifik (Jakarta) und Naher Osten () verfügbar: UAE • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior	20. September 2023

	• Discovery:IAMUser/AnomalousBehavior	
GuardDuty EKSRuntime Monitoring führt die Verwaltung des GuardDuty Security Agents auf Cluster-Ebene ein	EKSRuntime Monitoring bietet Unterstützung für die Verwaltung des GuardDuty Security Agents für einzelne EKS Cluster, sodass die Runtime-Ereignisse nur von diesen ausgewählten Clustern überwacht werden. EKSRuntime Monitoring erweitert diese Funktion um die Unterstützung von Tags.	13. September 2023
GuardDuty Malware Protection for EC2 erweitert die Unterstützung auf mehr AWS-Regionen	Malware Protection for EC2 ist jetzt im asiatisch-pazifischen Raum (Hyderabad), im asiatisch-pazifischen Raum (Melbourne), in Europa (Zürich) und in Europa (Spanien) verfügbar.	11. September 2023

GuardDuty ist jetzt in der Region Israel (Tel Aviv) verfügbar	Die Region Israel (Tel Aviv) wurde der Liste der Orte hinzugefügt AWS-Regionen , in denen sie jetzt verfügbar GuardDuty ist. Die folgenden Schutzpläne sind auch in der Region Israel (Tel Aviv) verfügbar: • EKSSchutzumfasst sowohl die Überwachung EKS des Auditprotokolls als auch die EKS Laufzeitüberwachung. • Lambda Protection. • Malware-Schutz für EC2. • S3-Schutz. Weitere Informationen zur Verfügbarkeit von Schutzplä nen in der Region Israel (Tel Aviv) finden Sie unter Regionen und Endpunkte.	24. August 2023
GuardDuty Konfiguration zur automatischen Aktivieru ng für Ihre Organisation auf Schutzplanebene hinzugefügt	Aktualisieren Sie die Organisat ionskonfiguration für die Schutzpläne in Ihrer Region. Mögliche Konfigurationsopti onen sind entweder „für alle Konten aktivieren“, „für neue Konten automatisch aktiviere n“ oder „für kein Konto in Ihrer Organisation automatisch aktivieren“.	16. August 2023

S3-Erkennungstypen, die anomales Verhalten mithilfe GuardDuty des ML-Modells (Machine Learning) zur Erkennung von Anomalien identifizieren, sind jetzt im asiatisch-pazifischen Raum (Osaka) verfügbar	Die folgenden Erkenntnistypen sind jetzt in der Region Asien-Pazifik (Osaka) verfügbar: • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	10. August 2023
EKSRuntime Monitoring ist jetzt im asiatisch-pazifischen Raum (Melbourne) verfügbar	EKSRuntime Monitoring within GuardDuty EKS Protection bietet Runtime-Bedrohungserkennung für Ihre EKS Amazon-Cluster in der AWS Umgebung. Die Funktion wird jetzt in der Region Asien-Pazifik (Melbourne) unterstützt.	08. August 2023
Die Liste der GuardDuty Ergebnisse, die einen GuardDuty -initiierten Malware-Scan auslösen, wurde aktualisiert	Bestimmte Erkennungstypen von EKS Runtime Monitoring können jetzt einen GuardDuty -initiierten Malware-Scan in Ihrem aufrufen. AWS-Konto	19. Juli 2023

GuardDuty unterstützt 10.000 Mitgliedskonten durch AWS Organizations	Mit einem GuardDuty Administratorkonto können jetzt maximal 10.000 Mitgliedskonten verwaltet AWS Organizations werden. Dazu gehören auch maximal 5000 Mitgliedskonten, die auf Einladung mit dem GuardDuty Administratorkonto verknüpft wurden.	29. Juni 2023
EKSRuntime Monitoring kündigt drei neue Findetypen an.	EKSRuntime Monitoring unterstützt drei neue Befundtypen, die auf der Process-Injection-Technik basieren. Die neuen Suchtypen sind: Runtime/ DefenseEvasion .Proc, :Runtime/ .Ptraceund:Runtime/. ProcessInjection DefenseEvasion ProcessInjection DefenseEvasion ProcessInjection VirtualMemoryWrite.	22. Juni 2023
EKSRuntime Monitoring hat den neuen Agenten v1.2.0 veröffentlicht, der Kubernetes Version 1.27 unterstützt	EKSRuntime Monitoring hat eine neue Agentenversion 1.2.0 veröffentlicht, die auch basierte Instanzen unterstützt. ARM64 Unterstützung für Bottlerocket hinzugefügt. Weitere Informationen finden Sie in der Versionshistorie des EKS Add-On-Agenten.	16. Juni 2023

