Guida per GuardDuty l'utente di Amazon

Amazon GuardDuty

Amazon GuardDuty: Guida per GuardDuty l'utente di Amazon

Table of Contents

Che cos'è Amazon GuardDuty?

Amazon GuardDuty è un servizio di rilevamento delle minacce che monitora, analizza ed elabora continuamente le fonti di AWS dati e i log nel tuo ambiente. AWS GuardDuty utilizza feed di intelligence sulle minacce, come elenchi di indirizzi IP e domini dannosi, hash di file e modelli di machine learning (ML) per identificare attività sospette e potenzialmente dannose nel tuo ambiente. AWS L'elenco seguente fornisce una panoramica dei potenziali scenari di minaccia che GuardDuty possono aiutarti a rilevare:

- Credenziali compromesse ed esfiltrate AWS .
- Efiltrazione e distruzione dei dati che possono portare a un evento ransomware. Modelli insoliti di eventi di accesso nelle versioni del motore supportate dei database Amazon Aurora e RDS Amazon, che indicano un comportamento anomalo.
- Attività di cryptomining non autorizzate nelle istanze di Amazon Elastic Compute Cloud (AmazonEC2) e nei carichi di lavoro dei container.
- Presenza di malware nelle EC2 istanze Amazon e nei carichi di lavoro dei container e file appena caricati nei bucket Amazon Simple Storage Service (Amazon S3).
- Eventi a livello di sistema operativo, di rete e di file che indicano un comportamento non autorizzato sui cluster Amazon Elastic Kubernetes Service (Amazon), sulle attività di EKS Amazon Elastic Container Service (Amazon), sulle istanze Amazon e sui carichi AWS Fargate (Fargate) di lavoro dei containerECS. EC2

Che cos'è Amazon GuardDuty

Indice

Caratteristiche di GuardDuty

Ecco alcuni dei modi principali in cui Amazon GuardDuty può aiutarti a monitorare, rilevare e gestire le potenziali minacce nel tuo AWS ambiente.

Monitora continuamente fonti di dati e registri di eventi specifici

- Rilevamento delle minacce fondamentali: quando attivi GuardDuty in an Account AWS, avvia GuardDuty automaticamente l'acquisizione delle fonti di dati di base associate a quell'account. Queste fonti di dati includono eventi di AWS CloudTrail gestione, log di VPC flusso (da EC2 istanze Amazon) e DNS log. Non è necessario abilitare nient'altro per iniziare GuardDuty ad analizzare ed elaborare queste fonti di dati per generare i risultati di sicurezza associati. Per ulteriori informazioni, consulta GuardDuty fonti di dati fondamentali.
- Piani di GuardDuty protezione incentrati sui casi d'uso: per una maggiore visibilità del rilevamento delle minacce nella sicurezza dell' AWS ambiente, GuardDuty offre piani di protezione dedicati che puoi scegliere di abilitare. I piani di protezione consentono di monitorare i registri e gli eventi di altri servizi. AWS Queste fonti includono registri di EKS controllo, attività di RDS accesso, eventi dati CloudTrail in Amazon S3EBS, volumi, monitoraggio del runtime su AmazonEKS, EC2 ECS Amazon e Amazon-Fargate e registri delle attività di rete Lambda. GuardDutyconsolida queste fonti di log ed eventi sotto il termine - Caratteristiche. È possibile abilitare uno o più piani di protezione dedicati in un servizio supportato in qualsiasi Regione AWS momento. GuardDuty inizierà a monitorare, elaborare e analizzare le attività in base al piano di protezione abilitato. Per ulteriori informazioni su ciascun piano di protezione e su come funziona, consulta il documento relativo al piano di protezione corrispondente.

Piano di protezione	Descrizione
Protezione S3	Identifica i potenziali rischi per la sicurezza, come i tentativi di esfiltrazione e distruzione dei dati nei bucket Amazon S3.
EKSProtezione	EKSAudit Log Monitoring analizza i log di controllo di Kubernetes dai tuoi cluster EKS Amazon alla ricerca di attività potenzialmente sospette e dannose.
Monitoraggio del runtime	Monitora e analizza gli eventi a livello di sistema operativo su Amazon, EKS Amazon EC2 e Amazon ECS (incluso AWS Fargate), per rilevare potenziali minacce di runtime.

Piano di protezione	Descrizione
Protezione da malware per EC2	Rileva la potenziale presenza di malware eseguendo la scansione dei EBS volumi Amazon associati alle tue EC2 istanze Amazon. È disponibile un'opzione per utilizzare questa funzionalità su richiesta.
Protezione da malware per S3	Rileva la potenziale presenza di malware negli oggetti appena caricati all'interno dei bucket Amazon S3.
RDSProtezione	Analizza e profila la tua attività di RDS accesso per potenziali minacce di accesso ai database Amazon Aurora e Amazon RDS supportati.
Protezione Lambda	Monitora i registri delle attività della rete Lambda, a VPC partire dai log di flusso, per rilevare le minacce alle tue funzioni. AWS Lambda Esempi di queste potenziali minacce includono il cryptomining e la comunicazione con server dannosi.

> **Abilita la protezione da malware per S3 in modo indipendente**
>
> GuardDuty offre la flessibilità necessaria per utilizzare Malware Protection for S3 in modo indipendente, senza abilitare il GuardDuty servizio Amazon. Per ulteriori informazioni su come iniziare a utilizzare solo Malware Protection for S3, consulta. GuardDuty Protezione da malware per S3 Per utilizzare tutti gli altri piani di protezione, è necessario abilitare il GuardDuty servizio.

Gestisci un ambiente con più account

Puoi gestire un AWS ambiente con più account utilizzando il metodo di invito AWS Organizations (consigliato) o quello precedente. Per ulteriori informazioni, consulta Gestione di più account .

Genera risultati di sicurezza per le minacce rilevate

Quando GuardDuty rileva potenziali minacce alla sicurezza associate alle AWS risorse, inizia a generare risultati di sicurezza che forniscono informazioni sulla risorsa potenzialmente compromessa. Dopo averlo abilitato GuardDuty nel tuo account, genera Risultati di esempio per

visualizzare il file associato. Dettagli degli esiti Per un elenco completo dei risultati di sicurezza, consultaTipi di esiti.

Con GuardDuty, puoi anche utilizzare uno script di tester che genera risultati GuardDuty di sicurezza specifici per capire come esaminare e rispondere ai GuardDuty risultati. Per ulteriori informazioni, consulta GuardDuty Risultati dei test in account dedicati.

Valutazione e gestione dei risultati di sicurezza

GuardDuty consolida i risultati di sicurezza tra gli account e visualizza i risultati nella dashboard di riepilogo sulla GuardDuty console. Puoi anche recuperare i risultati tramite AWS Security Hub API AWS Command Line Interface, o. AWS SDK Con una visione olistica dello stato di sicurezza attuale, è possibile identificare tendenze e potenziali problemi e adottare le misure correttive necessarie. Per ulteriori informazioni, consulta Gestione dei GuardDuty risultati.

Integrazione con i servizi di sicurezza correlati AWS

Per aiutarvi ulteriormente ad analizzare e indagare sulle tendenze di sicurezza nel vostro AWS ambiente, prendete in considerazione l'utilizzo dei seguenti servizi AWS relativi alla sicurezza in combinazione con. GuardDuty

- AWS Security Hub— Questo servizio offre una visione completa dello stato di sicurezza delle AWS risorse e consente di controllare l' AWS ambiente rispetto agli standard e alle best practice del settore della sicurezza. Lo fa in parte consumando, aggregando, organizzando e dando priorità ai risultati di sicurezza provenienti da più AWS servizi (incluso Amazon Macie) e prodotti AWS Partner Network () supportati. APN Security Hub ti aiuta ad analizzare le tendenze della sicurezza e a identificare i problemi di sicurezza con la massima priorità in tutto l' AWS ambiente.

  Per informazioni sull'utilizzo congiunto GuardDuty di Security Hub, vedereIntegrazione con GuardDuty AWS Security Hub. Per ulteriori informazioni su Security Hub, consulta la Guida AWS Security Hub per l'utente.

- Amazon Detective: questo servizio ti aiuta ad analizzare, indagare e identificare rapidamente la causa principale dei risultati di sicurezza o delle attività sospette. Detective raccoglie automaticamente i dati di registro dalle tue AWS risorse. Utilizza quindi il machine learning, l'analisi statistica e la teoria dei grafi per generare visualizzazioni che consentono di condurre indagini sulla sicurezza più rapide ed efficaci. Le aggregazioni, i riepiloghi e il contesto predefiniti di Detective ti aiutano ad analizzare e determinare la natura e l'entità dei potenziali problemi di sicurezza.

Per informazioni sull'uso combinato di Detective GuardDuty e Detective, vedereIntegrazione GuardDuty con Amazon Detective. Per ulteriori informazioni su Detective, consulta la Amazon Detective User Guide.

- Amazon EventBridge: questo servizio ti aiuta a ricevere notifiche e rispondere ai risultati GuardDuty di sicurezza quasi in tempo reale. GuardDutycrea un evento in caso di modifica dei risultati. Puoi scegliere la frequenza da cui desideri ricevere le notifiche EventBridge. Per ulteriori informazioni, consulta What is Amazon EventBridge nella Amazon EventBridge User Guide.

PCIDSSConformità

GuardDuty supporta l'elaborazione, l'archiviazione e la trasmissione dei dati delle carte di credito da parte di un commerciante o di un fornitore di servizi ed è stato convalidato come conforme al Payment Card Industry (PCI) Data Security Standard (). DSS Per ulteriori informazioni PCIDSS, incluso come richiedere una copia del AWS PCI Compliance Package, vedere PCIDSSLevel 1.

Per ulteriori informazioni, consulta la sezione Un nuovo test di terze parti confronta Amazon con i sistemi GuardDuty di rilevamento delle intrusioni di rete nel AWS Security Blog.

Prezzi in GuardDuty

Piano gratuito di AWS ti aiuta a esplorare e provare AWS servizi gratuitamente fino ai limiti specificati per ogni servizio. Esistono tre categorie: 12 mesi di prova gratuita, sempre gratuita e prova gratuita a breve termine. Amazon GuardDuty appartiene alla categoria delle prove gratuite a breve termine e offre una prova gratuita di 30 giorni. Se continui a utilizzare al GuardDuty termine del periodo di prova gratuito, comincerai a incorrere in costi in base al modo in cui utilizzi questo servizio.

La scansione antimalware su richiesta (in Malware Protection forEC2) e la protezione da malware per S3 non rientrano nella categoria di prova gratuita a breve termine di GuardDuty 30 giorni. Malware Protection for S3 rientra nella categoria dei 12 mesi gratuiti, Piano gratuito di AWS mentre la scansione antimalware On-demand segue un modello di costo. pay-as-you-use Non è disponibile una prova gratuita di 30 giorni o un modello a costo gratuito di 12 mesi con scansione antimalware su richiesta. Per ulteriori informazioni, consulta la pagina dei prezzi. GuardDuty

Utilizzo della GuardDuty prova gratuita di 30 giorni

Quando si utilizza GuardDuty per la prima volta in un Regione AWS, Account AWS si viene automaticamente iscritti a una prova gratuita di 30 giorni in quella regione. Alcuni piani di protezione verranno inoltre abilitati automaticamente e sono inclusi nella prova gratuita di 30 giorni. GuardDuty Trattandosi di un servizio regionale, quando lo attivi per la prima volta in un'altra regione, il tuo account riceverà una prova gratuita di 30 giorni GuardDuty e alcuni piani di protezione supportati in quella regione.

Quando si lavora con più account in un' GuardDuty organizzazione, ogni account riceve la propria prova gratuita di 30 giorni GuardDuty e i propri piani di protezione.

La tabella seguente mostra quali piani di protezione vengono abilitati automaticamente quando si attiva GuardDuty per la prima volta.

Piano di protezione	Incluso nella GuardDuty prova gratuita di 30 giorni	Ha una propria prova gratuita di 30 giorni [1]
EKSProtezione	Sì	Sì
Protezione Lambda	Sì	Sì
Protezione da malware per EC2 – GuardDuty-scansione antimalware avviata	Sì	Sì
Protezione da malware per EC2 – Scansione antimalware on demand	No	No
GuardDuty Protezione da malware per S3	No	No
RDSProtezione	Sì	Sì

Piano di protezione	Incluso nella GuardDuty prova gratuita di 30 giorni	Ha una propria prova gratuita di 30 giorni [1]	
Monitoraggio del runtime	No	Sì	
Protezione S3	Sì	Sì	

[1] Ogni piano di protezione prevede una propria prova gratuita. Ad esempio, quando attivi un piano di protezione dopo la scadenza del periodo di prova gratuito di GuardDuty 30 giorni per il tuo account e viene rilasciato un nuovo piano di protezione, puoi abilitare questo piano di protezione con una versione di prova gratuita dedicata. Per ulteriori informazioni sulle prove gratuite dei piani di protezione, consulta il documento associato a ciascun piano di protezione.

Visualizza i costi di utilizzo stimati durante la prova gratuita: durante la prova gratuita di 30 giorni GuardDuty e, potenzialmente, con un piano di protezione, GuardDuty fornisce il costo di utilizzo stimato per il tuo account. Se sei un account GuardDuty amministratore delegato, puoi visualizzare il costo di utilizzo totale stimato e la ripartizione a livello di account per tutti gli account membro abilitati. GuardDuty Per ulteriori informazioni, consulta Stima dei costi GuardDuty .

Costo di utilizzo al termine del periodo di prova gratuito: se continui a utilizzare GuardDuty uno dei suoi piani di protezione dopo la fine del periodo di prova gratuito, inizierai a incorrere nei relativi costi di utilizzo. Per visualizzare la fattura, accedi a Cost Explorer nella https://console.aws.amazon.com/billing/console. Per ulteriori informazioni sulla fatturazione AWS dell'account, consulta la Guida per l'AWS Billing utente.

Utilizzo di Malware Protection for S3 con piano gratuito di 12 mesi

Malware Protection for S3 utilizza un piano gratuito associato al tuo piano Account AWS che può essere nuovo, con un piano gratuito continuativo o con un piano gratuito scaduto di 12 mesi. Per ulteriori informazioni, consulta Prezzi di Malware Protection for S3.

Accedendo GuardDuty

È possibile utilizzare GuardDuty in uno dei seguenti modi:

GuardDuty console

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

La console è un'interfaccia basata su browser per l'accesso e l'utilizzo. GuardDuty La GuardDuty console fornisce l'accesso all' GuardDuty account, ai dati e alle risorse.

AWS strumenti da riga di comando

Con gli strumenti da riga di AWS comando, è possibile impartire comandi dalla riga di comando del sistema per eseguire GuardDuty operazioni e AWS operazioni. Gli strumenti a riga di comando sono utili per creare script che eseguono le attività.

Per informazioni sull'installazione e l'utilizzo AWS CLI, consulta la Guida AWS Command Line Interface per l'utente. Per visualizzare i AWS CLI comandi disponibili per GuardDuty, vedere CLICommand Reference.

GuardDuty HTTPS API

È possibile accedere GuardDuty e a AWS livello di codice utilizzando GuardDuty HTTPSAPI, che consente di inviare HTTPS richieste direttamente al servizio. Per ulteriori informazioni, consulta la pagina di riferimento. GuardDuty API

AWS SDKs

AWS fornisce kit di sviluppo software (SDKs) costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione (Java, Python, Ruby,. NET, iOS, Android e altro). SDKsForniscono un modo conveniente per creare un accesso programmatico a GuardDuty. Per informazioni su AWS SDKs, incluso come scaricarli e installarli, consulta Tools for Amazon Web Services.

Concetti e terminologia

Quando inizi a usare Amazon GuardDuty, puoi trarre vantaggio dalla conoscenza dei suoi concetti chiave.

Account

Un account Amazon Web Services (AWS) standard che contiene AWS le tue risorse. Puoi accedere AWS con il tuo account e abilitare GuardDuty.

Puoi anche invitare altri account ad attivarsi GuardDuty e ad associarsi al tuo AWS account in GuardDuty. Se gli inviti vengono accettati, il tuo account viene designato come GuardDuty account amministratore e gli account aggiunti diventano i tuoi account membro. Potrai quindi visualizzare e gestire i GuardDuty risultati di tali account per loro conto.

Gli utenti dell'account amministratore possono configurare GuardDuty , visualizzare e gestire GuardDuty i risultati per il proprio account e per tutti gli account dei membri. Puoi avere fino a 10.000 account membri in GuardDuty.

Gli utenti degli account membro possono configurare GuardDuty , visualizzare e gestire GuardDuty i risultati nel proprio account (tramite la console di GuardDuty gestione o GuardDuty API). Gli utenti degli account membri non possono consultare o gestire i risultati negli account degli altri membri.

Un non Account AWS può essere un account GuardDuty amministratore e un account membro allo stesso tempo. An Account AWS può accettare solo un invito all'iscrizione. L'accettazione di un invito è facoltativa.

Per ulteriori informazioni, consulta Gestione di più account in Amazon GuardDuty.

Rivelatore

Amazon GuardDuty è un servizio regionale. Quando GuardDuty abiliti uno specifico Regione AWS, il tuo Account AWS viene associato a un ID del rilevatore. Questo ID alfanumerico di 32 caratteri è unico per il tuo account in quella regione. Ad esempio, quando attivi GuardDuty lo stesso account in una regione diversa, il tuo account verrà associato a un ID rilevatore diverso. Il formato di a detectorId è`12abc34d567e8fa901bc2d34e56789f0`.

Tutti i GuardDuty risultati, gli account e le azioni relative alla gestione dei risultati e al GuardDuty servizio utilizzano l'ID del rilevatore per eseguire un'APIoperazione.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

> **Note**
>
> Negli ambienti con più account, viene eseguito il roll up degli esiti di ogni account membro fino al rilevatore dell'account amministratore.

Alcune GuardDuty funzionalità vengono configurate tramite il rilevatore, ad esempio la configurazione della frequenza di notifica CloudWatch degli eventi e l'attivazione o la disabilitazione di piani di protezione opzionali per l' GuardDuty elaborazione.

Utilizzo di Malware Protection for S3 all'interno GuardDuty

Quando abiliti Malware Protection for S3 in un account in cui GuardDuty è abilitata, le azioni di Malware Protection for S3 come l'attivazione, la modifica e la disabilitazione di una risorsa protetta non sono associate all'ID del rilevatore.

Se non abiliti GuardDuty e scegli l'opzione di rilevamento delle minacce Malware Protection for S3, non viene creato alcun ID di rilevamento per il tuo account.

Fonti di dati fondamentali

L'origine o la posizione di un set di dati. Per rilevare un'attività non autorizzata o imprevista nel proprio AWS ambiente. GuardDuty analizza ed elabora i dati provenienti dai registri AWS CloudTrail degli eventi, dagli eventi di AWS CloudTrail gestione, dagli eventi AWS CloudTrail relativi ai dati per S3, dai log di VPC flusso, dai log, vedi. DNS GuardDuty fonti di dati fondamentali

Funzionalità

Un oggetto funzionale configurato per il piano di GuardDuty protezione consente di rilevare un'attività non autorizzata o imprevista nell' AWS ambiente. Ogni piano di GuardDuty protezione configura l'oggetto feature corrispondente per analizzare ed elaborare i dati. Alcuni degli oggetti delle funzionalità includono registri di EKS controllo, monitoraggio delle attività di RDS accesso, registri delle attività di rete Lambda e volumi. EBS Per ulteriori informazioni, consulta Attivazione delle funzionalità in GuardDuty.

Risultato

Un potenziale problema di sicurezza rilevato da GuardDuty. Per ulteriori informazioni, consulta Comprendere i GuardDuty risultati di Amazon.

I risultati vengono visualizzati nella GuardDuty console e contengono una descrizione dettagliata del problema di sicurezza. Puoi anche recuperare i risultati generati chiamando ListFindingsAPIle operazioni GetFindingsand.

Puoi anche visualizzare i GuardDuty risultati tramite Amazon CloudWatch Events. GuardDuty invia i risultati ad Amazon CloudWatch tramite HTTPS protocollo. Per ulteriori informazioni, consulta Creazione di risposte personalizzate ai GuardDuty risultati con Amazon CloudWatch Events.

IAMruolo

Questo è il IAM ruolo con le autorizzazioni necessarie per scansionare l'oggetto S3. Quando l'etichettatura degli oggetti scansionati è abilitata, le IAM PassRole autorizzazioni aiutano ad GuardDuty aggiungere tag all'oggetto scansionato.

Risorsa del piano Malware Protection

Dopo aver abilitato Malware Protection for S3 per un bucket, GuardDuty crea una risorsa del EC2 piano Malware Protection for S3. Questa risorsa è associata a Malware Protection for EC2 plan ID, un identificatore univoco per il bucket protetto. Utilizza la risorsa del piano Malware Protection per eseguire API operazioni su una risorsa protetta.

Bucket protetto (risorsa protetta)

Un bucket Amazon S3 è considerato protetto quando si abilita Malware Protection for S3 per questo bucket e il suo stato di protezione cambia in Attivo.

GuardDuty supporta solo un bucket S3 come risorsa protetta.

Stato di protezione

Lo stato associato alla risorsa del piano Malware Protection. Dopo aver abilitato Malware Protection for S3 per il tuo bucket, questo stato indica se il bucket è configurato correttamente o meno.

Prefisso dell'oggetto S3

In un bucket Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), puoi usare prefissi per organizzare lo storage. Un prefisso è un raggruppamento logico degli

oggetti in un bucket S3. Per ulteriori informazioni, consulta Organizing and listing objects nella Amazon S3 User Guide.

Opzioni di scansione

Quando GuardDuty Malware Protection for EC2 è abilitato, consente di specificare quali EC2 istanze Amazon e volumi Amazon Elastic Block Store (EBS) scansionare o ignorare. Questa funzionalità consente di aggiungere i tag esistenti associati alle EC2 istanze e al EBS volume a un elenco di tag di inclusione o a un elenco di tag di esclusione. Le risorse associate ai tag che aggiungi a un elenco di tag di inclusione vengono analizzate alla ricerca di malware, mentre quelle associate a un elenco di tag di esclusione non vengono scansionate. Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente.

Conservazione delle istantanee

Quando GuardDuty Malware Protection for EC2 è abilitato, offre la possibilità di conservare le istantanee dei EBS volumi nell'account AWS . GuardDuty genera i EBS volumi di replica in base alle istantanee dei volumi. EBS È possibile conservare le istantanee dei EBS volumi solo se Malware Protection for EC2 scan rileva il malware nei volumi di replica. EBS Se non viene rilevato alcun malware nei EBS volumi di replica, elimina GuardDuty automaticamente le istantanee dei EBS volumi, indipendentemente dall'impostazione di conservazione delle istantanee. Per ulteriori informazioni, consulta Conservazione degli snapshot.

Regola di soppressione

Le regole di soppressione automatica ti consentono di creare combinazioni di attributi molto specifiche per eliminare i risultati. Ad esempio, puoi definire una regola tramite il GuardDuty filtro per archiviare automaticamente `Recon:EC2/Portscan` solo le istanze in uno specificoVPC, in esecuzione in uno specifico AMI o con un tag specificoEC2. Questa regola comporterebbe l'archiviazione automatica dei risultati di scansione delle porte dalle istanze che soddisfano i criteri. Tuttavia, consente comunque di inviare avvisi se GuardDuty rileva che le istanze svolgono altre attività dannose, come il mining di criptovalute.

Le regole di soppressione definite nell' GuardDuty account amministratore si applicano agli account dei membri. GuardDuty GuardDuty gli account membri non possono modificare le regole di soppressione.

Con le regole di soppressione, genera GuardDuty comunque tutti i risultati. Le regole di soppressione consentono di sopprimere i risultati mantenendo nel contempo uno storico non modificabile di tutte le attività.

In genere, le regole di soppressione vengono utilizzate per nascondere i risultati che sono stati determinati come falsi positivi per l'ambiente e ridurre il rumore derivante da risultati di basso valore, in modo da potersi concentrare sulle minacce più grandi. Per ulteriori informazioni, consulta Regole di eliminazione.

Elenco di indirizzi IP affidabili

Un elenco di indirizzi IP affidabili per comunicazioni altamente sicure con l' AWS ambiente in uso. GuardDuty non genera risultati basati su elenchi di IP affidabili. Per ulteriori informazioni, consulta Utilizzo di elenchi di indirizzi IP affidabili ed elenchi minacce.

Elenco di IP delle minacce

Un elenco degli indirizzi IP dannosi noti. Oltre a generare risultati a causa di un'attività potenzialmente sospetta, genera GuardDuty anche risultati basati su questi elenchi di minacce. Per ulteriori informazioni, consulta Utilizzo di elenchi di indirizzi IP affidabili ed elenchi minacce.

Guida introduttiva con GuardDuty

Questo tutorial fornisce un'introduzione pratica a. GuardDuty I requisiti minimi per l'abilitazione GuardDuty come account autonomo o come GuardDuty amministratore AWS Organizations sono descritti nella Fase 1. I passaggi da 2 a 5 riguardano l'utilizzo di funzionalità aggiuntive consigliate da GuardDuty per ottenere il massimo dai risultati.

Argomenti

Prima di iniziare

GuardDuty è un servizio di rilevamento delle minacce che monitora GuardDuty fonti di dati fondamentali registri degli AWS CloudTrail eventi, eventi di AWS CloudTrail gestione, Amazon VPC Flow Logs e log. DNS GuardDuty analizza anche le funzionalità associate ai suoi tipi di protezione solo se le abiliti separatamente. Le funzionalità includono registri di controllo Kubernetes, attività di RDS accesso, registri S3, EBS volumi, monitoraggio del runtime e registri delle attività di rete Lambda. L'utilizzo di queste fonti di dati e funzionalità (se abilitate), genera risultati di sicurezza per il tuo account. GuardDuty

Dopo l'attivazione GuardDuty, inizia a monitorare l'ambiente. Puoi disattivarlo GuardDuty per qualsiasi account in qualsiasi regione, in qualsiasi momento. Ciò GuardDuty impedirà l'elaborazione delle fonti di dati di base e di tutte le funzionalità che sono state abilitate separatamente.

Non è necessario abilitare esplicitamente le GuardDuty fonti di dati fondamentali. Amazon GuardDuty estrae flussi di dati indipendenti direttamente da tali servizi. Per un nuovo GuardDuty account, tutti i tipi di protezione disponibili supportati in un Regione AWS sono abilitati e inclusi nel periodo di prova gratuito di 30 giorni per impostazione predefinita. È possibile disattivarne alcuni o tutti. Se sei un GuardDuty cliente esistente, puoi scegliere di abilitare uno o tutti i piani di protezione disponibili nel tuo Regione AWS. Per ulteriori informazioni, consulta Funzionalità associate a ciascun tipo di protezione in GuardDuty.

Durante l'attivazione GuardDuty, considera i seguenti elementi:

- GuardDuty è un servizio regionale, il che significa che tutte le procedure di configurazione seguite in questa pagina devono essere ripetute in ogni regione con cui si desidera monitorare GuardDuty.

  Ti consigliamo vivamente di abilitarlo GuardDuty in tutte le AWS regioni supportate. Ciò consente di GuardDuty generare informazioni su attività non autorizzate o insolite anche nelle Regioni che non utilizzi attivamente. Ciò consente anche di GuardDuty monitorare AWS CloudTrail gli eventi per AWS servizi globali comeIAM. Se non GuardDuty è abilitato in tutte le regioni supportate, la sua capacità di rilevare attività che coinvolgono servizi globali è ridotta. Per un elenco completo delle regioni in cui GuardDuty è disponibile, consultaRegioni ed endpoint.
- Qualsiasi utente con privilegi di amministratore in un AWS account può eseguire l'attivazione GuardDuty, tuttavia, seguendo la migliore pratica di sicurezza del privilegio minimo, si consiglia di creare un IAM ruolo, un utente o un gruppo da gestire GuardDuty in modo specifico. Per informazioni sulle autorizzazioni necessarie per l'attivazione, vedere. GuardDuty Autorizzazioni necessarie per abilitare GuardDuty
- Quando si abilita GuardDuty per la prima volta in qualsiasi regione Regione AWS, per impostazione predefinita, vengono attivati anche tutti i tipi di protezione disponibili supportati in quella regione, inclusa Malware Protection forEC2. GuardDuty crea un ruolo collegato al servizio per il tuo account chiamato. `AWSServiceRoleForAmazonGuardDuty` Questo ruolo include le autorizzazioni e le politiche di fiducia che consentono GuardDuty di utilizzare e analizzare gli eventi direttamente dal GuardDuty fonti di dati fondamentali per generare risultati di sicurezza. Malware Protection for EC2 crea un altro ruolo collegato al servizio per l'account chiamato. `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Questo ruolo include le autorizzazioni e le politiche di fiducia che consentono a Malware Protection di EC2 eseguire scansioni senza agenti per rilevare il malware nell'account. GuardDuty Consente di GuardDuty creare un'istantanea di EBS volume nell'account e di condividerla con l'account del servizio. GuardDuty Per ulteriori informazioni, consulta Autorizzazioni di ruolo collegate ai servizi per GuardDuty. Per ulteriori informazioni sui ruoli collegati ai servizi, consulta Utilizzo di ruoli collegati ai servizi.

- Quando lo attivi GuardDuty per la prima volta in qualsiasi regione, il tuo AWS account viene automaticamente registrato a una prova GuardDuty gratuita di 30 giorni per quella regione.

Guida introduttiva: abilitare Amazon GuardDuty per ambienti autonomi o con più account

Passaggio 1: abilitare Amazon GuardDuty

Il primo passaggio per utilizzarlo GuardDuty è abilitarlo nel tuo account. Una volta abilitato, GuardDuty inizierà immediatamente a monitorare le minacce alla sicurezza nella regione corrente.

Se desideri gestire GuardDuty i risultati di altri account all'interno della tua organizzazione in qualità di GuardDuty amministratore, devi aggiungere e abilitare anche GuardDuty gli account dei membri.

> **Note**
>
> Se desideri abilitare GuardDuty Malware Protection for S3 senza attivarlo GuardDuty, per la procedura, consultaGuardDuty Protezione da malware per S3.

Standalone account environment

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/
2. Seleziona l'opzione Amazon GuardDuty - Tutte le funzionalità.
3. Scegli Avvia.
4. Nella GuardDuty pagina Benvenuto, visualizza i termini del servizio. Scegli Abilita GuardDuty.

Multi-account environment

> **Important**
>
> Come prerequisiti per questo processo, devi far parte della stessa organizzazione di tutti gli account che desideri gestire e avere accesso all'account di AWS Organizations gestione per delegare un amministratore GuardDuty all'interno dell'organizzazione. Potrebbero essere necessarie autorizzazioni aggiuntive per delegare un amministratore. Per maggiori informazioni, consulta Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty .

Per designare un account amministratore delegato GuardDuty

1. Apri la AWS Organizations console all'indirizzo https://console.aws.amazon.com/organizations/, utilizzando l'account di gestione.

2. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   È GuardDuty già abilitata nel tuo account?

   - Se non GuardDuty è già abilitato, puoi selezionare Inizia e quindi designare un amministratore GuardDuty delegato nella pagina Benvenuto GuardDuty.
   - Se GuardDuty è abilitato, puoi designare un amministratore GuardDuty delegato nella pagina Impostazioni.

3. Inserisci l'ID dell'account a dodici cifre dell' AWS account che desideri designare come amministratore delegato dell'organizzazione e scegli GuardDuty Delegato.

> **Note**
>
> Se non GuardDuty è già abilitato, la designazione di un amministratore delegato lo abiliterà per quell'account nella regione corrente. GuardDuty

Per aggiungere account membri

Questa procedura prevede l'aggiunta di account membri a un account amministratore GuardDuty delegato tramite. AWS Organizations In alternativa è possibile aggiungere membri tramite invito. Per ulteriori informazioni su entrambi i metodi di associazione dei membri in GuardDuty, consulta. Gestione di più account in Amazon GuardDuty

1. Accedere all'account amministratore delegato
2. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
3. Nel riquadro di navigazione, scegliere Settings (Impostazioni), quindi Accounts (Account).

   Nella tabella account vengono visualizzati tutti gli account dell'organizzazione.

4. Scegli gli account che desideri aggiungere come membri selezionando la casella accanto all'ID account. Quindi, dal menu Operazione seleziona Aggiungi membro.

> **Tip**
>
> Puoi automatizzare l'aggiunta di nuovi account come membri attivando la funzionalità di Abilitazione automatica, che però si applica solo agli account che entrano a far parte dell'organizzazione dopo l'abilitazione della funzionalità.

Fase 2: generare esiti di esempio ed esplorare le operazioni di base

Quando GuardDuty rileva un problema di sicurezza, genera un risultato. Un GuardDuty risultato è un set di dati contenente dettagli relativi a quell'unico problema di sicurezza. I dettagli dell'esito possono essere utilizzati per indagare sul problema.

GuardDuty supporta la generazione di risultati di esempio con valori segnaposto, che possono essere utilizzati per testare GuardDuty la funzionalità e acquisire familiarità con i risultati prima di dover rispondere a un problema di sicurezza reale scoperto da. GuardDuty Segui la guida riportata di seguito per generare risultati di esempio per ogni tipo di risultato disponibile. Per ulteriori modi per generare risultati di esempio GuardDuty, inclusa la generazione di un evento di sicurezza simulato all'interno del tuo account, consulta. Risultati di esempio

Per creare ed esplorare gli esiti di esempio

1. Nel pannello di navigazione scegli Impostazioni.
2. Nella pagina Settings (Impostazioni), in Sample findings (Risultati di esempio), selezionare Generate sample findings (Genera risultati di esempio).
3. Nel riquadro di navigazione, scegli Riepilogo per visualizzare le informazioni dettagliate sui risultati generati nel tuo AWS ambiente. Per ulteriori informazioni sui componenti del pannello di Riepilogo, consulta Pannello di riepilogo.
4. Nel riquadro di navigazione, seleziona Esiti. I risultati di esempio vengono visualizzati nella pagina Risultati correnti con il prefisso [SAMPLE].
5. Seleziona un esito dall'elenco per visualizzarne i dettagli.

    - È possibile esaminare i diversi campi informativi disponibili nel riquadro dei dettagli degli esiti. Diversi tipi di esiti possono avere campi diversi. Per ulteriori informazioni sui campi disponibili in tutti i tipi di esiti, consulta Dettagli degli esiti. Dal riquadro dei dettagli, puoi effettuare le operazioni seguenti:

        - Seleziona l'ID del risultato nella parte superiore del riquadro per aprire i JSON dettagli completi del risultato. Il JSON file completo può essere scaricato anche da questo pannello. JSONContiene alcune informazioni aggiuntive non incluse nella visualizzazione della console ed è il formato che può essere acquisito da altri strumenti e servizi.

- Visualizza la sezione Risorsa interessata. In realtà, le informazioni qui riportate ti aiuteranno a identificare una risorsa del tuo account che dovrebbe essere esaminata e includeranno collegamenti a risorse appropriate AWS Management Console per l'utilizzo.
- Seleziona l'icona che raffigura una lente di ingrandimento con i simboli "+" o "-" per creare un filtro inclusivo o esclusivo per il dettaglio selezionato. Per ulteriori informazioni sui filtri per gli esiti, consulta Filtro dei risultati.

6. Archiviare tutti gli esiti di esempio

   a. Seleziona tutti gli esiti tramite la casella di controllo nella parte superiore dell'elenco.

   b. Deseleziona gli esiti che desideri conservare.

   c. Seleziona il menu Operazioni, quindi scegli Archivia per nascondere gli esiti di esempio.

> **Note**
>
> Per visualizzare gli esiti archiviati, seleziona Correnti, quindi Archiviati per cambiare la visualizzazione degli esiti.

Fase 3: configurare l'esportazione dei GuardDuty risultati in un bucket Amazon S3

GuardDuty consiglia di configurare le impostazioni per esportare i risultati perché consente di esportare i risultati in un bucket S3 per l'archiviazione a tempo indeterminato oltre il periodo di conservazione di 90 giorni. GuardDuty Ciò consente di tenere traccia dei risultati o tenere traccia dei problemi all'interno del proprio ambiente nel tempo. AWS Il processo descritto qui ti guida nella configurazione di un nuovo bucket S3 e nella creazione di una nuova KMS chiave per crittografare i risultati dall'interno della console. Per ulteriori informazioni su questo argomento, ad esempio su come utilizzare il tuo bucket esistente o il bucket di un altro account, consulta Esportazione degli esiti.

Per configurare l'opzione di esportazione degli esiti in S3

1. Per crittografare i risultati, avrai bisogno di una KMS chiave con una politica che GuardDuty consenta di utilizzare tale chiave per la crittografia. I seguenti passaggi ti aiuteranno a creare una nuova KMS chiave. Se utilizzi una KMS chiave di un altro account, devi applicare la politica delle chiavi accedendo al Account AWS proprietario della chiave. La regione della KMS chiave e del

bucket S3 devono essere uguali. Tuttavia, puoi utilizzare lo stesso bucket e la stessa coppia di chiavi per ogni regione da cui desideri esportare gli esiti.

a. Apri la AWS KMS console in /kms. https://console.aws.amazon.com

b. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.

c. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.

d. Scegliere Create key (Crea chiave).

e. Scegli Simmetrico in Tipo di chiave, quindi Successivo.

> **Note**
>
> Per i passaggi dettagliati sulla creazione della KMS chiave, consulta Creazione delle chiavi nella Guida per gli sviluppatori.AWS Key Management Service

f. Fornisci un Alias per la tua chiave, quindi scegli Successivo.

g. Scegli Successivo, quindi nuovamente Successivo per accettare le autorizzazioni di amministrazione e utilizzo predefinite.

h. Dopo aver effettuato la Revisione della configurazione, scegli Fine per creare la chiave.

i. Nella pagina Chiavi gestite dal cliente, scegli l'alias della chiave.

j. Nella scheda Policy della chiave, scegli Passa alla visualizzazione della policy.

k. Scegli Modifica e aggiungi la seguente politica chiave alla tua KMS chiave, che GuardDuty consente l'accesso alla tua chiave. Questa dichiarazione consente di GuardDuty utilizzare solo la chiave a cui aggiungi questa politica. Quando modificate la politica dei tasti, assicuratevi che la JSON sintassi sia valida. Se aggiungi l'istruzione prima dell'istruzione finale, devi aggiungere una virgola dopo la parentesi di chiusura.

```
{
    "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"
        }
    }
}
```

Replace (Sostituisci) *Region1* con la regione della tua KMS chiave. Replace (Sostituisci) *444455556666* con quello Account AWS che possiede la KMS chiave. Replace (Sostituisci) *KMSKeyId* con l'ID della KMS chiave che hai scelto per la crittografia. Per identificare tutti questi valori: regione e ID chiave, visualizza ARNla KMS chiave. Account AWS Per individuare la chiaveARN, consulta Trovare l'ID della chiave e ARN.

Allo stesso modo, sostituisci *111122223333* con il Account AWS nome dell' GuardDuty account. Replace (Sostituisci) *Region2* con la regione dell' GuardDuty account. Replace (Sostituisci) *SourceDetectorID* con l'ID del rilevatore dell' GuardDuty account per *Region2*.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

l. Seleziona Salva.

2. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
3. Nel pannello di navigazione scegli Impostazioni.
4. Nella sezione Opzioni di esportazione dei risultati, scegli Configura ora.
5. Scegli Nuovo bucket. Fornisci un nome univoco per il bucket S3.
6. (Facoltativo) puoi testare le nuove impostazioni di esportazione generando esiti di esempio. Nel pannello di navigazione scegli Impostazioni.
7. Nella pagina Risultati di esempio, scegli Genera risultati di esempio. I nuovi risultati di esempio verranno visualizzati come voci nel bucket S3 creato da entro un massimo GuardDuty di cinque minuti.

Passaggio 4: configura gli avvisi di GuardDuty ricerca tramite SNS

GuardDuty si integra con Amazon EventBridge, che può essere utilizzato per inviare i dati dei risultati ad altre applicazioni e servizi per l'elaborazione. Con EventBridge puoi utilizzare GuardDuty i risultati

per avviare risposte automatiche ai tuoi risultati collegando gli eventi di ricerca a obiettivi come AWS Lambda funzioni, automazione di Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS) e altro ancora.

In questo esempio creerai un SNS argomento come obiettivo di una EventBridge regola, quindi lo utilizzerai EventBridge per creare una regola da cui acquisisca i dati dei risultati. GuardDuty La regola risultante inoltra i dettagli degli esiti a un indirizzo e-mail. Per scoprire come inviare gli esiti a Slack o Amazon Chime e come modificare i tipi di esiti per cui vengono inviati gli avvisi, consulta Impostare un argomento Amazon SNS e un endpoint.

Per creare un SNS argomento per i tuoi avvisi sui risultati

1. Apri la SNS console Amazon su https://console.aws.amazon.com/sns/v3/home.
2. Nel pannello di navigazione, scegli Topics (Argomenti).
3. Seleziona Create Topic (Crea argomento).
4. Per Tipo, seleziona Standard.
5. Per Nome, immetti **`GuardDuty`**.
6. Seleziona Create Topic (Crea argomento). Verranno aperti i dettagli dell'argomento per il nuovo argomento.
7. Nella sezione Subscriptions (Sottoscrizioni) scegliere Create subscription (Crea sottoscrizione).
8. Per Protocollo, scegli E-mail.
9. Per Endpoint, inserisci l'indirizzo e-mail a cui desideri che vengano inviate le notifiche.
10. Scegli Crea sottoscrizione.

    Dopo aver creato la sottoscrizione è necessario confermarla tramite e-mail.
11. Per verificare la presenza di un messaggio di sottoscrizione, vai alla tua casella di posta elettronica e nel messaggio di sottoscrizione scegli Conferma sottoscrizione.

> **Note**
>
> Per controllare lo stato dell'e-mail di conferma, vai alla SNS console e scegli Abbonamenti.

Per creare una EventBridge regola per acquisire GuardDuty i risultati e formattarli

1. Apri la EventBridge console all'indirizzo https://console.aws.amazon.com/events/.

2. Nel pannello di navigazione, scegli Regole.
3. Scegli Create rule (Crea regola).
4. Inserire un nome e una descrizione per la regola.

   Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso router di eventi.
5. Per Event bus (Bus di eventi), scegli default.
6. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
7. Scegli Next (Successivo).
8. Per Event source (Origine eventi), seleziona AWS events (Eventi).
9. Per Modello di eventi, scegli Modulo di modello di eventi.
10. Per Origine evento, scegli Servizi AWS .
11. Per Servizio AWS , scegli GuardDuty.
12. Per Tipo di evento, scegli GuardDutyRicerca.
13. Scegli Next (Successivo).
14. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).
15. Per Seleziona un obiettivo, scegli un SNSargomento e per Argomento, scegli il nome dell'SNSargomento che hai creato in precedenza.
16. Nella sezione Impostazioni aggiuntive, per Configura input di destinazione, scegli Trasformatore di input.

    L'aggiunta di un trasformatore di input formatta i dati di JSON ricerca inviati GuardDuty in un messaggio leggibile dall'uomo.
17. Seleziona Configure input transformer (Configura trasformatore di input).
18. Nella sezione Trasformatore di input di destinazione, in Percorso di input, incolla il codice seguente:

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

```
}
```

19. Per formattare l'e-mail, in Modello, incolla il codice seguente e assicurati di sostituire il testo in rosso con i valori appropriati alla tua regione:

```
"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. Scegli Conferma.
21. Scegli Next (Successivo).
22. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta i EventBridge tag Amazon nella Amazon EventBridge User Guide.
23. Scegli Next (Successivo).
24. Rivedi i dettagli della regola e scegli Create rule (Crea regola).
25. (Facoltativo) Testa la tua nuova regola generando esiti di esempio con il processo descritto nella fase 2. Riceverai un'e-mail per ogni esito di esempio generato.

Passaggi successivi

Continuando a utilizzare GuardDuty, imparerai a comprendere i tipi di risultati rilevanti per il tuo ambiente. Ogni volta che ricevi un nuovo esito, puoi trovare diverse informazioni, come i consigli su come correggerlo, selezionando Ulteriori informazioni dalla descrizione nel riquadro dei dettagli degli esiti o cercando il nome dell'esito su Tipi di esiti.

Le seguenti funzionalità ti aiuteranno a ottimizzare GuardDuty in modo che possa fornire i risultati più pertinenti per il tuo AWS ambiente:

- Per ordinare facilmente i risultati in base a criteri specifici, come l'ID dell'istanza, l'ID dell'account, il nome del bucket S3 e altro, puoi creare e salvare filtri all'interno. GuardDuty Per ulteriori informazioni, consulta Filtro dei risultati.
- Se ricevi esiti relativi al comportamento previsto nel tuo ambiente, puoi archiviarli automaticamente in base ai criteri definiti con le regole di eliminazione.

- Per evitare che i risultati vengano generati da un sottoinsieme di siti affidabili IPs o per far sì che il GuardDuty monitoraggio IPs non rientri nel normale ambito di monitoraggio, puoi impostare elenchi di indirizzi IP e minacce affidabili.

GuardDuty fonti di dati fondamentali

GuardDuty utilizza le fonti di dati di base per rilevare le comunicazioni con domini e indirizzi IP dannosi noti e identificare comportamenti potenzialmente anomali e attività non autorizzate. Durante il transito da queste fonti a GuardDuty, tutti i dati di registro vengono crittografati. GuardDutyestrae vari campi da queste fonti di log per la profilazione e il rilevamento delle anomalie, quindi elimina questi registri.

Quando si abilita GuardDuty per la prima volta in una regione, è disponibile una prova gratuita di 30 giorni che include il rilevamento delle minacce per tutte le fonti di dati di base. Durante questa prova gratuita, puoi monitorare un utilizzo mensile stimato suddiviso per ciascuna fonte di dati fondamentale. In qualità di account GuardDuty amministratore delegato, puoi visualizzare il costo di utilizzo mensile stimato suddiviso per ogni account membro che appartiene alla tua organizzazione e che è stato abilitato. GuardDuty Al termine del periodo di prova di 30 giorni, puoi utilizzarlo AWS Billing per ottenere informazioni sul costo di utilizzo.

Non sono previsti costi aggiuntivi per l' GuardDuty accesso agli eventi e ai log da queste fonti di dati fondamentali.

Dopo averlo abilitato GuardDuty Account AWS, inizia automaticamente a monitorare le fonti di registro spiegate nelle sezioni seguenti. Non è necessario abilitare nient'altro per iniziare GuardDuty ad analizzare ed elaborare queste fonti di dati per generare i risultati di sicurezza associati.

Argomenti

AWS CloudTrail eventi di gestione

AWS CloudTrail fornisce una cronologia delle AWS API chiamate relative all'account, incluse API le chiamate effettuate utilizzando gli AWS Management Console strumenti a riga di comando e determinati AWS servizi. AWS SDKs CloudTrail consente inoltre di identificare gli utenti e gli account richiamati AWS APIs per i servizi che supportano CloudTrail, l'indirizzo IP di origine da cui sono state richiamate le chiamate e l'ora in cui sono state richiamate le chiamate. Per ulteriori informazioni, consulta Che cos'è AWS CloudTrail? nella Guida per l'utente di AWS CloudTrail .

GuardDuty monitora gli eventi CloudTrail di gestione, noti anche come eventi del piano di controllo. Questi eventi forniscono informazioni dettagliate sulle operazioni di gestione eseguite sulle risorse dell' AWS account.

Di seguito sono riportati alcuni esempi di eventi CloudTrail gestionali GuardDuty monitorati:

- Configurazione della sicurezza (operazioni) IAM `AttachRolePolicy` API
- Configurazione delle regole per il routing dei dati (Amazon EC2 `CreateSubnet` API operations)
- Configurazione della registrazione (operazioni)AWS CloudTrail `CreateTrail` API

Quando viene abilitata GuardDuty, inizia a consumare gli eventi di CloudTrail gestione direttamente CloudTrail attraverso un flusso di eventi indipendente e duplicato e analizza i CloudTrail registri degli eventi.

GuardDuty non gestisce CloudTrail gli eventi né influisce sulle configurazioni esistenti. CloudTrail Allo stesso modo, le CloudTrail configurazioni non influiscono sul modo in cui GuardDuty utilizza ed elabora i registri degli eventi. Per gestire l'accesso e la conservazione dei tuoi CloudTrail eventi, utilizza la console di CloudTrail servizio o. API Per ulteriori informazioni, consulta Visualizzazione degli eventi con cronologia degli CloudTrail eventi nella Guida AWS CloudTrail per l'utente.

Come GuardDuty gestisce gli eventi AWS CloudTrail globali

Per la maggior parte AWS dei servizi, CloudTrail gli eventi vengono registrati nel Regione AWS luogo in cui vengono creati. Per i servizi globali come AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon e CloudFront Amazon Route 53 (Route 53), gli eventi vengono generati solo nella regione in cui si verificano, ma hanno un'importanza globale.

Quando GuardDuty utilizza eventi di servizio CloudTrail globali con valori di sicurezza come configurazioni di rete o autorizzazioni utente, replica tali eventi e li elabora in ogni regione in cui sono stati abilitati. GuardDuty Questo comportamento aiuta a GuardDuty mantenere i profili utente e di ruolo in ogni regione, il che è fondamentale per rilevare eventi anomali.

Ti consigliamo vivamente di abilitare GuardDuty tutto ciò che è abilitato per Regioni AWS il tuo. Account AWS Ciò aiuta a GuardDuty generare informazioni su attività non autorizzate o insolite anche in quelle regioni che potresti non utilizzare attivamente.

Log di flusso VPC

La funzionalità VPC Flow Logs di Amazon VPC acquisisce informazioni sul traffico IP in entrata e in uscita dalle interfacce di rete collegate alle istanze Amazon Elastic Compute Cloud (AmazonEC2) all'interno del tuo ambiente. AWS

Quando lo abiliti GuardDuty, inizia immediatamente ad analizzare i log di VPC flusso EC2 dalle istanze Amazon all'interno del tuo account. Utilizza gli eventi dei log di VPC flusso direttamente dalla funzione VPC Flow Logs attraverso un flusso indipendente e duplicato di log di flusso. Questo processo non altera alcuna configurazione di log di flusso esistente.

Protezione Lambda

> Lambda Protection è un miglioramento opzionale di Amazon. GuardDuty Attualmente, Lambda Network Activity Monitoring include i log di flusso VPC Amazon di tutte le funzioni Lambda del tuo account, anche quelli che non utilizzano la rete. VPC Per proteggere la tua funzione Lambda da potenziali minacce alla sicurezza, dovrai configurare Lambda Protection nel tuo account. GuardDuty Per ulteriori informazioni, consulta Protezione Lambda.

GuardDuty Monitoraggio del runtime

> Se gestisci il security agent (manualmente o tramite GuardDuty) in EKS Runtime Monitoring o Runtime Monitoring per EC2 istanze ed GuardDuty è attualmente distribuito su un'EC2istanza Amazon e riceve Tipi di eventi di runtime raccolti da questa istanza, non GuardDuty ti verrà addebitato alcun costo Account AWS per l'analisi dei log di VPC flusso di questa istanza Amazon. EC2 Questo aiuta a GuardDuty evitare il doppio dei costi di utilizzo dell'account.

GuardDuty non gestisce i log di flusso né li rende accessibili nel tuo account. Per gestire l'accesso e la conservazione dei log di flusso, devi configurare la funzione VPC Flow Logs.

Registri delle interrogazioni di Route53 Resolver DNS

Se utilizzi AWS DNS resolver per le tue EC2 istanze Amazon (l'impostazione predefinita), GuardDuty puoi accedere ed elaborare i log delle query di Route53 Resolver di richiesta e risposta tramite i DNS resolver interni. AWS DNS Se utilizzi un altro DNS resolver, come Open DNS o Google, o se configuri i tuoi resolverDNS, non puoi accedere ed elaborare i dati da questa fonte di dati. DNS GuardDuty

Quando lo abiliti GuardDuty, inizia immediatamente ad analizzare i log delle query di Route53 DNS Resolver da un flusso di dati indipendente. Questo flusso di dati è separato dai dati forniti tramite la funzionalità di Registrazione delle query del Route 53 Resolver. La configurazione di questa funzionalità non influisce sull'analisi. GuardDuty

> **Note**
>
> GuardDuty non supporta DNS i log di monitoraggio per EC2 le istanze Amazon avviate su AWS Outposts perché la funzionalità di registrazione delle Amazon Route 53 Resolver query non è disponibile in quell'ambiente.

Attivazione delle funzionalità in GuardDuty

Quando abiliti Amazon GuardDuty per la prima volta o abiliti un tipo di protezione all'interno GuardDuty, GuardDuty avvia l'elaborazione del corrispondente Origini dati fondamentali all'interno del tuo AWS ambiente. GuardDuty utilizza queste fonti di dati per elaborare un flusso di eventi, come registri di VPC flusso, DNS registri e registri di AWS CloudTrail eventi e gestione. Successivamente analizza questi eventi per identificare potenziali minacce alla sicurezza e genera esiti nel tuo account.

Oltre alle fonti di dati di registro, GuardDuty può utilizzare dati aggiuntivi provenienti da altri AWS servizi AWS dell'ambiente per monitorare e analizzare potenziali minacce alla sicurezza.

Attivazioni delle funzionalità

Quando aggiungi GuardDuty protezioni aggiuntive, ad esempio S3 Protection, Runtime Monitoring o EKS Protection, puoi configurare la GuardDuty funzionalità corrispondente al tipo di protezione. Storicamente, GuardDuty le protezioni venivano chiamate in. `dataSources` APIs Tuttavia, dopo marzo 2023, i nuovi tipi di GuardDuty protezione sono ora configurati come `features` e non. `dataSources` GuardDuty supporta ancora la configurazione dei tipi di protezione lanciati prima di marzo 2023, come `dataSources` tramite ilAPI, ma i nuovi tipi di protezione sono disponibili solo come`features`.

Se gestisci i tipi di GuardDuty configurazione e protezione tramite la console, non sei direttamente interessato da questa modifica e non devi intraprendere alcuna azione. L'attivazione delle funzionalità influisce sul comportamento di coloro APIs che vengono richiamati per abilitare GuardDuty o sui tipi di protezione inclusi. GuardDuty Per ulteriori informazioni, consulta GuardDuty APImodifiche.

GuardDuty APImodifiche a marzo 2023

GuardDuty APIsConfigura le funzionalità di protezione che non appartengono all'elenco diGuardDuty fonti di dati fondamentali. Gli oggetti funzionalità contengono dettagli sulla funzionalità, come il nome e lo stato, e possono contenere configurazioni aggiuntive per alcune funzionalità. Questa migrazione influisce su quanto segue APIs in Amazon GuardDuty API Reference:

- CreateDetector
- GetDetector
- UpdateDetector
- GetMemberDetectors

- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

Attivazione delle funzionalità rispetto alle origini dati

Storicamente, tutte le GuardDuty funzionalità venivano trasmesse attraverso un `dataSources` oggetto in. API A partire da marzo 2023, GuardDuty preferisce `features` l'oggetto anziché l'`dataSources`oggetto in. API Tutte le origini dati precedenti hanno funzionalità corrispondenti, ma le funzionalità più recenti potrebbero non avere origini dati corrispondenti.

L'elenco seguente mostra il confronto tra `dataSources` un `features` oggetto quando viene passato attraverso unAPI:

- L'oggetto `dataSources` contiene oggetti per ogni tipo di protezione e il relativo stato. L'`features`oggetto è un elenco di funzionalità disponibili che corrispondono a ciascun tipo di protezione all'interno GuardDuty.

  A partire da marzo 2023, l'attivazione delle funzionalità sarà l'unico modo per configurare nuove GuardDuty funzionalità nel proprio AWS ambiente.
- Lo `dataSources` schema nella API richiesta o nella risposta è lo stesso in tutti i paesi in Regione AWS cui GuardDuty è disponibile. Tuttavia, è possibile che non tutte le funzionalità siano disponibili in ogni regione. Pertanto, i nomi delle funzionalità disponibili possono variare in base alla regione.

Comprensione del funzionamento dell'attivazione delle funzionalità

GuardDuty APIsContinueranno a restituire un `dataSources` oggetto, se applicabile, e restituiranno anche un `features` oggetto contenente le stesse informazioni in un formato diverso. GuardDuty le funzionalità lanciate prima di marzo 2023 saranno disponibili tramite `dataSources` object and `features` object. GuardDuty le funzionalità lanciate a partire da marzo 2023 saranno disponibili solo tramite l'`features`oggetto. Non è possibile creare o aggiornare un rilevatore o descrivere AWS Organizations l'utilizzo di entrambi `dataSources` e della notazione `features` dell'oggetto nella stessa API richiesta. Per abilitare i tipi di GuardDuty protezione, è necessario migrare le fonti

di dati esistenti `features` sull'oggetto utilizzando le stesse fonti APIs che ora includono anche l'`features`oggetto.

> **Note**
>
> GuardDuty non aggiungerà una nuova fonte di dati dopo questa modifica.

GuardDuty ha reso obsoleto l'uso delle fonti di dati. Tuttavia, supporta ancora le GuardDuty fonti di dati fondamentali. Le GuardDuty migliori pratiche consigliano di utilizzare l'attivazione delle funzionalità per tutti i tipi di protezione già abilitati per l'account. Le best practice richiedono anche l'utilizzo dell'attivazione delle funzionalità quando abiliti un nuovo tipo di protezione per il tuo account.

Incorporazione delle modifiche all'attivazione delle funzionalità

- Se gestisci GuardDuty le configurazioni tramite APIsSDKs, o AWS CloudFormation template e desideri abilitare potenziali nuove GuardDuty funzionalità, dovrai modificare rispettivamente il codice e il modello. Per ulteriori informazioni, consulta l'aggiornamento APIs in Amazon GuardDuty API Reference.
- Per GuardDuty le funzionalità configurate prima di questo aggiornamento, puoi continuare a utilizzare il AWS CloudFormation modello APIsSDKs, o. Tuttavia, ti consigliamo di passare all'utilizzo dell'oggetto `feature`.

  Tutte le origini dati hanno un oggetto funzionalità equivalente. Per ulteriori informazioni, consulta Mappatura di `dataSources` su `features`.
- Attualmente, la `additionalConfiguration` nell'oggetto `features` è disponibile solo per determinati tipi di protezione.
  - Per questi tipi di protezione, se la funzionalità `AdditionalConfiguration` `status` è impostata su `ENABLED` ma la configurazione della funzionalità non `status` è impostata su`ENABLED`, non GuardDuty intraprenderà alcuna azione in questo caso.
  - Ciò influisce APIs su quanto segue:
    - UpdateDetector
    - UpdateMemberDetectors
    - UpdateOrganizationConfiguration

Mappatura di **`dataSources`** su **`features`**

La tabella seguente mostra la mappatura dei tipi di protezione, delle `dataSources` e delle `features`.

GuardDuty tipo di protezione	Nome della fonte di dati*	Nome della funzionalità
Log di flusso VPC	`flowLogs` (sola lettura; non possono essere modificati)	`FLOW_LOGS` (sola lettura; non possono essere modificati)
Registri delle interrogazioni di Route53 Resolver DNS	`dnsLogs` (sola lettura; non possono essere modificati)	`DNS_LOGS` (sola lettura; non possono essere modificati)
CloudTrail eventi	`cloudTrail` (sola lettura; non possono essere modificati)	`CLOUD_TRAIL` (sola lettura; non possono essere modificati)
S3	`s3Logs`	`S3_DATA_EVENTS`
EKSMonitoraggio dei registri di controllo	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Protezione da malware per EC2	`malwareProtection.scanEc2InstanceWithFindings.ebsVolumes`	`EBS_MALWARE_PROTECTION`
RDSEventi di accesso	GuardDuty fornisce solo il supporto per l'attivazione delle funzionalità per questi tipi di protezione.	`RDS_LOGIN_EVENTS`
EKSMonitoraggio del runtime		`EKS_RUNTIME_MONITORING`
Monitoraggio del runtime		`RUNTIME_MONITORING`

GuardDuty tipo di protezione	Nome della fonte di dati*	Nome della funzionalità

GuardDuty agente di sicurezza per EKS cluster Amazon		`EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`
		
		`RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`

GuardDuty agente di sicurezza per cluster Amazon ECS -Fargate		`RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT`
GuardDuty agente di sicurezza per EC2 istanze Amazon		`RUNTIME_MONITORING.additionalConfiguration.EC2_AGENT_MANAGEMENT`

GuardDuty tipo di protezione	Nome della fonte di dati*	Nome della funzionalità
Protezione Lambda		LAMBDA_NETWORK_LOGS

*GetUsageStatistics utilizza i propri nomi di `dataSource`. Per ulteriori informazioni, consulta Stima dei costi GuardDuty o GetUsageStatistics.

GuardDuty Protezione S3

S3 Protection aiuta Amazon a GuardDuty monitorare gli eventi AWS CloudTrail relativi ai dati per Amazon Simple Storage Service (Amazon S3) che includono API operazioni a livello di oggetto per identificare potenziali rischi per la sicurezza dei dati all'interno dei bucket Amazon S3.

GuardDuty monitora sia gli eventi di AWS CloudTrail gestione che gli eventi relativi ai dati AWS CloudTrail S3 per identificare potenziali minacce nelle tue risorse Amazon S3. Le due origini dati monitorano diversi tipi di attività. Esempi di eventi di CloudTrail gestione per S3 includono operazioni che elencano o configurano i bucket Amazon S3, `ListBuckets` come`DeleteBuckets`, e. `PutBucketReplication` Esempi di eventi CloudTrail relativi ai dati per S3 includono API operazioni a livello di oggetto, come,, e. `GetObject` `ListObjects` `DeleteObject` `PutObject`

Quando abiliti Amazon GuardDuty for an Account AWS, GuardDuty inizia a monitorare gli eventi CloudTrail di gestione. Non è necessario abilitare o configurare in modo esplicito la registrazione degli eventi di dati S3 AWS CloudTrail per utilizzare S3 Protection. Puoi abilitare la funzionalità S3 Protection (che monitora gli eventi CloudTrail relativi ai dati per S3) per qualsiasi account in qualsiasi Regione AWS luogo in cui questa funzionalità è disponibile in Amazon GuardDuty, in qualsiasi momento. Se è Account AWS già abilitata GuardDuty, puoi abilitare S3 Protection per la prima volta con un periodo di prova gratuito di 30 giorni. Per una versione Account AWS che viene abilitata GuardDuty per la prima volta, S3 Protection è già abilitata e inclusa in questa prova gratuita di 30 giorni. Per ulteriori informazioni, consulta Stima dei costi GuardDuty .

Ti consigliamo di abilitare S3 Protection in. GuardDuty Se questa funzionalità non è abilitata, non GuardDuty sarà possibile monitorare completamente i bucket Amazon S3 o generare rilevazioni di accessi sospetti ai dati archiviati nei bucket S3.

Come vengono utilizzati gli eventi relativi ai dati di S3 GuardDuty

Quando abiliti gli eventi relativi ai dati S3 (S3 Protection), GuardDuty inizia ad analizzare gli eventi relativi ai dati S3 provenienti da tutti i bucket S3 e li monitora per rilevare eventuali attività dannose e sospette. Per ulteriori informazioni, consulta AWS CloudTrail eventi relativi ai dati per S3.

Quando un utente non autenticato accede a un oggetto S3, significa che l'oggetto S3 è accessibile pubblicamente. Pertanto, GuardDuty non elabora tali richieste. GuardDuty elabora le richieste fatte agli oggetti S3 utilizzando credenziali valide IAM (AWS Identity and Access Management) o AWS STS (AWS Security Token Service).

> **Nota**
>
> Dopo aver abilitato S3 Protection, Amazon GuardDuty monitora gli eventi relativi ai dati da quei bucket Amazon S3 che risiedono nella stessa regione in cui hai abilitato. GuardDuty

Quando GuardDuty rileva una potenziale minaccia sulla base del monitoraggio degli eventi relativi ai dati di S3, genera una rilevazione di sicurezza. Per informazioni sui tipi di risultati che è GuardDuty possibile generare per i bucket Amazon S3, consulta. GuardDuty Tipi di ricerca S3

Se disabiliti S3 Protection, GuardDuty interrompe il monitoraggio degli eventi relativi ai dati archiviati nei bucket S3 di S3.

Funzionalità della Protezione S3

AWS CloudTrail eventi relativi ai dati per S3

Gli eventi di dati, anche conosciuti come operazioni del piano dati, forniscono informazioni dettagliate sulle operazioni eseguite su una risorsa o al suo interno e sono spesso attività che interessano volumi elevati di dati.

Di seguito sono riportati alcuni esempi di eventi CloudTrail relativi ai dati per S3 che è GuardDuty possibile monitorare:

- `GetObject`APIoperazioni
- `PutObject`APIoperazioni
- `ListObjects`APIoperazioni
- `DeleteObject`APIoperazioni

Quando si abilita GuardDuty per la prima volta, S3 Protection è abilitato per impostazione predefinita ed è incluso anche nel periodo di prova gratuito di 30 giorni. Tuttavia, questa funzionalità è facoltativa e puoi scegliere di abilitarla o disabilitarla in qualsiasi momento e per qualsiasi account o regione. Per ulteriori informazioni sulla configurazione della funzionalità di Amazon S3, consulta Protezione S3.

Configurazione della Protezione S3 per un account autonomo

Per gli account associati da AWS Organizations, questo processo può essere automatizzato tramite le impostazioni della console. Per ulteriori informazioni, consulta Configurazione della Protezione S3 in ambienti con più account.

Per abilitare o disabilitare la Protezione S3

Scegli il metodo di accesso che preferisci per configurare la Protezione S3 per un account autonomo.

Console

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Protezione S3.
3. La pagina Protezione S3 fornisce lo stato attuale della Protezione S3 per il tuo account. Scegli Abilita o Disabilita per abilitare o disabilitare in qualsiasi momento la Protezione S3.
4. Scegli Conferma per confermare la selezione.

API/CLI

1. Esegui updateDetector utilizzando l'ID rilevatore valido per la regione attuale e impostando il `name` dell'oggetto `features` da `S3_DATA_EVENTS` a `ENABLED` o `DISABLED` rispettivamente per abilitare o disabilitare la Protezione S3.

   > **Note**
   >
   > Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

2. In alternativa, puoi usare AWS Command Line Interface. Per abilitare la Protezione S3, esegui il comando seguente e assicurati di utilizzare il tuo ID rilevatore valido.

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

   Per disabilitare la Protezione S3, sostituisci `ENABLED` con `DISABLED` nell'esempio.

Configurazione della Protezione S3 in ambienti con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di configurare (abilitare o disabilitare) S3 Protection per gli account dei membri della propria organizzazione. AWS GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. L'account GuardDuty amministratore delegato può scegliere di abilitare automaticamente S3 Protection su tutti gli account, solo sui nuovi account o su nessun account dell'organizzazione. Per ulteriori informazioni, consulta Gestione degli account con AWS Organizations.

Configurazione di S3 Protection per l'account amministratore delegato GuardDuty

Scegli il metodo di accesso preferito per configurare S3 Protection per l'account amministratore delegato. GuardDuty

Console

1. Apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/

   Assicurati di utilizzare le credenziali dell'account di gestione.
2. Nel riquadro di navigazione, scegli Protezione S3.
3. Nella pagina Protezione S3, scegli Modifica.
4. Esegui una di queste operazioni:

   Utilizzando Abilita per tutti gli account

   - Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi AWS dell'organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
   - Seleziona Salva.

   Utilizzando Configura gli account manualmente

   - Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
   - Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
   - Seleziona Salva.

API/CLI

Esegui updateDetectorutilizzando l'ID del rilevatore dell'account GuardDuty amministratore delegato per la regione corrente e passando l'`features`oggetto di tanto in `name` tanto`S3_DATA_EVENTS`. `status` `ENABLED`

In alternativa, puoi configurare S3 Protection utilizzando. AWS Command Line Interface Esegui il comando seguente e assicurati di sostituirlo *`12abc34d567e8fa901bc2d34e56789f0`* con l'ID del rilevatore dell'account GuardDuty amministratore delegato per la regione corrente.

Per trovare il nome del `detectorId` tuo account e della regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

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

Abilitare automaticamente la Protezione S3 per tutti gli account membri dell'organizzazione

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando il tuo account amministratore.
2. Esegui una di queste operazioni:

   Utilizzando la pagina Protezione S3

   1. Nel riquadro di navigazione, scegli Protezione S3.
   2. Scegli Abilita per tutti gli account. Questa operazione abilita automaticamente la Protezione S3 per gli account dell'organizzazione esistenti e per quelli nuovi.
   3. Seleziona Salva.

   > **Note**
   >
   > L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, scegli Abilita per tutti gli account in Protezione S3.
4. Seleziona Salva.

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta Abilitare o disabilitare in modo selettivo la Protezione S3 negli account membri.

API/CLI

- Per abilitare o disabilitare in modo selettivo S3 Protection per i tuoi account membro, richiama l'updateMemberDetectorsAPIoperazione utilizzando il tuo *detector ID*.
- L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. Assicurati di sostituire *12abc34d567e8fa901bc2d34e56789f0* con `detector-id` l'account GuardDuty amministratore delegato e *111122223333*. Per disabilitare S3 Protection, sostituisci `ENABLED` con`DISABLED`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

  > **Note**
  >
  > Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle

impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare la Protezione S3 per tutti gli account membri attivi esistenti

Scegli il metodo di accesso che preferisci per abilitare la Protezione S3 per tutti gli account membri attivi esistenti dell'organizzazione.

Console

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, scegli Protezione S3.
3. Nella pagina Protezione S3, puoi visualizzare lo stato attuale della configurazione. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Conferma.

API/CLI

- Per abilitare o disabilitare in modo selettivo S3 Protection per i tuoi account membro, richiama l'operazione utilizzando le tue updateMemberDetectorsAPI *`detector ID`*.
- L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. Assicurati di sostituire *`12abc34d567e8fa901bc2d34e56789f0`* con `detector-id` l'account GuardDuty amministratore delegato e *`111122223333`*. Per disabilitare S3 Protection, sostituisci `ENABLED` con`DISABLED`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

> **Note**
>
> Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare automaticamente la Protezione S3 per i nuovi account membri

Scegli il metodo di accesso che preferisci per abilitare la Protezione S3 per i nuovi account che entrano a far parte dell'organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare nuovi account membro in un'organizzazione tramite la console, utilizzando la pagina S3 Protection o Account.

Per abilitare automaticamente la Protezione S3 per i nuovi account membri

1. Apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Esegui una di queste operazioni:
   - Utilizzando la pagina Protezione S3:
     1. Nel riquadro di navigazione, scegli Protezione S3.
     2. Nella pagina Protezione S3, scegli Modifica.
     3. Scegli Configura gli account manualmente.
     4. Seleziona Abilita automaticamente per i nuovi account membri. Questa fase garantisce l'abilitazione automatica della Protezione S3 per ogni nuovo account che entra a far parte dell'organizzazione. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
     5. Seleziona Salva.
   - Utilizzando la pagina Account:

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
3. Nella finestra Gestisci le preferenze di abilitazione automatica, seleziona Abilita per nuovi account in Protezione S3.
4. Seleziona Salva.

API/CLI

- Per abilitare o disabilitare in modo selettivo S3 Protection per i tuoi account membro, richiama l'operazione utilizzando il UpdateOrganizationConfigurationAPItuo *`detector ID`*.
- L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. Per disabilitarla, consulta Abilitare o disabilitare in modo selettivo la Protezione S3 negli account membri. Imposta le preferenze in modo da abilitare o disabilitare automaticamente il piano di protezione in una determinata regione per i nuovi account che entrano a far parte dell'organizzazione (`NEW`), per tutti gli account (`ALL`) o per nessuno degli account dell'organizzazione (`NONE`). Per ulteriori informazioni, consulta Membri. autoEnableOrganization In base alle tue preferenze, potrebbe essere necessario sostituire `NEW` con `ALL` o `NONE`.

  Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare o disabilitare in modo selettivo la Protezione S3 negli account membri

Scegli il metodo di accesso che preferisci per abilitare o disabilitare in modo selettivo la Protezione S3 per gli account membri.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).

   Nella pagina Account, consulta la colonna Protezione S3 per visualizzare lo stato del tuo account membro.

3. Per abilitare o disabilitare in modo selettivo la Protezione S3

   Seleziona l'account per il quale desideri configurare la Protezione S3. Puoi selezionare più account alla volta. Nel menu a discesa Modifica piani di protezione, scegli S3Pro, quindi scegli l'opzione appropriata.

API/CLI

Per abilitare o disabilitare in modo selettivo S3 Protection per i tuoi account membro, esegui l'updateMemberDetectorsAPIoperazione utilizzando il tuo ID di rilevamento. L'esempio seguente mostra come abilitare la Protezione S3 per un singolo account membro. Per disabilitarla, sostituisci `true` con `false`.

Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

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

> **Note**
>
> Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

> **Note**
>
> Se utilizzi script per inserire nuovi account e desideri disabilitare S3 Protection nei nuovi account, puoi modificare l'createDetectorAPIoperazione con l'`dataSources`oggetto opzionale come descritto in questo argomento.

Disabilitazione automatica di S3 Protection per nuovi account GuardDuty

> **Important**
>
> Per impostazione predefinita, S3 Protection è abilitata automaticamente per Account AWS quel join GuardDuty per la prima volta.

Se sei un account GuardDuty amministratore che abilita GuardDuty per la prima volta un nuovo account e non desideri che S3 Protection sia abilitato per impostazione predefinita, puoi disabilitarlo modificando l'createDetectorAPIoperazione con l'oggetto opzionale. `features` L'esempio seguente utilizza AWS CLI per abilitare un nuovo GuardDuty rilevatore con la protezione S3 disabilitata.

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

GuardDuty EKSProtezione

EKSAudit Log Monitoring ti aiuta a rilevare attività potenzialmente sospette nei EKS cluster all'interno di Amazon Elastic Kubernetes Service (Amazon). EKS EKSAudit Log Monitoring utilizza i log di EKS controllo per acquisire le attività cronologiche degli utenti, delle applicazioni che utilizzano Kubernetes e del piano di controllo. API Per ulteriori informazioni, consulta EKSmonitoraggio dei registri di controllo.

> **Note**
>
> EKSII Runtime Monitoring è gestito come parte di Runtime Monitoring. Per ulteriori informazioni, consulta GuardDuty Monitoraggio del runtime.

Funzionalità di EKS protezione

EKSmonitoraggio dei registri di controllo

EKSi log di controllo registrano le azioni sequenziali all'interno del EKS cluster Amazon, incluse le attività degli utenti, le applicazioni che utilizzano Kubernetes API e il piano di controllo. La registrazione di audit è un componente di tutti i cluster Kubernetes.

Per ulteriori informazioni, consultare Auditing nella documentazione Kubernetes.

Amazon EKS consente di EKS importare i log di controllo come Amazon CloudWatch Logs tramite la funzionalità di registrazione del piano di EKScontrollo. GuardDuty non gestisce la registrazione del piano di EKS controllo Amazon né rende accessibili i log di EKS controllo nel tuo account se non li hai abilitati per Amazon. EKS Per gestire l'accesso e la conservazione dei log di EKS controllo, devi configurare la funzionalità di registrazione del piano EKS di controllo di Amazon. Per ulteriori informazioni, consulta Abilitazione e disabilitazione dei log del piano di controllo nella Amazon EKS User Guide.

Per informazioni sulla configurazione di EKS Audit Log Monitoring, consulta. EKSMonitoraggio dei registri di controllo

EKSMonitoraggio dei registri di controllo

EKSAudit Log Monitoring ti aiuta a rilevare attività potenzialmente sospette nei tuoi EKS cluster all'interno di Amazon Elastic Kubernetes Service. Quando abiliti EKS Audit Log Monitoring, inizia GuardDuty immediatamente EKSmonitoraggio dei registri di controllo a monitorare EKS i cluster Amazon e ad analizzarli alla ricerca di attività potenzialmente dannose e sospette. Utilizza gli eventi dei log di controllo Kubernetes direttamente dalla funzionalità di registrazione del piano di EKS controllo di Amazon attraverso un flusso indipendente e duplicato di log di audit. Questo processo non richiede alcuna configurazione aggiuntiva né influisce sulle configurazioni di registrazione EKS del piano di controllo Amazon esistenti che potresti avere.

Quando disabiliti EKS Audit Log Monitoring, interrompe GuardDuty immediatamente il monitoraggio e l'analisi dei log di EKS audit per le tue risorse AmazonEKS.

EKSAudit Log Monitoring potrebbe non essere disponibile Regioni AWS ovunque GuardDuty sia disponibile. Per ulteriori informazioni, consulta Disponibilità di funzionalità specifiche per ogni regione.

In che modo il periodo di prova gratuito di 30 giorni influisce sugli account GuardDuty

- Quando lo abiliti GuardDuty per la prima volta, EKS Audit Log Monitoring è già incluso nel periodo di prova gratuito di 30 giorni.
- GuardDuty Gli account esistenti, per i quali è già terminata la prova gratuita di 30 giorni, possono abilitare EKS Audit Log Monitoring per la prima volta con un periodo di prova gratuito di 30 giorni.

Configurazione di EKS Audit Log Monitoring per un account autonomo

Scegli il tuo metodo di accesso preferito per abilitare o disabilitare il monitoraggio EKS dei log di controllo per un account autonomo.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli EKS Protezione.
3. Nella scheda Configurazione, puoi visualizzare lo stato di configurazione corrente di EKS Audit Log Monitoring. Nella sezione EKSAudit Log Monitoring, scegli Abilita per abilitare o Disabilita per disabilitare la funzionalità EKS Audit Log Monitoring.
4. Seleziona Salva.

API/CLI

- Esegui l'updateDetectorAPIoperazione utilizzando l'ID del rilevatore regionale dell'account GuardDuty amministratore delegato e passando il nome dell'`features`oggetto come `EKS_AUDIT_LOGS` e lo status come `ENABLED` o. `DISABLED`

  In alternativa, è anche possibile abilitare o disabilitare EKS Audit Log Monitoring eseguendo il comando a AWS CLI . Il codice di esempio seguente abilita GuardDuty EKS Audit Log Monitoring. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

Configurazione del monitoraggio EKS dei registri di controllo in ambienti con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di abilitare o disabilitare la funzionalità EKS Audit Log Monitoring per gli account membri della propria organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. Questo account GuardDuty amministratore delegato può scegliere di abilitare automaticamente il monitoraggio dei registri di EKS controllo per tutti i nuovi account quando entrano a far parte dell'organizzazione. Per ulteriori informazioni sugli ambienti con più account, consulta Gestione di più account in Amazon. GuardDuty

Configurazione del monitoraggio dei log EKS di controllo per l'account amministratore delegato GuardDuty

Scegli il metodo di accesso preferito per configurare EKS Audit Log Monitoring per l'account amministratore delegato. GuardDuty

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

Assicurati di utilizzare le credenziali dell'account di gestione.

2. Nel riquadro di navigazione, scegli EKS Protezione.
3. Nella scheda Configurazione, è possibile visualizzare lo stato di configurazione corrente di EKS Audit Log Monitoring nella rispettiva sezione. Per aggiornare la configurazione per l'account GuardDuty amministratore delegato, scegli Modifica nel riquadro EKSAudit Log Monitoring.
4. Esegui una di queste operazioni:

   Utilizzando Abilita per tutti gli account

   - Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi nell' AWS organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
   - Seleziona Salva.

   Utilizzando Configura gli account manualmente

   - Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
   - Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
   - Seleziona Salva.

API/CLI

Esegui l'updateDetectorAPIoperazione utilizzando il tuo ID regionale del rilevatore e passando l'`features`oggetto `name` come `EKS_AUDIT_LOGS` e `status` come `ENABLED` o. `DISABLED`

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

È possibile abilitare o disabilitare il monitoraggio dei registri di EKS controllo eseguendo il AWS CLI comando seguente. Assicurati di utilizzare un account di GuardDuty amministratore delegato valido *`detector ID`*.

> **Note**
>
> Il codice di esempio seguente abilita EKS Audit Log Monitoring. Assicurati di sostituire *12abc34d567e8fa901bc2d34e56789f0* con `detector-id` l'account GuardDuty amministratore delegato e *555555555555* con Account AWS l' GuardDuty account amministratore delegato.

Per trovare l'`detectorId`account e la regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

Per disabilitare EKS Audit Log Monitoring, sostituisci `ENABLED` con`DISABLED`.

Abilita automaticamente il monitoraggio EKS dei registri di controllo per tutti gli account membri

Scegli il metodo di accesso preferito per abilitare l'EKSAudit Log Monitoring per gli account membro esistenti nella tua organizzazione.

Console

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Esegui una di queste operazioni:

   Utilizzo della pagina Protezione EKS

   1. Nel riquadro di navigazione, scegli EKSProtezione.
   2. Nella scheda Configurazione, puoi visualizzare lo stato attuale di EKS Audit Log Monitoring per gli account dei membri attivi nell'organizzazione.

      Per aggiornare la configurazione EKS di Audit Log Monitoring, scegli Modifica.
   3. Scegli Abilita per tutti gli account. Questa azione abilita automaticamente il monitoraggio dei registri di EKS controllo sia per gli account esistenti che per quelli nuovi dell'organizzazione.

4. Seleziona Salva.

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di attivazione automatica, scegli Abilita per tutti gli account in Monitoraggio del registro di EKS controllo.
4. Seleziona Salva.

Se non puoi utilizzare l'opzione Abilita per tutti gli account e desideri personalizzare la configurazione di EKS Audit Log Monitoring per account specifici della tua organizzazione, consultaAbilita o disabilita in modo selettivo il monitoraggio EKS dei log di controllo per gli account dei membri.

API/CLI

- Per abilitare o disabilitare EKS in modo selettivo il monitoraggio dei log di controllo per i tuoi account membri, esegui l'updateMemberDetectorsAPIoperazione utilizzando il tuo *`detector ID`*.
- L'esempio seguente mostra come abilitare l'EKSAudit Log Monitoring per un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

> **Note**
>
> Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita EKS il monitoraggio dei log di controllo per tutti gli account membri attivi esistenti

Scegli il tuo metodo di accesso preferito per abilitare EKS Audit Log Monitoring per tutti gli account membri attivi esistenti nell'organizzazione.

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, scegli EKS Protezione.
3. Nella pagina EKSProtezione, puoi visualizzare lo stato corrente della configurazione della scansione antimalware GuardDuty avviata. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Seleziona Salva.

API/CLI

- Per abilitare o disabilitare EKS in modo selettivo il monitoraggio dei log di controllo per i tuoi account membri, esegui l'updateMemberDetectorsAPIoperazione utilizzando il tuo *detector ID*.

- L'esempio seguente mostra come abilitare l'EKSAudit Log Monitoring per un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

  > **Note**
  >
  > Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita automaticamente il monitoraggio EKS dei registri di controllo per gli account dei nuovi membri

Gli account membro appena aggiunti devono essere abilitati GuardDuty prima di selezionare la configurazione della scansione GuardDuty antimalware avviata. Gli account membri gestiti su invito possono configurare manualmente la scansione antimalware GuardDuty avviata per i propri account. Per ulteriori informazioni, consulta Step 3 - Accept an invitation.

Scegliete il metodo di accesso preferito per abilitare l'EKSAudit Log Monitoring per i nuovi account che entrano a far parte della vostra organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare il monitoraggio dei registri di EKS controllo per i nuovi account membri di un'organizzazione, utilizzando la pagina EKSAudit Log Monitoring o Account.

Per abilitare automaticamente il monitoraggio EKS dei registri di controllo per gli account dei nuovi membri

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una di queste operazioni:
   - Utilizzo della pagina EKSProtezione:
     1. Nel riquadro di navigazione, scegli EKSProtezione.
     2. Nella pagina EKSProtezione, scegli Modifica nel Monitoraggio del EKSregistro di controllo.
     3. Scegli Configura gli account manualmente.
     4. Seleziona Abilita automaticamente per i nuovi account membri. Questo passaggio garantisce che ogni volta che un nuovo account si unisce all'organizzazione, EKS Audit Log Monitoring venga automaticamente abilitato per tale account. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
     5. Seleziona Salva.
   - Utilizzando la pagina Account:
     1. Dal riquadro di navigazione, selezionare Accounts (Account).
     2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
     3. Nella finestra Gestisci le preferenze di attivazione automatica, seleziona Abilita per nuovi account in Monitoraggio del registro di EKS controllo.
     4. Seleziona Salva.

API/CLI

- Per abilitare o disabilitare EKS in modo selettivo il monitoraggio dei registri di controllo per i nuovi account, esegui l'UpdateOrganizationConfigurationAPIoperazione utilizzando il tuo *`detector ID`*.
- L'esempio seguente mostra come abilitare EKS Audit Log Monitoring per i nuovi membri che entrano a far parte dell'organizzazione. Puoi anche passare un elenco di account IDs separati da uno spazio.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

Abilita o disabilita in modo selettivo il monitoraggio EKS dei log di controllo per gli account dei membri

Scegli il metodo di accesso preferito per abilitare o disabilitare il monitoraggio EKS dei registri di controllo per gli account membri selettivi della tua organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Dal riquadro di navigazione, selezionare Accounts (Account).

   Nella pagina Account, consulta la colonna EKSAudit Log Monitoring per lo stato del tuo account membro.
3. Per abilitare o disabilitare il monitoraggio EKS dei registri di controllo

   Seleziona un account che desideri configurare per il monitoraggio EKS dei registri di controllo. Puoi selezionare più account alla volta. Nel menu a discesa Modifica piani di protezione, scegli EKSAudit Log Monitoring, quindi scegli l'opzione appropriata.

API/CLI

Per abilitare o disabilitare EKS in modo selettivo il monitoraggio dei log di controllo per i tuoi account membri, richiama l'updateMemberDetectorsAPIoperazione utilizzando la tua *`detector ID`*.

L'esempio seguente mostra come abilitare l'EKSAudit Log Monitoring per un account con un solo membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`. Puoi anche passare un elenco di account IDs separati da uno spazio.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

GuardDuty Monitoraggio del runtime

Runtime Monitoring osserva e analizza gli eventi a livello di sistema operativo, di rete e di file per aiutarti a rilevare potenziali minacce in carichi di AWS lavoro specifici del tuo ambiente.

AWS Risorse supportate in Runtime Monitoring: inizialmente GuardDuty aveva rilasciato Runtime Monitoring per supportare solo le risorse Amazon Elastic Kubernetes Service (Amazon). EKS Ora puoi utilizzare la funzionalità Runtime Monitoring per rilevare le minacce anche per le tue risorse AWS Fargate Amazon Elastic Container Service (AmazonECS) e Amazon Elastic Compute Cloud (AmazonEC2).

GuardDuty non supporta i EKS cluster Amazon in esecuzione su. AWS Fargate

In questo documento e in altre sezioni relative al Runtime Monitoring, GuardDuty utilizza la terminologia del tipo di risorsa per fare riferimento alle risorse AmazonEKS, Fargate ECS Amazon e EC2 Amazon.

Runtime Monitoring utilizza un agente di GuardDuty sicurezza che aggiunge visibilità al comportamento di runtime, come l'accesso ai file, l'esecuzione dei processi, gli argomenti della riga di comando e le connessioni di rete. Per ogni tipo di risorsa che desideri monitorare per rilevare potenziali minacce, puoi gestire l'agente di sicurezza per quel tipo di risorsa specifico automaticamente o manualmente (ad eccezione di Fargate (ECSsolo Amazon)). La gestione automatica del security agent significa che autorizzi GuardDuty l'installazione e l'aggiornamento del security agent per tuo conto. D'altra parte, quando gestisci manualmente il security agent per le tue risorse, sei responsabile dell'installazione e dell'aggiornamento del security agent, se necessario.

Grazie a questa funzionalità estesa, GuardDuty può aiutarvi a identificare e rispondere a potenziali minacce che possono colpire le applicazioni e i dati in esecuzione nei singoli carichi di lavoro e istanze. Ad esempio, una minaccia può iniziare potenzialmente compromettendo un singolo contenitore che esegue un'applicazione web vulnerabile. Questa applicazione Web potrebbe disporre delle autorizzazioni di accesso ai contenitori e ai carichi di lavoro sottostanti. In questo scenario, credenziali configurate in modo errato potrebbero potenzialmente portare a un accesso più ampio all'account e ai dati in esso archiviati.

Analizzando gli eventi di runtime dei singoli contenitori e carichi di lavoro, è GuardDuty possibile identificare eventuali violazioni di un container e delle relative AWS credenziali in una fase iniziale e rilevare tentativi di aumentare i privilegi, le API richieste sospette e l'accesso malevolo ai dati nell'ambiente.

Indice

Come funziona

Per utilizzare Runtime Monitoring, è necessario abilitare il Runtime Monitoring e quindi gestire il security agent. GuardDuty L'elenco seguente illustra questo processo in due fasi:

1. Abilita il monitoraggio del runtime per il tuo account in modo che GuardDuty possa accettare gli eventi di runtime che riceve dalle tue EC2 istanze Amazon, dai ECS cluster Amazon e dai carichi di lavoro AmazonEKS.
2. Gestisci l' GuardDuty agente per le singole risorse di cui desideri monitorare il comportamento di runtime. In base al tipo di risorsa, è possibile scegliere di distribuire il GuardDuty security agent manualmente o consentendone la gestione GuardDuty per conto dell'utente, operazione denominata configurazione automatizzata dell'agente.

   GuardDuty utilizza i ruoli di identità dell'istanza che autenticano il security agent per ogni tipo di risorsa per inviare gli eventi di runtime associati all'endpoint. VPC

> **Note**
>
> GuardDuty non rende gli eventi di runtime accessibili all'utente.

Se gestisci il security agent (manualmente o tramite GuardDuty) in EKS Runtime Monitoring o Runtime Monitoring per EC2 istanze ed GuardDuty è attualmente distribuito su un'EC2istanza Amazon e riceve Tipi di eventi di runtime raccolti da questa istanza, non GuardDuty ti verrà addebitato alcun costo Account AWS per l'analisi dei log di VPC flusso di questa istanza Amazon. EC2 Questo aiuta a GuardDuty evitare il doppio dei costi di utilizzo dell'account.

I seguenti argomenti spiegano come l'attivazione del Runtime Monitoring e la gestione del GuardDuty Security Agent funzionino in modo diverso per ogni tipo di risorsa.

Indice

Come funziona il monitoraggio del runtime con le EC2 istanze Amazon

Le tue EC2 istanze Amazon possono eseguire diversi tipi di applicazioni e carichi di lavoro nel tuo AWS ambiente. Quando abiliti il Runtime Monitoring e gestisci il GuardDuty security agent, ti GuardDuty aiuta a rilevare le minacce nelle EC2 istanze Amazon esistenti e in quelle potenzialmente nuove. Questa funzionalità supporta anche le EC2 istanze Amazon ECS gestite da Amazon.

L'abilitazione del Runtime GuardDuty Monitoring consente di utilizzare gli eventi di runtime provenienti dai processi attualmente in esecuzione e dai nuovi processi all'interno EC2 delle istanze Amazon. GuardDuty richiede un agente di sicurezza per inviare eventi di runtime dall'EC2istanza a GuardDuty.

Per EC2 le istanze Amazon, il GuardDuty security agent opera a livello di istanza. Puoi decidere se monitorare tutte le istanze Amazon o solo alcune EC2 istanze Amazon nel tuo account. Se desideri gestire istanze selettive, il security agent è necessario solo per queste istanze.

GuardDuty può anche utilizzare eventi di runtime da nuove attività e attività esistenti eseguite in EC2 istanze Amazon all'interno di ECS cluster Amazon.

Per installare l'agente GuardDuty di sicurezza, Runtime Monitoring offre le seguenti due opzioni:

- Utilizza la configurazione automatica degli agenti (scelta consigliata), oppure

- Gestisci manualmente l'agente di sicurezza

Utilizza la configurazione automatica degli agenti tramite GuardDuty (consigliato)

Utilizza la configurazione automatizzata dell'agente che consente GuardDuty di installare il security agent sulle tue EC2 istanze Amazon per tuo conto. GuardDuty gestisce anche gli aggiornamenti del security agent.

Per impostazione predefinita, GuardDuty installa il security agent su tutte le istanze dell'account. Se desideri GuardDuty installare e gestire il Security Agent solo per alcune EC2 istanze, aggiungi tag di inclusione o esclusione alle EC2 istanze, se necessario.

A volte, potresti non voler monitorare gli eventi di runtime per tutte le EC2 istanze Amazon che appartengono al tuo account. Nei casi in cui desideri monitorare gli eventi di runtime per un numero limitato di istanze, aggiungi un tag di inclusione come`GuardDutyManaged`: `true` a queste istanze selezionate. A partire dalla disponibilità della configurazione automatica dell'agente per AmazonEC2, se la tua EC2 istanza ha un tag di inclusione (`GuardDutyManaged`:`true`), GuardDuty rispetterà il tag e gestirà il security agent per le istanze selezionate anche quando non abiliti esplicitamente la configurazione automatica dell'agente.

D'altra parte, se esiste un numero limitato di EC2 istanze per le quali non desideri monitorare gli eventi di runtime, aggiungi un tag di esclusione (`GuardDutyManaged`:`false`) a queste istanze selezionate. GuardDuty rispetterà il tag di esclusione non installando né gestendo il security agent per queste risorse. EC2

Impatto

Quando utilizzi la configurazione automatica degli agenti in un'organizzazione Account AWS o in un'organizzazione, autorizzi GuardDuty a eseguire le seguenti operazioni per tuo conto:

- GuardDuty crea un'SSMassociazione per tutte le EC2 istanze Amazon SSM gestite e visualizzate in Fleet Manager nella https://console.aws.amazon.com/systems-manager/console.
- Utilizzo dei tag di inclusione con la configurazione automatica dell'agente disabilitata: dopo aver abilitato il Runtime Monitoring, quando non abiliti la configurazione automatica dell'agente ma aggiungi il tag di inclusione alla tua EC2 istanza Amazon, significa che stai autorizzando GuardDuty la gestione del security agent per tuo conto. SSMassociation installerà quindi il security agent in ogni istanza che ha il tag di inclusione (`GuardDutyManaged`:`true`).
- Se abiliti la configurazione automatica dell'agente, l'SSMassociazione installerà quindi il security agent in tutte le EC2 istanze che appartengono al tuo account.

- Utilizzo dei tag di esclusione con la configurazione automatica dell'agente: prima di abilitare la configurazione automatica dell'agente, quando aggiungi il tag di esclusione alla tua EC2 istanza Amazon, significa che stai autorizzando GuardDuty a impedire l'installazione e la gestione del security agent per l'istanza selezionata.

  Ora, quando abiliti la configurazione automatica dell'agente, l'SSMassociazione installerà e gestirà il security agent in tutte le EC2 istanze ad eccezione di quelle contrassegnate con il tag di esclusione.

- GuardDuty crea VPC endpoint in tutte le istanzeVPCs, comprese quelle condiviseVPCs, purché vi sia almeno un'EC2istanza Linux VPC che non si trova nello stato di terminazione o di chiusura dell'istanza. Ciò include la versione centralizzata e quella parlata. VPC VPCs GuardDuty non supporta la creazione di un VPC endpoint solo per utenti centralizzati. VPC Per ulteriori informazioni sul VPC funzionamento della soluzione centralizzata, consulta Interface VPC endpoints nel AWS Whitepaper - Building a Scalable and Secure Multi-Network Infrastructure. VPC AWS

  Per informazioni sui diversi stati delle istanze, consulta il ciclo di vita dell'istanza nella Amazon EC2 User Guide.

  GuardDuty supporta anche. Utilizzo: condiviso VPC con agenti di sicurezza automatizzati Quando tutti i prerequisiti sono stati presi in considerazione per l'organizzazione Account AWS, GuardDuty utilizzerà gli elementi condivisi VPC per ricevere eventi di runtime.

  > **Note**
  >
  > Non sono previsti costi aggiuntivi per l'utilizzo dell'VPCendpoint.

Gestisci manualmente l'agente di sicurezza

Esistono due modi per gestire EC2 manualmente il Security Agent per Amazon:

- Utilizza i documenti GuardDuty gestiti AWS Systems Manager per installare il security agent sulle EC2 istanze Amazon già SSM gestite.

  Ogni volta che avvii una nuova EC2 istanza Amazon, assicurati che sia SSM abilitata.

- Usa gli script RPM package manager (RPM) per installare il security agent sulle tue EC2 istanze Amazon, indipendentemente dal fatto che siano gestite SSM o meno.

Approfondimenti

Per iniziare a utilizzare la configurazione di Runtime Monitoring per monitorare le tue EC2 istanze Amazon, consultaPrerequisiti per il supporto delle EC2 istanze Amazon.

Come funziona il monitoraggio del runtime con Fargate (solo AmazonECS)

Quando abiliti il monitoraggio del runtime, GuardDuty diventa pronto a consumare gli eventi di runtime di un'attività. Queste attività vengono eseguite all'interno dei ECS cluster Amazon, che a loro volta vengono eseguiti sulle AWS Fargate (Fargate) istanze. GuardDuty Per ricevere questi eventi di runtime, devi utilizzare il security agent dedicato e completamente gestito.

Runtime Monitoring supporta la gestione del security agent per i tuoi ECS cluster Amazon (AWS Fargate) solo tramite GuardDuty. Non è disponibile alcun supporto per la gestione manuale del security agent sui ECS cluster Amazon.

Puoi consentire GuardDuty la gestione del GuardDuty security agent per tuo conto, utilizzando la configurazione automatizzata dell'agente per un AWS account o un'organizzazione. GuardDuty inizierà a distribuire il security agent alle nuove attività di Fargate che vengono lanciate nei cluster AmazonECS. L'elenco seguente specifica cosa aspettarsi quando si abilita il security agent. GuardDuty

Impatto dell'attivazione del GuardDuty Security Agent

GuardDuty crea un endpoint virtuale nel cloud privato (VPC)

Quando distribuisci il GuardDuty security agent, GuardDuty creerà un VPC endpoint attraverso il quale il security agent consegna gli eventi di runtime. GuardDuty

> **Note**
>
> - Utilizzo di agenti centralizzati VPC con agenti automatizzati: quando utilizzi la configurazione GuardDuty automatizzata degli agenti per un tipo di risorsa, GuardDuty creerà un VPC endpoint per tuo conto per tutti i. VPCs Ciò include quella centralizzata VPC e parlata. VPCs GuardDuty non supporta la creazione di un VPC endpoint solo per utenti centralizzati. VPC Per ulteriori informazioni sul VPC funzionamento della soluzione centralizzata, consulta Interface VPC endpoints nel AWS Whitepaper - Building a Scalable and Secure Multi-Network Infrastructure. VPC AWS
> - Non sono previsti costi aggiuntivi per l'utilizzo dell'endpoint. VPC

GuardDuty aggiunge un contenitore sidecar

Per una nuova attività o servizio Fargate che inizia a funzionare, un GuardDuty container (sidecar) si collega a ciascun contenitore all'interno dell'attività Amazon Fargate. ECS L'agente GuardDuty di sicurezza viene eseguito all'interno del contenitore collegato. GuardDuty Questo aiuta GuardDuty a raccogliere gli eventi di runtime di ogni contenitore in esecuzione nell'ambito di queste attività.

Quando si avvia un'attività Fargate, se il GuardDuty contenitore (sidecar) non è in grado di avviarsi in uno stato integro, il Runtime Monitoring è progettato per non impedire l'esecuzione delle attività.

Per impostazione predefinita, un'attività Fargate è immutabile. GuardDuty non distribuirà il sidecar quando un'attività è già in esecuzione. Se desideri monitorare un contenitore in un'attività già in esecuzione, puoi interrompere l'attività e riavviarla.

Come funziona il Runtime Monitoring con i EKS cluster Amazon

Runtime Monitoring utilizza un EKScomponente aggiuntivo `aws-guardduty-agent`, chiamato anche agente di GuardDuty sicurezza. Dopo che GuardDuty Security Agent è stato distribuito sui EKS cluster, GuardDuty è in grado di ricevere eventi di runtime per questi cluster. EKS

GuardDuty supporta i EKS cluster Amazon in esecuzione solo su EC2 istanze Amazon. GuardDuty non supporta i EKS cluster Amazon in esecuzione su. AWS Fargate

Puoi monitorare gli eventi di runtime dei tuoi EKS cluster Amazon a livello di account o di cluster. Puoi gestire l'agente GuardDuty di sicurezza solo per EKS i cluster Amazon che desideri monitorare per il rilevamento delle minacce. Puoi gestire il GuardDuty security agent manualmente o consentendone la gestione GuardDuty per tuo conto, utilizzando la configurazione automatizzata dell'agente.

Quando utilizzi l'approccio di configurazione automatizzata degli agenti GuardDuty per consentire di gestire l'implementazione del security agent per tuo conto, questo creerà automaticamente un endpoint Amazon Virtual Private Cloud (AmazonVPC). Il security agent fornisce gli eventi di runtime GuardDuty utilizzando questo VPC endpoint Amazon.

> **Note**
>
> - Non sono previsti costi aggiuntivi per l'utilizzo dell'VPCendpoint.

- Utilizzo di agenti centralizzati VPC con agenti automatizzati: quando utilizzi la configurazione GuardDuty automatica degli agenti per un tipo di risorsa, GuardDuty creerà un VPC endpoint per tuo conto per tutti. VPCs Ciò include quella centralizzata VPC e parlata. VPCs GuardDuty non supporta la creazione di un VPC endpoint solo per utenti centralizzati. VPC Per ulteriori informazioni sul VPC funzionamento della soluzione centralizzata, consulta Interface VPC endpoints nel AWS Whitepaper - Building a Scalable and Secure Multi-Network Infrastructure. VPC AWS

Dopo la configurazione del monitoraggio del runtime

Valuta la copertura del runtime

Dopo aver abilitato il Runtime Monitoring e distribuito il GuardDuty security agent, ti consigliamo di valutare continuamente lo stato di copertura della risorsa in cui hai distribuito il security agent. Lo stato della copertura potrebbe essere Inintegro o Non integro. Uno stato di copertura integro indica che GuardDuty sta ricevendo gli eventi di runtime dalla risorsa corrispondente quando è in corso un'attività a livello di sistema operativo.

Quando lo stato di copertura diventa Inattivo per la risorsa, GuardDuty è in grado di ricevere gli eventi di runtime e analizzarli per il rilevamento delle minacce. Quando GuardDuty rileva una potenziale minaccia alla sicurezza nelle attività o nelle applicazioni in esecuzione nei carichi di lavoro e nelle istanze del container, GuardDuty genera uno o più tipi di risultati di Runtime Monitoring.

Puoi anche configurare un Amazon EventBridge (EventBridge) per ricevere una notifica quando lo stato della copertura cambia da Insalutare a Healthy e altro. Per ulteriori informazioni, consulta Valutazione della copertura in termini di runtime delle risorse.

Configurazione CPU e monitoraggio della memoria per GuardDuty Security Agent

Dopo aver verificato che lo stato di copertura risulti integro, puoi valutare le prestazioni del security agent per il tuo tipo di risorsa. Per EKS i cluster Amazon con la versione Security Agent v1.5 o successiva, GuardDuty supporta la configurazione dei parametri del security agent (aggiuntivo). Per ulteriori informazioni, consulta Configurazione CPU e monitoraggio della memoria.

GuardDuty rileva potenziali minacce

Quando GuardDuty inizia a ricevere gli eventi di runtime della risorsa, inizia ad analizzarli. Quando GuardDuty rileva una potenziale minaccia alla sicurezza in una qualsiasi delle tue EC2 istanze Amazon, ECS cluster Amazon o EKS cluster Amazon, ne genera una o più. Tipi di risultati del monitoraggio del runtime Puoi accedere ai dettagli dei risultati per visualizzare i dettagli delle risorse interessate.

Come funziona la versione di prova gratuita di 30 giorni in Runtime Monitoring

Il periodo di prova gratuito di 30 giorni funziona in modo diverso per i nuovi GuardDuty account e per gli account esistenti che hanno già abilitato il EKS Runtime Monitoring prima che la funzionalità di Runtime Monitoring fosse estesa alle EC2 istanze AWS Fargate Amazon e (ECSsolo Amazon).

Sto usando il periodo di GuardDuty prova o non ho mai abilitato EKS il Runtime Monitoring

L'elenco seguente spiega come funziona il periodo di prova gratuito di 30 giorni se utilizzi il periodo di prova di GuardDuty 30 giorni o non hai mai abilitato il EKS Runtime Monitoring:

- Quando si abilita GuardDuty per la prima volta, il Runtime Monitoring e il EKS Runtime Monitoring non saranno abilitati per impostazione predefinita.

  Quando abiliti il Runtime Monitoring per il tuo account o la tua organizzazione, assicurati di configurare anche il GuardDuty security agent per la risorsa che desideri monitorare per il rilevamento delle minacce. Ad esempio, se desideri utilizzare Runtime Monitoring per le tue EC2 istanze Amazon, dopo aver abilitato il Runtime Monitoring, devi configurare anche il security agent per AmazonEC2. Puoi scegliere di farlo manualmente o automaticamente tramite GuardDuty.
- Il piano di protezione del Runtime Monitoring è abilitato a livello di account. Il periodo di prova gratuito di 30 giorni funziona a livello di risorse. Dopo la distribuzione del GuardDuty Security Agent su un tipo di risorsa specifico, la prova gratuita di 30 giorni inizia quando GuardDuty riceve il primo evento di runtime associato a questo tipo di risorsa. Ad esempio, hai distribuito l' GuardDuty agente a livello di risorsa (per l'EC2istanza Amazon, il ECS cluster Amazon e il EKS cluster Amazon). Quando GuardDuty riceve il primo evento di runtime per un'EC2istanza Amazon, la prova gratuita di 30 giorni inizierà EC2 solo per Amazon.

- Quando desideri abilitare solo il monitoraggio del EKS runtime: quando lo abiliti GuardDuty per la prima volta, il monitoraggio del EKS runtime non è abilitato per impostazione predefinita (dopo il rilascio di Runtime Monitoring). Dovrai abilitare il EKS Runtime Monitoring. Per utilizzarlo in modo ottimale, assicurati di gestire il GuardDuty security agent manualmente o di abilitare la configurazione automatica dell'agente in modo che GuardDuty gestisca l'agente per tuo conto. Il periodo di prova gratuito di 30 giorni per EKS Runtime Monitoring inizia quando GuardDuty riceve il primo evento di runtime per la EKS risorsa Amazon.

Ho abilitato EKS Runtime Monitoring prima del lancio di Runtime Monitoring

- Per un GuardDuty account esistente che ha il piano di protezione EKS Runtime Monitoring abilitato e utilizza l'esperienza della GuardDuty console per utilizzare questo piano di protezione: con l'annuncio di Runtime Monitoring, l'esperienza della console di EKS Runtime Monitoring è stata ora consolidata nel Runtime Monitoring. La configurazione esistente per EKS Runtime Monitoring rimane la stessa. È possibile continuare a utilizzareAPI/CLIsupport per eseguire operazioni associate al EKS Runtime Monitoring.
- Per utilizzare EKS Runtime Monitoring come parte di Runtime Monitoring, dovrai configurare Runtime Monitoring per il tuo account o la tua organizzazione. Per mantenere la stessa configurazione per Runtime Monitoring, vediMigrazione da EKS Runtime Monitoring a Runtime Monitoring. Tuttavia, ciò non influirà sulla prova gratuita di 30 giorni per la EKS risorsa Amazon.
- Il piano di protezione del Runtime Monitoring è abilitato a livello di account per regione. Dopo la distribuzione del GuardDuty security agent su uno dei tipi di risorse specificati (EC2istanza Amazon e ECS cluster Amazon), la prova gratuita di 30 giorni inizia quando GuardDuty riceve il primo evento di runtime associato alla risorsa. È disponibile una prova gratuita di 30 giorni associata a ciascun tipo di risorsa.

  Ad esempio, dopo aver abilitato il Runtime Monitoring, scegli di distribuire l' GuardDuty agente solo su EC2 un'istanza Amazon, la prova gratuita di 30 giorni per questa risorsa inizierà solo quando GuardDuty riceverà il primo evento di runtime per un'istanza AmazonEC2. Successivamente, quando distribuirai l' GuardDuty agente per Fargate (solo ECS Amazon), la prova gratuita di 30 giorni per questa risorsa inizierà solo GuardDuty quando riceverà il primo evento di runtime per il cluster Amazon. ECS Considerando che hai già abilitato il EKS Runtime Monitoring per il tuo account, GuardDuty non ripristina la prova gratuita di 30 giorni per una EKS risorsa Amazon.

Concetti chiave: approcci alla gestione degli agenti GuardDuty di sicurezza

Considera i concetti chiave che ti aiuteranno a gestire il security agent sui tuoi EKS cluster Amazon e sui ECS cluster Amazon.

Indice

Risorsa Fargate (ECSsolo Amazon) - Approcci alla gestione GuardDuty degli agenti di sicurezza

Runtime Monitoring ti offre la possibilità di rilevare potenziali minacce alla sicurezza su tutti i ECS cluster Amazon (a livello di account) o sui cluster selettivi (a livello di cluster) del tuo account. Quando abiliti la configurazione automatizzata degli agenti per ogni attività Amazon ECS Fargate che verrà eseguita, GuardDuty aggiungerà un contenitore secondario per ogni carico di lavoro del container all'interno di tale attività. L'agente GuardDuty di sicurezza viene distribuito in questo contenitore secondario. In questo modo si GuardDuty ottiene visibilità sul comportamento di runtime dei contenitori all'interno delle ECS attività di Amazon.

Runtime Monitoring supporta la gestione del security agent per i tuoi ECS cluster Amazon (AWS Fargate) solo tramite GuardDuty. Non è disponibile alcun supporto per la gestione manuale del security agent sui ECS cluster Amazon.

Prima di configurare i tuoi account, valuta come desideri gestire il GuardDuty security agent e potenzialmente monitora il comportamento di runtime dei contenitori che appartengono alle ECS attività di Amazon. Considera i seguenti approcci.

Argomenti

Gestisci l'agente GuardDuty di sicurezza per tutti i ECS cluster Amazon

Questo approccio ti aiuterà a rilevare potenziali minacce alla sicurezza a livello di account. Utilizza questo approccio quando desideri rilevare potenziali minacce GuardDuty alla sicurezza per tutti i ECS cluster Amazon che appartengono al tuo account.

Gestisci l'agente di GuardDuty sicurezza per la maggior parte dei ECS cluster Amazon ma escludi alcuni cluster Amazon ECS

Utilizza questo approccio quando desideri rilevare potenziali minacce GuardDuty alla sicurezza per la maggior parte dei ECS cluster Amazon nel tuo AWS ambiente ma escluderne alcuni. Questo approccio ti aiuta a monitorare il comportamento di runtime dei container all'interno delle tue ECS attività Amazon a livello di cluster. Ad esempio, il numero di ECS cluster Amazon che appartengono al tuo account è 1000. Tuttavia, desideri monitorare solo 930 ECS cluster Amazon.

Questo approccio richiede l'aggiunta di un GuardDuty tag predefinito ai ECS cluster Amazon che non desideri monitorare. Per ulteriori informazioni, consulta Gestione dell'agente di sicurezza automatizzato per Fargate (solo AmazonECS).

Gestisci l'agente GuardDuty di sicurezza per cluster Amazon ECS selettivi

Utilizza questo approccio quando desideri GuardDuty rilevare potenziali minacce alla sicurezza per alcuni ECS cluster Amazon. Questo approccio ti aiuta a monitorare il comportamento di runtime dei container all'interno delle tue ECS attività Amazon a livello di cluster. Ad esempio, il numero di ECS cluster Amazon che appartengono al tuo account è 1000. Tuttavia, desideri monitorare solo 230 cluster.

Questo approccio richiede l'aggiunta di un GuardDuty tag predefinito ai ECS cluster Amazon che desideri monitorare. Per ulteriori informazioni, consulta Gestione dell'agente di sicurezza automatizzato per Fargate (solo AmazonECS).

EKSCluster Amazon: approcci alla gestione degli agenti GuardDuty di sicurezza

GuardDuty Per utilizzare gli eventi di runtime EKS dei cluster a livello di account o di cluster, è necessario gestire il GuardDuty security agent per i cluster corrispondenti.

Approcci per gestire l'agente di sicurezza GuardDuty

Prima del 13 settembre 2023, era possibile GuardDuty configurare la gestione del security agent a livello di account. Questo comportamento indicava che, per impostazione predefinita, GuardDuty gestirà il security agent su tutti EKS i cluster che appartengono a un Account AWS. Ora GuardDuty offre una funzionalità granulare per aiutarti a scegliere EKS i cluster in cui GuardDuty gestire il security agent.

Se lo desideriGestisci manualmente l'agente di sicurezza GuardDuty , puoi comunque selezionare EKS i cluster che desideri monitorare. Tuttavia, per gestire l'agente manualmente, la creazione di un VPC endpoint Amazon per il tuo Account AWS è un prerequisito.

> **Note**
>
> Indipendentemente dall'approccio utilizzato per gestire il GuardDuty security agent, il EKS Runtime Monitoring è sempre abilitato a livello di account.

Argomenti

- Gestisci l'agente di sicurezza tramite GuardDuty
- Gestisci manualmente l'agente di sicurezza GuardDuty

Gestisci l'agente di sicurezza tramite GuardDuty

GuardDuty implementa e gestisce il security agent per tuo conto. In qualsiasi momento, puoi monitorare EKS i cluster del tuo account utilizzando uno dei seguenti approcci.

Argomenti

- Monitora tutti i cluster EKS
- Monitora tutti i EKS cluster ed escludi i cluster selettivi EKS
- Monitora i cluster selettivi EKS

Monitora tutti i cluster EKS

- Quando utilizzare questo approccio: utilizza questo approccio quando desideri GuardDuty implementare e gestire il security agent per tutti i EKS cluster del tuo account. Per impostazione

predefinita, GuardDuty distribuirà il security agent anche su un EKS cluster potenzialmente nuovo creato nel tuo account.

- Impatto dell'utilizzo di questo approccio:
  - GuardDuty crea un endpoint Amazon Virtual Private Cloud (AmazonVPC) attraverso il quale il GuardDuty security agent consegna gli eventi di GuardDuty runtime. Non sono previsti costi aggiuntivi per la creazione dell'VPCendpoint Amazon quando si gestisce il Security Agent tramite GuardDuty.
  - È necessario che il nodo di lavoro disponga di un percorso di rete valido verso un `guardduty-data` VPC endpoint attivo. GuardDuty distribuisce il security agent sui tuoi EKS cluster. Amazon Elastic Kubernetes Service (EKSAmazon) coordinerà l'implementazione del security agent sui nodi all'interno dei cluster. EKS
  - In base alla disponibilità dell'IP, GuardDuty seleziona la sottorete per creare un endpoint. VPC Se utilizzi topologie di rete avanzate, devi verificare che la connettività sia possibile.
- Considerazione: attualmente, quando si utilizza questa opzione, EKS Runtime Monitoring non crea una condivisione. VPC

Monitora tutti i EKS cluster ed escludi i cluster selettivi EKS

- Quando utilizzare questo approccio: utilizza questo approccio quando desideri GuardDuty gestire il Security Agent per tutti i EKS cluster del tuo account ma escludere i cluster selettivi. EKS Questo metodo utilizza un approccio [1] basato su tag in cui è possibile etichettare EKS i cluster per i quali non si desidera ricevere gli eventi di runtime. La coppia chiave-valore del tag predefinito deve essere `GuardDutyManaged-false`.
- Impatto dell'utilizzo di questo approccio:
  - Questo approccio richiede l'attivazione della gestione automatica degli GuardDuty agenti solo dopo aver aggiunto tag ai EKS cluster che si desidera escludere dal monitoraggio.

    Pertanto, Gestisci l'agente di sicurezza tramite GuardDuty incide anche su questo approccio. Quando aggiungi tag prima di abilitare la gestione automatica degli GuardDuty agenti, non GuardDuty distribuirà né gestirà il security agent per EKS i cluster esclusi dal monitoraggio.
- Considerazioni:
  - È necessario aggiungere la coppia chiave-valore del tag come`GuardDutyManaged`: `false` per EKS i cluster selettivi prima di abilitare la configurazione automatizzata dell'agente, altrimenti, il GuardDuty security agent verrà distribuito su tutti i cluster fino a quando non si utilizza il tag. EKS
  - È necessario fare in modo che i tag vengano modificati solo da identità affidabili.

> **Important**
>
> Gestisci le autorizzazioni per modificare il valore del `GuardDutyManaged` tag per il tuo EKS cluster utilizzando policy o policy di controllo del servizio. IAM Per ulteriori informazioni, consulta Service control policies (SCPs) nella Guida per l'AWS Organizations utente o Controllo dell'accesso alle AWS risorse nella Guida per l'IAMutente.

- Per un EKS cluster potenzialmente nuovo che non desideri monitorare, assicurati di aggiungere la `GuardDutyManaged` coppia `false` chiave-valore al momento della creazione del cluster. EKS
- La considerazione specificata per Monitora tutti i cluster EKS vale anche per questo approccio.

Monitora i cluster selettivi EKS

- Quando utilizzare questo approccio: utilizza questo approccio quando desideri GuardDuty distribuire e gestire gli aggiornamenti del Security Agent solo per i EKS cluster selettivi del tuo account. Questo metodo utilizza un approccio [1] basato su tag in cui è possibile etichettare il EKS cluster per il quale si desidera ricevere gli eventi di runtime.
- Impatto dell'utilizzo di questo approccio:
  - Utilizzando i tag di inclusione, GuardDuty implementerà e gestirà automaticamente il Security Agent solo per EKS i cluster selettivi contrassegnati con `GuardDutyManaged` - `true` come coppia chiave-valore.
  - L'utilizzo di questo approccio avrà lo stesso impatto specificato per Monitora tutti i cluster EKS.
- Considerazioni:
  - Se il valore del `GuardDutyManaged` tag non è impostato su`true`, il tag di inclusione non funzionerà come previsto e ciò potrebbe influire sul monitoraggio del cluster. EKS
  - Per garantire il monitoraggio EKS dei cluster selettivi, è necessario impedire che i tag vengano modificati, ad eccezione di identità attendibili.

> **Important**
>
> Gestisci le autorizzazioni per modificare il valore del `GuardDutyManaged` tag per il tuo EKS cluster utilizzando policy o policy di controllo del servizio. IAM Per ulteriori informazioni, consulta Service control policies (SCPs) nella Guida per l'AWS

Organizations utente o Controllo dell'accesso alle AWS risorse nella Guida per l'IAMutente.

- Per un EKS cluster potenzialmente nuovo che non desideri monitorare, assicurati di aggiungere la `GuardDutyManaged` coppia `false` chiave-valore al momento della creazione del cluster. EKS
- La considerazione specificata per Monitora tutti i cluster EKS vale anche per questo approccio.

[1] Per ulteriori informazioni sull'etichettatura di EKS cluster selettivi, consulta Tagging your Amazon resources nella EKS Amazon User Guide. EKS

Gestisci manualmente l'agente di sicurezza GuardDuty

- Quando utilizzare questo approccio: utilizza questo approccio quando desideri distribuire e gestire manualmente il GuardDuty security agent su tutti i EKS cluster. Assicurati che il EKS Runtime Monitoring sia abilitato per i tuoi account. Il GuardDuty security agent potrebbe non funzionare come previsto se non abiliti il EKS Runtime Monitoring.
- Impatto dell'utilizzo di questo approccio: sarà necessario coordinare l'implementazione del software GuardDuty Security Agent all'interno dei EKS cluster su tutti gli account e Regioni AWS laddove questa funzionalità sia disponibile.
- Considerazioni: è necessario mantenere un flusso di dati sicuro durante il monitoraggio e la risoluzione delle lacune di copertura man mano che vengono implementati nuovi cluster e carichi di lavoro.

Attivazione del monitoraggio del GuardDuty runtime

Prima di abilitare il monitoraggio del runtime nel tuo account, assicurati che il tipo di risorsa per cui desideri monitorare gli eventi di runtime supporti i requisiti della piattaforma. Per ulteriori informazioni, consulta Prerequisiti.

Se hai utilizzato EKS Runtime Monitoring prima del lancio di Runtime Monitoring, puoi utilizzare il Runtime Monitoring APIs per controllare e aggiornare la configurazione esistente per EKS Runtime Monitoring. È inoltre possibile migrare la configurazione esistente da EKS Runtime Monitoring a Runtime Monitoring. Per ulteriori informazioni, consulta Migrazione da EKS Runtime Monitoring a Runtime Monitoring.

> **Note**
>
> Attualmente, questa documentazione fornisce i passaggi per abilitare il monitoraggio del runtime per gli account e l'organizzazione solo tramite console. È inoltre possibile abilitare il monitoraggio del runtime utilizzando APIActions o AWS CLI for GuardDuty.

È possibile configurare il monitoraggio del runtime utilizzando i passaggi descritti nei seguenti argomenti.

Indice

Prerequisiti per abilitare il monitoraggio del runtime

Per abilitare il Runtime Monitoring e gestire il GuardDuty security agent, è necessario soddisfare i prerequisiti per ogni tipo di risorsa che si desidera monitorare per il rilevamento delle minacce.

Indice

Prerequisiti per il supporto delle EC2 istanze Amazon

Rendi gestite EC2 le istanze SSM

Le EC2 istanze Amazon per le quali desideri GuardDuty monitorare gli eventi di runtime devono essere gestite AWS Systems Manager (SSM). Questo indipendentemente dal fatto che tu lo utilizzi GuardDuty per gestire il security agent automaticamente o manualmente (tranneMetodo 2 - Utilizzando Linux Package Managers).

Per gestire le tue EC2 istanze Amazon con AWS Systems Manager, consulta Configurazione delle EC2 istanze di Systems Manager per Amazon nella Guida per l'AWS Systems Manager utente.

Convalida dei requisiti relativi all'architettura

L'architettura della distribuzione del sistema operativo potrebbe influire sul comportamento del GuardDuty security agent. È necessario soddisfare i seguenti requisiti prima di utilizzare Runtime Monitoring per EC2 le istanze Amazon:

- La tabella seguente mostra la distribuzione del sistema operativo che è stata verificata per supportare il GuardDuty security agent per EC2 le istanze Amazon.

Distribuzione del sistema operativo	Versione del kernel	Supporto del kernel	CPUarchitettura	
			x64 () AMD64	Gravitone () ARM64
• AL2e AL2 023 • Ubuntu 20.04 e Ubuntu 22.04 • Debian 11 e Debian 12	5.4, 5.10, 5.15, 6.1, 6.5, 6.8	eBPF, Tracepoints, Kprobe	Supportato	Supportato

- Requisiti aggiuntivi: solo se disponi di ECS Amazon/Amazon EC2

  Per ECS Amazon/AmazonEC2, ti consigliamo di utilizzare la versione più recente ECS ottimizzata per Amazon AMIs (datata 29 settembre 2023 o successiva) o di utilizzare la versione ECS dell'agente Amazon v1.77.0.

Convalida della politica di controllo dei servizi dell'organizzazione

Se avete impostato una politica di controllo del servizio (SCP) per gestire le autorizzazioni nella vostra organizzazione, verificate che il limite delle autorizzazioni non sia restrittivo. `guardduty:SendSecurityTelemetry` È necessario per supportare il monitoraggio del runtime GuardDuty su diversi tipi di risorse.

Se sei un account membro, connettiti con l'amministratore delegato associato. Per informazioni sulla gestione SCPs dell'organizzazione, consulta le politiche di controllo del servizio (SCPs).

Quando si utilizza la configurazione automatica degli agenti

Per Utilizza la configurazione automatica degli agenti (scelta consigliata) farlo, Account AWS è necessario soddisfare i seguenti prerequisiti:

- Quando utilizzi tag di inclusione con configurazione automatica degli agenti, GuardDuty per creare un'SSMassociazione per una nuova istanza, assicurati che la nuova istanza sia SSM gestita e venga visualizzata in Fleet Manager nella https://console.aws.amazon.com/systems-manager/console.
- Quando si utilizzano i tag di esclusione con la configurazione automatica degli agenti:
  - Aggiungi il `false` tag`GuardDutyManaged`: prima di configurare l'agente GuardDuty automatico per il tuo account.

    Assicurati di aggiungere il tag di esclusione alle tue EC2 istanze Amazon prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per AmazonEC2, qualsiasi EC2 istanza che viene avviata senza un tag di esclusione sarà coperta dalla configurazione GuardDuty automatizzata dell'agente.
  - Affinché i tag di esclusione funzionino, aggiorna la configurazione dell'istanza in modo che il documento di identità dell'istanza sia disponibile nel servizio di metadati dell'istanza (). IMDS La procedura per eseguire questo passaggio è già prevista Abilitazione del monitoraggio del runtime per il tuo account.

CPUe limite di memoria per l' GuardDuty agente

CPUlimite

Il CPU limite massimo per il GuardDuty security agent associato alle EC2 istanze Amazon è il 10% del totale dei v CPU core. Ad esempio, se l'EC2istanza ha 4 v CPU core, il security agent può utilizzare un massimo del 40 percento del 400 percento totale disponibile.

Memory limit (Limite memoria)

Dalla memoria associata alla tua EC2 istanza Amazon, c'è una memoria limitata che il GuardDuty Security Agent può utilizzare.

La tabella seguente mostra il limite di memoria.

Memoria dell'EC2istanza Amazon	Memoria massima per l' GuardDuty agente
Meno di 8 GB	128 MB
Meno di 32 GB	256 MB
Maggiore o uguale a 32 GB	1 GB

Approfondimenti

Il passaggio successivo consiste nella configurazione del Runtime Monitoring e nella gestione del security agent (automaticamente o manualmente).

Prerequisiti per il AWS Fargate supporto (ECSsolo Amazon)

Convalida dei requisiti relativi all'architettura

La piattaforma che utilizzi può influire sul modo GuardDuty in cui GuardDuty Security Agent supporta la ricezione degli eventi di runtime dai tuoi ECS cluster Amazon. Devi confermare di utilizzare una delle piattaforme verificate.

Considerazioni iniziali:

- La AWS Fargate (Fargate) piattaforma per i tuoi ECS cluster Amazon deve essere Linux. La versione della piattaforma corrispondente deve essere almeno`1.4.0`, o`LATEST`. Per ulteriori informazioni sulle versioni della piattaforma, consulta le versioni della piattaforma Linux nella Amazon Elastic Container Service Developer Guide.

- Le versioni della piattaforma Windows non sono ancora supportate.

Piattaforme verificate

La distribuzione e l'CPUarchitettura del sistema operativo influiscono sul supporto fornito dal GuardDuty security agent. La tabella seguente mostra la configurazione verificata per la distribuzione del GuardDuty security agent e la configurazione del Runtime Monitoring.

Distribuzione del sistema operativo	Supporto del kernel	CPUarchitettura	
		x64 () AMD64	Gravitone () ARM64

Linux	eBPF, Tracepoints, Kprobe	Supportato	Supportato

Fornisci ECR autorizzazioni e dettagli sulla sottorete

Prima di abilitare Runtime Monitoring, è necessario fornire i seguenti dettagli:

Fornisci un ruolo di esecuzione dell'attività con autorizzazioni

Il ruolo di esecuzione delle attività richiede che tu disponga di determinate autorizzazioni Amazon Elastic Container Registry (AmazonECR). Puoi utilizzare la politica mazonECSTask ExecutionRolePolicy gestita A o aggiungere le seguenti autorizzazioni alla tua `TaskExecutionRole` politica:

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

Per limitare ulteriormente le ECR autorizzazioni Amazon, puoi aggiungere il ECR repository Amazon URI che ospita il GuardDuty security agent per (ECSsolo AWS Fargate Amazon). Per ulteriori informazioni, consulta Repository per GuardDuty agente su AWS Fargate (ECSsolo Amazon).

Fornisci i dettagli della sottorete nella definizione dell'attività

Puoi fornire le sottoreti pubbliche come input nella definizione dell'attività o creare un endpoint Amazon ECRVPC.

- Utilizzo dell'opzione di definizione delle attività: l'esecuzione di CreateServicee UpdateServiceAPIsin Amazon Elastic Container Service API Reference richiede il trasferimento delle informazioni sulla sottorete. Per ulteriori informazioni, consulta le definizioni delle ECS attività di Amazon nella Amazon Elastic Container Service Developer Guide.
- Utilizzando l'opzione Amazon ECR VPC endpoint — Fornisci un percorso di rete ad Amazon ECR — Assicurati che il ECR repository Amazon URI che ospita il GuardDuty security agent sia accessibile dalla rete. Se le attività Fargate verranno eseguite in una sottorete privata, Fargate avrà bisogno del percorso di rete per scaricare il contenitore. GuardDuty

Per informazioni su come abilitare Fargate a scaricare il GuardDuty contenitore, consulta Using Amazon ECRimages with Amazon ECS nella Amazon Elastic Container Registry User Guide.

Convalida della politica di controllo dei servizi dell'organizzazione

Questo passaggio è necessario per GuardDuty supportare il monitoraggio del runtime e valutare la copertura tra diversi tipi di risorse.

Se avete impostato una policy di controllo del servizio (SCP) per gestire le autorizzazioni nella vostra organizzazione, verificate che il limite delle autorizzazioni non sia restrittivo nella vostra politica e `guardduty:SendSecurityTelemetry` nella relativa politica. `TaskExecutionRole`

La seguente politica è un esempio di autorizzazione della politica: `guardduty:SendSecurityTelemetry`

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

1. Utilizza i seguenti passaggi per verificare che il limite delle autorizzazioni non sia soggetto a restrizioni: `guardduty:SendSecurityTelemetry`

    1. Accedi a AWS Management Console e apri la console all'indirizzo. IAM https://console.aws.amazon.com/iam/
    2. Nel riquadro di navigazione, in Gestione degli accessi, scegli Ruoli.
    3. Scegli il nome del ruolo per la pagina dei dettagli.
    4. Espandi la sezione Limiti delle autorizzazioni. Assicurati che non `guardduty:SendSecurityTelemetry` sia negato o limitato.

2. Utilizza i seguenti passaggi per verificare che il limite delle autorizzazioni previsto dalla tua `TaskExecutionRole` politica non sia soggetto a restrizioni: `guardduty:SendSecurityTelemetry`

    1. Accedi a AWS Management Console e apri la console all'IAMindirizzo. https://console.aws.amazon.com/iam/
    2. Nel riquadro di navigazione, in Gestione degli accessi, scegli Politiche.
    3. Scegli il nome della politica per la pagina dei dettagli.
    4. Nella scheda Entità allegate, visualizza la sezione Allegato come limite di autorizzazioni. Assicurati che non `guardduty:SendSecurityTelemetry` sia negato o limitato.

Per informazioni sulle politiche e le autorizzazioni, consulta Limiti delle autorizzazioni nella Guida per l'IAMutente.

Se sei un account membro, connettiti con l'amministratore delegato associato. Per informazioni sulla gestione SCPs dell'organizzazione, consulta le politiche di controllo del servizio (SCPs).

CPUe limiti di memoria

Nella definizione dell'attività Fargate, è necessario specificare il valore CPU e la memoria a livello di attività. La tabella seguente mostra le combinazioni valide di valori a livello di attività e di memoria CPU e il limite massimo di memoria del GuardDuty Security Agent corrispondente per il contenitore. GuardDuty

CPUvalore	Valore memoria	GuardDuty limite massimo di memoria
256 (2,5 v) CPU	512 MiB, 1 GB, 2 GB	128 MB
512 (0,5 v) CPU	1 GB, 2 GB, 3 GB, 4 GB	
1024 (1 v) CPU	2 GB, 3 GB, 4 GB	
	5 GB, 6 GB, 7 GB, 8 GB	
2048 (2 vCPU)	Tra 4 GB e 16 GB in incrementi di 1 GB	

CPUvalore	Valore memoria	GuardDuty limite massimo di memoria
4096 (4 v) CPU	Tra 8 GB e 20 GB con incrementi di 1 GB	256 MB
8192 (8 v) CPU	Tra 16 GB e 28 GB con incrementi di 4 GB	
	Tra 32 GB e 60 GB con incrementi di 4 GB	512 MB
16384 (16 v) CPU	Tra 32 GB e 120 GB in incrementi di 8 GB	1 GB

Dopo aver abilitato il Runtime Monitoring e verificato che lo stato di copertura del cluster sia integro, puoi configurare e visualizzare le metriche di Container Insight. Per ulteriori informazioni, consulta Configurazione del monitoraggio sul ECS cluster Amazon.

Il passaggio successivo consiste nel configurare Runtime Monitoring e configurare anche il security agent.

Prerequisiti per il supporto dei EKS cluster Amazon

Convalida dei requisiti relativi all'architettura

La piattaforma utilizzata può influire sul modo GuardDuty in cui GuardDuty Security Agent supporta la ricezione degli eventi di runtime dai EKS cluster. Devi confermare di utilizzare una delle piattaforme verificate. Se gestisci l' GuardDuty agente manualmente, assicurati che la versione di Kubernetes supporti la versione dell' GuardDuty agente attualmente in uso.

Piattaforme verificate

La distribuzione del sistema operativo, la versione del kernel e CPU l'architettura influiscono sul supporto fornito dal security agent. GuardDuty La tabella seguente mostra la configurazione verificata per la distribuzione del GuardDuty security agent e la configurazione del Runtime EKS Monitoring.

Versione del kernel	Supporto del kernel	CPUarchitettura

Distribuzione del sistema operativo			x64 () AMD64	Gravitone () ARM64 (Graviton2 e versioni successive) [1]	Versione di Kubernetes supportata
Ubuntu AL2 AL2023 [3]	5.4, 5.10, 5.15, 6.1 [2]	e. Tracepoints, Kprobe BPF	Supportato	Supportato	v1.21 - v1.30
Bottlerocket					v1.23 - v1.30

1. Il monitoraggio del runtime per EKS i cluster Amazon non supporta le istanze Graviton di prima generazione come i tipi di istanze A1.
2. Attualmente, con la versione Kernel`6.1`, non è GuardDuty possibile generare Tipi di risultati del monitoraggio del runtime dati correlati a. DNSeventi
3. Runtime Monitoring supporta AL2 023 con il rilascio del GuardDuty security agent v1.6.0 e versioni successive. Per ulteriori informazioni, consulta GuardDuty agente di sicurezza per EKS cluster Amazon.

Versioni di Kubernetes supportate dal security agent GuardDuty

La tabella seguente mostra le versioni di Kubernetes per i tuoi EKS cluster supportate dal Security Agent. GuardDuty

Versione di Kubernetes	Versione del GuardDuty Security Agent EKS aggiuntivo di Amazon
1,28 - 1,30	v1.4.1 e versioni successive
1.27	v1.3.0, v1.3.1

Versione di Kubernetes	Versione del GuardDuty Security Agent EKS aggiuntivo di Amazon
1,26	v1.2.0
1,21 - 1,25	Tutte le versioni

Alcune versioni del GuardDuty Security Agent raggiungeranno la fine del supporto standard. Per informazioni sulle versioni di rilascio degli agenti, vedereGuardDuty agente di sicurezza per EKS cluster Amazon.

CPUe limiti di memoria

La tabella seguente mostra CPU i limiti di memoria per il EKS componente aggiuntivo Amazon per GuardDuty (`aws-guardduty-agent`).

Parametro	Limite minimo	Limite massimo
CPU	200 m	1000 m
Memoria	256 Mi	1024 Mi

Quando utilizzi la versione 1.5.0 o successiva del EKS componente aggiuntivo Amazon, GuardDuty offre la possibilità di configurare lo schema del componente aggiuntivo per i tuoi valori CPU e quelli della memoria. Per informazioni sull'intervallo configurabile, consulta. Parametri e valori configurabili

Dopo aver abilitato il EKS Runtime Monitoring e valutato lo stato di copertura dei EKS cluster, puoi configurare e visualizzare le metriche di Container Insight. Per ulteriori informazioni, consulta Configurazione CPU e monitoraggio della memoria.

Approfondimenti

Il passaggio successivo consiste nella configurazione del Runtime Monitoring e nella gestione del security agent manualmente o automaticamente tramite. GuardDuty

Utilizzo di Infrastructure as Code (IaC) con agenti di sicurezza GuardDuty automatizzati

Utilizza questa sezione solo se il seguente elenco si applica al tuo caso d'uso:

- Utilizzate strumenti Infrastructure as Code (IaC), come Terraform, per gestire AWS le vostre risorse AWS Cloud Development Kit (AWS CDK) e
- È necessario abilitare la configurazione GuardDuty automatica degli agenti per uno o più tipi di risorse: Amazon EKSEC2, Amazon o Amazon ECS -Fargate.

Panoramica del grafico delle dipendenze delle risorse IAc

Quando si abilita la configurazione GuardDuty automatizzata dell'agente per un tipo di risorsa, crea GuardDuty automaticamente un VPC endpoint e un gruppo di sicurezza associati a questo VPC endpoint e installa il security agent per questo tipo di risorsa. Per impostazione predefinita, GuardDuty eliminerà l'VPCendpoint e il gruppo di sicurezza associato solo dopo aver disabilitato il Runtime Monitoring. Per ulteriori informazioni, consulta Impatto della disabilitazione e della pulizia delle risorse.

Quando si utilizza uno strumento IAc, questo mantiene un grafico delle dipendenze delle risorse. Al momento dell'eliminazione delle risorse utilizzando lo strumento IAc, elimina solo le risorse che possono essere tracciate come parte del grafico delle dipendenze delle risorse. Gli strumenti IAc potrebbero non conoscere le risorse create al di fuori della configurazione specificata. Ad esempio, si crea uno strumento VPC con uno strumento IaC e quindi si aggiunge un gruppo di sicurezza VPC utilizzando la AWS console o un'APIoperazione. Nel grafico delle dipendenze delle risorse, la VPC risorsa creata dipende dal gruppo di sicurezza associato. Se si elimina questa VPC risorsa utilizzando lo strumento IAc, verrà visualizzato un errore. Il modo per aggirare questo errore consiste nell'eliminare manualmente il gruppo di sicurezza associato o nell'aggiornare la configurazione IAc per includere questa risorsa aggiunta.

Problema comune: eliminazione di risorse in IAc

Quando utilizzi la configurazione GuardDuty automatica degli agenti, potresti voler eliminare una risorsa (Amazon EKSEC2, Amazon o ECS Amazon-Fargate) che hai creato utilizzando uno strumento IaC. Tuttavia, questa risorsa dipende dall'VPCendpoint che ha creato. GuardDuty Ciò impedisce allo strumento IaC di eliminare la risorsa da solo e richiede la disattivazione del Runtime Monitoring, che elimina ulteriormente l'VPCendpoint automaticamente.

Ad esempio, quando tenti di eliminare l'VPCendpoint GuardDuty creato per tuo conto, riceverai un errore simile agli esempi seguenti.

Example

Esempio di errore durante l'utilizzo 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

Esempio di errore durante l'utilizzo di 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
```