GuardDuty Die Konsole bietet eine zusammengefasste Ansicht Ihrer Ergebnisse.	Das Übersichts-Dashboard in der GuardDuty Konsole bietet eine aggregierte Ansicht der GuardDuty Ergebnisse. Derzeit zeigt das Dashboard über verschiedene Widgets Daten für die letzten 10.000 Ergebnisse an, die für Ihr Konto (oder Mitgliedskonten, wenn Sie ein GuardDuty Administratorkonto haben) für die aktuelle Region generiert wurden.	12. Juni 2023
EKSAudit Log Monitoring ist jetzt in Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne), Europa (Zürich) und Europa (Spanien) verfügbar	Aktivieren Sie EKS Audit Log Monitoring (in EKS Protection) für Ihre Konten, um EKS Audit-Logs aus Ihren EKS Amazon-Clustern zu überwachen und sie auf potenziell bösartige und verdächtige Aktivitäten hin zu analysieren.	01. Juni 2023
EKSAudit Log Monitoring ist jetzt im Nahen Osten verfügbar (UAE)	EKSAudit Log Monitoring ist jetzt im Nahen Osten verfügbar (UAE). Aktivieren Sie EKS Audit Log Monitoring für Ihre Konten, um EKS Audit-Logs aus Ihren EKS Amazon-Clustern zu überwachen und sie auf potenziell bösartige und verdächtige Aktivitäten hin zu analysieren.	3. Mai 2023

GuardDuty Malware Protection for EC2 kündigt einen On-Demand-Malware-Scan an	Malware Protection for EC2 hilft Ihnen dabei, das potenzielle Vorhandensein von Malware in den EBS Amazon-Volumes zu erkennen, die an Ihre EC2 Amazon-Instances und Container-Workloads angehängt sind. Es bietet jetzt zwei Arten von Scans — GuardDuty initiierte Scans und Scans auf Abruf. GuardDuty -initiierter Malware-Scan initiiert nur dann automatisch einen agentenlosen Scan in den EBS Amazon-Volumes, wenn eines der Ergebnisse GuardDuty generiert wird, die den -initiierten Malware-Scan auslösen. GuardDuty Sie können einen On-Demand -Malware-Scan für EC2 Amazon-Instances in Ihrem Konto initiieren, indem Sie den Amazon-Ressourcennamen (ARN) angeben, der dieser EC2 Amazon-Instance zugeordnet ist. Weitere Informationen darüber, wie sich die beiden Scantypen unterscheiden, finden Sie unter Malware-Schutz für EC2. • GuardDuty-initiierter Malware-Scan • Malware-Scan auf Abruf	27. April 2023

GuardDuty kündigt Lambda Protection an	Lambda Protection hilft Ihnen, potenzielle Sicherheitsbedrohungen in Ihren AWS Lambda -Funktionen zu erkennen. • Lambda-Protection-Erkenntnistypen • Behebung einer potenziell gefährdeten Lambda-Funktion	20. April 2023
GuardDuty ist jetzt in der Region Asien-Pazifik (Melbourne) verfügbar	Asien-Pazifik (Melbourne) wurde der Liste der verfügbaren AWS-Regionen GuardDuty Orte hinzugefügt. Informationen darüber, welche Funktionen in dieser Region verfügbar sind, finden Sie unter Regionen und Endpunkte.	19. April 2023

GuardDuty Es wurden 3 neue Arten von EC2 Ergebnissen hinzugefügt	GuardDuty führt neue Erkennungstypen ein, um die Verwendung externer DNS Resolver und verschlüsselter DNS Technologien zu erkennen. Informationen darüber AWS-Regionen , wo diese Suchtypen unterstützt werden, finden Sie unter Regionen und Endpunkte. • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	5. April 2023

GuardDuty kündigt EKS Runtime Monitoring in Protection an EKS	EKSRuntime Monitoring within EKS Protection bietet Runtime-Bedrohungserkennung für Ihre EKS Amazon-Cluster in der AWS Umgebung. Es verwendet einen EKS Amazon-Zusatzagenten (`aws-guardduty-agent`), der Runtime-Ereignisse aus Ihren EKS Workloads sammelt. Nach dem GuardDuty Empfang dieser Runtime-Ereignisse werden sie überwacht und analysiert, um potenzielle verdächtige Sicherheitsbedrohungen zu identifizieren. Weitere Informationen finden Sie unter Suchen von Details und Suchtypen für EKS Runtime Monitoring.	30. März 2023