Soluzione: prevenire il problema dell'eliminazione delle risorse

Questa sezione consente di gestire l'VPCendpoint e il gruppo di sicurezza indipendentemente da. GuardDuty

Per ottenere la proprietà completa delle risorse configurate utilizzando lo strumento IaC, effettuate le seguenti operazioni nell'ordine elencato:

1. Crea unVPC. Per consentire l'autorizzazione di ingresso, associa un GuardDuty VPC endpoint al gruppo di sicurezza, a questo. VPC
2. Abilita la configurazione GuardDuty automatica degli agenti per il tuo tipo di risorsa

Dopo aver completato i passaggi precedenti, non GuardDuty creerà un proprio VPC endpoint e riutilizzerà quello creato utilizzando lo strumento IaC.

Per informazioni su come crearne uno personalizzatoVPC, consulta Create a VPC only in Amazon VPC Transit Gateways. Per informazioni sulla creazione di un VPC endpoint, consulta la sezione seguente relativa al tipo di risorsa:

- Per AmazonEC2, vediCreazione manuale di un VPC endpoint Amazon.

- Per AmazonEKS, vediPrerequisiti per l'implementazione del Security Agent GuardDuty .

Abilitazione del monitoraggio del runtime per un account autonomo

Utilizza i seguenti passaggi per abilitare il monitoraggio del runtime nel tuo account.

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Abilita per abilitare il monitoraggio del runtime per il tuo account.
4. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'EC2istanza Amazon, un ECS cluster Amazon o un EKS cluster Amazon, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

   Per abilitare l'agente GuardDuty di sicurezza

   - Gestione di agenti di sicurezza automatizzati per EC2 istanze Amazon
   - Gestione manuale del security agent per EC2 un'istanza Amazon
   - Gestione dell'agente di sicurezza automatizzato per Fargate (solo AmazonECS)
   - Gestione automatica dell'agente di sicurezza per i EKS cluster Amazon
   - Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon

Abilitazione del monitoraggio del runtime per ambienti con più account

In ambienti con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare il monitoraggio del runtime per gli account dei membri e gestire la configurazione automatica degli agenti per i tipi di risorse appartenenti agli account membri dell'organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti multi-account, consulta Gestione di più account.

Per l'account amministratore delegato GuardDuty

Per abilitare il monitoraggio del runtime per l'account amministratore delegato GuardDuty

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring.
4. Utilizzando Abilita per tutti gli account

   Se desideri abilitare il monitoraggio del runtime per tutti gli account che appartengono all'organizzazione, incluso l'account GuardDuty amministratore delegato, scegli Abilita per tutti gli account.
5. Utilizzando Configura gli account manualmente

   Se desideri abilitare il monitoraggio del runtime per ogni account membro singolarmente, scegli Configura gli account manualmente.

   - Scegli Abilita nella sezione Amministratore delegato (questo account).
6. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'EC2istanza Amazon, un ECS cluster Amazon o un EKS cluster Amazon, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

   Per abilitare l'agente GuardDuty di sicurezza

   - Gestione di agenti di sicurezza automatizzati per EC2 istanze Amazon
   - Gestione manuale del security agent per EC2 un'istanza Amazon
   - Gestione dell'agente di sicurezza automatizzato per Fargate (solo AmazonECS)
   - Gestione automatica dell'agente di sicurezza per i EKS cluster Amazon
   - Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon

Per tutti gli account dei membri

Per abilitare il monitoraggio del runtime per tutti gli account membri dell'organizzazione

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando l'account GuardDuty amministratore delegato.
2. Nel riquadro di navigazione, scegli Runtime Monitoring.
3. Nella pagina Runtime Monitoring, nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring.
4. Scegli Abilita per tutti gli account.
5. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'EC2istanza Amazon, un ECS cluster Amazon o un EKS cluster Amazon, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

   Per abilitare l'agente GuardDuty di sicurezza

   - Gestione di agenti di sicurezza automatizzati per EC2 istanze Amazon
   - Gestione manuale del security agent per EC2 un'istanza Amazon
   - Gestione dell'agente di sicurezza automatizzato per Fargate (solo AmazonECS)
   - Gestione automatica dell'agente di sicurezza per i EKS cluster Amazon
   - Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon

Per tutti gli account membri attivi esistenti

Per abilitare il monitoraggio del runtime per gli account dei membri esistenti nell'organizzazione

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando l'account GuardDuty amministratore delegato dell'organizzazione.
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella pagina Runtime Monitoring, nella scheda Configurazione, puoi visualizzare lo stato corrente della configurazione di Runtime Monitoring.
4. Nel riquadro Runtime Monitoring, nella sezione Account dei membri attivi, scegli Azioni.

5. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
6. Scegli Conferma.
7. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'EC2istanza Amazon, un ECS cluster Amazon o un EKS cluster Amazon, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

   Per abilitare l'agente GuardDuty di sicurezza

   - Gestione di agenti di sicurezza automatizzati per EC2 istanze Amazon
   - Gestione manuale del security agent per EC2 un'istanza Amazon
   - Gestione dell'agente di sicurezza automatizzato per Fargate (solo AmazonECS)
   - Gestione automatica dell'agente di sicurezza per i EKS cluster Amazon
   - Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Abilita automaticamente il monitoraggio del runtime solo per gli account dei nuovi membri

Per abilitare il monitoraggio del runtime per gli account dei nuovi membri dell'organizzazione

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando l'account GuardDuty amministratore delegato designato dell'organizzazione.
2. Nel riquadro di navigazione, scegli Runtime Monitoring
3. Nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring.
4. Scegli Configura gli account manualmente.
5. Seleziona Abilita automaticamente per i nuovi account membri.
6. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'EC2istanza Amazon, un ECS cluster Amazon o un EKS cluster Amazon, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

Per abilitare l'agente GuardDuty di sicurezza

- Gestione di agenti di sicurezza automatizzati per EC2 istanze Amazon
- Gestione manuale del security agent per EC2 un'istanza Amazon
- Gestione dell'agente di sicurezza automatizzato per Fargate (solo AmazonECS)
- Gestione automatica dell'agente di sicurezza per i EKS cluster Amazon
- Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon

Solo per account di membri attivi selettivi

Per abilitare il monitoraggio del runtime per i singoli account dei membri attivi

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Nella pagina Account, rivedi automaticamente i valori nelle colonne Runtime Monitoring e Manage agent. Questi valori indicano se il monitoraggio del runtime e la gestione degli GuardDuty agenti sono abilitati o meno per l'account corrispondente.
4. Dalla tabella Account, selezionate l'account per il quale desiderate abilitare il Runtime Monitoring. Puoi scegliere più account alla volta.
5. Scegli Conferma.
6. Scegli Modifica piani di protezione. Scegliere l'operazione appropriata.
7. Scegli Conferma.
8. GuardDuty Per ricevere gli eventi di runtime da uno o più tipi di risorse: un'EC2istanza Amazon, un ECS cluster Amazon o un EKS cluster Amazon, utilizza le seguenti opzioni per gestire l'agente di sicurezza per queste risorse:

   Per abilitare l'agente GuardDuty di sicurezza

   - Gestione di agenti di sicurezza automatizzati per EC2 istanze Amazon
   - Gestione manuale del security agent per EC2 un'istanza Amazon
   - Gestione dell'agente di sicurezza automatizzato per Fargate (solo AmazonECS)
   - Gestione automatica dell'agente di sicurezza per i EKS cluster Amazon

- Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon

Gestione degli agenti GuardDuty di sicurezza

È possibile gestire il GuardDuty security agent per la risorsa che si desidera monitorare. Se desideri monitorare più di un tipo di risorsa, assicurati di gestire l' GuardDuty agente per quella risorsa.

> **Important**
>
> Quando lavori con un agente GuardDuty di sicurezza per un'EC2istanza Amazon, puoi installare e utilizzare l'agente sull'host sottostante all'interno di un EKS cluster Amazon. Se hai già distribuito un agente di sicurezza su quel EKS cluster, sullo stesso host potrebbero essere in esecuzione due agenti di sicurezza contemporaneamente. Per informazioni su come GuardDuty funziona in questo scenario, consultaGestione dei doppi agenti di sicurezza.

I seguenti argomenti ti aiuteranno nei passaggi successivi per gestire il Security Agent.

Indice

Utilizzo: condiviso VPC con agenti di sicurezza automatizzati

Quando si sceglie GuardDuty di gestire automaticamente il security agent, Runtime Monitoring supporta l'utilizzo VPC di un nome condiviso Account AWS che appartiene alla stessa organizzazione AWS Organizations. Per tuo conto, GuardDuty puoi impostare la policy degli VPC endpoint di Amazon in base ai dettagli associati alla condivisione VPC per la tua organizzazione.

Prima di questa versione, GuardDuty supportava l'uso di shared VPCs solo quando sceglievi di gestire il GuardDuty security agent manualmente.

Indice

Come funziona

Quando l'account proprietario dell'account condiviso VPC abilita il monitoraggio del runtime e la configurazione automatica dell'agente per una qualsiasi delle risorse (Amazon EKS o AWS Fargate (ECSsolo Amazon)), tutte le risorse condivise VPCs diventano idonee per l'installazione automatica dell'VPCendpoint Amazon condiviso e del gruppo di sicurezza associato nell'account VPC proprietario condiviso. GuardDuty recupera l'ID dell'organizzazione associato all'Amazon VPC condiviso.

Ora, le Account AWS persone che appartengono alla stessa organizzazione dell'account VPC proprietario Amazon condiviso possono condividere anche lo stesso VPC endpoint Amazon. GuardDuty crea il file condiviso VPC quando l'account VPC proprietario condiviso o l'account partecipante necessita di un VPC endpoint Amazon. Esempi di necessità di un VPC endpoint Amazon includono l'abilitazione GuardDuty, il monitoraggio del runtime, il monitoraggio del EKS runtime o l'avvio di una nuova attività Amazon ECS -Fargate. Quando questi account abilitano il Runtime Monitoring e la configurazione automatica degli agenti per qualsiasi tipo di risorsa, GuardDuty crea un VPC endpoint Amazon e imposta la policy dell'endpoint con lo stesso ID dell'organizzazione dell'account VPC proprietario condiviso. GuardDuty aggiunge un `GuardDutyManaged` tag e lo imposta `true` per l'VPCendpoint Amazon che lo GuardDuty crea. Se l'account VPC proprietario Amazon condiviso non ha abilitato il Runtime Monitoring o la configurazione automatica degli agenti per nessuna delle risorse, non GuardDuty imposterà la policy degli VPC endpoint di Amazon. Per informazioni sulla configurazione del Runtime Monitoring e sulla gestione automatica del security agent nell'account VPC proprietario condiviso, consulta. Attivazione del monitoraggio del GuardDuty runtime

Ciascuno degli account che utilizzano la stessa politica VPC degli endpoint di Amazon viene chiamato AWS account partecipante dell'Amazon condiviso associato. VPC

L'esempio seguente mostra la policy VPC endpoint predefinita dell'account VPC proprietario condiviso e dell'account partecipante. `aws:PrincipalOrgID`Mostrerà l'ID dell'organizzazione associato alla risorsa VPC condivisa. L'uso di questa politica è limitato agli account dei partecipanti presenti nell'organizzazione dell'account del proprietario.

Example

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

Prerequisiti per l'utilizzo della modalità condivisa VPC

Prerequisiti per la configurazione iniziale

Esegui i seguenti passaggi se desideri essere il proprietario dello spazio condivisoVPC: Account AWS

1. Creazione di un'organizzazione: crea un'organizzazione seguendo i passaggi descritti in Creazione e gestione di un'organizzazione nella Guida per l'AWS Organizations utente.

   Per informazioni sull'aggiunta o la rimozione degli account dei membri, consulta Gestione Account AWS nell'organizzazione.
2. Creazione di una VPC risorsa condivisa: puoi creare una VPC risorsa condivisa dall'account del proprietario. Per ulteriori informazioni, consulta Condividi il tuo account VPC con altri account nella Amazon VPC User Guide.

Prerequisiti specifici per il monitoraggio del GuardDuty runtime

L'elenco seguente fornisce i prerequisiti specifici per: GuardDuty

- L'account proprietario dell'account condiviso VPC e dell'account partecipante possono appartenere a organizzazioni diverse in GuardDuty. Tuttavia, devono appartenere alla stessa organizzazione in AWS Organizations. Ciò è necessario per GuardDuty creare un VPC endpoint Amazon e un gruppo di sicurezza per gli utenti condivisiVPC. Per informazioni su come VPCs funziona la condivisione, consulta Condividi il tuo account VPC con altri account nella Amazon VPC User Guide.
- Abilita il Runtime Monitoring o EKS Runtime Monitoring e la configurazione GuardDuty automatica degli agenti per qualsiasi risorsa nell'account VPC proprietario condiviso e nell'account del partecipante. Per ulteriori informazioni, consulta Abilitazione del monitoraggio del runtime.

  Se hai già completato queste configurazioni, continua con il passaggio successivo.
- Quando lavori con un'attività Amazon EKS o Amazon ECS (AWS Fargate solo), assicurati di scegliere la VPC risorsa condivisa associata all'account del proprietario e di selezionarne le sottoreti.

Domande frequenti () FAQs

L'elenco seguente fornisce i passaggi per la risoluzione dei problemi relativi alle domande frequenti quando si utilizza una VPC risorsa condivisa con la configurazione GuardDuty automatica degli agenti abilitata in Runtime Monitoring:

Sto già utilizzando Runtime Monitoring (o EKS Runtime Monitoring). Come posso abilitare la condivisioneVPC?

Per informazioni sui prerequisiti per creare un file condivisoVPC, consultaPrerequisiti.

Quando sia l'account VPC proprietario condiviso che l'account partecipante soddisfano i prerequisiti, GuardDuty tenterà di impostare automaticamente la politica degli VPC endpoint di Amazon.

Se prima di questa versione, hai Account AWS riscontrato un problema di copertura dovuto al VPC mancato supporto della condivisione, segui i prerequisiti. Quando il tipo di risorsa (Amazon EKS o Amazon ECS (AWS Fargate only) task) richiama il requisito di un VPC endpoint condiviso, GuardDuty tenterà di impostare la nuova VPC policy per gli endpoint.

In qualità di account VPC proprietario condiviso, voglio che la policy condivisa sugli VPC endpoint sia limitata a un sottoinsieme di account partecipanti nella mia organizzazione. Come posso farlo?

Se hai un `true` tag`GuardDutyManaged`: associato all'endpoint, rimuovilo. Ciò impedisce GuardDuty di tentare di modificare o sovrascrivere la politica dell'VPCendpoint condivisa. VPC

Per ulteriori informazioni, consulta Controllare l'accesso agli VPC endpoint utilizzando le policy degli endpoint.

Perché l'VPCendpoint condiviso viene modificato da a? **`aws:PrincipalAccountaws:PrincipalOrgId`** Come posso evitarlo?

Quando GuardDuty rileva che VPC è condiviso da più account della stessa organizzazione in AWS Organizations, GuardDuty tenta di modificare la politica per specificare l'ID dell'organizzazione.

Per evitare che ciò accada, rimuovi il `true` tag`GuardDutyManaged`: dall'VPCendpoint condiviso. Ciò impedisce GuardDuty di tentare di modificare o sovrascrivere la politica dell'endpoint dell'VPCendpoint condiviso. VPC

Cosa succede quando l'account VPC proprietario condiviso o uno degli account dei partecipanti disabilita il Runtime Monitoring (GuardDuty o Runtime Monitoring)? EKS

Quando l'account VPC proprietario condiviso viene disabilitato GuardDuty o il Runtime Monitoring (o EKS Runtime Monitoring), GuardDuty verifica se un tipo di risorsa appartenente all'account del partecipante ha utilizzato l'VPCendpoint condiviso o se un account partecipante ha mai abilitato la gestione degli GuardDuty agenti per qualsiasi tipo di risorsa. In caso affermativo, GuardDuty non eliminerà l'VPCendpoint e il gruppo di sicurezza.

Se l'account VPC partecipante condiviso disabilita GuardDuty o il Runtime Monitoring (o EKS Runtime Monitoring), non vi è alcun impatto sull'account VPC proprietario condiviso e l'account proprietario non eliminerà né la VPC risorsa condivisa né il gruppo di sicurezza.

Come posso eliminare la risorsa condivisaVPC? Quale sarà il suo impatto?

In qualità di account VPC proprietario condiviso, puoi eliminare la VPC risorsa condivisa anche quando viene utilizzata dal tuo account o da uno degli account partecipanti a Runtime Monitoring. Per informazioni sull'eliminazione della condivisione VPC e sulla comprensione del suo impatto, consultaTo delete a VPC endpoint.

Gestione dei doppi agenti di sicurezza installati su un host

EC2Le istanze Amazon possono supportare diversi tipi di carichi di lavoro. Quando configuri un agente di sicurezza automatizzato su un'EC2istanza Amazon, sulla stessa EC2 istanza potrebbe essere utilizzato un altro agente di sicurezzaEKS.

Panoramica

Prendi in considerazione uno scenario in cui hai abilitato il Runtime Monitoring. Ora abiliti l'agente automatizzato per Amazon EKS tramite GuardDuty. Hai anche abilitato l'agente automatico per AmazonEC2. Può succedere che sullo stesso host sottostante vengano installati due agenti di sicurezza, uno per Amazon EKS e l'altro per AmazonEC2. Ciò potrebbe comportare l'esecuzione di due agenti di sicurezza all'interno dello stesso host, che raccolgono eventi di runtime e li inviano a GuardDuty, generando potenzialmente risultati duplicati.

Impatto

- Quando più di un security agent è in esecuzione sullo stesso host, l'account potrebbe avere una quantità doppia di requisiti di elaborazione CPU e di memoria. Per informazioni sui limiti CPU di memoria per ogni tipo di risorsa, consulta Prerequisiti per quella risorsa.
- GuardDuty ha progettato la funzionalità Runtime Monitoring in modo tale che, anche in caso di sovrapposizione di due security agent che raccolgono eventi di runtime dallo stesso host sottostante, all'account venga addebitato solo un flusso di eventi di runtime.

Come GuardDuty gestisce più agenti

GuardDuty rileva quando due security agent sono in esecuzione sullo stesso host e ne designa solo uno come agente di sicurezza che raccoglie attivamente gli eventi di runtime. Il secondo agente consumerà risorse di sistema minime in modo da prevenire qualsiasi impatto sulle prestazioni delle applicazioni.

GuardDuty considera i seguenti scenari:

- Quando un'EC2istanza rientra nell'ambito sia di Amazon EKS che degli agenti di EC2 sicurezza di Amazon, l'agente EKS di sicurezza ha la priorità. Ciò si applica solo quando utilizzi il security agent v1.1.0 o successivo per Amazon. EC2 Le versioni precedenti dell'agente continueranno a funzionare e a raccogliere eventi di runtime perché le versioni precedenti dell'agente non sono influenzate dalla prioritizzazione.

- Quando sia Amazon EKS che Amazon EC2 dispongono di agenti di sicurezza GuardDuty gestiti e anche la tua EC2 istanza Amazon è SSM gestita, entrambi i security agent verranno installati a livello di host. Una volta installati gli agenti, GuardDuty decide quale agente di sicurezza continuerà a funzionare. Quando entrambi i security agent sono in esecuzione, alla fine solo uno di essi raccoglierà gli eventi di runtime.
- Quando i security agent associati a entrambi EC2 EKS vengono eseguiti contemporaneamente, GuardDuty potrebbero generare risultati duplicati solo durante il periodo di sovrapposizione.

  Questo può accadere quando:

  - I Security Agent EKS sono configurati per entrambi EC2 GuardDuty (automaticamente) o
  - La tua EKS risorsa Amazon dispone di un agente di sicurezza automatizzato.
- Quando il EKS security agent è già in esecuzione, se lo distribuisci manualmente sullo stesso host sottostante e soddisfi tutti i prerequisiti, GuardDuty potresti non installare un secondo security agent. EC2

Gestione di agenti di sicurezza automatizzati per EC2 istanze Amazon

> **Note**
>
> Prima di continuare, assicurati di seguire tutti iPrerequisiti per il supporto delle EC2 istanze Amazon.

Migrazione dall'agente EC2 manuale di Amazon all'agente automatizzato

Questa sezione si applica a Account AWS chi in precedenza gestiva il Security Agent manualmente e ora desidera utilizzare la configurazione GuardDuty automatizzata dell'agente. Se ciò non ti riguarda, continua con la configurazione del security agent per il tuo account.

Quando abiliti l'agente GuardDuty automatizzato, GuardDuty gestisce l'agente di sicurezza per tuo conto. Per informazioni sui passaggi GuardDuty necessari, consultaUtilizza la configurazione automatica degli agenti (scelta consigliata).

Pulizia delle risorse

Eliminare SSM l'associazione

- Elimina qualsiasi SSM associazione che potresti aver creato durante la gestione EC2 manuale del Security Agent per Amazon. Per ulteriori informazioni, consulta Eliminazione delle associazioni.
- Questo viene fatto in modo che GuardDuty possa assumere il controllo della gestione delle SSM azioni indipendentemente dal fatto che si utilizzino agenti automatici a livello di account o di istanza (utilizzando tag di inclusione o esclusione). Per ulteriori informazioni sulle SSM azioni che possono essere GuardDuty intraprese, consultaAutorizzazioni di ruolo collegate ai servizi per GuardDuty.
- Quando si elimina manualmente un'SSMassociazione creata in precedenza per la gestione manuale del security agent, potrebbe verificarsi un breve periodo di sovrapposizione durante il quale viene GuardDuty creata un'SSMassociazione per la gestione automatica del security agent. Durante questo periodo, è possibile che si verifichino conflitti basati sulla SSM pianificazione. Per ulteriori informazioni, consulta Amazon EC2 SSM scheduling.

Gestisci i tag di inclusione ed esclusione per le tue istanze Amazon EC2

- Tag di inclusione: quando non abiliti la configurazione GuardDuty automatica dell'agente ma contrassegni una qualsiasi delle tue EC2 istanze Amazon con un tag di inclusione (`GuardDutyManaged:true`), GuardDuty crea un'SSMassociazione che installerà e gestirà il security agent sulle EC2 istanze selezionate. Si tratta di un comportamento previsto che ti aiuta a gestire il security agent solo su EC2 istanze selezionate. Per ulteriori informazioni, consulta Come funziona il monitoraggio del runtime con le EC2 istanze Amazon.

  Per GuardDuty impedire l'installazione e la gestione del security agent, rimuovi il tag di inclusione da queste EC2 istanze. Per ulteriori informazioni, consulta Aggiungere ed eliminare tag nella Amazon EC2 User Guide.
- Tag di esclusione: se desideri abilitare la configurazione GuardDuty automatica degli agenti per tutte le EC2 istanze del tuo account, assicurati che nessuna EC2 istanza sia contrassegnata con un tag di esclusione (:)`GuardDutyManaged. false`

Configurazione dell'agente GuardDuty per un account autonomo

Configure for all instances

Per configurare il Runtime Monitoring per tutte le istanze del tuo account standalone

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Modifica.
4. Nella EC2sezione, scegli Abilita.
5. Seleziona Salva.
6. Puoi verificare che l'SSMassociazione che GuardDuty crea installerà e gestirà il security agent su tutte le EC2 risorse appartenenti al tuo account.
   a. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
   b. Apri la scheda Target per l'SSMassociazione (`GuardDutyRuntimeMonitoring-do-not-delete`). Osservate che il tasto Tag appare come InstanceIds.

Using inclusion tag in selected instances

Per configurare il GuardDuty Security Agent per EC2 istanze Amazon selezionate

1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `true` tag`GuardDutyManaged`: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. È possibile verificare che l'SSMassociazione GuardDuty creata installerà e gestirà il Security Agent solo sulle EC2 risorse contrassegnate con i tag di inclusione.

   Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.

- Apri la scheda Target per l'SSMassociazione che viene creata (`GuardDutyRuntimeMonitoring-do-not-delete`). Il tasto Tag appare come tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Assicurati di aggiungere il tag di esclusione alle tue EC2 istanze Amazon prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per AmazonEC2, qualsiasi EC2 istanza che viene avviata senza un tag di esclusione sarà coperta dalla configurazione GuardDuty automatizzata dell'agente.

Per configurare il GuardDuty Security Agent per EC2 istanze Amazon selezionate

1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `false` tag`GuardDutyManaged`: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. Affinché i tag di esclusione siano disponibili nei metadati dell'istanza, effettuate le seguenti operazioni:

   a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

      Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.

   b. Seleziona l'istanza per la quale desideri consentire i tag.

   c. Nel menu Azioni, scegli Impostazioni istanza.

   d. Scegli Consenti tag nei metadati dell'istanza.

   e. In Accesso ai tag nei metadati dell'istanza, seleziona Consenti.

   f. Seleziona Salva.

4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. Copertura per EC2 istanze Amazon

Configurazione GuardDuty dell'agente in un ambiente con più account

Per account amministratore delegato GuardDuty

Configure for all instances

Se hai scelto Abilita per tutti gli account per il monitoraggio del runtime, scegli una delle seguenti opzioni per l'account GuardDuty amministratore delegato:

- Opzione 1

  In Configurazione automatica dell'agente, nella EC2sezione, seleziona Abilita per tutti gli account.
- Opzione 2
  - In Configurazione automatica dell'agente, nella EC2sezione, seleziona Configura gli account manualmente.
  - In Amministratore delegato (questo account), scegli Abilita.
- Seleziona Salva.

Se hai scelto Configura gli account manualmente per il monitoraggio del runtime, procedi nel seguente modo:

- In Configurazione automatica degli agenti, nella EC2sezione, seleziona Configura gli account manualmente.
- In Amministratore delegato (questo account), scegli Abilita.
- Seleziona Salva.

Indipendentemente dall'opzione scelta per abilitare la configurazione automatica dell'agente per l'account GuardDuty amministratore delegato, puoi verificare che l'SSMassociazione GuardDuty creata installerà e gestirà il security agent su tutte le EC2 risorse appartenenti a questo account.

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Apri la scheda Target per l'SSMassociazione (`GuardDutyRuntimeMonitoring-do-not-delete`). Osservate che il tasto Tag appare come InstanceIds.

Using inclusion tag in selected instances

Per configurare GuardDuty l'agente per EC2 istanze Amazon selezionate

1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `true` tag`GuardDutyManaged`: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.

   L'aggiunta di questo tag consentirà GuardDuty di installare e gestire il security agent per queste EC2 istanze selezionate. Non è necessario abilitare esplicitamente la configurazione automatica dell'agente.
3. È possibile verificare che l'SSMassociazione GuardDuty creata installi e gestisca il security agent solo sulle EC2 risorse contrassegnate con i tag di inclusione.

   Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.

   - Apri la scheda Target per l'SSMassociazione che viene creata (`GuardDutyRuntimeMonitoring-do-not-delete`). Il tasto Tag appare come tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Assicurati di aggiungere il tag di esclusione alle tue EC2 istanze Amazon prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per AmazonEC2, qualsiasi EC2 istanza che viene avviata senza un tag di esclusione sarà coperta dalla configurazione GuardDuty automatizzata dell'agente.

Per configurare GuardDuty l'agente per EC2 istanze Amazon selezionate

1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `false` tag`GuardDutyManaged`: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. Affinché i tag di esclusione siano disponibili nei metadati dell'istanza, effettuate le seguenti operazioni:

   a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

      Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.

   b. Nel menu Azioni, scegli Impostazioni istanza.

   c. Scegli Consenti tag nei metadati dell'istanza.
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. Copertura per EC2 istanze Amazon

Attivazione automatica per tutti gli account dei membri

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Configure for all instances

I passaggi seguenti presuppongono che tu abbia scelto Abilita per tutti gli account nella sezione Runtime Monitoring:

1. Scegli Abilita per tutti gli account nella sezione Configurazione automatica degli agenti per Amazon EC2.

2. Puoi verificare che l'SSMassociazione che GuardDuty crea (`GuardDutyRuntimeMonitoring-do-not-delete`) installerà e gestirà il security agent su tutte le EC2 risorse appartenenti a questo account.

   a. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.

   b. Apri la scheda Obiettivi per l'SSMassociazione. Osserva che il tasto Tag appare come InstanceIds.

Using inclusion tag in selected instances

Per configurare GuardDuty l'agente per EC2 istanze Amazon selezionate

1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `true` tag`GuardDutyManaged`: alle EC2 istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.

   L'aggiunta di questo tag consentirà GuardDuty di installare e gestire il security agent per queste EC2 istanze selezionate. Non è necessario abilitare esplicitamente la configurazione automatica dell'agente.
3. Puoi verificare che l'SSMassociazione che GuardDuty crea installerà e gestirà il security agent su tutte le EC2 risorse appartenenti al tuo account.

   a. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.

   b. Apri la scheda Target per l'SSMassociazione (`GuardDutyRuntimeMonitoring-do-not-delete`). Osservate che il tasto Tag appare come InstanceIds.

Using exclusion tag in selected instances

> **Note**
>
> Assicurati di aggiungere il tag di esclusione alle tue EC2 istanze Amazon prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per AmazonEC2,

qualsiasi EC2 istanza che viene avviata senza un tag di esclusione sarà coperta dalla configurazione GuardDuty automatizzata dell'agente.

Per configurare il GuardDuty Security Agent per EC2 istanze Amazon selezionate

1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `false` tag`GuardDutyManaged`: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. Affinché i tag di esclusione siano disponibili nei metadati dell'istanza, effettuate le seguenti operazioni:

   a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

      Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.

   b. Nel menu Azioni, scegli Impostazioni istanza.

   c. Scegli Consenti tag nei metadati dell'istanza.
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. Copertura per EC2 istanze Amazon

Attivazione automatica solo per gli account dei nuovi membri

L'account GuardDuty amministratore delegato può impostare la configurazione automatica dell'agente per la EC2 risorsa Amazon in modo che si abiliti automaticamente per i nuovi account membri quando entrano a far parte dell'organizzazione.

Configure for all instances

I passaggi seguenti presuppongono che tu abbia selezionato Abilita automaticamente gli account dei nuovi membri nella sezione Runtime Monitoring:

1. Nel riquadro di navigazione, scegli Runtime Monitoring.

2. Nella pagina Runtime Monitoring, scegli Modifica.
3. Seleziona Abilita automaticamente per i nuovi account membri. Questo passaggio garantisce che ogni volta che un nuovo account si unisce alla tua organizzazione, la configurazione automatizzata degli agenti per Amazon EC2 venga automaticamente abilitata per l'account. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa selezione.
4. Seleziona Salva.

Quando un nuovo account membro si unisce all'organizzazione, questa configurazione verrà abilitata automaticamente per lui. GuardDuty Per gestire il security agent per le EC2 istanze Amazon che appartengono a questo nuovo account membro, assicurati che tutti i prerequisiti Ad esempio EC2 siano soddisfatti.

Quando viene creata un'SSMassociazione (`GuardDutyRuntimeMonitoring-do-not-delete`), puoi verificare che l'SSMassociazione installerà e gestirà il security agent su tutte le EC2 istanze appartenenti al nuovo account membro.

- Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
- Apri la scheda Obiettivi per l'SSMassociazione. Osserva che il tasto Tag appare come InstanceIds.

Using inclusion tag in selected instances

Per configurare il GuardDuty Security Agent per istanze selezionate nel tuo account

1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `true` tag`GuardDutyManaged`: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.

   L'aggiunta di questo tag consentirà GuardDuty di installare e gestire il security agent per queste istanze selezionate. Non è necessario abilitare esplicitamente la configurazione automatica dell'agente.
3. È possibile verificare che l'SSMassociazione GuardDuty creata installi e gestisca il security agent solo sulle EC2 risorse contrassegnate con i tag di inclusione.

a. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
b. Apri la scheda Obiettivi per l'SSMassociazione che viene creata. Il tasto Tag appare come tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Assicurati di aggiungere il tag di esclusione alle tue EC2 istanze Amazon prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per AmazonEC2, qualsiasi EC2 istanza che viene avviata senza un tag di esclusione sarà coperta dalla configurazione GuardDuty automatizzata dell'agente.

Per configurare il GuardDuty Security Agent per istanze specifiche nel tuo account autonomo

1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `false` tag`GuardDutyManaged`: alle istanze in cui non desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. Affinché i tag di esclusione siano disponibili nei metadati dell'istanza, effettuate le seguenti operazioni:

   a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

      Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.

   b. Nel menu Azioni, scegli Impostazioni istanza.
   c. Scegli Consenti tag nei metadati dell'istanza.
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare il runtime. Copertura per EC2 istanze Amazon

Solo account membri selettivi

Configure for all instances

1. Nella pagina Account, seleziona uno o più account per i quali desideri abilitare la configurazione dell'agente Runtime Monitoring-Automated (Amazon EC2). Assicurati che gli account selezionati in questo passaggio abbiano già abilitato il Runtime Monitoring.
2. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare la configurazione automatica degli agenti di monitoraggio del runtime (Amazon EC2).
3. Scegli Conferma.

Using inclusion tag in selected instances

Per configurare il GuardDuty security agent per istanze selezionate

1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `true` tag`GuardDutyManaged`: alle istanze che desideri GuardDuty monitorare e rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.

   L'aggiunta di questo tag consentirà di GuardDuty gestire l'agente di sicurezza per le EC2 istanze Amazon con tag. Non è necessario abilitare esplicitamente la configurazione automatica degli agenti (Runtime Monitoring - Automated agent configuration () EC2.

Using exclusion tag in selected instances

> **Note**
>
> Assicurati di aggiungere il tag di esclusione alle tue EC2 istanze Amazon prima di avviarle. Dopo aver abilitato la configurazione automatizzata degli agenti per AmazonEC2, qualsiasi EC2 istanza che viene avviata senza un tag di esclusione sarà coperta dalla configurazione GuardDuty automatizzata dell'agente.

Per configurare l'agente GuardDuty di sicurezza per istanze selezionate

1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Aggiungi il `false` tag`GuardDutyManaged`: alle EC2 istanze in cui non desideri GuardDuty monitorare o rilevare potenziali minacce. Per informazioni sull'aggiunta di questo tag, consulta Per aggiungere un tag a una singola risorsa.
3. Affinché i tag di esclusione siano disponibili nei metadati dell'istanza, effettuate le seguenti operazioni:

   a. Nella scheda Dettagli dell'istanza, visualizza lo stato di Consenti i tag nei metadati dell'istanza.

      Se attualmente è Disabilitato, utilizza i seguenti passaggi per modificare lo stato in Abilitato. In caso contrario, puoi ignorare questo passaggio.

   b. Nel menu Azioni, scegli Impostazioni istanza.

   c. Scegli Consenti tag nei metadati dell'istanza.
4. Dopo aver aggiunto il tag di esclusione, esegui gli stessi passaggi specificati nella scheda Configura per tutte le istanze.

Ora puoi valutare. Copertura per EC2 istanze Amazon

Gestione manuale del security agent per EC2 un'istanza Amazon

Dopo aver abilitato il Runtime Monitoring, dovrai installare il GuardDuty security agent manualmente. Installando l'agente, GuardDuty riceverà gli eventi di runtime dalle EC2 istanze Amazon.

Per gestire il GuardDuty security agent, devi creare un VPC endpoint Amazon e quindi seguire i passaggi per installare il security agent manualmente.

Creazione manuale di un VPC endpoint Amazon

Prima di poter installare il GuardDuty security agent, devi creare un endpoint Amazon Virtual Private Cloud (AmazonVPC). Questo ti aiuterà a GuardDuty ricevere gli eventi di runtime delle tue EC2 istanze Amazon.

> **Note**
>
> Non sono previsti costi aggiuntivi per l'utilizzo dell'VPCendpoint.

Per creare un VPC endpoint Amazon

1. Accedi a AWS Management Console e apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, sotto cloud VPC privato, scegli Endpoints.
3. Scegliere Create Endpoint (Crea endpoint).
4. Nella pagina Crea endpoint per Categoria servizio, scegli Altri servizi endpoint.
5. Per Nome servizio, inserisci **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

   Assicurati di sostituire *`us-east-1`* con il tuo Regione AWS. Questa deve essere la stessa regione dell'EC2istanza Amazon che appartiene all'ID AWS del tuo account.
6. Scegli Verifica del servizio.
7. Dopo aver verificato con successo il nome del servizio, scegli VPCdove risiede l'istanza. Aggiungi la seguente politica per limitare l'utilizzo VPC degli endpoint Amazon solo all'account specificato. Con la `Condition` dell'organizzazione fornita sotto a questa policy, puoi aggiornare la policy seguente per limitare l'accesso all'endpoint. Per fornire il supporto degli VPC endpoint Amazon a un account IDs specifico della tua organizzazione, consultaOrganization 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": "*"
   }
  ]
}
```

L'ID `aws:PrincipalAccount` dell'account deve corrispondere all'account contenente l'VPCendpoint VPC and. L'elenco seguente mostra come condividere l'VPCendpoint con un altro AWS account: IDs

- Per specificare più account per accedere all'VPCendpoint, sostituiscilo `"aws:PrincipalAccount: "111122223333"` con il seguente blocco:

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

  Assicurati di sostituire l' AWS account IDs con l'account IDs degli account che devono accedere all'VPCendpoint.

- Per consentire a tutti i membri di un'organizzazione di accedere all'VPCendpoint, sostituiscilo `"aws:PrincipalAccount: "111122223333"` con la seguente riga:

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

  Assicurati di sostituire l'organizzazione *o-abcdef0123* con l'ID della tua organizzazione.

- Per limitare l'accesso a una risorsa tramite un ID dell'organizzazione, aggiungi il tuo `ResourceOrgID` alla politica. Per ulteriori informazioni, consulta `aws:ResourceOrgID`la Guida IAM per l'utente.

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

8. In Impostazioni aggiuntive, scegli Abilita DNS nome.
9. In Sottoreti, scegli le sottoreti in cui risiede l'istanza.
10. In Gruppi di sicurezza, scegli un gruppo di sicurezza con la porta in ingresso 443 abilitata dalla tua VPC (o dalla tua EC2 istanza Amazon). Se non disponi già di un gruppo di sicurezza con una

porta in ingresso 443 abilitata, consulta Creare un gruppo di sicurezza nella Amazon EC2 User Guide.

Se c'è un problema durante la limitazione delle autorizzazioni in ingresso alla tua VPC (o istanza), fornisci il supporto alla porta 443 in ingresso da qualsiasi indirizzo IP. `(0.0.0.0/0)`

Installazione manuale del security agent

GuardDuty fornisce i due metodi seguenti per installare il GuardDuty security agent sulle tue EC2 istanze Amazon:

- Metodo 1 AWS Systems Manager - Utilizzando: questo metodo richiede la AWS Systems Manager gestione dell'EC2istanza Amazon.
- Metodo 2 - Utilizzando Linux Package Manager: puoi utilizzare questo metodo indipendentemente dal fatto che le tue EC2 istanze Amazon siano AWS Systems Manager gestite o meno.

Metodo 1: utilizzando AWS Systems Manager

Per utilizzare questo metodo, assicurati che le tue EC2 istanze Amazon siano AWS Systems Manager gestite, quindi installa l'agente.

AWS Systems Manager EC2istanza Amazon gestita

Utilizza i seguenti passaggi per AWS Systems Manager gestire le tue EC2 istanze Amazon.

- AWS Systems Managerti aiuta a gestire AWS applicazioni e risorse end-to-end e a consentire operazioni sicure su larga scala.

  Per gestire le tue EC2 istanze Amazon con AWS Systems Manager, consulta Configurazione delle EC2 istanze di Systems Manager per Amazon nella Guida per l'AWS Systems Manager utente.
- La tabella seguente mostra i nuovi documenti GuardDuty gestiti AWS Systems Manager :

Nome del documento	Tipo di documento	Scopo
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distributor	Per impacchettare il GuardDuty security agent.

Nome del documento	Tipo di documento	Scopo
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Comando	Per eseguire lo script di installazione/disinstallazione per installare il security agent. GuardDuty

Per ulteriori informazioni AWS Systems Manager, consulta Amazon EC2 Systems Manager Documents nella Guida AWS Systems Manager per l'utente.

> **Per i server Debian**
>
> L'Amazon Machine Images (AMIs) per Debian Server fornito da AWS richiede l'installazione dell' AWS Systems Manager agente (SSMagente). È necessario eseguire un passaggio aggiuntivo per installare l'SSMagente per gestire le istanze SSM di Amazon EC2 Debian Server. Per informazioni sui passaggi da eseguire, vedere Installazione manuale dell'SSMagente sulle istanze di Debian Server nella Guida per l'utente.AWS Systems Manager

Per installare l' GuardDuty agente per l'EC2istanza Amazon utilizzando AWS Systems Manager

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, scegli Documenti
3. In Owned by Amazon, scegli`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
4. Scegliere Run Command.
5. Inserisci i seguenti parametri Run Command
   - Azione: Scegli Installa.
   - Tipo di installazione: scegli Installa o Disinstalla.
   - Valore: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`

- Versione: se rimane vuoto, otterrai la versione più recente del GuardDuty Security Agent. Per ulteriori informazioni sulle versioni di rilascio,GuardDuty agente di sicurezza per EC2 istanze Amazon.

6. Seleziona l'EC2istanza Amazon di destinazione. Puoi selezionare una o più EC2 istanze Amazon. Per ulteriori informazioni, consulta AWS Systems Manager Esecuzione dei comandi dalla console nella Guida per l'AWS Systems Manager utente
7. Verifica se l'installazione dell' GuardDuty agente è integra. Per ulteriori informazioni, consulta Convalida dello stato di installazione del GuardDuty Security Agent.

Metodo 2 - Utilizzando Linux Package Managers

Con questo metodo, è possibile installare l'agente GuardDuty di sicurezza eseguendo RPM script o script Debian. In base ai sistemi operativi, puoi scegliere un metodo preferito:

- Utilizza RPM gli script per installare il Security Agent sulle distribuzioni del sistema operativo AL2 o AL2 023.
- Usa gli script Debian per installare il security agent sulle distribuzioni del sistema operativo Ubuntu o Debian. Per informazioni sulle distribuzioni supportate di Ubuntu e Debian OS, vedere. Convalida dei requisiti relativi all'architettura

RPM installation

> **Important**
>
> Si consiglia di verificare la RPM firma del GuardDuty Security Agent prima di installarla sulla macchina.

1. Verifica la firma del GuardDuty Security Agent RPM

   a. Preparare il modello

      Prepara i comandi con la chiave pubblica appropriata, la firma di x86_64RPM, la firma di arm64 RPM e il collegamento di accesso corrispondente agli RPM script ospitati nei bucket Amazon S3. Sostituisci il valore dell'ID dell' AWS account e la Regione AWS versione dell'agente per accedere agli GuardDuty script. RPM

- Chiave pubblica:

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

- GuardDuty RPMfirma dell'agente di sicurezza:

  Firma di 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
```

  Firma di arm64 RPM

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

- Accedi ai link agli RPM script nel bucket Amazon S3:

  Link di accesso per 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
```

  Link di accesso per arm64 RPM

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

Regione AWS	Nome Regione	AWS ID dell'account
`eu-west-1`	Europa (Irlanda)	694911143906
`us-east-1`	Stati Uniti orientali (Virginia settentrionale)	593207742271
`us-west-2`	US West (Oregon)	733349766148
`eu-west-3`	Europa (Parigi)	665651866788

us-east-2	Stati Uniti orientali (Ohio)	307168627858
eu-central-1	Europa (Francoforte)	323658145986
ap-northeast-2	Asia Pacifico (Seoul)	914738172881
eu-north-1	Europa (Stoccolma)	591436053604
ap-east-1	Asia Pacifico (Hong Kong)	258348409381
me-south-1	Medio Oriente (Bahrein)	536382113932
eu-west-2	Europa (Londra)	892757235363
ap-northeast-1	Asia Pacifico (Tokyo)	533107202818
ap-southeast-1	Asia Pacifico (Singapore)	174946120834
ap-south-1	Asia Pacifico (Mumbai)	251508486986
ap-southeast-3	Asia Pacifico (Giacarta)	510637619217
sa-east-1	Sud America (San Paolo)	758426053663
ap-northeast-3	Asia Pacifico (Osaka-Locale)	273192626886
eu-south-1	Europa (Milano)	266869475730
af-south-1	Africa (Città del Capo)	197869348890
ap-southeast-2	Asia Pacifico (Sydney)	005257825471
me-central-1	Medio Oriente () UAE	000014521398
us-west-1	Stati Uniti occidentali (California settentrionale)	684579721401
ca-central-1	Canada (Centrale)	354763396469

ca-west-1	Canada occidentale (Calgary)	339712888787
ap-south-2	Asia Pacific (Hyderabad)	950823858135
eu-south-2	Europa (Spagna)	919611009337
eu-central-2	Europa (Zurigo)	529164026651
ap-southeast-4	Asia Pacifico (Melbourne)	251357961535
il-central-1	Israele (Tel Aviv)	870907303882

b. Scarica il modello

Nel seguente comando per scaricare la chiave pubblica appropriata, la firma di x86_64RPM, la firma di arm64 RPM e il collegamento di accesso corrispondente agli RPM script ospitati nei bucket Amazon S3, assicurati di sostituire l'ID dell'account con l' Account AWS ID appropriato e la regione con la regione corrente.

```
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. Importa la chiave pubblica

Usa il seguente comando per importare la chiave pubblica nel database:

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

gpg mostra l'importazione con successo

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

d. Verifica la firma

Utilizzate il seguente comando per verificare la firma

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

Se la verifica ha esito positivo, verrà visualizzato un messaggio simile al risultato riportato di seguito. È ora possibile procedere all'installazione del GuardDuty security agent utilizzandoRPM.

Output di esempio:

```
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
```

Se la verifica fallisce, significa che la firma RPM è stata potenzialmente manomessa. È necessario rimuovere la chiave pubblica dal database e ripetere il processo di verifica.

Esempio:

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

Usa il seguente comando per rimuovere la chiave pubblica dal database:

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

Ora prova di nuovo la procedura di verifica.

2. Connect con SSH Linux o macOS.
3. Installa il GuardDuty security agent utilizzando il seguente comando:

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

4. Verifica se l'installazione dell' GuardDuty agente è integra. Per ulteriori informazioni sui passaggi, vedereConvalida dello stato di installazione del GuardDuty Security Agent.

Debian installation

> **Important**
>
> Si consiglia di verificare la firma Debian dell'agente di GuardDuty sicurezza prima di installarla sulla macchina.

1. Verifica la firma Debian dell'agente GuardDuty di sicurezza

   a. Preparare i modelli per la chiave pubblica appropriata, la firma del pacchetto Debian amd64, la firma del pacchetto Debian arm64 e il collegamento di accesso corrispondente agli script Debian ospitati nei bucket Amazon S3

      Nei seguenti modelli, sostituisci il valore di Regione AWS, AWS account ID e la versione dell'agente per accedere agli script dei GuardDuty pacchetti Debian.

      - Chiave pubblica:

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

      - GuardDuty firma Debian dell'agente di sicurezza:

        Firma di amd64

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

        Firma di arm64

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

      - Accedi ai link agli script Debian nel bucket Amazon S3:

Link di accesso per amd64

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

Link di accesso per arm64

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

Regione AWS	Nome Regione	AWS ID dell'account
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Stati Uniti orientali (Virginia settentrionale)	593207742271
us-west-2	US West (Oregon)	733349766148
eu-west-3	Europa (Parigi)	665651866788
us-east-2	Stati Uniti orientali (Ohio)	307168627858
eu-central-1	Europa (Francoforte)	323658145986
ap-northeast-2	Asia Pacifico (Seoul)	914738172881
eu-north-1	Europa (Stoccolma)	591436053604
ap-east-1	Asia Pacifico (Hong Kong)	258348409381
me-south-1	Medio Oriente (Bahrein)	536382113932
eu-west-2	Europa (Londra)	892757235363
ap-northeast-1	Asia Pacifico (Tokyo)	533107202818
ap-southeast-1	Asia Pacifico (Singapore)	174946120834

ap-south-1	Asia Pacifico (Mumbai)	251508486986
ap-southeast-3	Asia Pacifico (Giacarta)	510637619217
sa-east-1	Sud America (San Paolo)	758426053663
ap-northeast-3	Asia Pacifico (Osaka-Locale)	273192626886
eu-south-1	Europa (Milano)	266869475730
af-south-1	Africa (Città del Capo)	197869348890
ap-southeast-2	Asia Pacifico (Sydney)	005257825471
me-central-1	Medio Oriente () UAE	000014521398
us-west-1	Stati Uniti occidentali (California settentrionale)	684579721401
ca-central-1	Canada (Centrale)	354763396469
ca-west-1	Canada occidentale (Calgary)	339712888787
ap-south-2	Asia Pacific (Hyderabad)	950823858135
eu-south-2	Europa (Spagna)	919611009337
eu-central-2	Europa (Zurigo)	529164026651
ap-southeast-4	Asia Pacifico (Melbourne)	251357961535
il-central-1	Israele (Tel Aviv)	870907303882

b. Scarica la chiave pubblica appropriata per il download, la firma di amd64, la firma di arm64 e il link di accesso corrispondente agli script Debian ospitati nei bucket Amazon S3

   Nei seguenti comandi, sostituisci l'ID dell'account con l' Account AWS ID appropriato e la regione con la regione corrente.

```
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. Importa la chiave pubblica nel database

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

gpg mostra che l'importazione è avvenuta con successo

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

d. Verifica la firma

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

Dopo una verifica avvenuta con successo, vedrai un messaggio simile al seguente risultato:

Output di esempio:

```
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
```

È ora possibile procedere all'installazione del GuardDuty security agent utilizzando Debian.

Tuttavia, se la verifica fallisce, significa che la firma nel pacchetto Debian è stata potenzialmente manomessa.

Esempio:

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

Usare il seguente comando per rimuovere la chiave pubblica dal database:

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

Ora riprova il processo di verifica.

2. Connect con SSH Linux o macOS.
3. Installa il GuardDuty security agent utilizzando il seguente comando:

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

4. Verifica se l'installazione dell' GuardDuty agente è integra. Per ulteriori informazioni sui passaggi, vedereConvalida dello stato di installazione del GuardDuty Security Agent.

Errore di memoria esaurita

Se riscontri un `out-of-memory` errore durante l'installazione o l'aggiornamento EC2 manuale del GuardDuty Security Agent per Amazon, consultaRisoluzione dell'errore di esaurimento della memoria.

Convalida dello stato di installazione del GuardDuty Security Agent

Per verificare se il GuardDuty Security Agent è integro

1. Connect con SSH Linux o macOS.
2. Esegui il comando seguente per verificare lo stato del GuardDuty security agent:

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

Se desideri visualizzare i registri di installazione del Security Agent, sono disponibili in`/var/log/amzn-guardduty-agent/`.

Per visualizzare i log, fai. `sudo journalctl -u amazon-guardduty-agent`

Aggiornamento manuale del GuardDuty Security Agent

È possibile aggiornare il GuardDuty security agent utilizzando il comando Run. È possibile seguire gli stessi passaggi utilizzati per installare il GuardDuty security agent.

Disinstallazione manuale del Security Agent

Questa sezione fornisce i metodi per disinstallare il GuardDuty security agent dalle tue EC2 risorse Amazon. Se prevedi di disabilitare ulteriormente il monitoraggio del runtime, consultaImpatto della disabilitazione.

Metodo 1: utilizzando il comando Esegui

Per disinstallare il GuardDuty security agent utilizzando il comando Run

1. È possibile disinstallare il GuardDuty security agent seguendo i passaggi specificati in AWS Systems Manager Esegui comando nella Guida per l'AWS Systems Manager utente. Utilizzare l'azione Disinstalla nei parametri per disinstallare il GuardDuty security agent.

   Nella sezione Target, assicurati che l'impatto riguardi solo EC2 le istanze Amazon da cui desideri disinstallare il security agent.

   Utilizza il seguente GuardDuty documento e distributore:

   - Nome del documento: `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
   - Distributore: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
2. Dopo aver fornito tutti i dettagli, quando scegli Esegui, l'agente di sicurezza che ha distribuito sulle EC2 istanze Amazon di destinazione viene rimosso.

   Per rimuovere la configurazione degli VPC endpoint Amazon, devi disabilitare sia Runtime Monitoring che Amazon EKS Runtime Monitoring.

Metodo 2 - Utilizzando Linux Package Managers

1. Connect con SSH da Linux o macOS.

2. Comando di disinstallazione

   Il comando seguente disinstallerà il GuardDuty security agent dall'EC2istanza Amazon a cui ti connetti:

   - PerRPM:

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

   - Per Debian:

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

   Dopo aver eseguito il comando, è possibile controllare anche i log associati al comando.

Eliminare l'VPCendpoint Amazon

Se desideri disabilitare il Runtime Monitoring o disinstallare il GuardDuty security agent per il tuo account, puoi anche scegliere di eliminare l'VPCendpoint Amazon creato manualmente (Creazione manuale di un VPC endpoint Amazon).

Per eliminare l'VPCendpoint Amazon utilizzando la console

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Seleziona l'endpoint che è stato creato manualmente al momento dell'attivazione del Runtime Monitoring.
4. Scegli Azioni, Elimina VPC endpoint.
5. Quando viene richiesta la conferma, immetti **`delete`**.
6. Scegli Elimina.

Per eliminare l'VPCendpoint Amazon utilizzando AWS CLI

- delete-vpc-endpoints (AWS Command Line Interface)
- Remove-EC2VpcEndpointCmdlet (strumenti per Windows) PowerShell

Gestione dell'agente di sicurezza automatizzato per Fargate (solo AmazonECS)

Runtime Monitoring supporta la gestione del security agent per i tuoi ECS cluster Amazon (AWS Fargate) solo tramite GuardDuty. Non è disponibile alcun supporto per la gestione manuale del security agent sui ECS cluster Amazon.

GuardDutyPer abilitare la gestione del security agent per le tue risorse ECS -Fargate, segui i passaggi indicati nelle sezioni seguenti.

Indice

Configurazione dell' GuardDuty agente per un account autonomo

Console

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione:

    a. Per gestire la configurazione automatizzata degli agenti per tutti i ECS cluster Amazon (a livello di account)

    Scegli Abilita nella sezione Configurazione automatica dell'agente per AWS Fargate (ECSsolo). Quando verrà avviata una nuova ECS attività Fargate Amazon, GuardDuty gestirà l'implementazione del security agent.

    - Seleziona Salva.

    b. Per gestire la configurazione automatizzata degli agenti escludendo alcuni ECS cluster Amazon (a livello di cluster)

    i. Aggiungi un tag al ECS cluster Amazon per il quale desideri escludere tutte le attività. La coppia chiave-valore deve essere `GuardDutyManaged` -. `false`

    ii. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati

nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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. Nella scheda Configurazione, scegli Abilita nella sezione Configurazione automatica dell'agente.

> **Note**
>
> Aggiungi sempre il tag di esclusione al tuo ECS cluster Amazon prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, il security agent verrà distribuito in tutte le attività avviate all'interno del cluster Amazon corrispondente. ECS

Per ECS i cluster Amazon che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.

iv. Seleziona Salva.

c. Per gestire la configurazione automatizzata degli agenti includendo alcuni ECS cluster Amazon (a livello di cluster)

i. Aggiungi un tag a un ECS cluster Amazon per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere `GuardDutyManaged` -. `true`

ii. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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. Quando si desidera GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.
   - update-service nel AWS CLI Command Reference.

Configurazione dell' GuardDuty agente per un ambiente multi-account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare la configurazione automatica degli agenti per gli account dei membri e gestire la configurazione automatizzata degli agenti per ECS i cluster Amazon che appartengono agli account dei membri della loro organizzazione. Un account GuardDuty membro non può modificare questa configurazione. L'account GuardDuty amministratore delegato gestisce i propri account membro utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti con più account, vedere Gestione di più account in. GuardDuty

Abilitazione della configurazione automatizzata degli agenti per l'account amministratore delegato GuardDuty

Manage for all Amazon ECS clusters (account level)

Se hai scelto Abilita per tutti gli account per il monitoraggio del runtime, hai le seguenti opzioni:

- Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty distribuirà e gestirà l'agente di sicurezza per tutte le ECS attività di Amazon che verranno lanciate.
- Scegli Configura gli account manualmente.

Se hai scelto Configura gli account manualmente nella sezione Runtime Monitoring, procedi come segue:

1. Scegli Configura gli account manualmente nella sezione Configurazione automatica degli agenti.
2. Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).

Seleziona Salva.

Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
- UpdateServicenell'Amazon Elastic Container Service API Reference.
- update-service nel AWS CLI Command Reference.

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

1. Aggiungi un tag a questo ECS cluster Amazon con la coppia chiave-valore come `GuardDutyManaged` -. `false`
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel pannello di navigazione, scegli Runtime Monitoring.
5.

> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi ECS cluster Amazon prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle ECS attività Amazon che vengono lanciate.

   Nella scheda Configurazione, scegli Abilita nella configurazione dell'agente automatizzato.

   Per ECS i cluster Amazon che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.
6. Seleziona Salva.
7. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova implementazione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.

- UpdateServicenell'Amazon Elastic Container Service API Reference.
- update-service nel AWS CLI Command Reference.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Aggiungi un tag a un ECS cluster Amazon per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere `GuardDutyManaged` -. `true`
2. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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**
>
> Quando utilizzi i tag di inclusione per i tuoi ECS cluster Amazon, non è necessario abilitare esplicitamente GuardDuty l'agente tramite la configurazione automatica degli agenti.

3. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova implementazione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.
   - update-service nel AWS CLI Command Reference.

Attivazione automatica per tutti gli account dei membri

Manage for all Amazon ECS clusters (account level)

I passaggi seguenti presuppongono che tu abbia scelto Abilita per tutti gli account nella sezione Runtime Monitoring.

1. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty distribuirà e gestirà l'agente di sicurezza per tutte le ECS attività di Amazon che verranno lanciate.
2. Seleziona Salva.
3. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
- UpdateServicenell'Amazon Elastic Container Service API Reference.
- update-service nel AWS CLI Command Reference.

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

1. Aggiungi un tag a questo ECS cluster Amazon con la coppia chiave-valore come `GuardDutyManaged` -. `false`
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel pannello di navigazione, scegli Runtime Monitoring.
5.

> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi ECS cluster Amazon prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle ECS attività Amazon che vengono lanciate.

   Nella scheda Configurazione, scegli Modifica.
6. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente

   Per ECS i cluster Amazon che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.
7. Seleziona Salva.
8. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova implementazione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.
   - update-service nel AWS CLI Command Reference.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Indipendentemente dal modo in cui scegli di abilitare il Runtime Monitoring, i seguenti passaggi ti aiuteranno a monitorare attività selettive di Amazon ECS Fargate per tutti gli account membri della tua organizzazione.

1. Non abilitare alcuna configurazione nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella selezionata nel passaggio precedente.
2. Seleziona Salva.
3. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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**
>
> Quando utilizzi i tag di inclusione per i tuoi ECS cluster Amazon, non è necessario abilitare esplicitamente la gestione automatica degli GuardDuty agenti.

4. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova implementazione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.
   - update-service nel AWS CLI Command Reference.

Abilitazione della configurazione automatica degli agenti per gli account dei membri attivi esistenti

Manage for all Amazon ECS clusters (account level)

1. Nella pagina Runtime Monitoring, nella scheda Configurazione, è possibile visualizzare lo stato corrente della configurazione automatizzata dell'agente.
2. Nel riquadro di configurazione dell'agente automatizzato, nella sezione Account membri attivi, scegli Azioni.
3. Da Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
4. Scegli Conferma.
5. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.
   - update-service nel AWS CLI Command Reference.

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

1. Aggiungi un tag a questo ECS cluster Amazon con la coppia chiave-valore come `GuardDutyManaged` -. `false`
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel pannello di navigazione, scegli Runtime Monitoring.

5.
> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi ECS cluster Amazon prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle ECS attività Amazon che vengono lanciate.

   Nella scheda Configurazione, nella sezione Configurazione automatizzata dell'agente, in Account membri attivi, scegli Azioni.
6. Da Operazioni, scegli Abilita per tutti gli account membri attivi.

   Per ECS i cluster Amazon che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.
7. Scegli Conferma.
8. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova implementazione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.
   - update-service nel AWS CLI Command Reference.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Aggiungi un tag a un ECS cluster Amazon per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere `GuardDutyManaged` -. `true`
2. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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**
>
> Quando utilizzi i tag di inclusione per i tuoi ECS cluster Amazon, non è necessario abilitare esplicitamente la configurazione degli agenti automatizzati.

3. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova implementazione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.

- update-service nel AWS CLI Command Reference.

Abilita automaticamente la configurazione automatizzata degli agenti per i nuovi membri

Manage for all Amazon ECS clusters (account level)

1. Nella pagina Runtime Monitoring, scegli Modifica per aggiornare la configurazione esistente.
2. Nella sezione Configurazione automatizzata dell'agente, seleziona Abilita automaticamente per nuovi account membro.
3. Seleziona Salva.
4. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.
   - update-service nel AWS CLI Command Reference.

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

1. Aggiungi un tag a questo ECS cluster Amazon con la coppia chiave-valore come `GuardDutyManaged` -. `false`
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel pannello di navigazione, scegli Runtime Monitoring.
5.

> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi ECS cluster Amazon prima di abilitare la configurazione automatizzata degli agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle ECS attività Amazon che vengono lanciate.

   Nella scheda Configurazione, seleziona Abilita automaticamente gli account dei nuovi membri nella sezione Configurazione automatica degli agenti.

   Per ECS i cluster Amazon che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.
6. Seleziona Salva.
7. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova implementazione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima

distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
- UpdateServicenell'Amazon Elastic Container Service API Reference.
- update-service nel AWS CLI Command Reference.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Aggiungi un tag a un ECS cluster Amazon per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere `GuardDutyManaged` -. `true`
2. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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**
>
> Quando utilizzi i tag di inclusione per i tuoi ECS cluster Amazon, non è necessario abilitare esplicitamente la configurazione degli agenti automatizzati.

3. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova implementazione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.
   - update-service nel AWS CLI Command Reference.

Abilitazione selettiva della configurazione automatizzata degli agenti per gli account dei membri attivi

Manage for all Amazon ECS (account level)

1. Nella pagina Account, selezionate gli account per i quali desiderate abilitare la configurazione automatica dell'agente di monitoraggio del runtime (ECS-Fargate). È possibile selezionare più account. Assicurati che gli account selezionati in questo passaggio siano già abilitati con Runtime Monitoring.
2. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare Runtime Monitoring-Automated agent configuration (ECS-Fargate).
3. Scegli Conferma.
4. Quando si desidera GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se

l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

- Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
- UpdateServicenell'Amazon Elastic Container Service API Reference.
- update-service nel AWS CLI Command Reference.

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

1. Aggiungi un tag a questo ECS cluster Amazon con la coppia chiave-valore come `GuardDutyManaged` -. `false`
2. Impedisci la modifica dei tag, tranne che da parte delle entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel pannello di navigazione, scegli Runtime Monitoring.
5.

> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi ECS cluster Amazon prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, il contenitore GuardDuty sidecar verrà collegato a tutti i contenitori delle ECS attività Amazon che vengono lanciate.

   Nella pagina Account, selezionate gli account per i quali desiderate abilitare la configurazione automatica dell'agente di monitoraggio del runtime (ECS-Fargate). È possibile selezionare più account. Assicurati che gli account selezionati in questo passaggio siano già abilitati con Runtime Monitoring.

   Per ECS i cluster Amazon che non sono stati esclusi, GuardDuty gestirà la distribuzione del security agent nel contenitore sidecar.
6. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare Runtime Monitoring-Automated agent configuration (ECS-Fargate).
7. Seleziona Salva.
8. Quando si desidera GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova distribuzione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.
   - update-service nel AWS CLI Command Reference.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Assicurati di non abilitare la configurazione automatizzata degli agenti (o la configurazione degli agenti automatizzati di Runtime Monitoring-Automated agent (ECS-Fargate)) per gli account selezionati che dispongono dei ECS cluster Amazon che desideri monitorare.
2. Aggiungi un tag a un ECS cluster Amazon per il quale desideri includere tutte le attività. La coppia chiave-valore deve essere `GuardDutyManaged` -. `true`
3. Impedisci la modifica di questi tag, tranne che da parte di entità attendibili. La politica fornita in Impedisci che i tag vengano modificati se non in base ai principi autorizzati nella Guida per l'AWS Organizations utente è stata modificata per essere applicabile qui.

```
{
    "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**
>
> Quando utilizzi i tag di inclusione per i tuoi ECS cluster Amazon, non è necessario abilitare esplicitamente la configurazione degli agenti automatizzati.

4. Quando desideri GuardDuty monitorare le attività che fanno parte di un servizio, è necessaria una nuova implementazione del servizio dopo aver abilitato il Runtime Monitoring. Se l'ultima distribuzione per un ECS servizio specifico è stata avviata prima di abilitare il Runtime Monitoring, è possibile riavviare il servizio o aggiornarlo utilizzando`forceNewDeployment`.

   Per la procedura di aggiornamento del servizio, consulta le seguenti risorse:

   - Aggiornamento di un ECS servizio Amazon utilizzando la console nell'Amazon Elastic Container Service Developer Guide.
   - UpdateServicenell'Amazon Elastic Container Service API Reference.
   - update-service nel AWS CLI Command Reference.