GuardDuty fügt eine neue Funktionalität hinzu — `autoEnableOrganizationMembers`	Amazon GuardDuty fügt eine neue Organisationskonfigurationsoption hinzu, mit der GuardDuty Administratorkonten geprüft und (falls erforderlich) durchgesetzt werden können. Diese Option GuardDuty ist für `ALL` die Mitglieder ihrer Organisation aktiviert. Die beste Vorgehensweise besteht jetzt darin, `autoEnableOrganizationMembers` anstelle von `autoEnable` zu verwenden. `autoEnable` ist veraltet, wird aber immer noch unterstützt. Folgende Personen APIs sind von dieser neuen Funktionalität betroffen: • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	23. März 2023

Die RDS Schutzfunktion in Amazon GuardDuty ist jetzt allgemein verfügbar	GuardDuty RDSDer Schutz überwacht und profiliert die RDS Anmeldeaktivitäten, um verdächtiges Anmeldeverhalten auf Ihren Amazon Aurora Aurora-Datenbank-Instances zu identifizieren. Informationen darüber, welche Unternehmen den RDS Schutz AWS-Regionen unterstützen, finden Sie unter Regionen und Endpunkte.	16. März 2023
GuardDuty kündigt die Aktivierung der Funktion an	In der Vergangenheit war die Konfiguration sowohl von Funktionen als auch von Datenquellen GuardDuty API zulässig, aber jetzt werden alle neuen GuardDuty Schutztypen als Funktionen und nicht als Datenquellen konfiguriert. GuardDuty unterstützt weiterhin die Datenquellen überAPI, fügt aber keine neuen hinzuAPI. Die Aktivierung von Funktionen wirkt sich auf das Verhalten des Benutzers aus, der aktiviert APIs wird, GuardDuty oder eines Schutztyps innerhalb GuardDuty. Wenn Sie Ihre GuardDuty Konten über die CFN Vorlage APISDK, oder verwalten, finden Sie hier die GuardDuty APIÄnderungen im März 2023.	16. März 2023

GuardDuty Malware Protection for EC2 ist jetzt in der Region Naher Osten (UAE) verfügbar	Die EC2 Funktion „Malware-Schutz für“ GuardDuty wird in der Region Naher Osten (UAE) unterstützt. Weitere Informationen finden Sie unter Regionen und Endpunkte.	13. März 2023
Amazon GuardDuty hat die mit dem Service verknüpfte Rolle aktualisiert () SLR	GuardDuty hat die folgenden neuen Berechtigungen hinzugefügt, um die kommende GuardDuty EKS Runtime Monitoring-Funktion zu unterstützen. • Verwenden Sie EKS Amazon-Aktionen, um Informationen zu den EKS Clustern zu verwalten und abzurufen und EKS Add-Ons auf EKS Clustern zu verwalten. Die EKS Aktionen rufen auch die Informationen über die zugehörigen Tags ab GuardDuty. `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	08. März 2023

Amazon GuardDuty hat die mit dem Service verknüpfte Rolle aktualisiert () SLR	Die GuardDuty SLR wurde aktualisiert und ermöglicht nun die Erstellung von Malware-Schutz für, EC2 SLR nachdem der Malware-Schutz für aktiviert EC2 wurde.	21. Februar 2023
GuardDuty erfordert TLS v1.2 oder höher	Für die Kommunikation mit AWS Ressourcen ist Version TLS 1.2 oder höher GuardDuty erforderlich und unterstützt diese Version. Weitere Informationen finden Sie unter Datenschutz und Infrastruktursicherheit.	14. Februar 2023
GuardDuty ist jetzt in der Region Asien-Pazifik (Hyderabad) verfügbar	Die Region Asien-Pazifik (Hyderabad) wurde zur Liste der verfügbaren AWS-Regionen Regionen hinzugefügt. GuardDuty Weitere Informationen finden Sie unter Regionen und Endpunkte.	14. Februar 2023
Das GuardDuty Amazon-Benutzerhandbuch entspricht den IAM Best Practices	Der Leitfaden wurde aktualisiert, um ihn an den IAM bewährten Methoden auszurichten. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden unter IAM.	10. Februar 2023