Gestione automatica dell'agente di sicurezza per i EKS cluster Amazon

Configurazione dell'agente automatizzato per un account autonomo

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/
2. Nel pannello di navigazione, scegli Runtime Monitoring.
3. Nella scheda Configurazione, scegli Abilita per abilitare la configurazione automatica degli agenti per il tuo account.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitora tutti i EKS cluster)	1. Scegli Abilita nella sezione Configurazione automatic a dell'agente. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster esistenti e potenzialmente nuovi del tuo account.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	2. Seleziona Salva.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
Monitora tutti i EKS cluster ma escludi alcuni di essi (utilizzando il tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un EKS cluster dal monitoraggio quando il GuardDuty Security Agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con`eks:TagResource` . • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	<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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/. 4. Nel pannello di navigazione, scegli Runtime Monitoring. **Note** Aggiungi sempre il tag di esclusione ai tuoi EKS cluster prima di abilitare la gestione automatica degli GuardDuty agenti per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account. 5. Nella scheda Configurazione, scegli Abilita nella sezione Gestione degli agenti. GuardDuty Per EKS i cluster che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 6. Seleziona Salva.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	Per escludere un EKS cluster dal monitoraggio dopo che il GuardDuty security agent è già stato distribuito su questo cluster 1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. Dopo questo passaggio, non GuardDuty aggiorner à il security agent per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo EKS cluster. Ciò potrebbe influire sulle statistiche di utilizzo. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con`eks:TagResource` . • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged`

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	• Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. Per interrompere la ricezione degli eventi di runtime da questo cluster, è necessario rimuovere il security agent distribuito da questo EKS cluster. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Impatto della disabilitazione e della pulizia delle risorse.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
Monitora i EKS cluster selettivi utilizzando i tag di inclusione	1. Assicurati di scegliere Disabilita nella sezione Configurazione automatica dell'agente. Mantieni abilitato il monitoraggio del runtime. 2. Seleziona Salva 3. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`true`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. GuardDuty gestirà la distribuzione e gli aggiornam enti del security agent per i EKS cluster selettivi che desideri monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile.

Approccio preferito per implementare un agente GuardDuty di sicurezza	Fasi
	Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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"]`
Gestire l'agente manualmente	1. Assicurati di scegliere Disabilita nella sezione Configurazione automatica dell'agente. Mantieni abilitato il monitoraggio del runtime. 2. Seleziona Salva. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Configurazione dell'agente automatizzato per ambienti con più account

In ambienti con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare la configurazione automatizzata degli agenti per gli account dei membri e gestire l'agente automatizzato per EKS i cluster appartenenti agli account membro dell'organizzazione. GuardDuty Gli account dei membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti multi-account, consulta Gestione di più account.

Configurazione della configurazione automatizzata dell'agente per l'account amministratore delegato GuardDuty

Approccio preferito per gestire il Security Agent GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitora tutti i EKS cluster)	Se hai scelto Abilita per tutti gli account nella sezione Runtime Monitoring, hai le seguenti opzioni: • Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty distribuirà e gestirà il security agent per tutti EKS i cluster che appartengono all'account GuardDuty amministratore delegato e anche per tutti i EKS cluster che appartengono a tutti gli account membro esistenti e potenzial mente nuovi dell'organizzazione. • Scegli Configura gli account manualmente. Se hai scelto Configura gli account manualmente nella sezione Runtime Monitoring, procedi come segue: 1. Scegli Configura gli account manualmente nella sezione Configura zione automatica degli agenti. 2. Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account). Seleziona Salva.
Monitora tutti i EKS cluster ma escludi alcuni di essi (utilizzando i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un EKS cluster dal monitoraggio quando il GuardDuty Security Agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`.

Approccio preferito per gestire il Security Agent GuardDuty	Fasi

Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide.

2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy:

   - Replace (Sostituisci) *ec2:CreateTags* coneks:TagResource .
   - Replace (Sostituisci) *ec2:DeleteTags* coneks:UntagResource .
   - Replace (Sostituisci) *access-project* con GuardDutyManaged
   - Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile.

     Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più PrincipalArn :

     ```
     "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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel pannello di navigazione, scegli Runtime Monitoring.

   > **Note**
   >
   > Aggiungi sempre il tag di esclusione ai tuoi EKS cluster prima di abilitare la gestione automatica degli GuardDuty

Approccio preferito per gestire il Security Agent GuardDuty	Fasi
	agenti per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account. 5. Nella scheda Configurazione, scegli Abilita nella sezione Gestione degli agenti. GuardDuty Per EKS i cluster che non sono stati esclusi dal monitorag gio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 6. Seleziona Salva. Per escludere un EKS cluster dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con `eks:TagResource` . • Replace (Sostituisci) *`ec2:DeleteTags`* con `eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged`

Approccio preferito per gestire il Security Agent GuardDuty	Fasi

- Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile.

  Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

```
"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. Se l'agente automatico era abilitato per questo EKS cluster, dopo questo passaggio non GuardDuty aggiornerà il security agent per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo EKS cluster. Ciò potrebbe influire sulle statistiche di utilizzo.

   Per interrompere la ricezione degli eventi di runtime da questo cluster, è necessario rimuovere il security agent distribuito da questo EKS cluster. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Impatto della disabilitazione e della pulizia delle risorse
4. Se stavi gestendo manualmente il GuardDuty Security Agent per questo EKS cluster, vediImpatto della disabilitazione e della pulizia delle risorse.

Approccio preferito per gestire il Security Agent GuardDuty	Fasi
Monitora i EKS cluster selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui hai scelto di abilitare il Runtime Monitoring, i seguenti passaggi ti aiuteranno a monitorare EKS i cluster selettivi nel tuo account: 1. Assicurati di scegliere Disattiva per l'account GuardDuty amministratore delegato (questo account) nella sezione Configurazione automatica dell'agente. Mantieni la configura zione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Seleziona Salva. 3. Aggiungi un tag al EKS cluster con la chiave as `GuardDuty Managed` e il relativo valore come`true`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i EKS cluster selettivi che desideri monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDuty Managed` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile.

Approccio preferito per gestire il Security Agent GuardDuty	Fasi
	Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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"]`
Gestisci manualmente l'agente di GuardDuty sicurezza	Indipendentemente dal modo in cui hai scelto di abilitare il Runtime Monitoring, puoi gestire manualmente il security agent per i tuoi EKS cluster. 1. Assicurati di scegliere Disattiva per l'account GuardDuty amministratore delegato (questo account) nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Seleziona Salva. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Abilita automaticamente l'agente automatizzato per tutti gli account dei membri

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitora tutti i EKS cluster)	Questo argomento riguarda l'abilitazione del monitoraggio del runtime per tutti gli account membri e, pertanto, i passaggi seguenti presuppongono che sia necessario aver scelto Abilita per tutti gli account nella sezione Runtime Monitoring. 1. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. GuardDuty distribuirà e gestirà il security agent per tutti EKS i cluster che appartengono all'account GuardDuty amministratore delegato e anche per tutti i EKS cluster che appartengono a tutti gli account membro esistenti e potenzialmente nuovi dell'organizzazione. 2. Seleziona Salva.
Monitora tutti i EKS cluster ma escludi alcuni di essi (utilizzando i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un EKS cluster dal monitoraggio quando il GuardDuty Security Agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* `coneks:TagResource` . • Replace (Sostituisci) *`ec2:DeleteTags`* `coneks:UntagResource` .

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi

- Replace (Sostituisci) *access-project* con `GuardDuty Managed`
- Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile.

  Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

```
"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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel pannello di navigazione, scegli Runtime Monitoring.

> **Note**
>
> Aggiungi sempre il tag di esclusione ai tuoi EKS cluster prima di abilitare Automated Agent per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account.

5. Nella scheda Configurazione, scegli Modifica nella sezione Configurazione di Runtime Monitoring.
6. Scegli Abilita per tutti gli account nella sezione Configurazione automatica dell'agente. Per EKS i cluster che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent.
7. Seleziona Salva.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Per escludere un EKS cluster dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. 2. Se la configurazione dell'agente automatizzato era abilitata per questo EKS cluster, dopo questo passaggio non GuardDuty aggiornerà l'agente di sicurezza per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo EKS cluster. Ciò potrebbe influire sulle statistiche di utilizzo. Per interrompere la ricezione degli eventi di runtime da questo cluster, è necessario rimuovere il security agent distribuito da questo EKS cluster. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Impatto della disabilitazione e della pulizia delle risorse 3. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *ec2:CreateTags* con `eks:TagResource` . • Replace (Sostituisci) *ec2:DeleteTags* con `eks:UntagResource` . • Replace (Sostituisci) *access-project* con `GuardDutyManaged`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	• Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. Se stavi gestendo manualmente il GuardDuty security agent per questo EKS cluster, vedi[Impatto della disabilitazione e della pulizia delle risorse]().

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitora i EKS cluster selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui hai scelto di abilitare il Runtime Monitoring, i seguenti passaggi ti aiuteranno a monitorare EKS i cluster selettivi per tutti gli account membri della tua organizzazione: 1. Non abilitate alcuna configurazione nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedent e. 2. Seleziona Salva. 3. Aggiungi un tag al EKS cluster con la chiave as `GuardDuty Managed` e il relativo valore come`true`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i EKS cluster selettivi che desideri monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDuty Managed` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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"]`
Gestisci manualmente l'agente di GuardDuty sicurezza	Indipendentemente dal modo in cui hai scelto di abilitare il Runtime Monitoring, puoi gestire manualmente il security agent per i tuoi EKS cluster. 1. Non abilitare alcuna configurazione nella sezione Configurazione automatica dell'agente. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Seleziona Salva. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Abilitazione dell'agente automatizzato per tutti gli account dei membri attivi esistenti

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Per gestire il GuardDuty Security Agent per gli account dei membri attivi esistenti nell'organizzazione

- GuardDuty Per ricevere gli eventi di runtime dai EKS cluster che appartengono agli account dei membri attivi esistenti nell'organizzazione, è necessario scegliere un approccio preferito per gestire il GuardDuty security agent per questi EKS cluster. Per ulteriori informazioni su ognuno di questi approcci, consulta Approcci per gestire l'agente di sicurezza GuardDuty.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitora tutti i EKS cluster)	Per monitorare tutti i EKS cluster per tutti gli account dei membri attivi esistenti 1. Nella pagina Runtime Monitoring, nella scheda Configurazione, è possibile visualizzare lo stato corrente della configurazione automatizzata dell'agente. 2. Nel riquadro di configurazione dell'agente automatizzato, nella sezione Account membri attivi, scegli Azioni. 3. Da Operazioni, scegli Abilita per tutti gli account membri attivi esistenti. 4. Scegli Conferma.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitora tutti EKS i cluster ma escludi alcuni di essi (utilizzando il tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un EKS cluster dal monitoraggio quando il GuardDuty Security Agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con`eks:TagResource` . • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::12 3456789012:role/org-admins/iam-`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi

```
admin", "arn:aws:iam::123456789012:
role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/ia
m-admin"]
```

3. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
4. Nel pannello di navigazione, scegli Runtime Monitoring.

> **Note**
>
> Aggiungi sempre il tag di esclusione ai EKS cluster prima di abilitare la configurazione automatizzata dell'agente per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account.

5. Nella scheda Configurazione, nel riquadro di configurazione dell'agente automatizzato, in Account membri attivi, scegli Azioni.
6. Da Operazioni, scegli Abilita per tutti gli account membri attivi.
7. Scegli Conferma.

Per escludere un EKS cluster dal monitoraggio dopo che il GuardDuty Security Agent è già stato distribuito su questo cluster

1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. Dopo questo passaggio, non GuardDuty aggiorner à il security agent per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo EKS cluster. Ciò potrebbe influire sulle statistiche di utilizzo. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *ec2:CreateTags* con `eks:TagResource` . • Replace (Sostituisci) *ec2:DeleteTags* con `eks:UntagResource` . • Replace (Sostituisci) *access-project* con `GuardDutyManaged` • Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi

	<pre>iam::123456789012:role/org-admins/ia
	m-admin"]</pre>
	3. Indipendentemente dalla modalità di gestione del security agent (tramite GuardDuty o manualmente), per interrompere la ricezione degli eventi di runtime da questo cluster, è necessario rimuovere il security agent distribuito da questo EKS cluster. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Impatto della disabilitazione e della pulizia delle risorse.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitora i EKS cluster selettivi utilizzando i tag di inclusione	1. Nella pagina Account, dopo aver abilitato Runtime Monitoring, non abilitate Runtime Monitoring - Configurazione automatica dell'agente. 2. Aggiungi un tag al EKS cluster che appartiene all'account selezionato che desideri monitorare. La coppia chiave-valore del tag deve essere `GuardDutyManaged -true`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i EKS cluster selettivi che desideri monitorare. 3. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l'Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	`"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"]`
Gestisci manualmente l'agente di GuardDuty sicurezza	1. Assicurati di non scegliere Abilita nella sezione Configurazione automatica dell'agente. Mantieni abilitato il monitoraggio del runtime. 2. Seleziona Salva. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Abilita automaticamente la configurazione automatica degli agenti per i nuovi membri

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitora tutti i EKS cluster)	1. Nella pagina Runtime Monitoring, scegli Modifica per aggiornare la configurazione esistente. 2. Nella sezione Configurazione automatizzata dell'agente, seleziona Abilita automaticamente per nuovi account membro. 3. Seleziona Salva.
Monitora tutti EKS i cluster ma escludi alcuni di essi (utilizzando i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Per escludere un EKS cluster dal monitoraggio quando il GuardDuty Security Agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con`eks:TagResource` . • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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"]`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	3. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/. 4. Nel pannello di navigazione, scegli Runtime Monitoring. **Note** Aggiungi sempre il tag di esclusione ai EKS cluster prima di abilitare la configurazione automatizzata dell'agente per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account. 5. Nella scheda Configurazione, seleziona Abilita automaticamente gli account dei nuovi membri nella sezione Gestione degli GuardDuty agenti. Per EKS i cluster che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del GuardDuty security agent. 6. Seleziona Salva. Per escludere un EKS cluster dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Indipendentemente dal fatto che tu gestisca il GuardDuty security agent tramite GuardDuty o manualmente, aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. Se l'agente automatizzato era abilitato per questo EKS cluster, dopo questo passaggio non GuardDuty aggiornerà l'agente di sicurezza per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo EKS cluster. Ciò potrebbe influire sulle statistic he di utilizzo. Per interrompere la ricezione degli eventi di runtime da questo cluster, è necessario rimuovere il security agent distribuito da questo EKS cluster. Per ulteriori informazi oni sulla rimozione dell'agente di sicurezza implement ato, consulta Impatto della disabilitazione e della pulizia delle risorse 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizza ti nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *ec2:CreateTags* coneks:TagResource . • Replace (Sostituisci) *ec2:DeleteTags* coneks:UntagResource . • Replace (Sostituisci) *access-project* con GuardDutyManaged • Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. Se stavi gestendo manualmente il GuardDuty security agent per questo EKS cluster, vedi[Impatto della disabilitazione e della pulizia delle risorse]().

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitora i EKS cluster selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui avete scelto di abilitare il Runtime Monitoring, i seguenti passaggi vi aiuterann o a monitorare EKS i cluster selettivi per i nuovi account membro della vostra organizzazione. 1. Assicurati di deselezionare Abilita automaticamente gli account dei nuovi membri nella sezione Configurazione automatica degli agenti. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Seleziona Salva. 3. Aggiungi un tag al EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`true`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per i EKS cluster selettivi che desideri monitorare. 4. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizza ti nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	• Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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"]`
Gestisci manualmente l'agente di GuardDuty sicurezza	Indipendentemente dal modo in cui hai scelto di abilitare il Runtime Monitoring, puoi gestire manualmente il security agent per i tuoi EKS cluster. 1. Assicurati di deselezionare la casella di controllo Abilita automaticamente gli account dei nuovi membri nella sezione Configurazione automatica degli agenti. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. 2. Seleziona Salva. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Configurazione selettiva dell'agente automatizzato per gli account dei membri attivi

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (Monitora tutti i EKS cluster)	1. Nella pagina Account, seleziona gli account per i quali desideri abilitare la configurazione automatica degli agenti. Puoi selezionare più di un account alla volta. Assicurati che gli account selezionati in questo passaggio abbiano già abilitato il EKS Runtime Monitoring. 2. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare Runtime Monitoring - Configurazione automatica degli agenti. 3. Scegli Conferma.
Monitora tutti EKS i cluster ma escludi alcuni di essi (utilizzando i tag di esclusione)	Scegli lo scenario più adatto a te tra le procedure seguenti. Per escludere un EKS cluster dal monitoraggio quando il GuardDuty Security Agent non è stato distribuito su questo cluster 1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* `coneks:TagResource` . • Replace (Sostituisci) *`ec2:DeleteTags`* `coneks:UntagResource` .

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi

- Replace (Sostituisci) *access-project* con `GuardDuty Managed`
- Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile.

  Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` :

```
"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. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   > **Note**
   >
   > Aggiungi sempre il tag di esclusione ai EKS cluster prima di abilitare la configurazione automatizzata dell'agente per il tuo account; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account.

4. Nella pagina Account, seleziona l'account per il quale desideri abilitare Gestisci automaticamente l'agente. Puoi selezionare più di un account alla volta.
5. Da Modifica piani di protezione, scegli l'opzione appropriata per abilitare la configurazione automatica dell'agente di monitoraggio del runtime per l'account selezionato.

   Per EKS i cluster che non sono stati esclusi dal monitoraggio, GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent. GuardDuty

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	6. Seleziona Salva. Per escludere un EKS cluster dal monitoraggio quando il GuardDuty security agent è stato distribuito su questo cluster 1. Aggiungi un tag a questo EKS cluster con la chiave as `GuardDutyManaged` e il relativo valore come`false`. Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. Se in precedenza avevi abilitato la configurazione dell'agente automatizzato per questo EKS cluster, dopo questo passaggio non GuardDuty aggiornerai l'agente di sicurezza per questo cluster. Tuttavia, il security agent rimarrà distribuito e GuardDuty continuerà a ricevere gli eventi di runtime da questo EKS cluster. Ciò potrebbe influire sulle statistiche di utilizzo. Per interrompere la ricezione degli eventi di runtime da questo cluster, è necessario rimuovere il security agent distribuito da questo EKS cluster. Per ulteriori informazioni sulla rimozione dell'agente di sicurezza implementato, consulta Impatto della disabilitazione e della pulizia delle risorse 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *ec2:CreateTags* coneks:TagResource . • Replace (Sostituisci) *ec2:DeleteTags* coneks:UntagResource .

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	• Replace (Sostituisci) *access-project* con `GuardDuty Managed` • Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. Se stavi gestendo manualmente il GuardDuty security agent per questo EKS cluster, devi rimuoverlo. Per ulteriori informazioni, consulta Impatto della disabilitazione e della pulizia delle risorse.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitora i EKS cluster selettivi utilizzando i tag di inclusione	Indipendentemente dal modo in cui hai scelto di abilitare il Runtime Monitoring, i seguenti passaggi ti aiuteranno a monitorare EKS i cluster selettivi che appartengono agli account selezionati: 1. Assicuratevi di non abilitare la configurazione automatica degli agenti di Runtime Monitoring-Automated Agent per gli account selezionati che contengono EKS i cluster che desiderate monitorare. 2. Aggiungi un tag al EKS cluster con la chiave as `GuardDuty Managed` e il relativo valore come. `true` Per ulteriori informazioni sull'etichettatura del tuo EKS cluster Amazon, consulta Lavorare con i tag utilizzando la console nella Amazon EKS User Guide. Dopo aver aggiunto il tag, GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per EKS i cluster selettivi che desideri monitorare. 3. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDuty Managed` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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"]`
Gestisci manualmente l'agente di GuardDuty sicurezza	1. Mantieni la configurazione di Runtime Monitoring uguale a quella configurata nel passaggio precedente. Assicurati di non abilitare Runtime Monitoring - Configurazione automatica degli agenti per nessuno degli account selezionati. 2. Scegli Conferma. 3. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon

Questa sezione descrive come gestire il tuo agente EKS aggiuntivo Amazon (GuardDuty agente) dopo aver abilitato il Runtime Monitoring. Per utilizzare Runtime Monitoring, devi abilitare Runtime Monitoring e configurare il EKS componente aggiuntivo Amazon,`aws-guardduty-agent`. L'esecuzione di una sola di queste due fasi non aiuterà a GuardDuty rilevare potenziali minacce o a generare risultati.

Prerequisiti per l'implementazione del Security Agent GuardDuty

Questa sezione descrive i prerequisiti per la distribuzione manuale del GuardDuty Security Agent per i cluster. EKS Prima di procedere, assicurati di aver già configurato il Runtime Monitoring per i tuoi account. L'agente GuardDuty di sicurezza (EKSComponente aggiuntivo) non funzionerà se non configuri Runtime Monitoring. Per ulteriori informazioni, consulta Attivazione del monitoraggio del GuardDuty runtime. Una volta completate la fasi seguenti, consulta Implementazione di un agente di sicurezza GuardDuty .

Scegli il tuo metodo di accesso preferito per creare un VPC endpoint Amazon.

Console

Crea un endpoint VPC

1. Apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Dal riquadro di navigazione, in Cloud privato virtuale, scegli Endpoint.
3. Scegliere Create Endpoint (Crea endpoint).
4. Nella pagina Crea endpoint per Categoria servizio, scegli Altri servizi endpoint.
5. Per Nome servizio, inserisci **com.amazonaws.*us-east-1*.guardduty-data**.

   Assicurati di sostituire *us-east-1* con la regione corretta. Questa deve essere la stessa regione del EKS cluster che appartiene al tuo Account AWS ID.
6. Scegli Verifica del servizio.
7. Dopo aver verificato con successo il nome del servizio, scegli VPCdove risiede il cluster. Aggiungi la seguente politica per limitare l'utilizzo VPC degli endpoint solo all'account specificato. Con la `Condition` dell'organizzazione fornita sotto a questa policy, puoi aggiornare la policy seguente per limitare l'accesso all'endpoint. Per fornire supporto VPC endpoint a un account specifico dell'IDsorganizzazione, consulta. Organization 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": "*"
   }
  ]
}
```

L'ID `aws:PrincipalAccount` dell'account deve corrispondere all'account contenente l'VPCendpoint VPC and. L'elenco seguente mostra come condividere l'VPCendpoint con altri: Account AWS IDs

Condizione dell'organizzazione per limitare l'accesso all'endpoint

- Per specificare più account per accedere all'VPCendpoint, sostituiscilo `"aws:PrincipalAccount": "111122223333"` con quanto segue:

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

- Per consentire a tutti i membri di un'organizzazione di accedere all'VPCendpoint, sostituiscilo `"aws:PrincipalAccount": "111122223333"` con quanto segue:

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

- Per limitare l'accesso a una risorsa da parte di un ID organizzazione, aggiungi il tuo `ResourceOrgID` alla policy.

  Per ulteriori informazioni, consulta ResourceOrgID.

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

8. In Impostazioni aggiuntive, scegli Abilita DNS nome.
9. In Sottoreti, scegli le sottoreti in cui risiede il cluster.
10. In Gruppi di sicurezza, scegli un gruppo di sicurezza con la porta in ingresso 443 abilitata dal tuo VPC (o dal tuo EKS cluster). Se non disponi già di un gruppo di sicurezza con una porta 443 in ingresso abilitata, Crea un gruppo di sicurezza.

    Se c'è un problema durante la limitazione delle autorizzazioni in ingresso alla tua VPC (o al cluster), fornisci il supporto alla porta 443 in ingresso da qualsiasi indirizzo IP (). `0.0.0.0/0`

API/CLI

- CreateVpcEndpointInvoca.
- Utilizza i seguenti valori per i parametri:
  - Per Nome servizio, inserisci **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

    Assicurati di sostituire *`us-east-1`* con la regione corretta. Questa deve essere la stessa regione del EKS cluster che appartiene al tuo Account AWS ID.
  - Per DNSOptions, abilita DNS l'opzione privata impostandola `sutrue`.
- Per AWS Command Line Interface, vedi create-vpc-endpoint.

Configura i parametri dell'agente di GuardDuty sicurezza (componente aggiuntivo) per Amazon EKS

Puoi configurare parametri specifici del tuo agente GuardDuty di sicurezza per AmazonEKS. Questo supporto è disponibile per la versione 1.5.0 e successive del GuardDuty Security Agent. Per informazioni sulle ultime versioni dei componenti aggiuntivi, consulta. GuardDuty agente di sicurezza per EKS cluster Amazon

Perché devo aggiornare lo schema di configurazione del Security Agent

> Lo schema di configurazione per il GuardDuty security agent è lo stesso in tutti i container all'interno EKS dei cluster Amazon. Quando i valori predefiniti non sono in linea con i carichi di lavoro associati e le dimensioni dell'istanza, prendi in considerazione la possibilità di configurare CPU le impostazioni, le impostazioni di memoria e le impostazioni. `PriorityClass` `dnsPolicy` Indipendentemente da come gestisci l' GuardDuty agente per i tuoi EKS cluster Amazon, puoi configurare o aggiornare la configurazione esistente di questi parametri.

Comportamento di configurazione automatizzato degli agenti con parametri configurati

Quando GuardDuty gestisce il Security Agent (EKScomponente aggiuntivo) per conto dell'utente, aggiorna il componente aggiuntivo, se necessario. GuardDuty imposterà il valore dei parametri configurabili su un valore predefinito. Tuttavia, è ancora possibile aggiornare i parametri al valore desiderato. Se ciò causa un conflitto, l'opzione predefinita resolveConflictsè`None`.

Parametri e valori configurabili

Per informazioni sui passaggi per configurare i parametri del componente aggiuntivo, consulta:

- Implementazione di un agente di sicurezza GuardDuty o

- Aggiornamento manuale del Security Agent

Le tabelle seguenti forniscono gli intervalli e i valori che puoi utilizzare per distribuire manualmente il EKS componente aggiuntivo Amazon o aggiornare le impostazioni del componente aggiuntivo esistenti.

CPUimpostazioni

Parametri	Valore predefinito	Intervallo configurabile
Richieste	200 m	Tra 200 m e 10000 m, entrambi inclusi
Limiti	1000 m	

Impostazioni della memoria

Parametri	Valore predefinito	Intervallo configurabile
Richieste	256 Mi	Tra 256 Mi e 20000 Mi, entrambi inclusi
Limiti	1024 Mi	

Impostazioni di **`PriorityClass`**

Quando GuardDuty crea un EKS componente aggiuntivo Amazon per te, l'assegnato `PriorityClass` è`aws-guardduty-agent.priorityclass`. Ciò significa che non verrà intrapresa alcuna azione in base alla priorità del pod dell'agente. È possibile configurare questo parametro aggiuntivo scegliendo una delle seguenti `PriorityClass` opzioni:

Configurabile **`PriorityClass`**	**`preemptionPolicy`** value	**`preemptionPolicy`** descrizione	valore del pod
`aws-guardduty-agent.priorityclass`	`Never`	Nessuna operazione	1000000

Configurabile **PriorityClass**	**preemptionPolicy** value	**preemptionPolicy** descrizione	valore del pod
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	L'assegnazione di questo valore impedirà l'esecuzione di un pod con il valore di priorità inferiore al valore del pod dell'agente.	100000000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2000000000
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] Kubernetes offre queste due opzioni: e. `PriorityClass` `system-cluster-critical` `system-node-critical` Per ulteriori informazioni, consulta la documentazione di PriorityClassKubernetes.

Impostazioni di **dnsPolicy**

Scegli una delle seguenti opzioni di DNS policy supportate da Kubernetes. Quando non viene specificata alcuna configurazione, `ClusterFirst` viene utilizzato come valore predefinito.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Per informazioni su queste politiche, consulta la DNSpolitica di Pod nella documentazione di Kubernetes.

Implementazione di un agente di sicurezza GuardDuty

Questa sezione descrive come implementare il GuardDuty Security Agent per la prima volta per cluster specificiEKS. Prima di procedere con questa sezione, assicurati di aver già impostato i

prerequisiti e abilitato il monitoraggio del runtime per i tuoi account. Il GuardDuty security agent (EKScomponente aggiuntivo) non funzionerà se non abiliti il Runtime Monitoring.

Scegliete il metodo di accesso preferito per implementare il GuardDuty security agent per la prima volta.

Console

1. Apri la EKS console Amazon a https://console.aws.amazon.com/eks/home#/clusters.
2. Scegli il Nome cluster.
3. Seleziona la scheda Componenti aggiuntivi.
4. Scegli Ottieni altri componenti aggiuntivi.
5. Nella pagina Seleziona componenti aggiuntivi, scegli Amazon GuardDuty Runtime Monitoring.
6. Nella pagina Configura le impostazioni dei componenti aggiuntivi selezionati, utilizza le impostazioni predefinite. Se lo stato del EKS componente aggiuntivo è Richiede attivazione, scegli Attiva. GuardDuty Questa azione aprirà la GuardDuty console per configurare il monitoraggio del runtime per i tuoi account.
7. Dopo aver configurato il Runtime Monitoring per i tuoi account, torna alla EKS console Amazon. Lo stato del EKS componente aggiuntivo dovrebbe essere cambiato in Pronto per l'installazione.
8. (Facoltativo) Fornire uno schema di EKS configurazione aggiuntivo

   Per la versione aggiuntiva, se si sceglie la versione 1.5.0 e successive, Runtime Monitoring supporta la configurazione di parametri specifici dell'agente. GuardDuty Per informazioni sugli intervalli di parametri, vedere. Configura i EKS parametri aggiuntivi

   a. Espandi le impostazioni di configurazione opzionali per visualizzare i parametri configurabili e il valore e il formato previsti.
   b. Imposta i parametri. I valori devono essere compresi nell'intervallo fornito inConfigura i EKS parametri aggiuntivi.
   c. Scegli Salva modifiche per creare il componente aggiuntivo in base alla configurazione avanzata.
   d. Per il metodo di risoluzione dei conflitti, l'opzione scelta verrà utilizzata per risolvere un conflitto quando si aggiorna il valore di un parametro a un valore non predefinito. Per

ulteriori informazioni sulle opzioni elencate, resolveConflictsconsulta Amazon EKS API Reference.

9. Scegli Next (Successivo).
10. Nella pagina Rivedi e crea, verifica tutti i dettagli, quindi scegli Crea.
11. Torna ai dettagli del cluster e scegli la scheda Risorse.
12. Puoi visualizzare i nuovi pod con il prefisso aws-guardduty-agent.

API/CLI

Puoi configurare l'agente EKS aggiuntivo Amazon (`aws-guardduty-agent`) utilizzando una delle seguenti opzioni:

- Esegui CreateAddonper ottenere il tuo account.
-

> **Note**
>
> Per il componente aggiuntivo`version`, se scegli la versione 1.5.0 e successive, Runtime Monitoring supporta la configurazione di parametri specifici dell'agente. GuardDuty Per ulteriori informazioni, consulta Configura i EKS parametri aggiuntivi.

Utilizza i valori seguenti per i parametri della richiesta:

- In `addonName`, immettere `aws-guardduty-agent`.

  È possibile utilizzare il seguente AWS CLI esempio quando si utilizzano valori configurabili supportati per le versioni aggiuntive v1.5.0 e successive. Assicurati di sostituire i valori segnaposto evidenziati in rosso e quelli associati ai valori configurati. `Example.json`

  ```
  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 Esempio.json

  ```
  {
   "priorityClassName": "aws-guardduty-agent.priorityclass-high",
   "dnsPolicy": "Default",
   "resources": {
  ```

```
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- Per informazioni sulle `addonVersion` supportate, consulta Versioni di Kubernetes supportate dal security agent GuardDuty .
- In alternativa, puoi usare. AWS CLI Per ulteriori informazioni, consulta create-addon.

Aggiornamento manuale del Security Agent

Quando gestisci il GuardDuty security agent manualmente, hai la responsabilità di aggiornarlo per il tuo account. Per ricevere notifiche sulle nuove versioni degli agenti, puoi iscriverti a un RSS feed aGuardDuty cronologia dei rilasci dell'agente.

È possibile aggiornare il Security Agent alla versione più recente per beneficiare del supporto e dei miglioramenti aggiuntivi. Se la versione corrente dell'agente sta per terminare il supporto standard, per continuare a utilizzare Runtime Monitoring (o EKS Runtime Monitoring), è necessario aggiornare la versione corrente dell'agente. Per informazioni sulle versioni di rilascio, vedereGuardDuty agente di sicurezza per EKS cluster Amazon.

Prerequisito

Prima di aggiornare la versione del Security Agent, assicurati che la versione dell'agente che intendi utilizzare ora sia compatibile con la tua versione di Kubernetes. Per ulteriori informazioni, consulta Versioni di Kubernetes supportate dal security agent GuardDuty .

Console

1. Apri la EKS console Amazon a https://console.aws.amazon.com/eks/home#/clusters.
2. Scegli il Nome cluster.
3. Scegli Componenti aggiuntivi.
4. In Componenti aggiuntivi, seleziona GuardDutyRuntime Monitoring.

5. Scegli Modifica per aggiornare i dettagli dell'agente.
6. Nella pagina Configura il monitoraggio del GuardDuty runtime, aggiorna i dettagli.
7. (Facoltativo) Aggiornamento dei parametri di configurazione del componente aggiuntivo

   Se la versione del EKS componente aggiuntivo è 1.5.0 o superiore, puoi anche aggiornare le impostazioni di configurazione del componente aggiuntivo.

   a. Espandi Impostazioni di configurazione opzionali per visualizzare lo schema di configurazione.
   b. Aggiorna i valori dei parametri in base all'intervallo fornito inConfigura i EKS parametri aggiuntivi.
   c. Scegli Salva modifiche per avviare l'aggiornamento.
   d. Per il metodo di risoluzione dei conflitti, l'opzione scelta verrà utilizzata per risolvere un conflitto quando si aggiorna il valore di un parametro a un valore non predefinito. Per ulteriori informazioni sulle opzioni elencate, resolveConflictsconsulta Amazon EKS API Reference.

API/CLI

Per aggiornare il GuardDuty security agent per i tuoi EKS cluster Amazon, consulta Aggiornamento di un componente aggiuntivo.

> **Note**
>
> Per il componente aggiuntivo`version`, se scegli la versione 1.5.0 e successive, Runtime Monitoring supporta la configurazione di parametri specifici dell'agente. GuardDuty Per informazioni sugli intervalli di parametri, vedere. Configura i EKS parametri aggiuntivi

È possibile utilizzare l' AWS CLI esempio seguente quando si utilizzano valori configurabili supportati per le versioni aggiuntive v1.5.0 e successive. Assicurati di sostituire i valori segnaposto evidenziati in rosso e quelli associati ai valori configurati. `Example.json`

```
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 Esempio.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Se la tua versione del EKS componente aggiuntivo Amazon è 1.5.0 o successiva e hai configurato lo schema del componente aggiuntivo, puoi verificare se i valori vengono visualizzati correttamente per il tuo cluster. Per ulteriori informazioni, consulta Verifica degli aggiornamenti dello schema di configurazione.

Verifica degli aggiornamenti dello schema di configurazione

Dopo aver configurato i parametri, effettuate le seguenti operazioni per verificare che lo schema di configurazione sia stato aggiornato:

1. Apri la EKS console Amazon a https://console.aws.amazon.com/eks/home#/clusters.
2. Nel pannello di navigazione scegliere Clusters (Cluster).
3. Nella pagina Cluster, seleziona il nome del cluster per il quale desideri verificare gli aggiornamenti.
4. Scegliere la scheda Resources (Risorse).
5. Dal riquadro Tipi di risorse, in Carichi di lavoro, scegli. DaemonSets
6. Seleziona aws-guardduty-agent.
7. Nella aws-guardduty-agentpagina, scegli Vista raw per visualizzare la risposta non formattata. JSON Verifica che i parametri configurabili visualizzino il valore che hai fornito.

Dopo la verifica, passa alla GuardDuty console. Seleziona il corrispondente Regione AWS e visualizza lo stato della copertura per i tuoi EKS cluster Amazon. Per ulteriori informazioni, consulta Copertura per i EKS cluster Amazon.

Configurazione del monitoraggio del EKS runtime (solo) API

Prima di configurare EKS Runtime Monitoring nel tuo account, assicurati di utilizzare una delle piattaforme verificate che supportano la versione di Kubernetes attualmente in uso. Per ulteriori informazioni, consulta Convalida dei requisiti relativi all'architettura.

GuardDuty ha consolidato l'esperienza della console per EKS Runtime Monitoring in Runtime Monitoring. GuardDuty consiglia Verifica dello stato della configurazione EKS di Runtime Monit e. Migrazione da EKS Runtime Monitoring a Runtime Monitoring

Come parte della migrazione al Runtime Monitoring, assicurati diDisabilita EKS il monitoraggio del runtime. Questo è importante perché se in seguito scegliete di disabilitare il Runtime Monitoring e non disattivate il EKS Runtime Monitoring, continuerete a incorrere in costi di utilizzo per EKS il Runtime Monitoring.

Configurazione del EKS Runtime Monitoring per un account indipendente

Per gli account associati a AWS Organizations, consulta Configurazione del monitoraggio del EKS runtime per ambienti con più account.

Scegli il metodo di accesso preferito per abilitare il EKS Runtime Monitoring per il tuo account.

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i EKS cluster)	1. Eseguilo updateDetectorAPIutilizzando il tuo ID regionale del rilevatore e passando il nome dell'`features`oggetto `EKS_RUNTIME_MONITORING` e lo status as. `ENABLED`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon del tuo account. 2. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitora tutti EKS i cluster ma escludi alcuni di essi (utilizzando il tag di esclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -false`. Per ulteriori informazi oni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. **Note** Aggiungi sempre il tag di esclusione al EKS cluster prima di impostare `STATUS` of

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	`EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account. Eseguilo updateDetectorAPIutilizzando il tuo ID di rilevamento regionale e passando il nome dell'`features`oggetto as e lo status as`EKS_RUNTIME_MONITORING` . `ENABLED` Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID di rilevamento regionale. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitora EKS i cluster selettivi (utilizzando il tag di inclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -true`. Per ulteriori informazioni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l'Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. Eseguilo updateDetectorAPIutilizzando il tuo ID regionale del rilevatore e passando il nome dell'`features`oggetto as `EKS_RUNTIME_MONITORING` e lo status as`ENABLED`.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon etichettati con la coppia `true` `GuardDutyManaged`-. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestire l'agente di sicurezza manualmente	1. Eseguilo updateDetectorAPIutilizzando il tuo ID regionale del rilevatore e passando il nome `features` dell'oggetto `EKS_RUNTIME_MONITORING` e lo status as`ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Configurazione del monitoraggio del EKS runtime per ambienti con più account

In ambienti con più account, solo l'account GuardDuty amministratore delegato può abilitare o disabilitare il EKS Runtime Monitoring per gli account membro e gestire la gestione degli GuardDuty

agenti per i EKS cluster appartenenti agli account membro dell'organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. Per ulteriori informazioni sugli ambienti multi-account, consulta Gestione di più account.

Configurazione del monitoraggio del EKS runtime per l'account amministratore delegato GuardDuty

Scegliete il metodo di accesso preferito per abilitare il EKS Runtime Monitoring e gestire il GuardDuty security agent per EKS i cluster che appartengono all'account amministratore delegato GuardDuty .

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i EKS cluster)	Eseguilo updateDetectorAPIutilizzando il tuo ID regionale del rilevatore e passando il nome dell'`features`oggetto `EKS_RUNTIME_MONITORING` e lo status as. `ENABLED` Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon del tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzan do il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` :

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitora tutti EKS i cluster ma escludi alcuni di essi (utilizzando il tag di esclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -false`. Per ulteriori informazi oni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *ec2:CreateTags* con. `eks:TagResource` • Replace (Sostituisci) *ec2:DeleteTags* con`eks:UntagResource` . • Replace (Sostituisci) *access-project* con `GuardDutyManaged` • Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. **Note** Aggiungi sempre il tag di esclusione al EKS cluster prima di impostare `STATUS` of

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	`EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account. Eseguilo updateDetectorAPIutilizzando il tuo ID di rilevamento regionale e passando il nome dell'`features`oggetto as e lo status as`EKS_RUNTIME_MONITORING` . `ENABLED` Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID di rilevamento regionale. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitora EKS i cluster selettivi (utilizzando il tag di inclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -true`. Per ulteriori informazioni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l'Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. Eseguilo updateDetectorAPIutilizzando il tuo ID regionale del rilevatore e passando il nome dell'`features`oggetto as `EKS_RUNTIME_MONITORING` e lo status as`ENABLED`.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon etichettati con la coppia `true` `GuardDutyManaged`-. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestire l'agente di sicurezza manualmente	1. Eseguilo updateDetectorAPIutilizzando il tuo ID regionale del rilevatore e passando il nome `features` dell'oggetto `EKS_RUNTIME_MONITORING` e lo status as`ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Abilita automaticamente il monitoraggio del EKS runtime per tutti gli account membri

Scegli il metodo di accesso preferito per abilitare il monitoraggio del EKS runtime per tutti gli account membri. Ciò include l'account GuardDuty amministratore delegato, gli account dei membri esistenti e i

nuovi account che entrano a far parte dell'organizzazione. Scegli il tuo approccio preferito per gestire il GuardDuty Security Agent per EKS i cluster che appartengono a questi account membri.

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i EKS cluster)	Per abilitare selettivamente il monitoraggio del EKS runtime per i tuoi account membri, esegui l'updateMemberDetectorsAPIoperazione utilizzando i tuoi *detector ID*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon del tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Note Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitora tutti EKS i cluster ma escludi alcuni di essi (usando il tag di esclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDuty Managed -false`. Per ulteriori informazioni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *ec2:CreateTags* con. `eks:TagResource` • Replace (Sostituisci) *ec2:DeleteTags* con`eks:UntagResource` . • Replace (Sostituisci) *access-project* con `GuardDuty Managed` • Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. **Note** Aggiungi sempre il tag di esclusione al EKS cluster prima di impostare `STATUS` of `EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario,

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account. Eseguilo updateDetectorAPIutilizzando il tuo ID di rilevamento regionale e passando il nome dell'`features`oggetto as e lo status as`EKS_RUNTIME_MONITORING` . `ENABLED` Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID di rilevamento regionale. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Note Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitora EKS i cluster selettivi (utilizzando il tag di inclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDuty Managed -true`. Per ulteriori informazioni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *ec2:CreateTags* con. `eks:TagResource` • Replace (Sostituisci) *ec2:DeleteTags* con`eks:UntagResource` . • Replace (Sostituisci) *access-project* con `GuardDuty Managed` • Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. Eseguilo updateDetectorAPIutilizzando il tuo ID regionale del rilevatore e passando il nome dell'`features`oggetto as `EKS_RUNTIME_MONITORING` e lo status as`ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon etichettati con la `true` coppia `GuardDutyManaged` -. In alternativa, puoi utilizzare il AWS CLI comando utilizzan do il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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** Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestire l'agente di sicurezza manualmente	1. Eseguilo updateDetectorAPIutilizzando il tuo ID regionale del rilevatore e passando il nome dell'`features`oggetto as `EKS_RUNTIME_MONITORING` e lo status as`ENABLED`. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Configurazione del EKS Runtime Monitoring per tutti gli account membri attivi esistenti

Scegliete il metodo di accesso preferito per abilitare il EKS Runtime Monitoring e gestire il GuardDuty security agent per gli account dei membri attivi esistenti nella vostra organizzazione.

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i EKS cluster)	Per abilitare selettivamente il monitoraggio del EKS runtime per i tuoi account membri, esegui l'updateMemberDetectorsAPIoperazione utilizzando i tuoi *detector ID*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon del tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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** Puoi anche passare un elenco di account IDs separati da uno spazio.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitora tutti EKS i cluster ma escludi alcuni di essi (usando il tag di esclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDuty Managed -false`. Per ulteriori informazioni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *ec2:CreateTags* con. `eks:TagResource` • Replace (Sostituisci) *ec2:DeleteTags* con`eks:UntagResource` . • Replace (Sostituisci) *access-project* con `GuardDuty Managed` • Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. **Note** Aggiungi sempre il tag di esclusione al EKS cluster prima di impostare `STATUS` of `EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario,

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account. Per abilitare selettivamente il EKS Runtime Monitoring per i tuoi account membro, esegui l'operazione utilizzando il updateMemberDetectorsAPItuo *detector ID*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID di rilevamento regionale. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	> **Note** > Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitora EKS i cluster selettivi (utilizzando il tag di inclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDuty Managed -true`. Per ulteriori informazioni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDuty Managed` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. Per abilitare selettivamente il EKS Runtime Monitoring per i tuoi account membro, esegui l'updateMemberDetectorsAPIoperazione utilizzando i tuoi *`detector ID`*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon etichettati con la `true` coppia `GuardDutyManaged` -. In alternativa, puoi utilizzare il AWS CLI comando utilizzan do il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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** Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestire l'agente di sicurezza manualmente	1. Per abilitare selettivamente il EKS Runtime Monitoring per i tuoi account membri, esegui l'updateMemberDetectorsAPIoperazione utilizzando i tuoi *detector ID*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Abilita automaticamente il monitoraggio del EKS runtime per i nuovi membri

L'account GuardDuty amministratore delegato può abilitare automaticamente il EKS Runtime Monitoring e scegliere un approccio per la gestione del GuardDuty security agent per i nuovi account che entrano a far parte dell'organizzazione.

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i EKS cluster)	Per abilitare selettivamente il EKS Runtime Monitoring per i nuovi account, richiamate l'UpdateOrganizationConfigurationAPIoperazione utilizzando il vostro *detector ID*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon del tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON_MANAGEMENT` per un singolo account. Puoi anche passare un elenco di account IDs separati da uno spazio. Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --feature`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	s '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}]]' Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitora tutti EKS i cluster ma escludi alcuni di essi (utilizzando il tag di esclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -false`. Per ulteriori informazi oni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. **Note** Aggiungi sempre il tag di esclusione al EKS cluster prima di impostare `STATUS` of

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	`EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account. Per abilitare selettivamente il EKS Runtime Monitorin g per i tuoi nuovi account, richiama l'operazione utilizzando il tuo UpdateOrganizationConfigurationAPI *`detector ID`*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID di rilevamento regionale. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazi oni nella https://console.aws.amazon.com/gua rdduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `EKS_ADDON _MANAGEMENT` per un singolo account. Puoi anche passare un elenco di account IDs separati da uno spazio. Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	.com/guardduty/console oppure esegui il ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Monitora EKS i cluster selettivi (utilizzando il tag di inclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -true`. Per ulteriori informazioni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. Per abilitare selettivamente il EKS Runtime Monitoring per i tuoi nuovi account, richiama l'UpdateOrganizationConfigurationAPIoperazione utilizzando il tuo *`detector ID`*.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon etichettati con la coppia `true` `GuardDutyManaged` -. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente viene abilitato `EKS_RUNTIME_MONITORING` e disabilitato `EKS_ADDON_MANAGEMENT` per un singolo account. Puoi anche passare un elenco di account IDs separati da uno spazio. Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
Gestire l'agente di sicurezza manualmente	1. Per abilitare selettivamente il EKS Runtime Monitoring per i tuoi nuovi account, richiama l'UpdateOrganizationConfigurationAPIoperazione utilizzando il tuo *detector ID*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente viene abilitato `EKS_RUNTIME_MONITORING` e disabilitato `EKS_ADDON_MANAGEMENT` per un singolo account. Puoi anche passare un elenco di account IDs separati da uno spazio. Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'`

Approccio preferito per gestire l'agente di sicurezza GuardDuty	Fasi
	Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema. 2. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Abilita il monitoraggio del EKS runtime per i singoli account dei membri attivi

API/CLI

In base a Approcci per gestire l'agente di sicurezza GuardDuty, puoi scegliere l'approccio che preferisci e seguire le fasi indicate nella tabella seguente.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Gestisci l'agente di sicurezza tramite GuardDuty (monitora tutti i EKS cluster)	Per abilitare selettivamente il monitoraggio del EKS runtime per i tuoi account membri, esegui l'updateMemberDetectorsAPIoperazione utilizzando i tuoi *`detector ID`*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon del tuo account. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	`detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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** Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitora tutti EKS i cluster ma escludi alcuni di essi (usando il tag di esclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -false`. Per ulteriori informazi oni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizat ions . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *ec2:CreateTags* con. `eks:TagResource` • Replace (Sostituisci) *ec2:DeleteTags* con`eks:UntagResource` . • Replace (Sostituisci) *access-project* con `GuardDutyManaged` • Replace (Sostituisci) *123456789012* con l' Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. **Note** Aggiungi sempre il tag di esclusione al EKS cluster prima di impostare `STATUS` of

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	`EKS_RUNTIME_MONITORING` to`ENABLED`; in caso contrario, il GuardDuty security agent verrà distribuito su tutti i EKS cluster del tuo account. Per abilitare selettivamente il EKS Runtime Monitoring per i tuoi account membro, esegui l'operazione utilizzando il updateMemberDetectorsAPItuo *`detector ID`*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `ENABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon che non sono stati esclusi dal monitoraggio. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID di rilevamento regionale. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. Nell'esempio seguente vengono abilitati sia `EKS_RUNTIME_MONITORING` che `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"}] ]'`

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Note Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituis ce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
Monitora EKS i cluster selettivi (utilizzando il tag di inclusione)	1. Aggiungi un tag al EKS cluster che desideri escludere dal monitoraggio. La coppia chiave-valore è `GuardDutyManaged -true`. Per ulteriori informazioni sull'aggiunta del tag, consulta Lavorare con i tag usando CLIAPI, o eksctl nella Amazon EKS User Guide. 2. Per consentire la modifica dei tag solo alle entità attendibili, utilizza la policy fornita in Impedire la modifica dei tag se non da parte dei principali autorizzati nella Guida per l'utente di AWS Organizations . Sostituisci i seguenti dettagli nella policy: • Replace (Sostituisci) *`ec2:CreateTags`* con. `eks:TagResource` • Replace (Sostituisci) *`ec2:DeleteTags`* con`eks:UntagResource` . • Replace (Sostituisci) *`access-project`* con `GuardDutyManaged` • Replace (Sostituisci) *`123456789012`* con l'Account AWS ID dell'entità attendibile. Se hai diverse entità attendibili, utilizza l'esempio seguente per aggiungere più `PrincipalArn` : `"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. Per abilitare selettivamente il EKS Runtime Monitoring per i tuoi account membro, esegui l'updateMemberDetectorsAPIoperazione utilizzando i tuoi *`detector ID`*.

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. GuardDuty gestirà la distribuzione e gli aggiornamenti del security agent per tutti i EKS cluster Amazon etichettati con la coppia `true` `GuardDutyManaged`-. In alternativa, puoi utilizzare il AWS CLI comando utilizzando il tuo ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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** Puoi anche passare un elenco di account IDs separati da uno spazio. Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts` . Se si verifica qualsiasi problema durante la modifica

Approccio preferito per gestire l'agente GuardDuty di sicurezza	Fasi
	delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.
Gestire l'agente di sicurezza manualmente	1. Per abilitare selettivamente il EKS Runtime Monitoring per i tuoi account membri, esegui l'updateMemberDetectorsAPIoperazione utilizzando i tuoi *detector ID*. Imposta lo stato di `EKS_ADDON_MANAGEMENT` su `DISABLED`. In alternativa, è possibile utilizzare il AWS CLI comando utilizzando il proprio ID regionale del rilevatore. Per trovare il codice `detectorId` relativo al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI. L'esempio seguente abilita `EKS_RUNTIME_MONITORING` e disabilita `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. Per gestire l'agente di sicurezza, consulta Gestione manuale dell'agente di sicurezza per il EKS cluster Amazon.

Migrazione da EKS Runtime Monitoring a Runtime Monitoring

Con il lancio di GuardDuty Runtime Monitoring, la copertura per il rilevamento delle minacce è stata estesa ai ECS contenitori Amazon e alle EC2 istanze Amazon. EKSL'esperienza di Runtime Monitoring è stata ora consolidata in Runtime Monitoring. Puoi abilitare il monitoraggio del runtime e gestire singoli agenti di GuardDuty sicurezza per ogni tipo di risorsa (EC2istanza Amazon, ECS cluster Amazon e EKS cluster Amazon) per cui desideri monitorare il comportamento di runtime.

GuardDuty ha consolidato l'esperienza della console per EKS Runtime Monitoring in Runtime Monitoring. GuardDuty consiglia Verifica dello stato della configurazione EKS di Runtime Monit e. Migrazione da EKS Runtime Monitoring a Runtime Monitoring

Come parte della migrazione al Runtime Monitoring, assicurati diDisabilita EKS il monitoraggio del runtime. Questo è importante perché se in seguito scegliete di disabilitare il Runtime Monitoring e non disattivate il EKS Runtime Monitoring, continuerete a incorrere in costi di utilizzo per EKS il Runtime Monitoring.

Per migrare dal EKS Runtime Monitoring al Runtime Monitoring

1. La GuardDuty console supporta il EKS Runtime Monitoring come parte del Runtime Monitoring.

   Puoi iniziare a utilizzare Runtime Monitoring in base Verifica dello stato della configurazione EKS di Runtime Monit alla tua organizzazione e ai tuoi account.

   Assicurati di non disabilitare il EKS Runtime Monitoring prima di abilitare il Runtime Monitoring. Se disabiliti il EKS Runtime Monitoring, anche la gestione dei EKS componenti aggiuntivi di Amazon verrà disabilitata. Continua con i seguenti passaggi nell'ordine indicato.
2. Assicurati di soddisfare tutti iPrerequisiti per abilitare il monitoraggio del runtime.
3. Abilita il monitoraggio del runtime replicando le stesse impostazioni di configurazione dell'organizzazione per il monitoraggio del runtime utilizzate per il monitoraggio del EKS runtime. Per ulteriori informazioni, consulta Abilitazione del monitoraggio del runtime.
   - Se disponi di un account autonomo, devi abilitare il Runtime Monitoring.

     Se il GuardDuty security agent è già distribuito, le impostazioni corrispondenti vengono replicate automaticamente e non è necessario configurarle nuovamente.
   - Se hai un'organizzazione con impostazioni di attivazione automatica, assicurati di replicare le stesse impostazioni di attivazione automatica per Runtime Monitoring.

- Se hai un'organizzazione con impostazioni configurate singolarmente per gli account dei membri attivi esistenti, assicurati di abilitare il Runtime Monitoring e di configurare il GuardDuty security agent per questi membri singolarmente.

4. Dopo esserti assicurato che le impostazioni di Runtime Monitoring e GuardDuty Security Agent siano corrette, disabilita il EKS Runtime Monitoring utilizzando il AWS CLI comando API o.
5. (Facoltativo) se desideri pulire qualsiasi risorsa associata al GuardDuty security agent, consultaImpatto della disabilitazione e della pulizia delle risorse.

Se desideri continuare a utilizzare EKS Runtime Monitoring senza abilitare il Runtime Monitoring, consultaConfigurazione del monitoraggio del EKS runtime (solo) API.

Verifica dello stato della configurazione EKS di Runtime Monit

Utilizza i seguenti AWS CLI comandi APIs per verificare lo stato di configurazione esistente di EKS Runtime Monitoring.

Per verificare lo stato della configurazione EKS di Runtime Monitoring esistente nel tuo account

- Esegui GetDetectorper controllare lo stato di configurazione del tuo account.
- In alternativa, puoi eseguire il seguente comando utilizzando AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

  Assicurati di sostituire l'ID del rilevatore della tua regione Account AWS e di quella attuale. Per trovare il nome del `detectorId` tuo account e della regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

Per verificare lo stato della configurazione EKS di Runtime Monitoring esistente per la tua organizzazione (solo come account GuardDuty amministratore delegato)

- Esegui DescribeOrganizationConfigurationper verificare lo stato di configurazione della tua organizzazione.

  In alternativa, puoi eseguire il seguente comando usando AWS CLI:

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Assicurati di sostituire l'ID del rilevatore con l'ID del tuo account GuardDuty amministratore delegato e la regione con la regione corrente. Per trovare il nome del `detectorId` tuo account e della regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

Disattivazione EKS di Runtime Monitoring dopo la migrazione a Runtime Monitoring

Dopo esserti assicurato che le impostazioni esistenti per il tuo account o la tua organizzazione siano state replicate in Runtime Monitoring, puoi disabilitare il EKS Runtime Monitoring.

Per EKS disabilitare il monitoraggio del runtime

- Per disabilitare il EKS Runtime Monitoring nel proprio account

  Eseguilo UpdateDetectorAPIcon il tuo regionale *detector-id*.

  In alternativa, puoi usare il seguente AWS CLI comando. Replace (Sostituisci) *12abc34d567e8fa901bc2d34e56789f0* con il tuo regionale *detector-id*.

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

- Per disabilitare il monitoraggio del EKS runtime per gli account dei membri dell'organizzazione

  Esegui il programma UpdateMemberDetectorsAPIcon il programma regionale *detector-id* dell'account GuardDuty amministratore delegato dell'organizzazione.

  In alternativa, è possibile utilizzare il seguente AWS CLI comando. Replace (Sostituisci) *12abc34d567e8fa901bc2d34e56789f0* con il regionale *detector-id* dell'account GuardDuty amministratore delegato dell'organizzazione e *111122223333* con l' Account AWS ID dell'account membro per il quale desideri disabilitare questa funzione.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "DISABLED"}]'
```

- Per aggiornare le impostazioni EKS di Runtime Monitoring, abilita automaticamente le impostazioni per la tua organizzazione

  Esegui il passaggio seguente solo se hai configurato le impostazioni di attivazione automatica EKS di Runtime Monitoring per gli account nuovi (NEW) o per tutti (ALL) i membri dell'organizzazione. Se l'hai già configurato comeNONE, puoi saltare questo passaggio.

  > **Note**
  >
  > L'impostazione della configurazione EKS di attivazione automatica di EKS Runtime Monitoring NONE significa che il Runtime Monitoring non verrà abilitato automaticamente per nessun account membro esistente o quando un nuovo account membro si unisce all'organizzazione.

  Esegui UpdateOrganizationConfigurationAPIcon la versione regionale *detector-id* dell'account GuardDuty amministratore delegato dell'organizzazione.

  In alternativa, è possibile utilizzare il seguente AWS CLI comando. Replace (Sostituisci) *12abc34d567e8fa901bc2d34e56789f0* con il regionale *detector-id* dell'account GuardDuty amministratore delegato dell'organizzazione. Sostituire il *EXISTING_VALUE* con la configurazione corrente per l'attivazione automatica GuardDuty.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
   --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
  ```

Valutazione della copertura in termini di runtime delle risorse

Dopo aver abilitato il Runtime Monitoring e aver installato il GuardDuty security agent sulla risorsa, GuardDuty fornisce le statistiche di copertura per il tipo di risorsa corrispondente e lo stato di copertura individuale per le risorse che appartengono al tuo account. Lo stato della copertura viene determinato assicurandoti di aver abilitato il Runtime Monitoring, che il tuo VPC endpoint Amazon

sia stato creato e che il GuardDuty security agent per la risorsa corrispondente sia stato distribuito. Uno stato di copertura integro indica che, quando si verifica un evento di runtime relativo alla risorsa, GuardDuty è in grado di ricevere tale evento di runtime tramite l'VPCendpoint Amazon e monitorarne il comportamento. Se si è verificato un problema al momento della configurazione del Runtime Monitoring, della creazione di un VPC endpoint Amazon o della distribuzione del GuardDuty security agent, lo stato di copertura appare come Non integro. Quando lo stato di copertura non è integro, non GuardDuty sarà in grado di ricevere o monitorare il comportamento di runtime della risorsa corrispondente o generare alcun risultato di Runtime Monitoring.

I seguenti argomenti ti aiuteranno a rivedere le statistiche sulla copertura, configurare EventBridge le notifiche e risolvere i problemi di copertura per un tipo di risorsa specifico.

Indice

Copertura per EC2 istanze Amazon

Per una EC2 risorsa Amazon, la copertura del runtime viene valutata a livello di istanza. Le tue EC2 istanze Amazon possono eseguire diversi tipi di applicazioni e carichi di lavoro, tra gli altri, nel tuo AWS ambiente. Questa funzionalità supporta anche EC2 le istanze Amazon ECS gestite da Amazon e, se hai ECS cluster Amazon in esecuzione su EC2 un'istanza Amazon, i problemi di copertura a livello di istanza verranno visualizzati nella sezione Amazon EC2 runtime coverage.

Argomenti

Revisione delle statistiche di copertura

Le statistiche di copertura per le EC2 istanze Amazon associate ai tuoi account o ai tuoi account membro sono la percentuale delle EC2 istanze integre rispetto a tutte le EC2 istanze selezionate. Regione AWS L'equazione seguente rappresenta questa percentuale come:

(Istanze integre/Tutte le istanze) *100

Se hai anche distribuito il GuardDuty security agent per i tuoi ECS cluster Amazon, qualsiasi problema di copertura a livello di istanza associato ai ECS cluster Amazon in esecuzione su un'EC2istanza Amazon verrà visualizzato come un problema di copertura del runtime dell'EC2istanza Amazon.

Scegli uno dei metodi di accesso per esaminare le statistiche di copertura dei tuoi account.

Console

- Accedi a AWS Management Console e apri la console all' GuardDuty indirizzo. https://console.aws.amazon.com/guardduty/
- Nel pannello di navigazione, scegli Runtime Monitoring.
- Scegli la scheda Runtime coverage.
- Nella scheda Copertura del runtime dell'EC2istanza, puoi visualizzare le statistiche di copertura aggregate in base allo stato di copertura di ogni EC2 istanza Amazon disponibile nella tabella Elenco istanze.
  - Puoi filtrare la tabella dell'elenco delle istanze in base alle seguenti colonne:
    - ID account
    - Tipo di gestione dell'agente
    - Versione dell'agente
    - Stato copertura
    - ID dell'istanza
    - Cluster ARN
- Se in una delle tue EC2 istanze lo stato di Copertura è impostato su Non integro, la colonna Problema include informazioni aggiuntive sul motivo dello stato Non integro.

API/CLI

- Eseguila ListCoverageAPIcon l'ID del rilevatore, la regione corrente e l'endpoint del servizio validi. È possibile filtrare e ordinare l'elenco delle istanze utilizzando questo. API
  - Puoi modificare il `filter-criteria` di esempio con una delle opzioni seguenti per `CriterionKey`:
    - `ACCOUNT_ID`

    - RESOURCE_TYPE
    - COVERAGE_STATUS
    - AGENT_VERSION
    - MANAGEMENT_TYPE
    - INSTANCE_ID
    - CLUSTER_ARN
  - Quando `filter-criteria` include RESOURCE_TYPE as EC2, Runtime Monitoring non supporta l'uso di ISSUEas`AttributeName`. Se lo usi, la API risposta risulterà in`InvalidInputException`.

    Puoi modificare il `AttributeName` di esempio in `sort-criteria` con una delle opzioni seguenti:

    - ACCOUNT_ID
    - COVERAGE_STATUS
    - INSTANCE_ID
    - UPDATED_AT
  - È possibile modificare il *`max-results`* (fino a 50).
  - Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il 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
```

- Esegui GetCoverageStatisticsAPIper recuperare le statistiche aggregate sulla copertura basate su. `statisticsType`
  - Puoi modificare il `statisticsType` di esempio con una delle opzioni seguenti:
    - COUNT_BY_COVERAGE_STATUS— Rappresenta le statistiche di copertura per EKS i cluster aggregate per stato di copertura.
    - COUNT_BY_RESOURCE_TYPE— Statistiche di copertura aggregate in base al tipo di AWS risorsa nell'elenco.

- È possibile modificare il `filter-criteria` di esempio nel comando. Puoi utilizzare le seguenti opzioni per `CriterionKey`:
  - `ACCOUNT_ID`
  - `RESOURCE_TYPE`
  - `COVERAGE_STATUS`
  - `AGENT_VERSION`
  - `MANAGEMENT_TYPE`
  - `INSTANCE_ID`
  - `CLUSTER_ARN`
- Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

```
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"}}] }'
```

Se lo stato di copertura della tua EC2 istanza è Inadeguato, consultaRisoluzione dei problemi di copertura.

Configurazione delle notifiche delle modifiche dello stato di copertura

Lo stato di copertura della tua EC2 istanza Amazon potrebbe apparire come Non sano. Per sapere quando lo stato della copertura cambia, ti consigliamo di monitorare periodicamente lo stato della copertura e di risolvere i problemi se lo stato diventa Non integro. In alternativa, puoi creare una EventBridge regola Amazon per ricevere una notifica quando lo stato della copertura cambia da Insalutare a Healthy o altro. Per impostazione predefinita, GuardDuty lo pubblica nel EventBridge bus relativo al tuo account.

Schema di esempio delle notifiche

EventBridge Di norma, è possibile utilizzare gli eventi e i modelli di eventi di esempio predefiniti per ricevere notifiche sullo stato della copertura. Per ulteriori informazioni sulla creazione di una EventBridge regola, consulta Create rule nella Amazon EventBridge User Guide.

Inoltre, puoi creare un pattern di eventi personalizzato utilizzando lo schema di esempio delle notifiche seguente. Assicurati di sostituire i valori per il tuo account. Per ricevere una notifica quando lo stato di copertura della tua EC2 istanza Amazon cambia da `Healthy` a`Unhealthy`, `detail-type` dovresti *`GuardDuty Runtime Protection Unhealthy`*. Per ricevere una notifica quando lo stato della copertura cambia da `Unhealthy` a`Healthy`, sostituisci il valore di `detail-type` con *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Account AWS ID",
  "time": "event timestamp (string)",
  "region": "Regione AWS",
  "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"
  }
}
```

Risoluzione dei problemi di copertura

Se lo stato di copertura della tua EC2 istanza Amazon è Inadeguato, puoi visualizzarne il motivo nella colonna Problema.

Se la tua EC2 istanza è associata a un EKS cluster e il security agent per EKS è stato installato manualmente o tramite la configurazione automatica dell'agente, per risolvere il problema di copertura, consulta. Copertura per i EKS cluster Amazon

La tabella seguente elenca i tipi di problemi e i passaggi di risoluzione corrispondenti.

Tipo di problema	Invia messaggio	Fasi per la risoluzione dei problemi
Nessuna segnalazione da parte dell'agente	In attesa di SSM notifica	La ricezione della SSM notifica potrebbe richiedere alcuni minuti. Assicurati che l'EC2istanza Amazon sia SSM gestita. Per ulteriori informazioni, vedere la procedura riportata in Metodo 1 - Usare AWS Systems Manager inInstallazione manuale del security agent.
	(Vuoto apposta)	Se gestisci il GuardDuty security agent manualmente, assicurati di aver seguito i passaggi seguentiGestione manuale del security agent per EC2 un'istanza Amazon.
		Se hai abilitato la configurazione automatica dell'agente: • La tua EC2 istanza è SSM gestita. • Visualizza periodicamente lo stato del tuo agente di sicurezza. Per ulteriori informazioni, consulta Convalida dello stato di installazione del GuardDuty Security Agent.
		Verifica che l'VPCendpoint per la tua EC2 istanza Amazon sia configurato correttamente. Per ulteriori informazioni, consulta Come posso verificare che la configurazione dell'VPCendpoint sia corretta?.
		Se la tua organizzazione ha una politica di controllo del servizio (SCP), verifica che il limite delle autorizzazioni

Tipo di problema	Invia messaggio	Fasi per la risoluzione dei problemi
		non limiti l'autorizzazione. `guardduty:SendSecurityTelemetry` Per ulteriori informazioni, consulta Convalida della politica di controllo dei servizi dell'organizzazione.
	Agente disconnesso	• Visualizza lo stato del tuo agente di sicurezza. Per ulteriori informazioni, consulta Convalida dello stato di installazione del GuardDuty Security Agent. • Visualizza i log del Security Agent per identificare la potenziale causa principale. I log forniscono errori dettagliati che è possibile utilizzare per risolvere autonomamente il problema. I file di registro sono disponibili in. `/var/log/amzn-guardduty-agent/` Fare `sudo journalctl -u amazon-guardduty-agent` .
SSMCreazione dell'associazione non riuscita	GuardDuty SSMl'associazione esiste già nel tuo account	1. Elimina manualmente l'associazione esistente. Per ulteriori informazioni, vedere Eliminazione delle associazioni nella Guida per l'AWS Systems Manager utente. 2. Dopo aver eliminato l'associazione, disabilita e riattiva la configurazione GuardDuty automatica dell'agente per AmazonEC2.

Tipo di problema	Invia messaggio	Fasi per la risoluzione dei problemi
	Il tuo account ha troppe associazioni SSM	Scegli una delle due opzioni seguenti: • Eliminare tutte le SSM associazioni non utilizzate. Per ulteriori informazioni, vedere Eliminazione delle associazioni nella Guida per l'AWS Systems Manager utente. • Verifica se il tuo account è idoneo per un aumento della quota. Per ulteriori informazioni, vedere le quote del servizio Systems Manager nel Riferimenti generali di AWS.
SSMAggiornamento dell'associazione non riuscito	GuardDuty SSMl'associazione non esiste nel tuo account	GuardDuty SSMl'associazione non è presente nel tuo account. Disabilita e quindi riattiva il monitoraggio del runtime.
SSMEliminazione dell'associazione non riuscita	GuardDuty SSMl'associazione non esiste nel tuo account	L'SSMassociazione non è presente nel tuo account. Se l'SSMassociazione è stata eliminata intenzionalmente, non è necessaria alcuna azione.

Tipo di problema	Invia messaggio	Fasi per la risoluzione dei problemi
SSMEsecuzione dell'associazione di istanze non	I requisiti architettonici o altri prerequisiti non sono soddisfatti.	Per informazioni sulle distribuzioni verificate del sistema operativo, vedere. Prerequisiti per il supporto delle EC2 istanze Amazon Se il problema persiste, i seguenti passaggi ti aiuteranno a identificare e potenzialmente risolvere il problema: 1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/. 2. Nel riquadro di navigazione, in Gestione dei nodi, seleziona State Manager. 3. Filtra per proprietà Document Name e inserisci AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Selezionate l'ID dell'associazione corrispondente e visualizzatene la cronologia di esecuzione. 5. Utilizzando la cronologia di esecuzione, visualizza gli errori, identifica la potenziale causa principale e prova a risolverla.
VPCCreazione dell'endpoint non riuscita	VPCla creazione di endpoint non è supportata per la condivisione VPC *vpcId*	Runtime Monitoring supporta l'uso di un file condiviso VPC all'interno di un'organizzazione. Per ulteriori informazioni, consulta Utilizzo: condiviso VPC con agenti di sicurezza automatizzati.

Tipo di problema	Invia messaggio	Fasi per la risoluzione dei problemi
	Solo quando si utilizza la configurazione condivisa VPC con agente automatizzato ID dell'account del proprietario *111122223333* per condiviso VPC *vpcId* non è abilitato né il Runtime Monitoring, né la configurazione automatizzata degli agenti né entrambi	L'account VPC proprietario condiviso deve abilitare il monitoraggio del runtime e la configurazione automatica degli agenti per almeno un tipo di risorsa (Amazon EKS o Amazon ECS (AWS Fargate)). Per ulteriori informazioni, consulta Prerequisiti specifici per il monitoraggio del GuardDuty runtime.

Tipo di problema	Invia messaggio	Fasi per la risoluzione dei problemi
	L'abilitazione privata DNS richiede entrambi `enableDnsSupport` e `enableDnsHostnames` VPC gli attributi sono impostati su `true` for *`vpcId`* (Servizio: Ec2, Codice di stato:400, ID richiesta: *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Assicuratevi che i seguenti VPC attributi siano impostati su — e. `true` `enableDnsSupport` `enableDnsHostnames` Per ulteriori informazioni, consulta DNSgli attributi nel tuo VPC. Se utilizzi Amazon VPC Console https://console.aws.amazon.com/vpc/per creare AmazonVPC, assicurati di selezionare sia Abilita DNS nomi host che Abilita DNS risoluzione. Per ulteriori informazioni, consulta le opzioni VPC di configurazione.
Eliminazione VPC dell'endpoint condiviso non riuscita	L'eliminazione condivisa VPC dell'endpoint non è consentita per l'ID dell'account *`111122223333`* , condiviso VPC *`vpcId`*, ID dell'account del proprietario *`555555555555`* .	Potenziali passaggi: • La disabilitazione dello stato di monitoraggio del runtime dell'account VPC partecipante condiviso non influisce sulla politica condivisa degli VPC endpoint e sul gruppo di sicurezza esistente nell'account del proprietario. Per eliminare l'VPCendpoint e il gruppo di sicurezza condivisi, è necessario disabilitare il Runtime Monitoring o lo stato di configurazione automatica dell'agente nell'account proprietario condiviso. VPC • L'account VPC partecipante condiviso non può eliminare l'VPCendpoint condiviso e il gruppo di sicurezza ospitati nell'account del proprietario condiviso VPC.

Tipo di problema	Invia messaggio	Fasi per la risoluzione dei problemi
L'agente non effettua la segnalazione	(Vuoto apposta)	Il tipo di problema ha raggiunto la fine del supporto. Se continui a riscontrare questo problema e non lo hai ancora fatto, abilita l'agente GuardDuty automatico per AmazonEC2. Se il problema persiste, prendi in considerazione la possibilità di disattivare il Runtime Monitoring per alcuni minuti, quindi riattivalo.

Copertura per i ECS cluster Amazon

La copertura del runtime per ECS i cluster Amazon include le attività in esecuzione AWS Fargate (Fargate) e le istanze [1] di ECS container Amazon.

Per un ECS cluster Amazon eseguito su Fargate, la copertura del runtime viene valutata a livello di attività. La copertura del runtime ECS dei cluster include le attività Fargate che sono iniziate a essere eseguite dopo aver abilitato il monitoraggio del runtime e la configurazione automatica degli agenti per ECS Fargate (solo). Per impostazione predefinita, un'attività Fargate è immutabile. GuardDuty non sarà in grado di installare il security agent per monitorare i contenitori sulle attività già in esecuzione. Per includere un'attività Fargate di questo tipo, è necessario interromperla e riavviarla. Assicurati di controllare se il servizio associato è supportato.

Per informazioni su Amazon ECS Container, consulta Creazione di capacità.

Indice

Revisione delle statistiche di copertura

Le statistiche di copertura per le ECS risorse Amazon associate al tuo account o ai tuoi account membro sono la percentuale di ECS cluster Amazon integri rispetto a tutti ECS i cluster Amazon selezionati. Regione AWS Ciò include la copertura per ECS i cluster Amazon associati alle istanze Fargate e AmazonEC2. L'equazione seguente rappresenta questa percentuale come:

(Cluster integri/Tutti i cluster)*100

Considerazioni

- Le statistiche di copertura per il ECS cluster includono lo stato di copertura delle attività di Fargate o delle istanze di ECS container associate a quel cluster. ECS Lo stato di copertura delle attività di Fargate include le attività che sono in esecuzione o che sono state completate di recente.
- Nella scheda ECSClusters runtime coverage, il campo Istanze di container coperte indica lo stato di copertura delle istanze di container associate al tuo cluster Amazon. ECS

  Se il tuo ECS cluster Amazon contiene solo attività Fargate, il conteggio appare come 0/0.
- Se il tuo ECS cluster Amazon è associato a un'EC2istanza Amazon che non dispone di un agente di sicurezza, il ECS cluster Amazon avrà anche lo stato di copertura Unhealthy.

  Per identificare e risolvere il problema di copertura per l'EC2istanza Amazon associata, consulta per le istanze Risoluzione dei problemi di copertura AmazonEC2.

Scegli uno dei metodi di accesso per esaminare le statistiche di copertura dei tuoi account.

Console

- Accedi AWS Management Console e apri la console all'indirizzo. GuardDuty https://console.aws.amazon.com/guardduty/
- Nel pannello di navigazione, scegli Runtime Monitoring.
- Scegli la scheda Runtime coverage.
- Nella scheda ECSClusters Runtime Coverage, puoi visualizzare le statistiche di copertura aggregate in base allo stato di copertura di ogni ECS cluster Amazon disponibile nella tabella con l'elenco dei cluster.
  - Puoi filtrare la tabella dell'elenco dei cluster in base alle seguenti colonne:
    - ID account
    - Nome del cluster
    - Tipo di gestione dell'agente
    - Stato copertura
- Se uno dei tuoi ECS cluster Amazon ha lo stato di Copertura come Non integro, la colonna Problema include informazioni aggiuntive sul motivo dello stato Non integro.

Se i tuoi ECS cluster Amazon sono associati a un'EC2istanza Amazon, vai alla scheda Copertura del runtime dell'EC2istanza e filtra in base al campo Nome cluster per visualizzare il problema associato.

API/CLI

- Eseguilo ListCoverageAPIcon il tuo ID rilevatore, la tua regione corrente e l'endpoint di servizio validi. È possibile filtrare e ordinare l'elenco delle istanze utilizzando questo. API
  - Puoi modificare il `filter-criteria` di esempio con una delle opzioni seguenti per `CriterionKey`:
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`
  - Puoi modificare il `AttributeName` di esempio in `sort-criteria` con una delle opzioni seguenti:
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`
    - `ISSUE`
    - `ECS_CLUSTER_NAME`
    - `UPDATED_AT`

      Il campo viene aggiornato solo quando viene creata una nuova attività nel ECS cluster Amazon associato o viene modificato lo stato di copertura corrispondente.
  - È possibile modificare il *`max-results`* (fino a 50).
  - Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il 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
```

- Esegui GetCoverageStatisticsAPIper recuperare le statistiche aggregate sulla copertura basate su. `statisticsType`
  - Puoi modificare il `statisticsType` di esempio con una delle opzioni seguenti:
    - `COUNT_BY_COVERAGE_STATUS`— Rappresenta le statistiche di copertura per ECS i cluster aggregate per stato di copertura.
    - `COUNT_BY_RESOURCE_TYPE`— Statistiche di copertura aggregate in base al tipo di AWS risorsa nell'elenco.
    - È possibile modificare il `filter-criteria` di esempio nel comando. Puoi utilizzare le seguenti opzioni per `CriterionKey`:
      - `ACCOUNT_ID`
      - `ECS_CLUSTER_NAME`
      - `COVERAGE_STATUS`
      - `MANAGEMENT_TYPE`
      - `INSTANCE_ID`
  - Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

```
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"}}] }'
```

Per ulteriori informazioni sui problemi di copertura, consultaRisoluzione dei problemi di copertura.

Configurazione delle notifiche delle modifiche dello stato di copertura

Lo stato di copertura del tuo ECS cluster Amazon potrebbe apparire come Non integro. Per sapere quando lo stato della copertura cambia, ti consigliamo di monitorare periodicamente lo stato della copertura e di risolvere i problemi se lo stato diventa Non integro. In alternativa, puoi creare una EventBridge regola Amazon per ricevere una notifica quando lo stato della copertura cambia da Insalutare a Healthy o altro. Per impostazione predefinita, GuardDuty lo pubblica nel EventBridge bus relativo al tuo account.

Schema di esempio delle notifiche

EventBridge Di norma, è possibile utilizzare gli eventi e i modelli di eventi di esempio predefiniti per ricevere notifiche sullo stato della copertura. Per ulteriori informazioni sulla creazione di una EventBridge regola, consulta Create rule nella Amazon EventBridge User Guide.

Inoltre, puoi creare un pattern di eventi personalizzato utilizzando lo schema di esempio delle notifiche seguente. Assicurati di sostituire i valori per il tuo account. Per ricevere una notifica quando lo stato di copertura del tuo ECS cluster Amazon cambia da `Healthy` a`Unhealthy`, `detail-type` dovrebbe *`GuardDuty Runtime Protection Unhealthy`*. Per ricevere una notifica quando lo stato della copertura cambia da `Unhealthy` a`Healthy`, sostituisci il valore di `detail-type` con *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Account AWS ID",
  "time": "event timestamp (string)",
  "region": "Regione AWS",
  "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"
  }
}
```

Risoluzione dei problemi di copertura

Se lo stato di copertura del tuo ECS cluster Amazon non è integro, puoi visualizzare il motivo nella colonna Problema.

La tabella seguente fornisce i passaggi consigliati per la risoluzione dei problemi di Fargate (ECSsolo Amazon). Per informazioni sui problemi di copertura delle EC2 istanze Amazon, consulta Risoluzione dei problemi di copertura per EC2 le istanze Amazon.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
L'agente non effettua la segnalazione	Agente che non effettua la segnalazione delle attività in `TaskDefinition - ' TASK_DEFINITION '`	Verifica che l'VPCendpoint per l'attività del tuo ECS cluster Amazon sia configurato correttamente. Per ulteriori informazioni, consulta Come posso verificare che la configurazione dell'VPCendpoint sia corretta?. Se la tua organizzazione ha una politica di controllo del servizio (SCP), verifica che il limite delle autorizzazioni non limiti l'autorizzazione. `guardduty:SendSecurityTelemetry` Per ulteriori informazioni, consulta Convalida della politica di controllo dei servizi dell'organizzazione.
	`VPC_ISSUE ; for task in TaskDefinition - ' TASK_DEFINITION '`	Visualizza i dettagli del VPC problema nelle informazioni aggiuntive.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
L'agente è uscito	ExitCode: `EXIT_CODE` per le attività in `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Visualizza i dettagli del problema nelle informazioni aggiuntive.
	Motivo: *`REASON`* per attività in `TaskDefinition - '`*`TASK_DEFINITION`*` '`	
	ExitCode: `EXIT_CODE` con motivo: '*`EXIT_CODE`*' per le attività in `TaskDefinition - '`*`TASK_DEFINITION`*` '`	

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi

	Agente chiuso: MotivoCannotPullContainerError : pull image manifest è stato riprovato...	Il ruolo di esecuzione dell'attività deve disporre delle seguenti autorizzazioni Amazon Elastic Container Registry (AmazonECR):
		`...`
		`"ecr:GetAuthorizationToken",`
		`"ecr:BatchCheckLayerAvailability",`
		`"ecr:GetDownloadUrlForLayer",`
		`"ecr:BatchGetImage",`
		`...`
		Per ulteriori informazioni, consulta Fornisci ECR autorizzazioni e dettagli sulla sottorete.
		Dopo aver aggiunto le ECR autorizzazioni Amazon, devi riavviare l'attività.
		Se il problema persiste, consulta. Il mio AWS Step Functions flusso di lavoro non funziona in modo imprevisto

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
VPCCreazione dell'endpoint non riuscita	L'attivazione della modalità privata DNS richiede entrambi `enableDnsSupport` e `enableDnsHostnames` VPC gli attributi sono impostati su for `true` *`vpcId`* (Servizio:ECS, Codice di stato:400, ID richiesta: *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Assicuratevi che i seguenti VPC attributi siano impostati su `true` — `enableDnsSupport` e. `enableDnsHostnames` Per ulteriori informazioni, consulta DNSgli attributi nel tuo VPC. Se utilizzi Amazon VPC Console https://console.aws.amazon.com/vpc/per creare AmazonVPC, assicurati di selezionare sia Abilita DNS nomi host che Abilita DNS risoluzione. Per ulteriori informazioni, consulta le opzioni VPC di configurazione.
Agente non fornito	Richiamata non supportata da *`SERVICE`* for task (s) in `TaskDefinition -` *`'TASK_DEFINITION '`*	Questa attività è stata richiamata da un comando *`SERVICE`* non supportato.
	Architettura non supportata CPU *`'TYPE'`*per le attività in `TaskDefinition - '` *`TASK_DEFINITION '`*	Questa attività è in esecuzione su un'CPUarchitettura non supportata. Per informazioni sulle CPU architetture supportate, vedere. Convalida dei requisiti relativi all'architettura
	`TaskExecutionRole` mancante da `TaskDefinition -` *`'TASK_DEFINITION '`*	Manca il ruolo di esecuzione dell'ECSattività. Per informazioni sull'assegnazione del ruolo di esecuzione dell'attività e delle autorizzazioni richieste, vedereFornisci ECR autorizzazioni e dettagli sulla sottorete.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
	Configurazione di rete '*CONFIGURATION_DETAILS* ' mancante per le attività in `TaskDefinition` - '*TASK_DEFINITION* '	I problemi di configurazione della rete possono verificarsi a causa della VPC configurazione mancante o di sottoreti mancanti o vuote. Verifica che la configurazione di rete sia corretta. Per ulteriori informazioni, consulta Fornisci ECR autorizzazioni e dettagli sulla sottorete. Per ulteriori informazioni, consulta i parametri di definizione delle ECS attività di Amazon nella Amazon Elastic Container Service Developer Guide.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Altri	Problema non identificato, per le attività in `TaskDefinition - '`*`TASK_DEFINITION`*` '`	Utilizza le seguenti domande per identificare la causa principale del problema: • L'attività è iniziata prima di abilitare il Runtime Monitoring? In AmazonECS, le attività sono immutabili. Per valutare il comportamento di runtime di un'attività Fargate in esecuzione, assicuratevi che Runtime Monitoring sia già abilitato, quindi riavviate l'attività per GuardDuty aggiungere il sidecar del contenitore. • Questa attività fa parte di una distribuzione di servizi iniziata prima di abilitare il Runtime Monitoring? In caso affermativo, è possibile riavviare il servizio o aggiornar lo `forceNewDeployment` utilizzando la procedura descritta in Aggiornamento di un servizio. Puoi anche usare UpdateServiceo AWS CLI. • L'attività è stata avviata dopo aver escluso il ECS cluster dal Runtime Monitoring? Quando si modifica il GuardDuty tag predefinito da `GuardDutyManaged - true` a `GuardDutyManaged -false`, non GuardDuty riceverà gli eventi di runtime per il ECS cluster.

Tipo di problema	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
		• Il tuo servizio contiene un'attività che ha un vecchio formato di `taskArn`? GuardDuty Runtime Monitoring non supporta la copertura per le attività che hanno il vecchio formato di `taskArn`. Per informazioni su Amazon Resource Names (ARNs) per ECS le risorse Amazon, consulta Amazon Resource Names (ARNs) e IDs.

Copertura per i EKS cluster Amazon

Dopo aver abilitato il Runtime Monitoring e installato il GuardDuty security agent (componente aggiuntivo) per la configurazione manuale EKS o automatizzata dell'agente, puoi iniziare a valutare la copertura per i tuoi cluster. EKS

Indice

Revisione delle statistiche di copertura

Le statistiche di copertura per EKS i cluster associati ai tuoi account o ai tuoi account membro sono la percentuale dei EKS cluster integri rispetto a tutti EKS i cluster selezionati. Regione AWS L'equazione seguente rappresenta questa percentuale come:

(Cluster integri/Tutti i cluster)*100

Scegli uno dei metodi di accesso per esaminare le statistiche di copertura dei tuoi account.

Console

- Accedi a AWS Management Console e apri la console all' GuardDuty indirizzo. https://console.aws.amazon.com/guardduty/
- Nel pannello di navigazione, scegli Runtime Monitoring.
- Scegli la scheda EKSClusters Runtime Coverage.
- Nella scheda Copertura in fase di esecuzione EKS dei cluster, puoi visualizzare le statistiche di copertura aggregate in base allo stato di copertura, disponibili nella tabella con l'elenco dei cluster.
  - Puoi filtrare la tabella Elenco cluster in base alle seguenti colonne:
    - Nome cluster
    - ID account
    - Tipo di gestione dell'agente
    - Stato copertura
    - Versione del componente aggiuntivo
- Se uno dei tuoi EKS cluster ha lo stato di Copertura come Non integro, la colonna Problema può includere informazioni aggiuntive sul motivo dello stato Non integro.

API/CLI

- Eseguilo ListCoverageAPIcon il tuo ID rilevatore, la tua regione e l'endpoint di servizio validi. È possibile filtrare e ordinare l'elenco dei cluster utilizzando questo. API
  - Puoi modificare il `filter-criteria` di esempio con una delle opzioni seguenti per `CriterionKey`:
    - `ACCOUNT_ID`
    - `CLUSTER_NAME`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `ADDON_VERSION`
    - `MANAGEMENT_TYPE`
  - Puoi modificare il `AttributeName` di esempio in `sort-criteria` con una delle opzioni seguenti:
    - `ACCOUNT_ID`

    - CLUSTER_NAME
    - COVERAGE_STATUS
    - ISSUE
    - ADDON_VERSION
    - UPDATED_AT
  - È possibile modificare il *max-results* (fino a 50).
  - Per trovare le detectorId impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il 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
```

- Esegui GetCoverageStatisticsAPIper recuperare le statistiche aggregate sulla copertura basate su. statisticsType
  - Puoi modificare il statisticsType di esempio con una delle opzioni seguenti:
    - COUNT_BY_COVERAGE_STATUS— Rappresenta le statistiche di copertura per EKS i cluster aggregate per stato di copertura.
    - COUNT_BY_RESOURCE_TYPE— Statistiche di copertura aggregate in base al tipo di AWS risorsa nell'elenco.
    - È possibile modificare il filter-criteria di esempio nel comando. Puoi utilizzare le seguenti opzioni per CriterionKey:
      - ACCOUNT_ID
      - CLUSTER_NAME
      - RESOURCE_TYPE
      - COVERAGE_STATUS
      - ADDON_VERSION
      - MANAGEMENT_TYPE
  - Per trovare le detectorId informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

```
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"}}] }'
```

Se lo stato di copertura del EKS cluster non è integro, consultaRisoluzione dei problemi di EKS copertura.

Configurazione delle notifiche delle modifiche dello stato di copertura

Lo stato di copertura di un EKS cluster nel tuo account potrebbe essere visualizzato come Non salutare. Per rilevare quando lo stato di copertura diventa Non integro, ti consigliamo di monitorarlo periodicamente e di risolvere i problemi se è Non integro. In alternativa, puoi creare una EventBridge regola Amazon per avvisarti quando lo stato della copertura cambia `Unhealthy` da `Healthy` o in altro modo. Per impostazione predefinita, GuardDuty lo pubblica nel EventBridgebus per il tuo account.

Schema di esempio delle notifiche

EventBridge Di norma, è possibile utilizzare gli eventi e i modelli di eventi di esempio predefiniti per ricevere notifiche sullo stato della copertura. Per ulteriori informazioni sulla creazione di una EventBridge regola, consulta Create rule nella Amazon EventBridge User Guide.

Inoltre, puoi creare un pattern di eventi personalizzato utilizzando lo schema di esempio delle notifiche seguente. Assicurati di sostituire i valori per il tuo account. Per ricevere una notifica quando lo stato di copertura del tuo EKS cluster Amazon cambia da `Healthy` a`Unhealthy`, `detail-type` dovrebbe *`GuardDuty Runtime Protection Unhealthy`*. Per ricevere una notifica quando lo stato della copertura cambia da `Unhealthy` a`Healthy`, sostituisci il valore di `detail-type` con *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Account AWS ID",
  "time": "event timestamp (string)",
  "region": "Regione AWS",
```

```
  "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"
  }
}
```

Risoluzione dei problemi di EKS copertura

Se lo stato di copertura per il EKS cluster è ugualeUnhealthy, puoi visualizzare l'errore corrispondente nella colonna Problema della GuardDuty console o utilizzando il tipo di CoverageResourcedati.

Quando utilizzi tag di inclusione o esclusione per monitorare selettivamente EKS i cluster, la sincronizzazione dei tag potrebbe richiedere del tempo. Ciò potrebbe influire sullo stato di copertura del cluster associato. EKS Puoi provare a rimuovere e aggiungere nuovamente il tag corrispondente (di inclusione o di esclusione). Per ulteriori informazioni, consulta Taggare le EKS risorse Amazon nella Amazon EKS User Guide.

La struttura di un problema di copertura è `Issue type:Extra information`. In genere, in caso di problemi vengono fornite Informazioni supplementari facoltative che possono includere specifiche eccezioni o descrizioni del problema sul lato client. In base a informazioni aggiuntive, le seguenti tabelle forniscono i passaggi consigliati per risolvere i problemi di copertura dei cluster. EKS

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Creazione del componente aggiuntivo non riuscita	L'addon non `aws-guardduty-agent` è compatibile con la versione corrente del cluster *`ClusterName`* . L'addon specificato non è supportato.	Assicurati di utilizzare una di quelle versioni di Kubernetes che supportano la distribuzione del componente aggiuntivo. `aws-guardduty-agent` EKS Per ulteriori informazioni, consulta Versioni di Kubernetes supportate dal security agent GuardDuty . Per informazioni sull'aggiornamento della versione di Kubernetes, consulta Aggiornamento di una versione di Kubernetes EKS del cluster Amazon.
Creazione del componente aggiuntivo non riuscita Aggiornamento del componente aggiuntivo non riuscito Stato del componente aggiuntivo non integro	EKSProblema relativo al componente aggiuntivo: `AddonIssueCode` `AddonIssueMessage`	Per informazioni sui passaggi consigliati per un codice di problema specifico del componente aggiuntivo, consulta. Troubleshooting steps for Addon creation/updatation error with Addon issue code Per un elenco dei codici di problema relativi ai componenti aggiuntivi che potresti riscontra

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
		re in questo problema, consulta. AddonIssue
VPCCreazione dell'endpoint non riuscita	VPCla creazione di endpoint non è supportata per la condivisione VPC *vpcId*	Il Runtime Monitoring ora supporta l'uso di un file condiviso VPC all'interno di un'organizzazione. Assicurati che i tuoi account soddisfino tutti i prerequisiti. Per ulteriori informazioni, consulta Prerequisiti per l'utilizzo della modalità condivisa VPC.
	Solo quando si utilizza la configurazione condivisa VPC con agente automatizzato ID dell'account del proprietario *111122223333* per condiviso VPC *vpcId* non ha né il Runtime Monitoring né la configurazione automatica degli agenti abilitati o entrambi.	L'account VPC proprietario condiviso deve abilitare il monitoraggio del runtime e la configurazione automatica degli agenti per almeno un tipo di risorsa (Amazon EKS o Amazon ECS (AWS Fargate)). Per ulteriori informazioni, consulta Prerequisiti specifici per il monitoraggio del GuardDuty runtime.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
	L'abilitazione privata DNS richiede entrambi `enableDnsSupport` e `enableDnsHostnames` VPC gli attributi sono impostati su `true` for *`vpcId`* (Servizio: Ec2, Codice di stato:400, ID richiesta: *`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`*).	Assicuratevi che i seguenti VPC attributi siano impostati su — e. `true` `enableDnsSupport` `enableDnsHostnames` Per ulteriori informazioni, consulta DNSgli attributi nel tuo VPC. Se utilizzi Amazon VPC Console https://console.aws.amazon.com/vpc/per creare AmazonVPC, assicurati di selezionare sia Abilita DNS nomi host che Abilita DNS risoluzione. Per ulteriori informazioni, consulta le opzioni VPC di configurazione.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Eliminazione VPC dell'endpoint condiviso non riuscita	L'eliminazione condivisa VPC dell'endpoint non è consentita per l'ID dell'account *111122223333* , condiviso VPC *vpcId*, ID dell'account del proprietario *555555555555* .	Potenziali passaggi: • La disabilitazione dello stato di monitoraggio del runtime dell'account VPC partecipante condiviso non influisce sulla politica condivisa degli VPC endpoint e sul gruppo di sicurezza esistente nell'account del proprietario. Per eliminare l'VPCendpoint e il gruppo di sicurezza condivisi, è necessario disabilitare il Runtime Monitoring o lo stato di configurazione automatica dell'agente nell'account proprietario condiviso. VPC • L'account VPC partecipante condiviso non può eliminare l'VPCendpoint condiviso e il gruppo di sicurezza ospitati nell'account del proprietario condiviso VPC.

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
Cluster locali EKS	EKSi componenti aggiuntivi non sono supportati sui cluster Outpost locali.	Non utilizzabile. Per ulteriori informazioni, consulta Amazon EKS on AWS Outposts.
EKSAutorizzazione di attivazione del Runtime Monitoring non concessa	(può mostrare o meno informazioni aggiuntive)	1. Se sono disponibili informazioni supplementari per questo problema, correggine la causa principale e segui la fase successiva. 2. Attiva EKS Runtime Monitoring per disattivarlo e riaccenderlo. Assicurati che anche l' GuardDuty agente venga distribuito, automaticamente o manualmente. GuardDuty

Tipo di problema (prefisso)	Informazioni supplementari	Fasi consigliate per la risoluzione dei problemi
EKSRuntime Monitoring (attivazione, approvvigionamento delle risorse) in corso	(può mostrare o meno informazioni aggiuntive)	Non utilizzabile. Dopo aver abilitato il EKS Runtime Monitoring, lo stato di copertura potrebbe rimanere `Unhealthy` invariato fino al completamento della fase di approvvigionamento delle risorse. Lo stato di copertura viene monitorato e aggiornato periodicamente.
Altri (qualsiasi altro problema)	Errore dovuto a un errore di autorizzazione	Attiva EKS Runtime Monitoring per disattivarlo e riaccenderlo. Assicurati che anche l' GuardDuty agente venga distribuito, automaticamente o manualmente. GuardDuty

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
EKSProblema relativo al componente aggiuntivo `InsufficientNumberOfReplicas` : il componente aggiuntivo non è integro perché non ha il numero di repliche desiderato.	• Utilizzando il messaggio relativo al problema, è possibile identificare e correggere la causa principale. Puoi iniziare descrivendo il tuo cluster. Ad esempio, `kubectl describe`

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
	pods da utilizzare per identificare la causa principale dell'errore del pod. Dopo aver corretto la causa principale, riprova il passaggio (creazione o aggiornamento del componente aggiuntivo). • Se il problema persiste, verifica che l'VPCendpoint per il tuo EKS cluster Amazon sia configurato correttamente. Per ulteriori informazioni, consulta Come posso verificare che la configurazione dell'VPCendpoint sia corretta?.
EKSProblema relativo all'addonAdmission RequestDenied : webhook di ammissione "validate.kyverno.svc-fail" ha negato la richiesta: policy DaemonSet/amazon-guardduty/aws-guardduty-agent per violazione delle risorse:::... restrict-image-registries autogen-validate-registries	1. Il EKS cluster Amazon o l'amministratore della sicurezza devono rivedere la politica di sicurezza che blocca l'aggiornamento dell'Addon. 2. Devi disabilitare il controller (webhook) o fare in modo che il controller accetti le richieste di AmazonEKS.
EKSProblema aggiuntivoConfigurationConflict : sono stati rilevati conflitti durante il tentativo di candidatura. Non continuerà a causa della modalità di risoluzione dei conflitti. Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image	Quando crei o aggiorni l'Addon, fornisci il flag di OVERWRITE risoluzione del conflitto. Ciò potrebbe sovrascrivere qualsiasi modifica apportata direttamente alle risorse correlate in Kubernetes utilizzando Kubernetes. API Puoi prima eliminare l'Addon e poi reinstallarlo.

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi

EKSProblema aggiuntivo - `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`	È necessario aggiungere `eks:addon-cluster-admin ClusterRoleBinding` manualmente l'autorizzazione mancante. Aggiungi quanto segue `yaml` a`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`
	`---`
	
	Ora puoi applicarlo `yaml` al tuo EKS cluster Amazon utilizzando il seguente comando:
	
	`kubectl apply -f eks-addon-cluster-admin.yaml`

Errore di creazione o aggiornamento del componente aggiuntivo	Fasi per la risoluzione dei problemi
EKSProblema aggiuntivo - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	Devi disabilitare il controller o fare in modo che il controller accetti le richieste dal EKS cluster Amazon. Prima di creare o aggiornare il componente aggiuntivo, puoi anche creare uno spazio dei GuardDuty nomi ed etichettarlo come. `owner`

Domande frequenti () FAQs

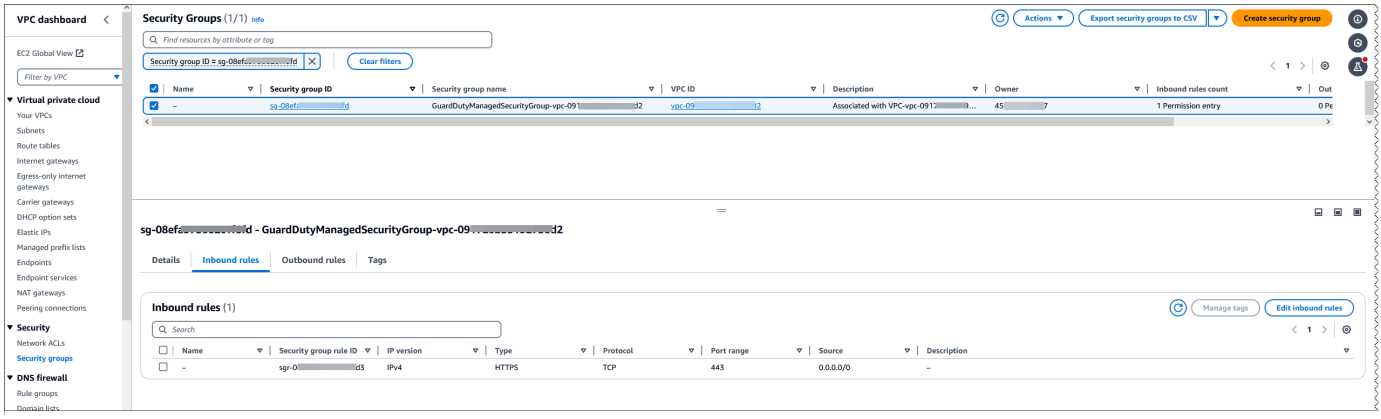
Indice

Come posso verificare che la configurazione dell'VPCendpoint sia corretta?

Utilizza i seguenti passaggi per verificare che la configurazione dell'VPCendpoint per il tuo tipo di risorsa sia impostata correttamente nell'account del proprietario: VPC

1. Accedi a AWS Management Console e apri la VPC console Amazon all'indirizzo https://console.aws.amazon.com/vpc/.
2. Dal riquadro di navigazione, in Cloud privato virtuale, scegli Endpoint.
3. Nella tabella Endpoints, seleziona la riga con il nome del servizio simile a com.amazonaws.***us-east-1***.guardduty-data. La regione (`us-east-1`) potrebbe essere diversa a seconda dell'endpoint.

4. Apparirà un pannello con i dettagli dell'endpoint. Nella scheda Gruppi di sicurezza, seleziona il link ID del gruppo associato per maggiori dettagli.
5. Nella tabella Gruppi di sicurezza, seleziona la riga con l'ID del gruppo di sicurezza associato per visualizzare i dettagli.
6. Nella scheda Regole in entrata, assicurati che esista una politica di ingresso con l'intervallo di porte pari a 443 e l'origine a 0.0.0.0/0. Le regole in entrata controllano il traffico in entrata a cui è consentito raggiungere l'istanza. L'immagine seguente mostra le regole in entrata per un gruppo di sicurezza associato a quello VPC utilizzato dal GuardDuty security agent.



Se non disponi già di un gruppo di sicurezza con una porta in ingresso 443 abilitata, crea un gruppo di sicurezza nella Amazon EC2 User Guide.

Se c'è un problema durante la limitazione delle autorizzazioni in ingresso alla tua VPC (o al cluster), fornisci il supporto alla porta 443 in ingresso da qualsiasi indirizzo IP (0.0.0.0/0).

Perché lo stato di copertura della mia risorsa? **`Unhealthy`**

Se hai appena distribuito il GuardDuty Security Agent (tramite la configurazione automatica dell'agente o manualmente) o hai seguito i passaggi consigliati per risolvere un problema di copertura, potrebbero essere necessari alcuni minuti prima che lo stato della copertura diventi integro. Puoi controllare periodicamente lo stato della copertura o configurare Amazon EventBridge (EventBridge) per ricevere una notifica quando lo stato della copertura cambia.

Inoltre, puoi anche verificare che la configurazione degli VPC endpoint per la tua risorsa sia corretta. Per ulteriori informazioni, consulta Come posso verificare che la configurazione dell'VPCendpoint sia corretta?.

Chi può visualizzare lo stato di copertura in fase di esecuzione di una risorsa che appartiene alla mia? Account AWS

Come account membro o account autonomo, puoi visualizzare le statistiche di copertura delle risorse associate ai tuoi account. In qualità di account GuardDuty amministratore delegato di un'organizzazione, puoi visualizzare le statistiche di copertura per le risorse associate al tuo account e gli account dei membri che appartengono alla tua organizzazione.

Come posso verificare se il GuardDuty security agent è in esecuzione su un'attività Fargate?

L'agente GuardDuty di sicurezza funge da contenitore secondario per le attività di Fargate.

Scegliete un metodo preferito per verificare se il contenitore del sidecar viene visualizzato mentre l'attività è in esecuzione.

Amazon ECS console

1. Apri la console nella versione 2. https://console.aws.amazon.com/ecs/
2. Nel pannello di navigazione scegliere Clusters (Cluster).
3. Nella pagina Cluster, seleziona il nome del cluster associato per maggiori dettagli.
4. Selezionare la scheda Tasks (Attività).
5. Seleziona il link all'attività associata per visualizzare i dettagli dell'attività.
6. Nella pagina dei dettagli dell'attività, la tabella Contenitori include i dettagli del sidecar. L'ID di runtime del contenitore avrà il prefisso del tuo Task ID.

CLI

Esegui `describe-tasks` e cerca il contenitore con un nome impostato su `aws-gd-agent` e lastStatusimpostato `RUNNING` su.

L'esempio seguente mostra l'output per il cluster predefinito per l'attività `aws:ecs:`*`us-east-1`*`:`*`123456789012`*`:task/`*`0b69d5c0-d655-4695-98cd-5d2d5EXAMPLE`

Output

Il contenitore denominato aws-gd-agentsi trova nello `RUNNING` stato.