GuardDuty ist jetzt in der Region Europa (Spanien) verfügbar	Europa (Spanien) wurde zur Liste der AWS-Regionen verfügbaren GuardDuty Standorte hinzugefügt. Weitere Informationen finden Sie unter Regionen und Endpunkte.	8. Februar 2023
GuardDuty ist jetzt in der Region Europa (Zürich) verfügbar	Europa (Zürich) wurde zur Liste der AWS-Regionen verfügbaren GuardDuty Standorte hinzugefügt. Weitere Informationen finden Sie unter Regionen und Endpunkte.	12. Dezember 2022
Vorabversion einer neuen Funktion — GuardDuty RDS Schutz	GuardDuty RDSDer Schutz überwacht und profiliert die RDS Anmeldeaktivitäten, um verdächtiges Anmeldeverhalten auf Ihren Amazon Aurora Aurora-Datenbank-Instances zu identifizieren. Derzeit ist es als Vorabversion in fünf AWS-Regionen verfügbar. Weitere Informationen finden Sie unter Regionen und Endpunkte.	30. November 2022
GuardDuty ist jetzt in der Region Naher Osten (UAE) verfügbar	Naher Osten (UAE) wurde der Liste der verfügbaren AWS-Regionen GuardDuty Orte hinzugefügt. Weitere Informationen finden Sie unter Regionen und Endpunkte.	6. Oktober 2022

Inhalt für eine neue Funktion hinzugefügt — GuardDuty Malware-Schutz für EC2	GuardDuty Malware Protection for EC2 ist eine optionale Erweiterung für Amazon GuardDuty. Malware Protection for GuardDuty identifiziert zwar die gefährdeten Ressourcen, EC2 erkennt aber auch die Malware, die die Quelle der Bedrohung sein könnte. Wenn Malware Protection for EC2 aktiviert ist, EC2 leitet Malware Protection for bei jedem GuardDuty verdächtigen Verhalten auf einer EC2 Amazon-Instance oder einem Container-Workload, das auf Malware hindeutet, einen agentenlosen Scan der EBS Volumes ein, die den betroffenen EC2 Instance- oder Container-Workloads zugeordnet sind, um das Vorhandensein von GuardDuty Malware zu erkennen. Informationen zur EC2 Funktionsweise von Malware Protection for und zur Konfiguration dieser Funktion finden Sie unter Malware Protection for. GuardDuty EC2 • Informationen zu den EC2 Ergebnissen des Malware-Schutzes finden Sie unter Suchen nach Einzelheiten.	26. Juli 2022

	• Informationen zur Behebung der gefährdeten EC2 Instance und eines eigenständigen Containers finden Sie unter Behebung von Sicherheitsproblemen, die von entdeckt wurden. GuardDuty • Informationen zur Überwachung von CloudWatch Protokollen für Malware-Scans und zu den Gründen für das Übersprin gen einer Ressource beim Malware-Scan finden Sie unter Grundlegendes zu CloudWatch Protokollen und Gründen für das Übersprin gen von Dateien. • Informationen zu falsch positiven Bedrohung serkennungen finden Sie unter Falschmeldungen melden in GuardDuty Malware Protection for. EC2	
Ein Erkenntnistyp wurde außer Betrieb genommen	Exfiltration:S3/ObjectRead. Unusual wurde außer Betrieb genommen.	5. Juli 2022

Es wurden neue S3-Findetypen hinzugefügt, die anomales Verhalten mithilfe GuardDuty des ML-Modells (Machine Learning) zur Erkennung von Anomalien identifizieren.	Die folgenden neuen S3-Erkenntnistypen wurden hinzugefügt. Diese Erkennungstypen identifizieren, ob eine API Anfrage eine IAM Entität auf anomale Weise aufgerufen hat. Das ML-Modell bewertet alle API Anfragen in Ihrem Konto und identifiziert ungewöhnliche Ereignisse, die mit den von Gegnern verwendeten Techniken zusammenhängen. Weitere Informationen zu den einzelnen neuen Erkenntnissen finden Sie unter S3-Erkenntnistypen. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	5. Juli 2022