```
"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"
      }
    ]
```

Per ulteriori informazioni, consulta describe-tasks.

Altre domande sulla risoluzione dei problemi

Per ulteriori domande sulla risoluzione dei problemi relativi alle attività di Fargate, consulta la sezione Risoluzione dei problemi di monitoraggio del runtime FAQs nella Amazon Elastic Container Service Developer Guide.

Configurazione CPU e monitoraggio della memoria

Dopo aver abilitato il monitoraggio del runtime e verificato che lo stato di copertura del cluster sia integro, puoi configurare e visualizzare le metriche di analisi.

I seguenti argomenti possono aiutarti a valutare le prestazioni dell'agente distribuito rispetto ai CPU limiti di memoria per l' GuardDuty agente.

Configurazione del monitoraggio sul ECS cluster Amazon

I seguenti passaggi della Amazon CloudWatch User Guide possono aiutarti a valutare le prestazioni dell'agente distribuito rispetto ai limiti di memoria per l' GuardDuty agente: CPU

1. Configurazione di Container Insights su Amazon ECS per i parametri a livello di cluster e servizio
2. Metriche di Amazon ECS Container Insights

Configurazione del monitoraggio sul EKS cluster Amazon

Dopo aver distribuito il GuardDuty security agent e verificato che lo stato di copertura del cluster sia integro, puoi configurare e visualizzare le metriche di Container Insight.

Valuta le prestazioni del security agent

1. Configurazione di Container Insights su Amazon EKS e Kubernetes nella Amazon User Guide CloudWatch
2. I parametri di Amazon EKS e Kubernetes Container Insights nella Amazon User Guide CloudWatch

Gestisci le prestazioni con Security Agent v1.5.0 e versioni successive

Con Security Agent v1.5.0 e versioni successive, quando le informazioni indicano che l' GuardDuty agente associato sta raggiungendo i limiti assegnati, puoi configurare parametri specifici. Per ulteriori informazioni, consulta Configura i EKS parametri aggiuntivi.

Tipi di eventi di runtime raccolti che utilizza GuardDuty

Il GuardDuty security agent raccoglie i seguenti tipi di eventi e li invia al GuardDuty backend per il rilevamento e l'analisi delle minacce. GuardDuty non rende questi eventi accessibili all'utente. Se GuardDuty rileva una potenziale minaccia e genera un risultato di Runtime Monitoring, puoi visualizzare i dettagli del risultato corrispondente. Per ulteriori informazioni su come GuardDuty utilizza i tipi di eventi raccolti, vedereRifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio.

Eventi di processo

Nome campo	Descrizione
Process name (Nome del processo)	Nome del processo osservato.
Percorso del processo	Percorso assoluto dell'eseguibile del processo.
ID processo	L'ID che il sistema operativo assegna al processo.
Namespace PID	L'ID del processo in uno spazio dei PID nomi secondario diverso dallo spazio dei nomi a

Nome campo	Descrizione
	livello di host. PID Per i processi all'interno di un container, corrisponde all'ID processo osservabile nel container.
ID utente del processo	L'ID univoco dell'utente che ha eseguito il processo.
Processo UUID	L'ID univoco assegnato al processo da GuardDuty.
Processo GID	L'ID processo del gruppo di processi.
Processo EGID	L'ID di gruppo effettivo del gruppo di processi.
Processo EUID	L'ID utente effettivo del processo.
Nome utente del processo	Il nome dell'utente che ha eseguito il processo.
Ora di inizio del processo	L'ora in cui è stato creato il processo. Questo campo è nel formato della stringa di UTC data (`2023-03-22T19:37:20.168Z`).
Eseguibile del processo SHA -256	L'hash `SHA256` dell'eseguibile del processo.
Percorso dello script di processo	Il percorso del file di script che è stato eseguito.
Variabile di ambiente del processo	La variabile di ambiente messa a disposizi one del processo. Vengono raccolti solo `LD_PRELOAD` e `LD_LIBRARY_PATH` .
Elabora la directory di lavoro attuale () PWD	La directory di lavoro presente del processo.
Processo padre	I dettagli del processo padre. Un processo padre è un processo che ha creato quello osservato.

Nome campo	Descrizione
Argomenti della riga di comando Attualmente, questo campo è limitato a versioni di agenti specifiche corrispondenti al tipo di risorsa: • Fargate (ECSsolo Amazon) con GuardDuty Security Agent v1.0.0 e versioni successive. • EC2Istanze Amazon con GuardDuty Security Agent v1.0.0 e versioni successive. • EKSCluster Amazon con Security Agent v1.4.0 e versioni successive. Per ulteriori informazioni, consulta GuardDuty cronologia dei rilasci dell'agente.	Argomenti della riga di comando forniti al momento dell'esecuzione del processo. Questo campo potrebbe contenere dati sensibili dei clienti.

Eventi del container

Nome campo	Descrizione
Nome container	Il nome del container. Se disponibile, questo campo mostra il valore dell'etichetta `io.kubenetes.container.name` .
Contenitore UID	L'ID univoco del container assegnato dal runtime del container.
Runtime del container	Il runtime del container (ad esempio `docker` o `containerd`) utilizzato per eseguire il container.
ID immagine del container	L'ID dell'immagine del container.
Nome immagine del container	Il nome dell'immagine del container.

AWS Fargate (ECSsolo Amazon) eventi relativi alle attività

Nome campo	Descrizione
Nome risorsa Amazon dell'attività (ARN)	La ARN parte dell'attività.
Nome del cluster	Il nome del ECS cluster Amazon.
Cognome	Cognome della definizione dell'attività. `family`Viene utilizzato come nome per la definizione dell'attività utilizzata per avviare l'attività.
Nome del servizio	Il nome del ECS servizio Amazon, se l'attività è stata avviata come parte di un servizio.
Tipo di lancio	L'infrastruttura su cui viene eseguita l'attività. Per il Runtime Monitoring con tipo di risorsa as`ECSCluster` , il tipo di avvio potrebbe essere uno `EC2` o`FARGATE`.
CPU	Il numero di CPU unità utilizzate dall'attività, espresso nella definizione dell'attività.

Eventi pod di Kubernetes

Nome campo	Descrizione
ID pod	L'ID del pod di Kubernetes.
Nome pod	Il nome del pod di Kubernetes.
Spazio dei nomi pod	Il nome dello spazio dei nomi di Kubernetes a cui appartiene il carico di lavoro di Kubernetes.
Nome del cluster Kubernetes	Il nome del cluster Kubernetes.

DNSeventi

Nome campo	Descrizione
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio `SOCK_RAW`.
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi `AF_INET` viene utilizzata per il protocollo IPv4.
ID direzione	L'ID della direzione della connessione.
Numero di protocollo	Il numero di protocollo di livello 4, ad esempio 17 per UDP e 6 perTCP.
DNSIP dell'endpoint remoto	L'IP remoto della connessione.
DNSPorta endpoint remota	Il numero di porta della connessione.
DNSIP dell'endpoint locale	L'IP locale della connessione.
DNSPorta endpoint locale	Il numero di porta della connessione.
DNSCarico utile	Il payload di DNS pacchetti che contiene DNS domande e risposte.

Eventi aperti

Nome campo	Descrizione
Percorso del file	Il percorso del file aperto in questo evento.
Flag	Descrive la modalità di accesso ai file, ad esempio sola lettura, sola scrittura e lettura e scrittura.

Evento modulo di caricamento

Nome campo	Descrizione
Nome del modulo	Il nome del modulo caricato nel kernel.

Eventi mprotect

Nome campo	Descrizione
Intervallo di indirizzi	L'intervallo di indirizzi per il quale sono state modificate le protezioni di accesso.
Regioni di memoria	Specifica la regione dello spazio degli indirizzi di un processo, ad esempio stack e heap.
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.

Eventi di montaggio

Nome campo	Descrizione
Destinazione di montaggio	Il percorso in cui è montata l'origine di montaggio.
Origine di montaggio	Il percorso sull'host montato sulla destinazione di montaggio.
Tipo di file system	Rappresenta il tipo di dispositivo montato. fileSystem
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.

Eventi di collegamento

Nome campo	Descrizione
Percorso di collegamento	Il percorso in cui viene creato il collegamento fisico.
Percorso di destinazione	Il percorso del file a cui punta il collegamento fisico.

Eventi collegamento simbolico

Nome campo	Descrizione
Percorso di collegamento	Il percorso in cui viene creato il collegamento simbolico.
Percorso di destinazione	Il percorso del file a cui punta il collegamento simbolico.

Eventi dup

Nome campo	Descrizione
Vecchio descrittore di file	Un descrittore di file che rappresenta un oggetto file aperto.
Nuovo descrittore di file	Un nuovo descrittore di file che è un duplicato di quello vecchio. Sia il descrittore di file vecchio che quello nuovo rappresentano lo stesso oggetto file aperto.
IP dell'endpoint remoto dup	L'indirizzo IP remoto del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.
Porta dell'endpoint remoto dup	La porta remota del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.

Nome campo	Descrizione
IP dell'endpoint locale dup	L'indirizzo IP locale del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.
Porta dell'endpoint locale dup	La porta locale del socket di rete rappresentato dal vecchio descrittore di file. Applicabile solo quando il vecchio descrittore di file rappresenta un socket di rete.

Evento mappa di memoria

Nome campo	Descrizione
Percorso del file	Il percorso del file su cui la memoria viene mappata.

Eventi socket

Nome campo	Descrizione
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi `AF_INET` viene utilizzata per la versione IP del protocollo 4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio `SOCK_RAW`.
Numero di protocollo	Specifica un protocollo particolare all'interno della famiglia di indirizzi. In genere esiste un unico protocollo nelle famiglie di indirizzi. Ad esempio, la famiglia di indirizzi `AF_INET` ha solo il protocollo IP.

Connetti eventi

Nome campo	Descrizione
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi `AF_INET` viene utilizzata per il protocollo IPv4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio `SOCK_RAW`.
Numero di protocollo	Specifica un protocollo particolare all'interno della famiglia di indirizzi. In genere esiste un unico protocollo nelle famiglie di indirizzi. Ad esempio, la famiglia di indirizzi `AF_INET` ha solo il protocollo IP.
Percorso del file	Il percorso del file socket se la famiglia di indirizzi è `AF_UNIX`.
IP dell'endpoint remoto	L'IP remoto della connessione.
Porta dell'endpoint remoto	Il numero di porta della connessione.
IP dell'endpoint locale	L'IP locale della connessione.
Porta dell'endpoint locale	Il numero di porta della connessione.

Eventi VM Readv processo

Nome campo	Descrizione
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.
Obiettivo PID	L'ID processo del processo da cui viene letta la memoria.
Processo obiettivo UUID	L'ID univoco del processo di destinazione.

Nome campo	Descrizione
Percorso eseguibile di destinazione	Il percorso assoluto del file eseguibile del processo di destinazione.

Eventi VM Writev processo

Nome campo	Descrizione
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.
Obiettivo PID	L'ID processo del processo su cui viene scritta la memoria.
Processo obiettivo UUID	L'ID univoco del processo di destinazione.
Percorso eseguibile di destinazione	Il percorso assoluto del file eseguibile del processo di destinazione.

Eventi ptrace

Nome campo	Descrizione
Obiettivo PID	L'ID processo del processo di destinazione.
Processo obiettivo UUID	L'ID univoco del processo di destinazione.
Percorso eseguibile di destinazione	Il percorso assoluto del file eseguibile del processo di destinazione.
Flag	Rappresenta le opzioni che controllano il comportamento di questo evento.

Associa eventi

Nome campo	Descrizione
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi `AF_INET` viene utilizzata per il protocollo IPv4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio `SOCK_RAW`.
Numero di protocollo	Il numero di protocollo di livello 4, ad esempio 17 for UDP e 6 forTCP.
IP dell'endpoint locale	L'IP locale della connessione.
Porta endpoint locale	Il numero di porta della connessione.

Ascolta gli eventi

Nome campo	Descrizione
Famiglia di indirizzi	Rappresenta il protocollo di comunicazione associato all'indirizzo. Ad esempio, la famiglia di indirizzi `AF_INET` viene utilizzata per il protocollo IPv4.
Tipo di socket	Il tipo di socket per indicare la semantica della comunicazione. Ad esempio `SOCK_RAW`.
Numero di protocollo	Il numero di protocollo di livello 4, ad esempio 17 for UDP e 6 forTCP.
IP dell'endpoint locale	L'IP locale della connessione.
Porta endpoint locale	Il numero di porta della connessione.

Rinomina gli eventi

Nome campo	Descrizione
Percorso del file	Percorso in cui si trova il file che viene rinominato.
Target	Il nuovo percorso del file.

Imposta UID eventi

Nome campo	Descrizione
Nuovo EUID	Il nuovo ID utente effettivo del processo.
Nuovo UID	Il nuovo ID utente del processo.

Eventi Chmod

Nome campo	Descrizione
Percorso del file	Percorso del file che richiama questo evento.
Modalità file	Le autorizzazioni di accesso aggiornate per il file associato.

Agente di hosting ECR GuardDuty di repository Amazon

Le seguenti sezioni elencano i repository Amazon Elastic Container Registry (AmazonECR) in cui è GuardDuty ospitato l'agente di sicurezza che viene distribuito sui tuoi cluster Amazon e EKS AmazonECS.

Indice

Repository per la versione dell'EKSagente 1.6.0 o successiva

La tabella seguente mostra i ECR repository Amazon che ospitano l'agente EKS aggiuntivo Amazon versione (`aws-guardduty-agent`) 1.6.0 e successive, per ciascuno di essi. Regione AWS

Regione AWS	ECRArchivio Amazon URI
US West (Oregon)	`602401143452.dkr.ecr.us-west-2.amazonaws.com`
Europa (Parigi)	`602401143452.dkr.ecr.eu-west-3.amazonaws.com`
Asia Pacifico (Mumbai)	`602401143452.dkr.ecr.ap-south-1.amazonaws.com`
Asia Pacific (Hyderabad)	`900889452093.dkr.ecr.ap-south-2.amazonaws.com`
Canada (Centrale)	`602401143452.dkr.ecr.ca-central-1.amazonaws.com`
Canada occidentale (Calgary)	`761377655185.dkr.ecr.ca-west-1.amazonaws.com`
Medio Oriente () UAE	`759879836304.dkr.ecr.me-central-1.amazonaws.com`
Europa (Londra)	`602401143452.dkr.ecr.eu-west-2.amazonaws.com`
Stati Uniti occidentali (California settentrionale)	`602401143452.dkr.ecr.us-west-1.amazonaws.com`
Stati Uniti orientali (Virginia settentrionale)	`602401143452.dkr.ecr.us-east-1.amazonaws.com`

Regione AWS	ECRArchivio Amazon URI
Stati Uniti orientali (Ohio)	602401143452.dkr.ecr.us-east-2.amazonaws.com
Europa (Irlanda)	602401143452.dkr.ecr.eu-west-1.amazonaws.com
Sud America (San Paolo)	602401143452.dkr.ecr.sa-east-1.amazonaws.com
Europa (Stoccolma)	602401143452.dkr.ecr.eu-north-1.amazonaws.com
Europa (Francoforte)	602401143452.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zurigo)	900612956339.dkr.ecr.eu-central-2.amazonaws.com
Asia Pacifico (Singapore)	602401143452.dkr.ecr.ap-southeast-1.amazonaws.com
Asia Pacifico (Sydney)	602401143452.dkr.ecr.ap-southeast-2.amazonaws.com
Asia Pacifico (Giacarta)	296578399912.dkr.ecr.ap-southeast-3.amazonaws.com
Asia Pacifico (Tokyo)	602401143452.dkr.ecr.ap-northeast-1.amazonaws.com
Asia Pacifico (Seoul)	602401143452.dkr.ecr.ap-northeast-2.amazonaws.com
Asia Pacifico (Osaka-Locale)	602401143452.dkr.ecr.ap-northeast-3.amazonaws.com
Asia Pacifico (Hong Kong)	800184023465.dkr.ecr.ap-east-1.amazonaws.com

Regione AWS	ECRArchivio Amazon URI
Medio Oriente (Bahrein)	759879836304.dkr.ecr.me-south-1.amazonaws.com
Europa (Milano)	590381155156.dkr.ecr.eu-south-1.amazonaws.com
Europa (Spagna)	455263428931.dkr.ecr.eu-south-2.amazonaws.com
Africa (Città del Capo)	877085696533.dkr.ecr.af-south-1.amazonaws.com
Asia Pacifico (Melbourne)	491585149902.dkr.ecr.ap-southeast-4.amazonaws.com
Israele (Tel Aviv)	066635153087.dkr.ecr.il-central-1.amazonaws.com

Repository per la versione EKS dell'agente 1.5.0 e precedenti

La tabella seguente mostra i ECR repository Amazon che ospitano l'agente EKS aggiuntivo Amazon versione (`aws-guardduty-agent`) 1.5.0 e precedenti, per ciascuno di essi. Regione AWS

Regione AWS	ECRArchivio Amazon URI
US West (Oregon)	039403964562.dkr.ecr.us-west-2.amazonaws.com
Europa (Parigi)	113643092156.dkr.ecr.eu-west-3.amazonaws.com
Asia Pacifico (Mumbai)	610108029387.dkr.ecr.ap-south-1.amazonaws.com
Asia Pacific (Hyderabad)	618745550137.dkr.ecr.ap-south-2.amazonaws.com
Canada (Centrale)	001188825231.dkr.ecr.ca-central-1.amazonaws.com

Regione AWS	ECRArchivio Amazon URI
Medio Oriente () UAE	601769779514.dkr.ecr.me-central-1.amazonaws.com
Europa (Londra)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
Stati Uniti occidentali (California settentrionale)	373421517865.dkr.ecr.us-west-1.amazonaws.com
Stati Uniti orientali (Virginia settentrionale)	031903291036.dkr.ecr.us-east-1.amazonaws.com
Stati Uniti orientali (Ohio)	591382732059.dkr.ecr.us-east-2.amazonaws.com
Europa (Irlanda)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
Sud America (San Paolo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europa (Stoccolma)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europa (Francoforte)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zurigo)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Asia Pacifico (Singapore)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Asia Pacifico (Sydney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Asia Pacifico (Giacarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com

Regione AWS	ECRArchivio Amazon URI
Asia Pacifico (Tokyo)	`781592569369.dkr.ecr.ap-northeast-1.amazonaws.com`
Asia Pacifico (Seoul)	`732248494576.dkr.ecr.ap-northeast-2.amazonaws.com`
Asia Pacifico (Osaka-Locale)	`810724417379.dkr.ecr.ap-northeast-3.amazonaws.com`
Asia Pacifico (Hong Kong)	`790429075973.dkr.ecr.ap-east-1.amazonaws.com`
Medio Oriente (Bahrein)	`541829937850.dkr.ecr.me-south-1.amazonaws.com`
Europa (Milano)	`528450769569.dkr.ecr.eu-south-1.amazonaws.com`
Europa (Spagna)	`531047660167.dkr.ecr.eu-south-2.amazonaws.com`
Africa (Città del Capo)	`379032919888.dkr.ecr.af-south-1.amazonaws.com`
Asia Pacifico (Melbourne)	`750462861327.dkr.ecr.ap-southeast-4.amazonaws.com`
Israele (Tel Aviv)	`292660727137.dkr.ecr.il-central-1.amazonaws.com`

Repository per GuardDuty agente su AWS Fargate (ECSsolo Amazon)

La tabella seguente mostra i ECR repository Amazon che ospitano l' GuardDuty agente per AWS Fargate (ECSsolo Amazon) per ciascuno Regione AWS di essi.

Regione AWS	ECRArchivio Amazon URI
US West (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate`

Regione AWS	ECRArchivio Amazon URI
Europa (Parigi)	665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Mumbai)	251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacific (Hyderabad)	950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate
Canada (Centrale)	354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate
Medio Oriente () UAE	000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Londra)	892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate
Stati Uniti occidentali (California settentrionale)	684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate
Stati Uniti orientali (Virginia settentrionale)	593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate
Stati Uniti orientali (Ohio)	307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate
Europa (Irlanda)	694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate
Sud America (San Paolo)	758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate

Regione AWS	ECRArchivio Amazon URI
Europa (Stoccolma)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Francoforte)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Zurigo)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Singapore)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Sydney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Giacarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Tokyo)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Seoul)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Osaka-Locale)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacifico (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Medio Oriente (Bahrein)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Milano)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Spagna)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate

Regione AWS	ECRArchivio Amazon URI
Africa (Città del Capo)	`197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Asia Pacifico (Melbourne)	`251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate`
Israele (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate`

GuardDuty cronologia dei rilasci dell'agente

Le seguenti sezioni forniscono la versione di rilascio per GuardDuty l'agente che viene distribuito su EC2 istanze Amazon, ECS cluster Amazon e cluster Amazon EKS

GuardDuty agente di sicurezza per EC2 istanze Amazon

Versione agente	Note di rilascio	Data di disponibilità
v1.3.0	Ottimizzazione e miglioramenti generali delle prestazioni Include il supporto per l'acquisizione di segnali di sicurezza aggiuntivi per il futuroTipi di risultati del monitoraggio del runtime.	19 agosto 2024
v1.2.0	Supporta le distribuzioni del sistema operativo Ubuntu 20.04, Ubuntu 22.04, Debian 11 e Debian 12 Supporta kernel 6.5 e 6.8 Ottimizzazione e miglioramenti generali delle prestazioni	13 giugno 2024

Versione agente	Note di rilascio	Data di disponibilità
v1.1.0	Supporta la configurazione GuardDuty automatizzata degli agenti in Runtime Monitoring per le EC2 istanze Amazon Supporta nuovi segnali e risultati di sicurezza rilasciati con l'annuncio della disponibilità generale di Runtime Monitoring per EC2 le istanze Ottimizzazione e miglioramenti generali delle prestazioni	26 marzo 2024
v1.0.2	Supporta la versione più recente di Amazon ECSAMIs.	2 febbraio 2024
v1.0.1	Le versioni degli agenti rilasciate prima della v1.0.2 non sono compatibili con Amazon ECS AMIs lanciate dopo il 31 gennaio 2024. Ottimizzazione e miglioramenti generali delle prestazioni	23 gennaio 2024
v1.0.0	Versione iniziale dell'installazione RPM Le versioni degli agenti rilasciate prima della v1.0.2 non sono compatibili con Amazon ECS AMIs lanciate dopo il 31 gennaio 2024.	26 novembre 2023

RPM S3 bucket example script

La chiave pubblica, la firma di x86_64RPM, la firma di arm64 RPM e il collegamento di accesso corrispondente agli RPM script ospitati nei bucket Amazon S3 possono essere formati dai seguenti modelli. Sostituisci il valore dell'ID dell' AWS account e la Regione AWS versione dell'agente per accedere agli GuardDuty script. RPM I seguenti modelli includono l'ultima versione dell'agente per le EC2 istanze Amazon.

- Chiave pubblica:

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

- GuardDuty RPMfirma dell'agente di sicurezza:

  Firma di 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
  ```

  Firma di arm64 RPM

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

- Accedi ai link agli RPM script nel bucket Amazon S3:

  Link di accesso per 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
  ```

  Link di accesso per 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

La chiave pubblica, la firma con arm64 e il collegamento di accesso corrispondente agli script ospitati nei bucket Amazon S3 possono essere formati dai seguenti modelli. Sostituisci il valore

dell' Regione AWS ID dell' AWS account e la versione dell' GuardDuty agente per accedere agli script. I seguenti modelli includono l'ultima versione dell'agente per le EC2 istanze Amazon.

- Chiave pubblica:

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

- GuardDuty firma dell'agente di sicurezza:

  Firma di amd64

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

  Firma di arm64

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

- Accedi ai link agli script nel bucket Amazon S3:

  Link di accesso per amd64

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

  Link di accesso per arm64

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

Regione AWS	Nome Regione	AWS ID dell'account
`eu-west-1`	Europa (Irlanda)	694911143906
`us-east-1`	Stati Uniti orientali (Virginia settentrionale)	593207742271
`us-east-2`	Stati Uniti orientali (Ohio)	733349766148

eu-west-3	Europa (Parigi)	665651866788
us-east-2	Stati Uniti orientali (Ohio)	307168627858
eu-central-1	Europa (Francoforte)	323658145986
ap-northeast-2	Asia Pacifico (Seoul)	914738172881
eu-north-1	Europa (Stoccolma)	591436053604
ap-east-1	Asia Pacifico (Hong Kong)	258348409381
me-south-1	Medio Oriente (Bahrein)	536382113932
eu-west-2	Europa (Londra)	892757235363
ap-northeast-1	Asia Pacifico (Tokyo)	533107202818
ap-southeast-1	Asia Pacifico (Singapore)	174946120834
ap-south-1	Asia Pacifico (Mumbai)	251508486986
ap-southeast-3	Asia Pacifico (Giacarta)	510637619217
sa-east-1	Sud America (San Paolo)	758426053663
ap-northeast-3	Asia Pacifico (Osaka-Locale)	273192626886
eu-south-1	Europa (Milano)	266869475730
af-south-1	Africa (Città del Capo)	197869348890
ap-southeast-2	Asia Pacifico (Sydney)	005257825471
me-central-1	Medio Oriente () UAE	000014521398
us-west-1	Stati Uniti occidentali (Californ ia settentrionale)	684579721401
ca-central-1	Canada (Centrale)	354763396469
ap-south-2	Asia Pacific (Hyderabad)	950823858135

eu-south-2	Europa (Spagna)	919611009337
eu-central-2	Europa (Zurigo)	529164026651
ap-southeast-4	Asia Pacifico (Melbourne)	251357961535
il-central-1	Israele (Tel Aviv)	870907303882

GuardDuty agente di sicurezza per AWS Fargate (ECSsolo Amazon)

La tabella seguente mostra la cronologia delle versioni di rilascio del GuardDuty Security Agent per Fargate (ECSsolo Amazon).

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità
v1.3.0	x86_64 (): AMD64 `sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831` Gravitone (): ARM64 `sha256:ff81a755d46681e409f55a95beedae9ebbcf5336e1c0b1e6348af7c6518bdbb1`	Ottimizzazione e miglioramenti generali delle prestazioni. Include il supporto per l'acquisizione di segnali di sicurezza aggiuntivi per il futuro GuardDuty Tipi di risultati del monitoraggio del runtime.	9 agosto 2024
v1.2.0	x86_64 (): AMD64 `sha256:1dbad20ac2dc66d52d00bb28dde4281fe0d3c5f261b1649b247c2369d9e26b93`	Ottimizzazione e miglioramenti generali delle prestazioni.	31 maggio 2024

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità
	Gravitone (): ARM64 `sha256:91930f8446f5f95b93b8ccb18773992affa401eb3f42da89d68077a56bafa6cd`		
v1.1.0	x86_64 (): AMD64 `sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c9f673f2835823957e9dcf71657` Gravitone (): ARM64 `sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dcccfe8c9383dc7`	Supporta nuovi segnali e risultati di sicurezza. Ottimizzazione e miglioramenti generali delle prestazioni.	01 maggio 2024
v1.0.1	x86_64 (): AMD64 `sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68` Gravitone (): ARM64 `sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7`	Ottimizzazione e miglioramenti generali delle prestazioni.	26 gennaio 2024

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità
v1.0.0	x86_64 (): AMD64 `sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017` Gravitone (): ARM64 `sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984`	Versione iniziale di GuardDuty Security Agent per AWS Fargate (ECSsolo Amazon).	26 novembre 2023

GuardDuty agente di sicurezza per EKS cluster Amazon

La tabella seguente mostra la cronologia delle versioni di rilascio dell' GuardDuty agente EKS aggiuntivo Amazon.

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard [1]
v1.7.0	x86_64 (): AMD64 `sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffcd7e68554a423d610cea8c7e8f2185ec` Gravitone (): ARM64 `sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a`	Ottimizzazione e miglioramenti generali delle prestazioni. Include il supporto per l'acquisizione di segnali di sicurezza aggiuntivi per il futuroTipi	17 agosto 2024	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard [1]
		di risultati del monitoraggio del runtime.		
v1.6.1	x86_64 (): AMD64 `sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bdb07c3ab1` Gravitone (): ARM64 `sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019`	Ottimizzazione e miglioramenti generali delle prestazioni.	14 maggio 2024	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard [1]

v1.6.0	x86_64 (): AMD64
	`sha256:7dabcbee30d8b053676752fbc19e89f77272d9a6a53cc93731f5872180ef9010`
	
	Gravitone (): ARM64
	`sha256:9710f53afccdf4f22b265a1a6fc27f1469403af1f7d5d08c4869a7269cdd2650`
		• Supporta la configurazione GuardDuty automatica degli agenti perEKS/EC2resources.
		• Supporta i nuovi segnali e risultati di sicurezza. Per ulteriori informazioni, consulta Tipi di eventi di runtime raccolti che utilizza GuardDuty e Tipi di risultati del monitoraggio del runtime.
		• Ottimizzazione e miglioram
			29 aprile 2024	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard [1]
		enti generali delle prestazioni.		
v1.5.0	x86_64 (): AMD64 `sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d` Gravitone (): ARM64 `sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6`	• Ottimizzazione e miglioramenti generali delle prestazioni. • Miglioramenti della sicurezza, inclusi nuovi tipi di eventi in. Tipi di eventi di runtime raccolti • Miglioramenti delle prestazioni in relazione all'utilizzo. CPU	07 marzo 2024	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard [1]
v1.4.1	x86_64 (): AMD64 `sha256:66d4919277637426 60faa87cc2c39bb97b 7873039157ae8b90bc 999cb73d0b9c` Gravitone (): ARM64 `sha256:537a330b2dd82357 024fb6daeb8761034 b7defd43b10dffe0792 c9e6d0778b40`	Ottimizzazione e miglioramenti generali delle prestazioni.	16 gennaio 2024	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard [1]
v1.4.0	x86_64 (): AMD64 `sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f` Gravitone (): ARM64 `sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e`	Il punto di montaggio Manifest supporta una migliore raccolta dei dati AppArmor configurazione in manifest Raccogli l'argomento della riga di comando Ottimizzazione e miglioramenti generali delle prestazioni	21 dicembre 2023	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard [1]
v1.3.1	x86_64 (): AMD64 `sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29` Gravitone (): ARM64 `sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd`	Patch di sicurezza e aggiornamenti importanti.	23 ottobre 2023	–
v1.3.0	x86_64 (): AMD64 `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Gravitone (): ARM64 `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Supporta la piattaforma Ubuntu Supporta la versione 1.28 di Kubernetes Miglioramenti generali delle prestazioni e miglioramento della stabilità.	5 ottobre 2023	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard [1]
v1.2.0	x86_64 (): AMD64 `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Gravitone (): ARM64 `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	Oltre alle istanze AMD64 basate, la versione 1.2.0 ora supporta anche le istanze basate. ARM64 È stato aggiunto e verificato il supporto per Bottlerocket Supporta la versione 1.27 di Kubernetes Miglioramenti generali delle prestazioni e miglioramenti della stabilità.	16 giugno 2023	–

Versione agente	Immagine di container	Note di rilascio	Data di disponibilità	Fine del supporto standard [1]
v1.1.0	`sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c`	Oltre a Versioni di Kubernetes supportate dal security agent GuardDuty, questa versione dell'agente supporta anche la versione 1.26 di Kubernetes. Miglioramenti generali delle prestazioni e miglioramenti della stabilità.	2 maggio 2023	14 maggio 2024
v1.0.0	`sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e`	Versione iniziale dell'agente EKS aggiuntivo Amazon.	30 marzo 2023	14 maggio 2024

[1] Per informazioni sull'aggiornamento della versione corrente dell'agente che si avvicina alla fine del supporto standard, consulta. Aggiornamento manuale del Security Agent

Impatto della disabilitazione e della pulizia delle risorse

Questa sezione si applica Account AWS se si sceglie di disabilitare il Runtime Monitoring o solo la configurazione GuardDuty automatica dell'agente per un tipo di risorsa.

Disabilitazione della configurazione GuardDuty automatica degli agenti

GuardDuty non rimuove il security agent distribuito sulla tua risorsa. Tuttavia, GuardDuty smetterà di gestire gli aggiornamenti del security agent.

GuardDuty continua a ricevere gli eventi di runtime dal tipo di risorsa in uso. Per evitare un impatto sulle statistiche di utilizzo, assicurati di rimuovere il GuardDuty security agent dalla tua risorsa.

Indipendentemente dal fatto che un utente Account AWS utilizzi o meno un VPC endpoint condiviso, GuardDuty non elimina l'VPCendpoint. Se necessario, dovrai eliminare l'VPCendpoint manualmente.

Disabilitazione del monitoraggio del runtime e EKS del monitoraggio del runtime

Questa sezione si applica ai seguenti scenari:

- Non hai mai abilitato il EKS Runtime Monitoring separatamente e ora hai disabilitato il Runtime Monitoring.
- Stai disabilitando sia il Runtime Monitoring che il EKS Runtime Monitoring. Se non sei sicuro dello stato di configurazione di EKS Runtime Monitoring, consulta. Verifica dello stato della configurazione EKS di Runtime Monit

> Disabilitare il monitoraggio del runtime senza EKS disabilitare il monitoraggio del runtime
>
> In questo scenario, a un certo punto è stato abilitato il EKS Runtime Monitoring e, successivamente, è stato abilitato anche il Runtime Monitoring senza disabilitare EKS il Runtime Monitoring.
> Ora, quando si disabilita il Runtime Monitoring, sarà necessario disabilitare anche il EKS Runtime Monitoring; in caso contrario, si continueranno a sostenere costi di utilizzo per EKS il Runtime Monitoring.

Se ti riguardano gli scenari elencati in precedenza, GuardDuty eseguirà le seguenti azioni nel tuo account:

- GuardDuty elimina il tag VPC che ha il `true` tag`GuardDutyManaged`:. Questo è VPC quello che è GuardDuty stato creato per gestire l'agente di sicurezza automatizzato.
- GuardDuty elimina il gruppo di sicurezza contrassegnato come`GuardDutyManaged:true`.
- Per una condivisione VPC che è stata utilizzata da almeno un account partecipante, GuardDuty non elimina né l'VPCendpoint né il gruppo di sicurezza associato alla risorsa condivisa. VPC
- Per una EKS risorsa Amazon, GuardDuty elimina il security agent. Ciò è indipendente dal fatto che sia gestito manualmente o tramite GuardDuty.

  Per una ECS risorsa Amazon, poiché un'ECSattività è immutabile, non è GuardDuty possibile disinstallare il security agent da quella risorsa. Ciò è indipendente dal modo in cui gestisci il security agent, manualmente o automaticamente tramite. GuardDuty Dopo aver disabilitato il monitoraggio del runtime, non GuardDuty collegherà un contenitore secondario quando inizia l'esecuzione di una nuova ECS attività. Per informazioni sull'utilizzo delle ECS attività di Fargate, vedere. Come funziona il monitoraggio del runtime con Fargate (solo AmazonECS)

  Per una EC2 risorsa Amazon, GuardDuty disinstalla il security agent da tutte le EC2 istanze Amazon gestite da Systems Manager (SSM) solo quando soddisfa le seguenti condizioni:

  - La tua risorsa non è etichettata con`GuardDutyManaged`: `false` tag di esclusione.
  - GuardDuty deve disporre delle autorizzazioni per accedere ai tag nei metadati dell'istanza. Per questa EC2 risorsa, l'accesso ai tag nei metadati dell'istanza è impostato su Consenti.

Quando si interrompe la gestione manuale del Security Agent

Indipendentemente dall'approccio utilizzato per distribuire e gestire il GuardDuty security agent, per interrompere il monitoraggio degli eventi di runtime nella risorsa, è necessario rimuovere il GuardDuty security agent. Se desideri interrompere il monitoraggio degli eventi di runtime da un tipo di risorsa in un account, puoi anche eliminare l'VPCendpoint Amazon.

Procedura per ripulire le risorse del Security Agent

Per eliminare un VPC endpoint Amazon

- Senza una condivisioneVPC: quando non desideri più monitorare una risorsa in un account, valuta la possibilità di eliminare l'VPCendpoint Amazon.
- Con un account condivisoVPC: quando un account VPC proprietario condiviso elimina la VPC risorsa condivisa che era ancora in uso, lo stato di copertura del Runtime Monitoring (e, se applicabile, del EKS Runtime Monitoring) per le risorse nell'account VPC proprietario condiviso

e nell'account partecipante potrebbe diventare inadeguato. Per informazioni sullo stato della copertura, consulta. Valutazione della copertura in termini di runtime delle risorse

Per ulteriori informazioni, consulta Eliminazione di un endpoint dell'interfaccia.

Per eliminare il gruppo di sicurezza

- Senza condivisioneVPC: quando non desideri più monitorare un tipo di risorsa in un account, valuta la possibilità di eliminare il gruppo di sicurezza associato ad AmazonVPC.
- Con un account condivisoVPC: quando l'account VPC proprietario condiviso elimina il gruppo di sicurezza, qualsiasi account partecipante che attualmente utilizza il gruppo di sicurezza associato all'account condivisoVPC, allo stato di copertura del Runtime Monitoring per le risorse del tuo account VPC proprietario condiviso e dell'account partecipante potrebbe diventare non integro. Per ulteriori informazioni, consulta Valutazione della copertura in termini di runtime delle risorse.

Per ulteriori informazioni, consulta Eliminare un gruppo di sicurezza.

Per rimuovere il GuardDuty security agent da un EKS cluster

Per rimuovere il security agent dal EKS cluster che non desideri più monitorare, vedi Eliminazione di un componente aggiuntivo.

La rimozione dell'agente EKS aggiuntivo non rimuove lo `amazon-guardduty` spazio dei nomi dal cluster. EKS Per eliminare lo spazio dei nomi `amazon-guardduty`, consulta Eliminazione di uno spazio dei nomi.

Per eliminare lo **`amazon-guardduty`** spazio dei nomi (cluster) EKS

La disabilitazione della configurazione automatizzata dell'agente non rimuove automaticamente lo `amazon-guardduty` spazio dei nomi dal cluster. EKS Per eliminare lo spazio dei nomi `amazon-guardduty`, consulta Eliminazione di uno spazio dei nomi.

GuardDuty Protezione da malware per EC2

Malware Protection for ti EC2 aiuta a rilevare la potenziale presenza di malware scansionando i volumi Amazon Elastic Block Store (AmazonEBS) collegati alle istanze di Amazon Elastic Compute Cloud (AmazonEC2) e ai carichi di lavoro dei container. Malware Protection for EC2 offre opzioni di scansione in cui puoi decidere se includere o escludere EC2 istanze Amazon e carichi di lavoro di container specifici al momento della scansione. Offre inoltre la possibilità di conservare le istantanee dei EBS volumi Amazon collegati alle EC2 istanze Amazon o ai carichi di lavoro dei container nei tuoi account. GuardDuty Le istantanee vengono conservate solo quando viene rilevato un malware e viene generata la protezione da malware per i risultati. EC2

Malware Protection for EC2 è un miglioramento opzionale ed è progettato in modo da non influire sulle prestazioni delle risorse. GuardDuty Per informazioni su come EC2 funziona Malware Protection for all'interno GuardDuty, consulta. Funzionalità di protezione da malware per EC2 Per informazioni sulla disponibilità di Malware Protection for EC2 in different Regioni AWS, vedereRegioni ed endpoint.

> **Nota**
>
> GuardDuty Malware Protection for EC2 non supporta Fargate né con Amazon né con EKS Amazon. ECS

Malware Protection for EC2 offre due tipi di scansioni per rilevare attività potenzialmente dannose nelle EC2 istanze Amazon e nei carichi di lavoro dei container: la scansione antimalware GuardDuty avviata e la scansione antimalware su richiesta. La tabella seguente mostra il confronto tra i due tipi di scansione.

Factor	GuardDuty-scansione antimalware avviata	Scansione antimalware on demand
Come viene richiamata la scansione	Dopo aver GuardDuty abilitato la scansione antimalwa re avviata, ogni volta che GuardDuty genera un risultato che indica la potenziale presenza di malware in	Puoi avviare una scansione antimalware On-demand fornendo l'Amazon Resource Name (ARN) associato al carico di lavoro dell'EC2i stanza o del container

Factor	GuardDuty-scansione antimalware avviata	Scansione antimalware on demand
	un'EC2istanza Amazon o in un carico di lavoro di container, avvia GuardDuty automaticamente una scansione antimalware senza agenti sui EBS volumi Amazon collegati alla risorsa potenzialmente interessa ta. Per ulteriori informazioni, consulta GuardDuty-scansione antimalware avviata.	Amazon. Puoi avviare una scansione antimalware su richiesta anche quando non viene generato alcun GuardDuty risultato per la tua risorsa. Per ulteriori informazi oni, consulta Scansione antimalware on demand.
Configurazione necessaria	Per utilizzare GuardDuty - initiated malware scan, devi abilitarla per il tuo account. Per ulteriori informazioni, consulta Configurazione della scansione antimalware avviata GuardDuty.	Il tuo account deve essere abilitato GuardDuty . Per utilizzare la scansione antimalware su richiesta, non è richiesta alcuna configura zione a livello di funzionalità.
Tempo di attesa per avviare una nuova scansione	Ogni volta che ne GuardDuty genera unoRisultati che richiamano la scansione GuardDuty antimalware avviata, una scansione antimalware viene avviata automaticamente solo una volta ogni 24 ore.	È possibile avviare una scansione antimalware su richiesta sulla stessa risorsa in qualsiasi momento dopo 1 ora dall'inizio della scansione precedente.

Factor	GuardDuty-scansione antimalware avviata	Scansione antimalware on demand
Disponibilità del periodo di prova gratuito di 30 giorni	Quando attivi la scansione antimalware GuardDuty avviata per la prima volta nel tuo account, puoi utilizzare un periodo di prova gratuito di 30 giorni*. Per ulteriori informazioni su GuardDuty -initiated malware scan, consulta. Prova gratuita di 30 giorni	Non è previsto un periodo di prova gratuito* con la scansione antimalware su richiesta per account nuovi o esistenti. GuardDuty
Opzioni di scansione	Dopo aver configurato la scansione antimalwa re GuardDuty avviata, Malware Protection for ti aiuta EC2 anche a selezionare quali risorse scansionare o ignorare. Malware Protectio n for non EC2 avvierà una scansione automatica delle risorse che scegli di escludere dalla scansione.	La scansione antimalwa re su richiesta supporta un tag globale:. `GuardDuty Excluded` Opzioni di scansione con tag definiti dall'utentenon è applicabile alla scansione antimalware su richiesta perché la risorsa ARN viene fornita manualmen te.

*Saranno sostenuti i costi di utilizzo per la creazione di istantanee di EBS volume e la conservazione delle istantanee. Per ulteriori informazioni sulla configurazione dell'account per conservare le istantanee, consulta. Conservazione degli snapshot

Funzionalità di protezione da malware per EC2

Volume Elastic Block Storage (EBS)

Questa sezione spiega in che modo Malware Protection forEC2, inclusa la scansione antimalware GuardDuty avviata e la scansione antimalware su richiesta, analizza i volumi Amazon associati alle istanze EBS EC2 Amazon e ai carichi di lavoro dei container. Prima di procedere, considera le personalizzazioni seguenti:

- Opzioni di scansione: Malware Protection for EC2 offre la possibilità di specificare tag per includere o escludere EC2 istanze Amazon e EBS volumi Amazon dal processo di scansione. Solo la scansione antimalware GuardDuty avviata supporta opzioni di scansione con tag definiti dall'utente. Sia la scansione antimalware GuardDuty avviata che la scansione antimalware su richiesta supportano il tag globale. `GuardDutyExcluded` Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente.
- Conservazione delle istantanee: Malware Protection for EC2 offre un'opzione per conservare le istantanee dei EBS volumi Amazon nel tuo AWS account. Per impostazione predefinita, questa opzione è disattivata. Puoi optare per la conservazione delle istantanee sia per le scansioni antimalware GuardDuty avviate che per quelle su richiesta. Per ulteriori informazioni, consulta Conservazione degli snapshot.

Quando GuardDuty genera un risultato indicativo della potenziale presenza di malware in un'EC2istanza Amazon o in un carico di lavoro di container e hai abilitato il tipo di scansione GuardDuty avviata in Malware Protection forEC2, è possibile che venga richiamata una scansione antimalware GuardDuty avviata sulla base delle opzioni di scansione.

Per avviare una scansione antimalware On-demand sui EBS volumi Amazon associati a un'EC2istanza Amazon, fornisci l'Amazon Resource Name (ARN) dell'istanza AmazonEC2.

In risposta a una scansione antimalware su richiesta o a una scansione antimalware GuardDuty avviata automaticamente, GuardDuty crea istantanee dei EBS volumi pertinenti collegati alla risorsa potenzialmente interessata e le condivide con. GuardDuty account di servizio Da queste istantanee, GuardDuty crea un volume di replica crittografato nell'account del servizio. EBS

Per informazioni sulla metodologia di rilevamento del GuardDuty malware e sui motori di scansione utilizzati, vedere. GuardDuty motore di scansione per il rilevamento di malware

Al termine della scansione, GuardDuty elimina i volumi di replica crittografati e le istantanee EBS dei volumi. EBS Se viene rilevato del malware e hai attivato l'impostazione di conservazione delle istantanee, le istantanee dei tuoi EBS volumi non verranno eliminate e verranno automaticamente conservate nel tuo account. AWS Se non viene rilevato alcun malware, le istantanee dei EBS volumi non verranno conservate, indipendentemente dall'impostazione di conservazione delle istantanee. Per impostazione predefinita, la conservazione degli snapshot è disattivata. Per informazioni sui costi delle istantanee e sulla loro conservazione, consulta i EBSprezzi di Amazon.

GuardDuty conserverà ogni EBS volume di replica nell'account di servizio per un massimo di 55 ore. In caso di interruzione del servizio o di errore relativo a un EBS volume di replica e alla relativa

scansione antimalware, GuardDuty conserverà tale EBS volume per non più di sette giorni. Il periodo di conservazione prolungato del volume serve a valutare e risolvere l'interruzione o l'errore. GuardDuty Malware Protection for EC2 eliminerà i EBS volumi di replica dall'account di servizio dopo aver risolto l'interruzione o l'errore o una volta scaduto il periodo di conservazione prolungato.

EBSVolumi Amazon supportati per la scansione di malware

In tutti i paesi in Regioni AWS cui GuardDuty supporta la EC2 funzionalità Malware Protection for, puoi scansionare i EBS volumi Amazon non crittografati o crittografati. Puoi avere EBS volumi Amazon crittografati con una delle due chiavi Chiave gestita da AWSo con una chiave gestita dal cliente. Attualmente, alcuni Regioni AWS supportano entrambi i modi di crittografare i EBS volumi Amazon, mentre altri supportano solo la chiave gestita dal cliente.

Per ulteriori informazioni sui casi in cui questa funzionalità non è ancora supportata, consulta China Regions

L'elenco seguente descrive la chiave che GuardDuty utilizza indipendentemente dal fatto che i EBS volumi Amazon siano crittografati o meno:

- EBSVolumi Amazon non crittografati o crittografati con Chiave gestita da AWS: GuardDuty utilizza la propria chiave per crittografare i volumi Amazon EBS di replica.

  Se il tuo account appartiene a una Regione AWS società che non supporta la scansione di EBS volumi Amazon crittografati con l'impostazione predefinita Chiave gestita da AWS per EBS, consultaModifica dell'ID AWS KMS chiave predefinito di un volume Amazon EBS.
- EBSVolumi Amazon crittografati con chiave gestita dal cliente: GuardDuty utilizza la stessa chiave per crittografare il volume di replicaEBS.

Malware Protection for EC2 non supporta la scansione EC2 delle istanze Amazon con `productCode` as`marketplace`. Se viene avviata una scansione antimalware per un'EC2istanza Amazon di questo tipo, la scansione verrà ignorata. Per ulteriori informazioni, consulta `UNSUPPORTED_PRODUCT_CODE_TYPE` in Motivi per cui una risorsa viene ignorata durante la scansione malware.

Modifica dell'ID AWS KMS chiave predefinito di un volume Amazon EBS

Per impostazione predefinita, richiamando CreateVolumeAPIwith encryption set to `true` e non specificando l'ID della KMS chiave, viene creato un EBS volume Amazon che viene

crittografato con la AWS KMS chiave di EBS crittografia predefinita. Tuttavia, quando una chiave di crittografia non viene fornita in modo esplicito, puoi modificare la chiave predefinita richiamando ModifyEbsDefaultKmsKeyIdAPIo utilizzando il comando corrispondente. AWS CLI

Per modificare l'ID della chiave EBS predefinita, aggiungi la seguente autorizzazione necessaria alla tua IAM politica:. `ec2:modifyEbsDefaultKmsKeyId` Qualsiasi EBS volume Amazon appena creato che scegli di crittografare ma che non specifica un ID KMS chiave associato, utilizzerà l'ID chiave predefinito. Utilizza uno dei seguenti metodi per aggiornare l'ID della chiave EBS predefinita:

Per modificare l'ID KMS chiave predefinito di un EBS volume Amazon

Esegui una di queste operazioni:

- Utilizzando un API: è possibile utilizzare il ModifyEbsDefaultKmsKeyIdAPI. Per informazioni su come visualizzare lo stato di crittografia del volume, consulta Create Amazon EBS volume.
- Utilizzo del AWS CLI comando: l'esempio seguente modifica l'ID KMS chiave predefinito che crittograferà EBS i volumi Amazon se non fornisci un ID KMS chiave. Assicurati di sostituire la regione con l'ID Regione AWS della tua chiave KM.

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
id AKIAIOSFODNN7EXAMPLE
```