GuardDuty EKSSchutzinhalt hinzugefügt für GuardDuty	GuardDuty kann jetzt durch die Überwachung von EKS Auditprotokollen Ergebnisse für Ihre EKS Amazon-Ressourcen generieren. Informationen zur Konfiguration dieser Funktion finden Sie unter EKSSchutz bei Amazon GuardDuty. Eine Liste der Ergebnisse, die für EKS Amazon-Ressourcen generiert GuardDuty werden können, finden Sie unter Kubernetes-Ergebnisse. Es wurden neue Anleitungen zur Behebung hinzugefügt, um die Behebung dieser Erkenntnisse zu unterstützen im Leitfaden zur Behebung von Erkenntnissen in Kubernetes.	25 Januar 2022
Es wurde eine neue Erkenntnis hinzugefügt	Die neue Erkenntnis UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS wurde hinzugefügt. Dieses Ergebnis informiert Sie darüber, wenn ein AWS Konto außerhalb Ihrer Umgebung auf Ihre Instance-Anmeldeinformationen zugreift. AWS	20. Januar 2022

Die Erkenntnistypen wurden aktualisiert, um Probleme im Zusammenhang mit log4j leichter identifizieren zu können	Amazon GuardDuty hat die folgenden Suchtypen aktualisiert, um Probleme im Zusammenhang mit CVE -2021-44228 und CVE -2021-45046 zu identifiz ieren und zu priorisieren: Backdoor: /C & .B; Backdoor: EC2 /C & .B! CActivity EC2 CActivity DNS; Verhalten:/. EC2 NetworkPortUnusual	22. Dezember 2021
Erkenntnis-Änderungen	UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion wurde geändert zu UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.OutsideAWS. Diese verbesserte Version der Erkenntnisse erfasst die typischen Standorte, von denen aus Ihre Anmeldein formationen verwendet werden, und reduziert so die Anzahl der Erkenntnisse aus dem Datenverkehr, der über lokale Netzwerke geleitet wird. UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.OutsideAWS	7. September 2021
Update auf GuardDuty SLR	Das GuardDuty SLR wurde mit neuen Aktionen zur Verbesser ung der Suchgenauigkeit aktualisiert.	3. August 2021

Es wurden Datenquelleninformationen für jeden Erkenntnistyp hinzugefügt.	Die Beschreibungen der Ergebnisse enthalten jetzt Informationen über Datenquellen, die zur Generierung dieses Ergebnisses GuardDuty verwendet wurden.	10. Mai 2021
13 Erkenntnistypen entfernt.	13 Ergebnisse wurden zurückgezogen, um durch neue AnomalousBehavoir Ergebnisse ersetzt zu werden. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissions, Persistence:IAMUser/UserPermissions, PrivilegeEscalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissionsRecon:IAMUser/UserPermissions, ResourceConsumption:IAMUser/ComputeResources, Stealth:IAMUser/LoggingConfigurationModified, Discovery:S3/BucketEnumeration.Unusual, Impact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual.	12. März 2021

Es wurden 8 neue Erkenntnistypen für anomales Verhalten hinzugefügt.	Es wurden 8 neue IAMUser Erkennungstypen hinzugefügt, die auf anomalem Verhalten von Schulleitern basieren. IAM CredentialAccess:IAMUser/AnomalousBehavior,, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior. Persistence:IAMUser/AnomalousBehaviorPrivilegeEscalation:IAMUser/AnomalousBehavior	12. März 2021
Es wurden EC2 Ergebnisse hinzugefügt, die auf der Reputation der Domain basieren.	Es wurden 4 neue Arten von Erkenntnistypen hinzugefügt, die auf der Domain-Reputation basieren. Impact:EC2/AbusedDomainRequest.Reputation , Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. Außerdem wurde ein neues EC2 Ergebnis für C& CActivity hinzugefügt. Impact:EC2/SuspiciousDomainRequest.Reputation	27. Januar 2021

Es wurden 4 neue Erkenntnistypen hinzugefügt.	Es wurden 3 neue S3 aliciousIPCaller M-Ergebnisse hinzugefügt. Discovery:S3/MaliciousIPCaller, Exfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. Außerdem wurde ein neues EC2 Ergebnis für C& CActivity hinzugefügt. Backdoor:EC2/C&CActivity.B	21. Dezember 2020
Der Erkenntnistyp UnauthorizedAccess:EC2/TorIPCaller wurde außer Betrieb genommen.	Der UnauthorizedAccess:EC2/TorIPCaller Befundtyp ist jetzt nicht mehr gültig GuardDuty. Weitere Informationen.	1. Oktober 2020
Der Erkenntnistyp Impact:EC2/WinRmBruteForce wurde hinzugefügt.	Eine neue Auswirkungs-Erkenntnis Impact:EC2/WinRmBruteForce wurde hinzugefügt. Weitere Informationen.	17. September 2020
Der Erkenntnistyp Impact:EC2/PortSweep wurde hinzugefügt.	Eine neue Auswirkungs-Erkenntnis Impact:EC2/PortSweep wurde hinzugefügt. Weitere Informationen.	17. September 2020
GuardDuty ist jetzt in den Regionen Afrika (Kapstadt) und Europa (Mailand) verfügbar.	Afrika (Kapstadt) und Europa (Mailand) wurden zur Liste der AWS Regionen hinzugefügt, in denen diese Option verfügbar GuardDuty ist. Weitere Informationen	31. Juli 2020

Es wurden neue Nutzungsdetails für die GuardDuty Kostenüberwachung hinzugefügt.	Sie können jetzt neue Messwerte verwenden, um GuardDuty Nutzungskostendaten für Ihr Konto und die von Ihnen verwalteten Konten abzufragen. Eine neue Übersicht der Nutzungskosten ist in der Konsole unter verfügbar https://console.aws.amazon.com/guardduty/. Auf detailliertere Informationen kann über die zugegriffen werdenAPI.	31. Juli 2020
Es wurden Inhalte zum S3-Schutz durch die Überwachung von S3-Datenereignissen in hinzugefügt GuardDuty.	GuardDuty S3 Protection ist jetzt durch die Überwachung von Ereignissen auf der S3-Datenebene als neue Datenquelle verfügbar. Bei neuen Konten wird dieses Feature automatisch aktiviert. Wenn Sie die neue Datenquelle bereits verwenden, können GuardDuty Sie sie für sich selbst oder Ihre Mitgliedskonten aktivieren.	31. Juli 2020
Es wurden 14 neue S3-Erkenntnisse hinzugefügt.	14 neue S3-Erkenntnistypen wurden für Quellen der S3-Steuerebene und -Datenebene hinzugefügt.	31. Juli 2020

Zusätzliche Unterstützung für S3-Erkenntnisse hinzugefügt und zwei vorhandene Erkenntnistyp-Namen geändert.	GuardDuty Die Ergebnisse enthalten jetzt mehr Details zu Ergebnissen, die S3-Buckets betreffen. Bestehende Erkenntnistypen, die sich auf die S3-Aktivität bezogen, wurden umbenannt: Policy:IAMUser/S3BlockPublicAccessDisabled wurde zu Policy:S3/BucketBlockPublicAccessDisabled geändert. Stealth:IAMUser/S3ServerAccessLoggingDisabled wurde geändert zu Stealth:S3/ServerAccessLoggingDisabled.	28. Mai 2020
Inhalt für die AWS Organizations Integration hinzugefügt.	GuardDuty lässt sich jetzt mit AWS Organizations delegierten Administratoren integrieren, sodass Sie GuardDuty Konten innerhalb Ihrer Organisation verwalten können. Wenn Sie einen delegierten Administrator als Ihr GuardDuty Administratorkonto festlegen, können Sie automatisch GuardDuty für jedes Organisationsmitglied die Verwaltung durch das delegierte Administratorkonto aktivieren. Sie können Konten auch automatisch für neue AWS Organizations Mitglieder aktivieren GuardDuty . Weitere Informationen.	20. April 2020

Inhalt für das Feature zum Export von Erkenntnissen hinzugefügt.	Inhalt hinzugefügt, der die Funktion „Ergebnisse exportieren“ von beschreibt GuardDuty.	14. November 2019
Der Erkenntnistyp UnauthorizedAccess:EC2/MetadataDNSRebind wurde hinzugefügt.	Eine neue unautorisierte Erkenntnis UnauthorizedAccess:EC2/MetadataDNSRebind wurde hinzugefügt. Weitere Informationen.	10. Oktober 2019
Der Erkenntnistyp Stealth:IAMUser/S3ServerAccessLoggingDisabled wurde hinzugefügt.	Eine neue Stealth-Erkenntnis Stealth:IAMUser/S3ServerAccessLoggingDisabled wurde hinzugefügt. Weitere Informationen.	10. Oktober 2019
Der Erkenntnistyp Policy:IAMUser/S3BlockPublicAccessDisabled wurde hinzugefügt.	Eine neue Richtlinien-Erkenntnis Policy:IAMUser/S3BlockPublicAccessDisabled wurde hinzugefügt. Weitere Informationen.	10. Oktober 2019
Der Erkenntnistyp Backdoor:EC2/XORDDOS wurde außer Betrieb genommen.	Der Backdoor:EC2/XORDDOS Befundtyp ist jetzt nicht mehr verfügbar GuardDuty. Erfahren Sie mehr	12. Juni 2019
Der Erkenntnistyp Privilege Escalation wurde hinzugefügt.	Der PrivilegeEscalation-Erkenntnistyp erkennt, wenn Benutzer versuchen, ihren Konten eskalierte Berechtigungen mit weniger Einschränkungen zuzuweisen. Weitere Informationen	14. Mai 2019

GuardDuty ist jetzt in der Region Europa (Stockholm) verfügbar.	Europa (Stockholm) wurde zur Liste der AWS Regionen hinzugefügt, in denen GuardDuty es verfügbar ist. Weitere Informationen	9. Mai 2019
Ein neuer Erkenntnistyp Recon:EC2/PortProbeEMRUnprotectedPort wurde hinzugefügt.	Dieses Ergebnis informiert Sie darüber, dass EMR ein verwandter sensibler Port auf einer EC2 Instance nicht blockiert ist und aktiv geprüft wird. Weitere Informationen	8. Mai 2019
Es wurden 5 neue Erkennungstypen hinzugefügt, die erkennen, ob Ihre EC2 Instances möglicherweise für Denial-of-Service-Angriffe (DoS) verwendet werden.	Diese Ergebnisse informieren Sie über EC2 Instanzen in Ihrer Umgebung, die sich so verhalten, dass sie möglicherweise darauf hindeuten, dass sie für Denial of Service (DoS) -Angriffe verwendet werden. Weitere Informationen	8. März 2019
Ein neuer Erkenntnistyp Policy:IAMUser/RootCredentialUsage wurde hinzugefügt.	Policy:IAMUser/RootCredentialUsageDer Suchtyp informiert Sie darüber, dass Ihre Root-Benutzeranmeldedaten verwendet AWS-Konto werden, um programmatische Anfragen an Dienste zu stellen. AWS Weitere Informationen	24. Januar 2019

Der UnauthorizedAccess :IAMUser/UnusualASNCaller-Erkenntnistyp wurde außer Betrieb genommen	Der UnauthorizedAccess :IAMUser/UnusualASNCaller-Erkenntnistyp wurde außer Betrieb genommen. Sie werden nun über Aktivitäten informiert, die von ungewöhnl ichen Netzwerken aus über andere aktive GuardDuty Suchtypen aufgerufen wurden. Der generierte Befundtyp basiert auf der Kategorie vonAPI, die von einem ungewöhnlichen Netzwerk aus aufgerufen wurde. Weitere Informationen	21. Dezember 2018
Zwei neue Erkenntnistypen wurden hinzugefügt: PenTest:I AMUser/ParrotLinux und PenTest:IAMUser/PentooLinux	PenTest:IAMUser/ParrotLinux Der Suchtyp informiert Sie darüber, dass ein Computer, auf dem Parrot Security Linux ausgeführt wird, API Anrufe mit Anmeldeinformationen tätigt, die zu Ihrem AWS Konto gehören. PenTest:IAMUser/ PentooLinuxDer Suchtyp informiert Sie darüber, dass ein Computer, auf dem Pentoo Linux ausgeführt wird, API Anrufe mit Zugangsdaten tätigt, die zu Ihrem AWS Konto gehören. Weitere Informati onen	21. Dezember 2018

Unterstützung für das SNS Thema GuardDuty Amazon-Ankündigungen hinzugefügt	Sie können jetzt das SNS Thema GuardDuty Ankündigungen abonnieren, um Benachrichtigungen über neu veröffentlichte Ergebnisarten, Aktualisierungen der vorhandenen Ergebnisarten und andere Funktionsänderungen zu erhalten. Benachrichtigungen sind in allen Formaten verfügbar, die Amazon SNS unterstützt. Weitere Informationen	21. November 2018
Zwei neue Erkenntnistypen wurden hinzugefügt: UnauthorizedAccess:EC2/TorClient und UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClientDer Suchtyp informiert dich darüber, dass eine EC2 Instance in deiner AWS Umgebung Verbindungen zu einem Tor Guard- oder einem Authority-Knoten herstellt. UnauthorizedAccess:EC2/TorRelayWenn Sie den Typ finden, werden Sie darüber informiert, dass eine EC2 Instanz in Ihrer AWS Umgebung Verbindungen zu einem Tor-Netzwerk auf eine Weise herstellt, die darauf hindeutet, dass sie als Tor-Relay fungiert. Weitere Informationen	16. November 2018

Ein neuer Erkenntnistyp CryptoCurrency:EC2/BitcoinTool.B wurde hinzugefügt.	Dieser Befund informiert dich darüber, dass eine EC2 Instanz in deiner AWS Umgebung einen Domainnamen abfragt, der mit Bitcoin oder einer anderen kryptowährungsbezogenen Aktivität verknüpft ist. Weitere Informationen	9. November 2018
Unterstützung für die Aktualisierung der Häufigkeit von Benachrichtigungen, die an Ereignisse gesendet werden, hinzugefügt CloudWatch	Sie können jetzt die Häufigkeit der an CloudWatch Ereignisse gesendeten Benachrichtigungen für das spätere Auftreten vorhandener Ergebnisse aktualisieren. Mögliche Werte sind 15 Minuten, 1 Stunde oder standardmäßig 6 Stunden. Weitere Informationen	9. Oktober 2018
Zusätzliche Unterstützung für Regionen hinzugefügt	Unterstützung für Regionen AWS GovCloud (US-West) hinzugefügt Erfahren Sie mehr	25. Juli 2018
Unterstützung für AWS CloudFormation StackSets in hinzugefügt GuardDuty	Sie können die GuardDuty Vorlage „Amazon aktivieren“ verwenden, um die Aktivierung GuardDuty gleichzeitig in mehreren Konten durchzuführen. Weitere Informationen	25. Juni 2018

Unterstützung für Regeln zur GuardDuty automatischen Archivierung hinzugefügt	Kunden können jetzt granulare Regeln für die automatische Archivierung erstellen, um Ergebnisse zu unterdrücken. Markiert Ergebnisse, die einer Regel für die automatische Archivierung entsprechen, GuardDuty automatisch als archiviert. Auf diese Weise können Kunden weitere Anpassungen GuardDuty vornehmen, sodass nur relevante Ergebnisse in der Tabelle mit den aktuellen Ergebnissen angezeigt werden. Weitere Informationen	4. Mai 2018
GuardDuty ist in der Region Europa (Paris) verfügbar	GuardDuty ist jetzt in Europa (Paris) verfügbar, sodass Sie die kontinuierliche Sicherheitsüberwachung und Bedrohungserkennung in dieser Region ausweiten können. Weitere Informationen	29. März 2018
Das Erstellen von GuardDuty Administratorkonten und Mitgliedskonten über AWS CloudFormation wird jetzt unterstützt.	Weitere Informationen erhalten Sie unter `AWS::GuardDuty::master` und `AWS::GuardDuty::member`.	6. März 2018
Neun neue CloudTrail basierte Anomalieerkennungen wurden hinzugefügt.	Diese neuen Erkennungstypen werden automatisch GuardDuty in allen unterstützten Regionen aktiviert. Weitere Informationen	28. Februar 2018

Es wurden drei neue Erkennungsmöglichkeiten von Bedrohungen (Erkenntnistypen) hinzugefügt.	Diese neuen Suchtypen werden automatisch GuardDuty in allen unterstützten Regionen aktiviert. Weitere Informationen	5. Februar 2018
Erhöhung des Limits für GuardDuty Mitgliedskonten.	Mit dieser Version können Sie bis zu 1000 GuardDuty Mitgliedskonten pro AWS Konto hinzufügen (GuardDuty Administratorkonto). Weitere Informationen	25. Januar 2018
Änderungen beim Upload und bei der weiteren Verwaltung von Listen vertrauenswürdiger IP-Adressen und Bedrohungslisten für GuardDuty Administratorkonten und Mitgliedskonten.	Mit dieser Version können Benutzer mit GuardDuty Administratorkonten vertrauenswürdige IP-Listen und Bedrohungslisten hochladen und verwalten. Benutzer mit GuardDuty Mitgliedskonten können keine Listen hochladen und verwalten. Vertrauenswürdige IP-Adressen und Bedrohungslisten, die vom Administratorkonto hochgeladen werden, wirken sich negativ auf die GuardDuty Funktionalität der Mitgliedskonten aus. Weitere Informationen	25. Januar 2018

Frühere Aktualisierungen

Änderung	Beschreibung	Datum
Erste Veröffentlichung	Erstveröffentlichung des GuardDuty Amazon-Benutzerhandbuchs.	28. November 2017

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.