Il comando precedente genererà un output simile al seguente:

```
{
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

Per ulteriori informazioni, vedi modify-ebs-default-kms-key-id.

Personalizzazioni nella protezione da malware per EC2

Questa sezione descrive come personalizzare le opzioni di scansione per le EC2 istanze Amazon o i carichi di lavoro dei container quando viene richiamata una scansione antimalware, avviata su richiesta o tramite. GuardDuty

Impostazioni generali

Conservazione degli snapshot

GuardDuty ti offre la possibilità di conservare le istantanee dei tuoi volumi nel tuo account. EBS AWS Per impostazione predefinita, la conservazione degli snapshot è disattivata. Gli snapshot verranno conservati solo se questa impostazione viene attivata prima dell'avvio della scansione.

All'avvio della scansione, GuardDuty genera i volumi di replica in base alle istantanee dei EBS volumi. EBS Una volta completata la scansione e attivata l'impostazione di conservazione delle istantanee nell'account, le istantanee dei EBS volumi verranno conservate solo quando viene rilevato e generato malware. Protezione da malware per tipi di ricerca EC2 Indipendentemente dal fatto che tu abbia attivato o meno l'impostazione di conservazione delle istantanee, quando non viene rilevato alcun malware, le istantanee dei volumi GuardDuty vengono eliminate automaticamente. EBS

Costo di utilizzo degli snapshot

Durante la scansione antimalware, quando vengono GuardDuty create le istantanee dei EBS volumi Amazon, a questo passaggio è associato un costo di utilizzo. Se attivi l'impostazione di conservazione degli snapshot per il tuo account, quando viene rilevato un malware dovrai sostenere i costi di utilizzo per conservare gli snapshot. Per informazioni sul costo delle istantanee e sulla loro conservazione, consulta i EBSprezzi di Amazon.

Scegli il metodo di accesso che preferisci per attivare l'impostazione di conservazione degli snapshot.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, in Piani di protezione, scegli Malware Protection for EC2.
3. Scegli Impostazioni generali nella sezione inferiore della console. Per conservare gli snapshot, attiva la Conservazione degli snapshot.

API/CLI

1. Esegui UpdateMalwareScanSettingsper aggiornare la configurazione corrente per l'impostazione di conservazione delle istantanee.
2. In alternativa, è possibile eseguire il AWS CLI comando seguente per conservare automaticamente le istantanee quando GuardDuty Malware Protection for EC2 genera dei risultati.

Assicurarsi di sostituire il *detector-id* con il tuo validodetectorId.

3. Per trovare le detectorId impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

4. Se desideri disattivare la conservazione degli snapshot, sostituisci RETENTION_WITH_FINDING con NO_RETENTION.

Opzioni di scansione con tag definiti dall'utente

Utilizzando GuardDuty -initiated malware scan, puoi anche specificare tag per includere o escludere le EC2 istanze Amazon e i EBS volumi Amazon dal processo di scansione e rilevamento delle minacce. Puoi personalizzare ogni scansione antimalware GuardDuty avviata modificando i tag nell'elenco dei tag di inclusione o di esclusione. Ogni elenco può includere fino a 50 tag.

Se non disponi già di tag definiti dall'utente associati alle tue EC2 risorse, consulta Tagga le tue EC2 risorse Amazon nella Amazon EC2 User Guide o Tagga le tue EC2 risorse Amazon nella Amazon EC2 User Guide.

> **Note**
>
> La scansione antimalware on demand non supporta le opzioni di scansione con tag definiti dall'utente. Supporta Tag GuardDutyExcluded globale.

Per escludere le EC2 istanze dalla scansione antimalware

Se desideri escludere EC2 un'istanza o un EBS volume Amazon durante il processo di scansione, puoi impostare il GuardDutyExcluded tag su qualsiasi EC2 istanza Amazon o EBS volume Amazon e GuardDuty non eseguirne la scansione. true Per ulteriori informazioni sul tag GuardDutyExcluded, consulta Autorizzazioni di ruolo collegate al servizio per Malware Protection for EC2. Puoi anche aggiungere un tag di EC2 istanza Amazon a un elenco di esclusione. Se aggiungi più tag all'elenco dei tag di esclusione, qualsiasi EC2 istanza Amazon che contiene almeno uno di questi tag verrà esclusa dal processo di scansione malware.

Scegli il tuo metodo di accesso preferito per aggiungere un tag associato a un'EC2istanza Amazon a un elenco di esclusione.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, in Piani di protezione, scegli Malware Protection for EC2.
3. Espandi la sezione Tag di inclusione/esclusione. Scegli Aggiungi tag.
4. Scegli Tag di esclusione, quindi Conferma.
5. Specifica la coppia di **`Key`** e **`Value`** del tag che desideri escludere. Fornire il **`Value`** è facoltativo. Dopo aver aggiunto tutti i tag, scegli Salva.

   > **Important**
   >
   > Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta Restrizioni relative ai tag nella Amazon EC2 User Guide o Restrizioni sui tag nella Amazon EC2 User Guide.

   Se non viene fornito un valore per una chiave e l'EC2istanza è etichettata con la chiave specificata, questa EC2 istanza verrà esclusa dal processo di scansione antimalware GuardDuty avviato, indipendentemente dal valore assegnato al tag.

API/CLI

- Aggiorna le impostazioni di scansione antimalware escludendo un'EC2istanza o un carico di lavoro del contenitore dal processo di scansione.

  Il comando di AWS CLI esempio seguente aggiunge un nuovo tag all'elenco dei tag di esclusione. Assicurati di sostituire l'esempio *`detector-id`* con il tuo validodetectorId.

  `MapEquals` è un elenco di coppie `Key`/`Value`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il 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**
>
> Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta Restrizioni relative ai tag nella Amazon EC2 User Guide o Restrizioni sui tag nella Amazon EC2 User Guide.

Per includere le EC2 istanze nella scansione antimalware

Se desideri scansionare un'EC2istanza, aggiungi il relativo tag all'elenco di inclusione. Quando aggiungi un tag a un elenco di tag di inclusione, un'EC2istanza che non contiene nessuno dei tag aggiunti viene ignorata dalla scansione antimalware. Se aggiungi più tag all'elenco dei tag di inclusione, un'EC2istanza che contiene almeno uno di questi tag viene inclusa nella scansione antimalware. A volte, un'EC2istanza può essere ignorata durante il processo di scansione. Per ulteriori informazioni, consulta Motivi per cui una risorsa viene ignorata durante la scansione malware.

Scegliete il metodo di accesso preferito per aggiungere un tag associato a un'EC2istanza a un elenco di inclusione.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, in Piani di protezione, scegli Malware Protection for EC2.
3. Espandi la sezione Tag di inclusione/esclusione. Scegli Aggiungi tag.
4. Scegli Tag di inclusione, quindi Conferma.
5. Scegli Aggiungi nuovo tag di inclusione e specifica la coppia di **`Key`** e **`Value`** del tag che desideri includere. Fornire il **`Value`** è facoltativo.

   Dopo aver aggiunto tutti i tag di inclusione, scegli Salva.

Se non viene fornito un valore per una chiave, un'EC2istanza viene contrassegnata con la chiave specificata, l'EC2istanza verrà inclusa nel processo di EC2 scansione di Malware Protection for Scan, indipendentemente dal valore assegnato al tag.

API/CLI

- Aggiorna le impostazioni di scansione antimalware per includere un'EC2istanza o un carico di lavoro del contenitore nel processo di scansione.

  Il comando di AWS CLI esempio seguente aggiunge un nuovo tag all'elenco dei tag di inclusione. Assicuratevi di sostituire l'esempio *`detector-id`* con il tuo validodetectorId. Sostituisci l'esempio *`TestKey`* e *`TestValue`* con la `Value` coppia `Key` e del tag associata alla tua EC2 risorsa.

  `MapEquals` è un elenco di coppie `Key`/`Value`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il 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

  Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta Restrizioni relative ai tag nella Amazon EC2 User Guide o Restrizioni sui tag nella Amazon EC2 User Guide.

Note

Potrebbero essere necessari fino a 5 minuti GuardDuty per rilevare un nuovo tag.

In qualsiasi momento, puoi scegliere tra i Tag di inclusione o i Tag di esclusione, ma non entrambi. Se desideri passare da un tag all'altro, sceglilo dal menu a discesa quando aggiungi nuovi tag e Conferma la selezione. Questa operazione cancella tutti i tag correnti.

Tag **`GuardDutyExcluded`** globale

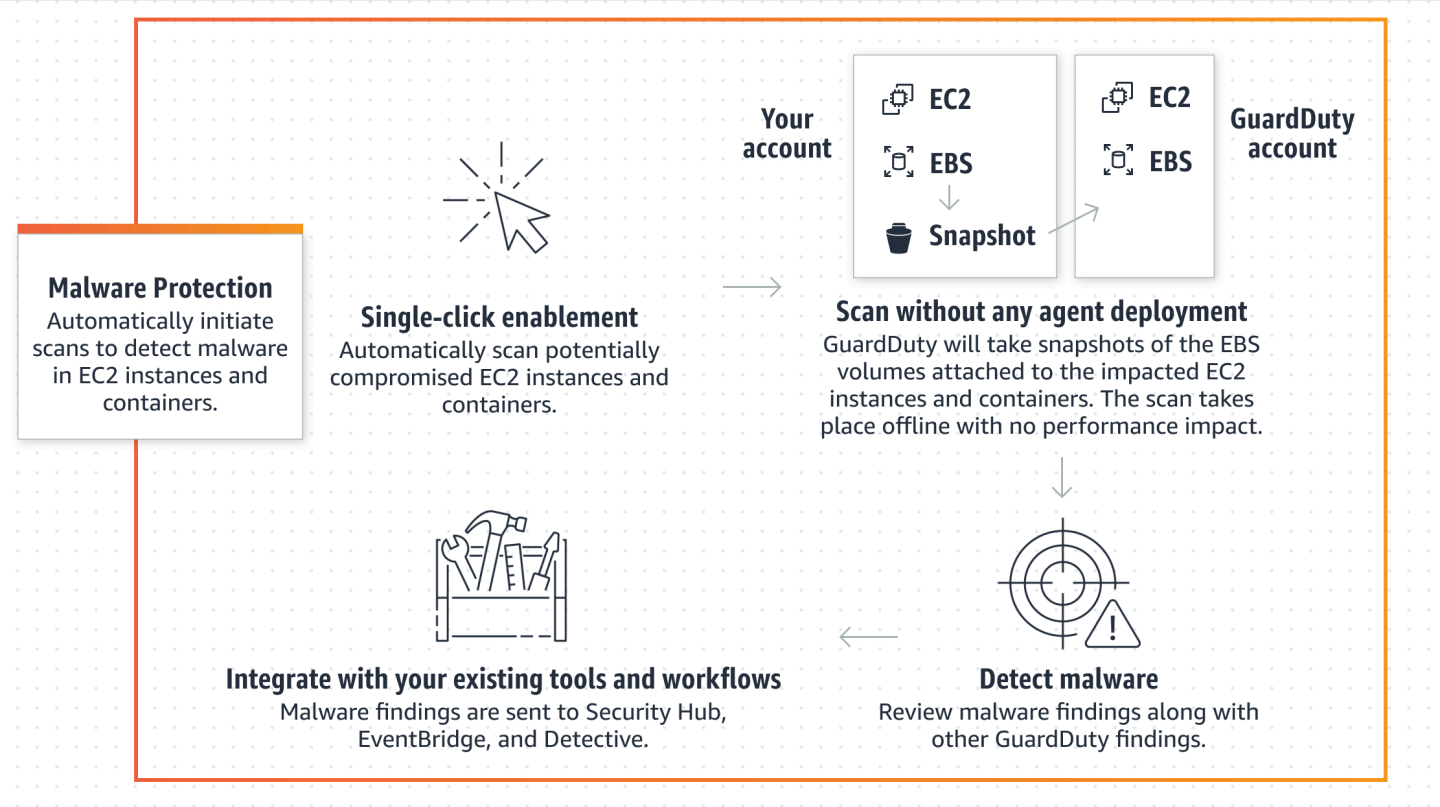
Per impostazione predefinita, le istantanee dei EBS volumi vengono create con un `GuardDutyScanId` tag. Non rimuovete questo tag perché così facendo si GuardDuty impedirà l'accesso alle istantanee. Entrambi i tipi di scansione in Malware Protection for EC2 non eseguono la scansione EC2 delle istanze Amazon o EBS dei volumi Amazon con il `GuardDutyExcluded` tag impostato `true` su. Se una protezione da malware EC2 esegue la scansione di una risorsa di questo tipo, verrà generato un ID di scansione, ma la scansione verrà ignorata indicando un `EXCLUDED_BY_SCAN_SETTINGS` motivo. Per ulteriori informazioni, consulta Motivi per cui una risorsa viene ignorata durante la scansione malware.

GuardDuty-scansione antimalware avviata

Con la scansione antimalware GuardDuty avviata, ogni volta che GuardDuty rileva un'attività dannosa che indica la potenziale presenza di malware nell'EC2istanza Amazon o nel container e GuardDuty generaRisultati che richiamano la scansione GuardDuty antimalware avviata, avvia GuardDuty automaticamente una scansione senza agenti sui volumi Amazon Elastic Block Store (AmazonEBS) collegati all'istanza o al carico di lavoro del contenitore EC2 Amazon potenzialmente interessato per rilevare la presenza di malware. Grazie alle opzioni di scansione, puoi aggiungere tag di inclusione associati alle risorse che desideri scansionare o aggiungere tag di esclusione associati alle risorse che desideri ignorare durante il processo di scansione. L'avvio automatico della scansione terrà sempre sconto delle opzioni di scansione. Puoi anche scegliere di attivare l'impostazione di conservazione delle istantanee per conservare le istantanee dei tuoi EBS volumi solo se Malware Protection for EC2 rileva la presenza di malware. Per ulteriori informazioni, consulta Personalizzazioni nella protezione da malware per EC2.

Per ogni EC2 istanza e carico di lavoro di container Amazon per cui vengono GuardDuty generati risultati, viene richiamata una scansione antimalware GuardDuty avviata automaticamente una volta ogni 24 ore. Per informazioni su come vengono scansionati EBS i volumi Amazon collegati al carico di lavoro dell'EC2istanza Amazon o del container, consulta. Funzionalità di protezione da malware per EC2

L'immagine seguente descrive come funziona la scansione GuardDuty antimalware avviata.



Per informazioni sulla metodologia di rilevamento del GuardDuty malware e sui motori di scansione utilizzati, vedere. GuardDuty motore di scansione per il rilevamento di malware

Quando viene rilevato un malware, GuardDuty generaProtezione da malware per tipi di ricerca EC2. Se GuardDuty non genera un risultato indicativo della presenza di malware sulla stessa risorsa, non verrà richiamata alcuna scansione antimalware GuardDuty avviata. Puoi anche avviare una scansione antimalware on demand sulla stessa risorsa. Per ulteriori informazioni, consulta Scansione antimalware on demand.

Prova gratuita di 30 giorni

Puoi scegliere di abilitare o disabilitare la scansione antimalware GuardDuty avviata per un accesso supportato Account AWS in qualsiasi Regione AWS momento. Se hai un'organizzazione, ogni account membro ha la propria prova gratuita di 30 giorni.

Per capire come funziona la prova gratuita di 30 giorni, considera i seguenti scenari:

- Quando si abilita GuardDuty per la prima volta (nuovo GuardDuty account), viene abilitata anche la scansione antimalware GuardDuty avviata, inclusa nella versione di prova gratuita di 30 giorni associata al servizio. GuardDuty

- Un GuardDuty account esistente può abilitare la scansione antimalware GuardDuty avviata per la prima volta con una prova gratuita di 30 giorni. Quando attivi questa funzionalità in un'altra regione per la prima volta, riceverai una prova gratuita di 30 giorni in quella regione.
- Se disponi già di un GuardDuty account che utilizza Malware Protection da EC2 prima che venisse annunciata la scansione antimalware su richiesta e tale GuardDuty account utilizza già il relativo modello di prezzo Regione AWS, puoi continuare a utilizzare GuardDuty -initiated malware scan.

> **Note**
>
> Anche se è in corso un periodo di prova gratuito di 30 giorni, si applicano i costi di utilizzo standard per la creazione e la conservazione degli snapshot dei EBS volumi Amazon. Per ulteriori informazioni, consulta i EBSprezzi di Amazon.

Per informazioni sull'attivazione della scansione antimalware GuardDuty avviata, consulta. Configurazione della scansione antimalware avviata GuardDuty

Configurazione della scansione antimalware avviata GuardDuty

Configurazione della scansione GuardDuty antimalware avviata per un account indipendente

Per gli account associati a AWS Organizations, è possibile automatizzare questo processo tramite le impostazioni della console, come descritto nella sezione successiva.

Per abilitare o disabilitare la scansione GuardDuty antimalware avviata

Scegli il tuo metodo di accesso preferito per configurare la scansione antimalware GuardDuty avviata per un account autonomo.

Console

1. Apri la console all' GuardDuty indirizzo. https://console.aws.amazon.com/guardduty/
2. Nel riquadro di navigazione, in Piani di protezione, scegli Malware Protection for EC2.
3. Il EC2 riquadro Malware Protection for elenca lo stato attuale della scansione antimalware GuardDuty avviata per il tuo account. Puoi abilitarla o disabilitarla in qualsiasi momento selezionando rispettivamente Abilita o Disabilita.

4. Seleziona Salva.

API/CLI

- Esegui l'updateDetectorAPIoperazione utilizzando il tuo ID di rilevamento regionale e passando l'`dataSources`oggetto con `EbsVolumes` set to o. `true` `false`

  È inoltre possibile abilitare o disabilitare GuardDuty -initiated malware scan utilizzando gli strumenti della riga di AWS comando eseguendo il comando seguente. AWS CLI Assicurati di usare il tuo codice valido *`detector ID`*.

  > **Note**
  >
  > Il codice di esempio seguente abilita la scansione antimalware GuardDuty avviata dall'utente. Per disabilitarla, sostituisci `true` con `false`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

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

Configurazione della scansione antimalware GuardDuty avviata in ambienti con più account

In un ambiente con più account, solo gli account di GuardDuty amministratore possono configurare la scansione antimalware avviata. GuardDuty GuardDuty gli account amministratore possono abilitare o disabilitare l'uso della scansione antimalware GuardDuty avviata da un utente per i propri account membri. Una volta che l'account amministratore ha configurato GuardDuty -initiated malware scan per un account membro, l'account membro seguirà le impostazioni dell'account amministratore e non potrà modificare tali impostazioni tramite la console. GuardDuty gli account amministratore che gestiscono i propri account membri con AWS Organizations supporto possono scegliere di abilitare automaticamente la scansione antimalware GuardDuty avviata su tutti gli account esistenti e nuovi dell'organizzazione. Per ulteriori informazioni, consulta Gestione GuardDuty degli account con AWS Organizations.

Stabilire un accesso affidabile per abilitare la scansione GuardDuty antimalware avviata

Se l'account amministratore GuardDuty delegato non è lo stesso dell'account di gestione dell'organizzazione, l'account di gestione deve abilitare la scansione antimalware GuardDuty avviata dall'organizzazione. In questo modo, l'account amministratore delegato può creare gli account dei membri Autorizzazioni di ruolo collegate al servizio per Malware Protection for EC2 interni gestiti tramite. AWS Organizations

> **Note**
>
> Prima di designare un account GuardDuty amministratore delegato, consulta. Considerazioni e raccomandazioni

Scegliete il metodo di accesso preferito per consentire all'account GuardDuty amministratore delegato di abilitare la scansione antimalware GuardDuty avviata dagli account dei membri dell'organizzazione.

Console

1. Apri la console all' GuardDuty indirizzo. https://console.aws.amazon.com/guardduty/

   Per accedere, utilizza l'account di gestione della tua AWS Organizations organizzazione.

2. a. Se non hai designato un account GuardDuty amministratore delegato, allora:

      Nella pagina Impostazioni, in Account GuardDuty amministratore delegato, inserisci le 12 cifre **`account ID`** che desideri designare per amministrare la politica nella tua organizzazione. GuardDuty Scegli Delega.

   b. i. Se hai già designato un account GuardDuty amministratore delegato diverso dall'account di gestione, allora:

         Nella pagina Impostazioni, in Amministratore delegato, attiva l'impostazione Autorizzazioni. Questa azione consentirà all'account GuardDuty amministratore delegato di allegare le autorizzazioni pertinenti agli account dei membri e di abilitare la scansione antimalware GuardDuty avviata in tali account membro.

      ii. Se hai già designato un account GuardDuty amministratore delegato uguale all'account di gestione, puoi abilitare direttamente la scansione GuardDuty antimalware avviata per gli account dei membri. Per ulteriori informazioni, consulta

Attiva automaticamente la scansione antimalware GuardDuty avviata per tutti gli account dei membri.

> **Tip**
>
> Se l'account GuardDuty amministratore delegato è diverso dal tuo account di gestione, devi fornire le autorizzazioni all'account GuardDuty amministratore delegato per consentire l'attivazione della scansione GuardDuty antimalware avviata per gli account dei membri.

3. Se desideri consentire all'account GuardDuty amministratore delegato di abilitare la scansione antimalware GuardDuty avviata per gli account dei membri in altre regioni, modifica la tua e ripeti i passaggi precedenti. Regione AWS

API/CLI

1. Esegui il comando segunte tramite le credenziali dell'account di gestione:

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (Facoltativo) per abilitare la scansione antimalware GuardDuty avviata dall'account di gestione che non è un account amministratore delegato, l'account di gestione la creerà prima Autorizzazioni di ruolo collegate al servizio per Malware Protection for EC2 esplicitamente nel proprio account, quindi abiliterà la scansione antimalware GuardDuty avviata dall'account amministratore delegato, in modo analogo a qualsiasi altro account membro.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. L'account amministratore delegato è stato designato nell'account attualmente selezionato GuardDuty . Regione AWS Se hai designato un account come account GuardDuty amministratore delegato in una regione, quell'account deve essere il tuo account GuardDuty amministratore delegato in tutte le altre regioni. Ripeti la fase precedente per tutte le altre regioni.

Configurazione della scansione GuardDuty antimalware avviata per l'account amministratore delegato GuardDuty

Scegliete il metodo di accesso preferito per abilitare o disabilitare la scansione antimalware GuardDuty avviata per un account amministratore delegato. GuardDuty

Console

1. Apri la console all' GuardDuty indirizzo. https://console.aws.amazon.com/guardduty/

   Assicurati di utilizzare le credenziali dell'account di gestione.
2. Nel riquadro di navigazione, scegli Malware Protection for EC2.
3. Nella EC2 pagina Malware Protection for, scegli Modifica accanto a GuardDuty-initiated malware scan.
4. Esegui una di queste operazioni:

   Utilizzando Abilita per tutti gli account

   - Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi nell' AWS organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
   - Seleziona Salva.

   Utilizzando Configura gli account manualmente

   - Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
   - Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
   - Seleziona Salva.

API/CLI

Esegui l'updateDetectorAPIoperazione utilizzando il tuo ID regionale del rilevatore e passando l'`features`oggetto `name` come `EBS_MALWARE_PROTECTION` e `status` come `ENABLED` o. `DISABLED`

È possibile abilitare o disabilitare GuardDuty -initiated malware scan eseguendo il comando seguente. AWS CLI Assicurati di utilizzare un account di GuardDuty amministratore delegato valido *detector ID*.

> **Note**
>
> Il codice di esempio seguente abilita la scansione GuardDuty antimalware avviata dall'utente. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Attiva automaticamente la scansione antimalware GuardDuty avviata per tutti gli account dei membri

Scegli il metodo di accesso preferito per abilitare la funzionalità di scansione antimalware GuardDuty avviata per tutti gli account membri. inclusi gli account membri esistenti e i nuovi account che entrano a far parte dell'organizzazione.

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una di queste operazioni:

   Utilizzo della pagina Malware Protection for EC2

   1. Nel riquadro di navigazione, scegli Protezione da malware per EC2.
   2. Nella EC2 pagina Malware Protection for, scegli Modifica nella sezione GuardDuty - initiated malware scan.

3. Scegli Abilita per tutti gli account. Questa azione abilita automaticamente la scansione antimalware GuardDuty avviata sia per gli account esistenti che per quelli nuovi dell'organizzazione.
4. Seleziona Salva.

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di attivazione automatica, scegli Abilita per tutti gli account sottoposti alla scansione GuardDutyantimalware avviata.
4. Nella EC2 pagina Protezione da malware per, scegli Modifica nella sezione GuardDuty - initiated malware scan.
5. Scegli Abilita per tutti gli account. Questa azione abilita automaticamente la scansione antimalware GuardDuty avviata sia per gli account esistenti che per quelli nuovi dell'organizzazione.
6. Seleziona Salva.

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.

3. Nella finestra Gestisci le preferenze di attivazione automatica, scegli Abilita per tutti gli account sottoposti alla scansione GuardDutyantimalware avviata.
4. Seleziona Salva.

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta Abilita o disabilita in modo selettivo la scansione antimalware GuardDuty avviata dagli account dei membri.

API/CLI

- Per abilitare o disabilitare in modo selettivo la scansione antimalware GuardDuty avviata per i tuoi account membri, richiama l'operazione utilizzando la tua updateMemberDetectorsAPI *`detector ID`*.
- L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata da un solo utente. Per disabilitare un account membro, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

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

  Puoi anche passare un elenco di account IDs separati da uno spazio.
- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita la scansione antimalware GuardDuty avviata per tutti gli account dei membri attivi esistenti

Scegliete il metodo di accesso preferito per abilitare la scansione antimalware GuardDuty avviata per tutti gli account dei membri attivi esistenti nell'organizzazione.

Per configurare la scansione antimalware GuardDuty avviata per tutti gli account dei membri attivi esistenti

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, scegli Malware Protection for. EC2
3. In Malware Protection for EC2, puoi visualizzare lo stato corrente della configurazione di scansione antimalware GuardDuty avviata. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Seleziona Salva.

Attiva automaticamente la scansione GuardDuty antimalware avviata per gli account dei nuovi membri

Gli account membri appena aggiunti devono essere abilitati GuardDuty prima di selezionare la configurazione GuardDuty della scansione antimalware avviata. Gli account membri gestiti su invito possono configurare manualmente la scansione antimalware GuardDuty avviata per i propri account. Per ulteriori informazioni, consulta Step 3 - Accept an invitation.

Scegliete il metodo di accesso preferito per abilitare la scansione antimalware GuardDuty avviata dai nuovi account che entrano a far parte della vostra organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare la scansione antimalware GuardDuty avviata per gli account di nuovi membri di un'organizzazione, utilizzando la pagina Malware Protection for o Accounts. EC2

Per abilitare automaticamente la scansione antimalware GuardDuty avviata per i nuovi account dei membri

1. Apri la console all' GuardDuty indirizzo. https://console.aws.amazon.com/guardduty/

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Esegui una di queste operazioni:

- Utilizzo della pagina Malware Protection for EC2:

  1. Nel riquadro di navigazione, scegli Protezione da malware per EC2.
  2. Nella EC2 pagina Protezione da malware per, scegli Modifica nella scansione antimalware GuardDuty avviata.
  3. Scegli Configura gli account manualmente.
  4. Seleziona Abilita automaticamente per i nuovi account membri. Questo passaggio garantisce che ogni volta che un nuovo account si unisce alla tua organizzazione, la scansione antimalware GuardDuty avviata venga automaticamente abilitata per tale account. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
  5. Seleziona Salva.

- Utilizzando la pagina Account:

  1. Dal riquadro di navigazione, selezionare Accounts (Account).
  2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
  3. Nella finestra Gestisci le preferenze di attivazione automatica, seleziona Abilita per nuovi account nella sezione GuardDuty-initiated malware scan.
  4. Seleziona Salva.

API/CLI

- Per abilitare o disabilitare la scansione antimalware GuardDuty avviata per gli account di nuovi membri, richiama l'operazione utilizzando la tua UpdateOrganizationConfigurationAPI *`detector ID`*.
- L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata da un solo utente. Per disabilitarlo, consulta Abilita o disabilita in modo selettivo la scansione antimalware GuardDuty avviata dagli account dei membri. Se non desideri abilitarlo per tutti i nuovi account che entrano a far parte dell'organizzazione, imposta `AutoEnable` su `NONE`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

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

Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita o disabilita in modo selettivo la scansione antimalware GuardDuty avviata dagli account dei membri

Scegli il tuo metodo di accesso preferito per configurare selettivamente la scansione antimalware GuardDuty avviata per gli account dei membri.

Console

1. Apri la console all' GuardDuty indirizzo. https://console.aws.amazon.com/guardduty/
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Nella pagina Account, controlla lo stato del tuo account membro nella colonna «GuardDutyInitiated Malware Scan».
4. Seleziona l'account per il quale desideri configurare GuardDuty -initiated malware scan. Puoi selezionare più account alla volta.
5. Dal menu Modifica piani di protezione, scegli l'opzione appropriata per GuardDuty-initiated malware scan.

API/CLI

Per abilitare o disabilitare in modo selettivo la scansione antimalware GuardDuty avviata dagli account dei membri, richiamate l'operazione utilizzando la vostra updateMemberDetectorsAPI *`detector ID`*.

L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata da un solo utente. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

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

> **Note**
>
> Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Per abilitare o disabilitare in modo selettivo la scansione antimalware GuardDuty avviata per i tuoi account membri, esegui l'updateMemberDetectorsAPIoperazione utilizzando la tua *`detector ID`*. L'esempio seguente mostra come abilitare la scansione antimalware GuardDuty avviata da un singolo account membro. Per disabilitarla, sostituisci `true` con `false`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

> **Note**
>
> Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita la scansione antimalware GuardDuty avviata per gli account esistenti nell'organizzazione gestiti tramite invito

Il ruolo GuardDuty Malware Protection for EC2 service-linked (SLR) deve essere creato negli account dei membri. L'account amministratore non può abilitare la funzionalità di scansione antimalware GuardDuty avviata da. AWS Organizations

Attualmente, è possibile eseguire i seguenti passaggi tramite la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/per abilitare la scansione antimalware GuardDuty avviata dagli account membri esistenti.

Console

1. Apri la console all' GuardDuty indirizzo. https://console.aws.amazon.com/guardduty/

   Accedi utilizzando le credenziali del tuo account amministratore.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Seleziona l'account membro per il quale desideri abilitare la scansione GuardDuty antimalware avviata. Puoi selezionare più account alla volta.
4. Scegli Azioni.
5. Scegli Disassocia membro.
6. Nel tuo account membro, nel riquadro di navigazione, scegli Protezione da malware in Piani di protezione.
7. Scegli Abilita la scansione GuardDuty antimalware avviata. GuardDuty ne creerà uno SLR per l'account del membro. Per ulteriori informazioni suSLR, vedereAutorizzazioni di ruolo collegate al servizio per Malware Protection for EC2.
8. Nel tuo account amministratore, scegli Account nel riquadro di navigazione.
9. Scegli l'account membro da aggiungere nuovamente all'organizzazione.
10. Scegli Operazioni, quindi Aggiungi membro.

API/CLI

1. Utilizza l'account amministratore per eseguire l'esecuzione DisassociateMembersAPIsugli account dei membri che desiderano abilitare la scansione GuardDuty antimalware avviata.
2. Usa il tuo account membro per invocare e UpdateDetectorabilitare la scansione GuardDuty antimalware avviata.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. Utilizza l'account amministratore per eseguire l'CreateMembersAPIoperazione per aggiungere nuovamente il membro all'organizzazione.

Risultati che richiamano la scansione GuardDuty antimalware avviata

Una scansione antimalware GuardDuty avviata viene richiamata quando GuardDuty rileva comportamenti sospetti indicativi di malware sui carichi di lavoro di istanze o container di AmazonEC2.

- 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 (solo in uscita)

- 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 (solo in uscita)
- UnauthorizedAccess:EC2/SSHBruteForce (solo in uscita)
- 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

Scansione antimalware on demand

La scansione antimalware su richiesta ti aiuta a rilevare la presenza di malware sui volumi di Amazon Elastic Block Store (AmazonEBS) collegati alle tue EC2 istanze Amazon. Senza necessità di configurazione, puoi avviare una scansione antimalware su richiesta fornendo l'Amazon Resource Name (ARN) dell'EC2istanza Amazon che desideri scansionare. Puoi avviare una scansione antimalware su richiesta tramite la console o. GuardDuty API Prima di avviare una scansione antimalware on demand, puoi impostare l'impostazione di Conservazione degli snapshot che preferisci. I seguenti scenari possono aiutarti a identificare quando utilizzare il tipo di scansione antimalware On-demand con: GuardDuty

- Vuoi rilevare la presenza di malware nelle tue EC2 istanze Amazon senza abilitare la scansione GuardDuty antimalware avviata.
- Hai abilitato la scansione antimalware GuardDuty avviata e una scansione è stata richiamata automaticamente. Dopo aver eseguito la correzione consigliata per il tipo di protezione antimalware generato, se desideri avviare una scansione sulla stessa risorsa, puoi avviare una scansione antimalware su richiesta dopo che è trascorsa 1 ora dall'ora di inizio della scansione precedente. EC2

  Per la scansione antimalware on demand non è necessario che siano trascorse 24 ore dal momento in cui è stata avviata la scansione precedente. Deve trascorrere 1 ora prima di avviare una scansione antimalware on demand sulla stessa risorsa. Per evitare di duplicare una scansione

antimalware sulla stessa istanza, consulta. EC2 Scansionare nuovamente la stessa istanza Amazon EC2

> **Note**
>
> La scansione antimalware su richiesta non è inclusa nel periodo di prova gratuito di 30 giorni con. GuardDuty Il costo di utilizzo si applica al EBS volume totale di Amazon scansionato per ogni scansione di malware. Per ulteriori informazioni, consulta i GuardDuty prezzi di Amazon. Per informazioni sui costi di creazione degli snapshot dei EBS volumi Amazon e sulla loro conservazione, consulta i EBSprezzi di Amazon.

Come funziona la scansione antimalware on demand

Con On-demand Malware Scan, puoi avviare una richiesta di scansione antimalware per la tua EC2 istanza Amazon anche quando è attualmente in uso. Dopo aver avviato una scansione antimalware On-demand, GuardDuty crea istantanee dei EBS volumi Amazon collegati all'istanza Amazon il EC2 cui Amazon Resource Name (ARN) è stato fornito per la scansione. Successivamente, GuardDuty condivide queste istantanee con. GuardDuty account di servizio GuardDuty crea EBS volumi di replica crittografati da tali istantanee nell'account del GuardDuty servizio. Per ulteriori informazioni su come vengono scansionati EBS i volumi Amazon, consultaVolume Elastic Block Storage (EBS).

> **Note**
>
> GuardDuty crea le istantanee dei dati che sono già stati scritti nei EBS volumi Amazon al momento dell' point-in-time avvio di una scansione antimalware On-demand.

Se viene rilevato del malware e hai abilitato l'impostazione di conservazione delle istantanee, le istantanee del EBS volume vengono automaticamente conservate nel tuo. Account AWS La scansione antimalware on demand genera Protezione da malware per tipi di ricerca EC2. Se non viene rilevato malware, indipendentemente dall'impostazione di conservazione delle istantanee, le istantanee dei volumi vengono eliminate. EBS

Per impostazione predefinita, le istantanee dei EBS volumi vengono create con un tag. `GuardDutyScanId` Non rimuovete questo tag perché così facendo si GuardDuty impedirà l'accesso alle istantanee. Entrambi i tipi di scansione in Malware Protection for EC2 non eseguono

la scansione EC2 delle istanze Amazon o EBS dei volumi Amazon con il `GuardDutyExcluded` tag impostato `true` su. Se una protezione da malware EC2 esegue la scansione di una risorsa di questo tipo, verrà generato un ID di scansione, ma la scansione verrà ignorata indicando un `EXCLUDED_BY_SCAN_SETTINGS` motivo. Per ulteriori informazioni, consulta Motivi per cui una risorsa viene ignorata durante la scansione malware.

AWS Organizations politica di controllo del servizio: accesso negato

Utilizzando le policy di controllo del servizio (SCPs) in AWS Organizations, l'account GuardDuty amministratore delegato può limitare le autorizzazioni e negare azioni come l'avvio di una scansione antimalware su richiesta per l'EC2istanza Amazon di proprietà dei tuoi account.

In qualità di account GuardDuty membro, quando avvii una scansione antimalware su richiesta per le tue EC2 istanze Amazon, potresti ricevere un errore. Puoi connetterti all'account di gestione per capire perché SCP è stato configurato un account per il tuo account membro. Per ulteriori informazioni, consulta SCPeffetti sulle autorizzazioni.

Nozioni di base sulla scansione antimalware on demand

In qualità di account GuardDuty amministratore, puoi avviare una scansione antimalware su richiesta per conto dei tuoi account membri attivi che hanno i seguenti prerequisiti impostati nei rispettivi account. Gli account autonomi e gli account membro attivi GuardDuty possono anche avviare una scansione antimalware su richiesta per le proprie istanze Amazon. EC2

Prerequisiti

- GuardDuty deve essere abilitato nel punto in Regioni AWS cui desideri avviare la scansione antimalware su richiesta.
- Assicurati che AWS politica gestita: AmazonGuardDutyFullAccess sia collegato all'IAMutente o al IAM ruolo. Avrai bisogno della chiave di accesso e della chiave segreta associate all'IAMutente o al IAM ruolo.
- In qualità di account GuardDuty amministratore delegato, hai la possibilità di avviare una scansione antimalware su richiesta per conto di un account membro attivo.
- Se sei un account membro che non dispone diAutorizzazioni di ruolo collegate al servizio per Malware Protection for EC2, l'avvio di una scansione antimalware su richiesta per un'EC2istanza Amazon che appartiene al tuo account creerà automaticamente la funzione di protezione da malware SLR per. EC2

> **Important**
>
> Assicurati che nessuno elimini le SLRautorizzazioni per Malware Protection per EC2 quando la scansione antimalware, GuardDuty avviata o su richiesta, è ancora in corso. Ciò impedirebbe il corretto completamento della scansione e comprometterebbe la precisione dell'esito.

Prima di avviare una scansione antimalware on demand, assicurati che non sia stata avviata alcuna scansione sulla stessa risorsa nell'ultima ora, altrimenti verrà duplicata. Per ulteriori informazioni, consulta Esecuzione di una nuova scansione della stessa risorsa.

Avvio della scansione antimalware on demand

Scegli il metodo di accesso che preferisci per avviare una scansione antimalware on demand.

Console

1. Apri la console all'indirizzo. GuardDuty https://console.aws.amazon.com/guardduty/
2. Avvia la scansione utilizzando una delle opzioni seguenti:
   a. Utilizzo della EC2 pagina Malware Protection for:
      i. Nel riquadro di navigazione, in Piani di protezione, scegli Protezione da malware per EC2.
      ii. Nella EC2 pagina Malware Protection for, fornisci l'EC2istanza Amazon ARN [1] per la quale desideri avviare la scansione.
   b. Utilizzando la pagina Scansioni malware:
      i. Nel riquadro di navigazione, scegli Scansioni malware.
      ii. Scegli Avvia scansione su richiesta e fornisci l'EC2istanza Amazon ARN [1] per la quale desideri avviare la scansione.
      iii. Se si tratta di una nuova scansione, seleziona un ID di EC2 istanza Amazon nella pagina Malware Scans.

      Espandi il menu a discesa Avvia scansione on demand e scegli Esegui nuovamente la scansione dell'istanza selezionata.

3. Dopo aver avviato correttamente una scansione utilizzando uno dei due metodi, viene generato un ID che può essere utilizzato per tenere traccia dello stato di avanzamento della scansione. Per ulteriori informazioni, consulta Monitoraggio dello stato e del risultato delle scansioni malware.

API/CLI

Invoke StartMalwareScanthat accetta l'`resourceArn`EC2istanza Amazon [1] per la quale desideri avviare una scansione antimalware su richiesta.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

Dopo aver avviato correttamente una scansione, `StartMalwareScan` restituisce uno `scanId`. Invoke DescribeMalwareScansmonitora l'avanzamento della scansione avviata.

[1] Per informazioni sul formato della tua EC2 istanza AmazonARN, consulta Amazon Resource Name (ARN). Per EC2 le istanze Amazon, puoi utilizzare il seguente ARN formato di esempio sostituendo i valori per la partizione, la regione, l'ID e l' Account AWS ID dell'EC2istanza Amazon. Per informazioni sulla lunghezza dell'ID dell'istanza, consulta Resource. IDs

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

Scansionare nuovamente la stessa istanza Amazon EC2

Indipendentemente dal fatto che una scansione sia GuardDuty avviata o su richiesta, puoi avviare una nuova scansione antimalware su richiesta sulla stessa EC2 istanza dopo 1 ora dall'inizio della scansione antimalware precedente. Se la nuova scansione malware viene avviata entro 1 ora dall'avvio della scansione antimalware precedente, la richiesta genererà il seguente errore e non verrà generato alcun ID di scansione.

```
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.
```

Per informazioni su come avviare una nuova scansione sulla stessa risorsa, consulta Avvio della scansione antimalware on demand.

Per monitorare lo stato delle scansioni malware, consulta Monitoraggio degli stati e dei risultati della scansione in Malware Protection for GuardDuty EC2.

Monitoraggio degli stati e dei risultati della scansione in Malware Protection for GuardDuty EC2

È possibile monitorare lo stato di scansione di ogni GuardDuty Malware Protection per la EC2 scansione. I valori possibili per lo Stato delle scansioni sono `Completed`, `Running`, `Skipped` e `Failed`.

Al termine della scansione, il Risultato della scansione viene compilato per le scansioni con lo Stato corrispondente a `Completed`. I valori possibili per il Risultato della scansione sono `Clean` e `Infected`. Tramite il Tipo di scansione, puoi identificare se la scansione malware era `GuardDuty initiated` or `On demand`.

I risultati di ogni scansione malware vengono conservati per 90 giorni. Scegli il metodo di accesso che preferisci per monitorare lo stato della scansione malware.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Scansioni malware.
3. Puoi filtrare le scansioni malware in base alle seguenti Proprietà disponibili nei criteri di filtro.

   - ID scansione
   - ID account
   - EC2istanza ARN
   - Tipo di scansione
   - Stato della scansione

   Per informazioni sulle proprietà utilizzate per i criteri di filtro, consulta Dettagli degli esiti.

API/CLI

- Dopo che la scansione ha prodotto un risultato, puoi filtrare le scansioni malware sulla base di `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` e `SCAN_START_TIME`.

  I criteri di `GUARDDUTY_FINDING_ID` filtro sono disponibili quando `SCAN_TYPE` viene GuardDuty avviato. Per informazioni su qualsiasi criterio di filtro, consulta Dettagli degli esiti.

- È possibile modificare l'esempio *filter-criteria* nel comando seguente. Attualmente, puoi applicare filtri utilizzando una `CriterionKey` alla volta. Le opzioni per la `CriterionKey` sono `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` e `SCAN_START_TIME`.

  Se usi lo stesso di `CriterionKey` seguito, assicurati di sostituire l'esempio `EqualsValue` con il tuo valido AWS *scan-id*.

  Sostituisci il `detector-id` di esempio con il tuo *detector-id* valido. È possibile modificare il *max-results* (fino a 50) e il *sort-criteria*. `AttributeName`È obbligatorio e deve esserlo`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"}}] }'
  ```

- La risposta di questo comando mostra al massimo un risultato contenente i dettagli sulla risorsa interessata e sugli esiti relativi ai malware (se `Infected`).

GuardDuty account di servizio di Regione AWS

Quando un'istantanea viene creata e condivisa con un account di GuardDuty servizio, nei CloudTrail registri viene creato un nuovo evento. Questo evento specifica l'`snapshotId`and `userId` (account di GuardDuty servizio corrispondente). Regione AWS Per ulteriori informazioni, consulta Funzionalità di protezione da malware per EC2.

L'esempio seguente è un frammento di un CloudTrail evento che mostra il corpo della richiesta: `ModifySnapshotAttribute`

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
```

```
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

La tabella seguente mostra gli account GuardDuty di servizio per ogni regione. `userId`È l'account del GuardDuty servizio e dipende dalla regione selezionata.

Regione AWS	Codice regione	GuardDuty ID dell'account di servizio (**`userId`**)
Stati Uniti orientali (Virginia settentrionale)	us-east-1	652050842985
Stati Uniti orientali (Ohio)	us-east-2	178123968615
Stati Uniti occidentali (California settentrionale)	us-west-1	669213148797
US West (Oregon)	us-west-2	447226417196
Asia Pacifico (Mumbai)	ap-south-1	913179291432
Asia Pacifico (Osaka-Locale)	ap-northeast-3	089661699081
Asia Pacifico (Seoul)	ap-northeast-2	039163547507
Asia Pacifico (Tokyo)	ap-northeast-1	874749492622
Asia Pacifico (Singapore)	ap-southeast-1	247460962669
Asia Pacifico (Sydney)	ap-southeast-2	124839743349
Canada (Centrale)	ca-central-1	175877067165
Canada occidentale (Calgary)	ca-west-1	894794104037
Europa (Francoforte)	eu-central-1	002294850712

Regione AWS	Codice regione	GuardDuty ID dell'account di servizio (**`userId`**)
Europa (Irlanda)	eu-west-1	283769539786
Europa (Londra)	eu-west-2	310125036783
Europa (Parigi)	eu-west-3	866607715269
Europa (Stoccolma)	eu-north-1	693780578038
Cina (Pechino)	cn-north-1	448721096076
Cina (Ningxia)	cn-northwest-1	480864352451
Sud America (San Paolo)	sa-east-1	546914126324
Asia Pacifico (Hyderabad) (con consenso esplicito)	ap-south-2	682251015962
Asia Pacifico (Melbourne) (con consenso esplicito)	ap-southeast-4	353488359550
Europa (Spagna) (con consenso esplicito)	eu-south-2	936182149045
Europa (Zurigo) (con consenso esplicito)	eu-central-2	867642063380
Israele (Tel Aviv) (con consenso esplicito)	il-central-1	619233833001
Europa (Milano) (con consenso esplicito)	eu-south-1	977238331021
Asia Pacifico (Hong Kong) (con consenso esplicito)	ap-east-1	249472122084

Regione AWS	Codice regione	GuardDuty ID dell'account di servizio (**`userId`**)
Medio Oriente (Bahrein) (con consenso esplicito)	me-south-1	404001805210
Africa (Città del Capo) (con consenso esplicito)	af-south-1	957664736811
Asia Pacifico (Giacarta) (con consenso esplicito)	ap-southeast-3	452118225523
Medio Oriente () (Opt-in) UAE	me-central-1	828603743433

Protezione da malware per le quote EC2

Malware Protection for EC2 ha la seguente disponibilità predefinita delle varie risorse utilizzate dalla funzionalità.

Ambito	Predefinita	Commenti
Estrazione e analisi dei dati in file compressi o archiviati	5	Il numero massimo di livelli nidificati consentiti in un file archiviato.
Numero di file all'interno di un file archiviato	1000	Il numero massimo di file che possono essere scansiona ti all'interno di un archivio. Questo conteggio è la somma del numero di file estratti dall'archivio e del numero di file estratti da tutti gli archivi annidati.
Numero delle minacce	32	Il numero massimo di minacce che è possibile visualizzare

Ambito	Predefinita	Commenti
		nel pannello dei risultati. GuardDuty Malware Protection for EC2 potrebbe aver rilevato più nomi di minacce. Se il numero di nomi di minacce rilevate è superiore al valore predefinito, puoi visualizzare i JSON dettagli selezionando Finding ID sotto il nome del risultato nel pannello dei dettagli della GuardDuty console.
Numero di file per minaccia rilevata	5	Il numero massimo di file identificati per ogni minaccia rilevata. Ad esempio, se GuardDuty rileva 10 file associati a una singola minaccia, la minaccia mostrerà un massimo di 5 file.
EBSvolumi per scansione per istanza	11	Il numero massimo di EBS volumi che è GuardDuty possibile scansionare per EC2 istanza. Se ci sono più di 11 EBS volumi da scansionare, GuardDuty Malware Protection for li EC2 ordina `deviceName` alfabeticamente e seleziona i primi 11 volumi. EBS

Ambito	Predefinita	Commenti
Dimensione dei volumi EBS	2048 GB	Associato a un'EC2istanza Amazon e a un carico di lavoro di container, GuardDuty Malware Protection for EC2 può scansionare ogni EBS volume Amazon con dimensioni fino a 2048 GB. Questa quota si applica a tutti i paesi Regione AWS in cui EC2 è disponibile il supporto per Malware Protection for.
Tipi di file system supportati	GuardDuty Malware Protection for EC2 è in grado di eseguire la scansione dei seguenti tipi di file system: • File system di nuova tecnologia (NTFS) • File system X (XFS) • File System second extended (ext2) • File System fourth extended (ext4) • File system della tabella di allocazione dei file (FAT) • File system della tabella di allocazione dei file virtuale (VFAT)	N/D.

Ambito	Predefinita	Commenti
Tag delle opzioni di scansione	50	Il numero massimo dei tag delle risorse che puoi aggiungere per personalizzare l'impostazione delle opzioni di scansione malware. Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente.
Ritrovamento del periodo di conservazione	90	Il numero massimo di giorni in cui viene GuardDuty conservato un risultato. Per le informazioni più recenti, consulta GuardDuty Quote Amazon.
Periodo di conservazione delle scansioni malware	90	Il numero massimo di giorni in cui GuardDuty Malware Protection EC2 conserva la cronologia di una scansione. Per ulteriori informazioni sulla visualizzazione delle scansioni malware recenti, consulta Monitoraggio degli stati e dei risultati della scansione in Malware Protection for GuardDuty EC2.
Transazioni al secondo (TPS) per la scansione antimalware su richiesta	1	Il numero di richieste di scansione antimalware on demand che possono essere avviate al secondo in ciascuna regione.

Ambito	Predefinita	Commenti
Limite di burst per la scansione antimalware on demand	1	Il numero di richieste simultanee di scansione antimalware on demand che possono essere avviate al secondo in ciascuna regione.

GuardDuty Protezione da malware per S3

Malware Protection for S3 ti aiuta a rilevare la potenziale presenza di malware scansionando gli oggetti appena caricati nel bucket Amazon Simple Storage Service (Amazon S3) selezionato. Quando un oggetto S3 o una nuova versione di un oggetto S3 esistente viene caricato nel bucket selezionato, GuardDuty avvia automaticamente una scansione antimalware.

Protezione da malware per S3: panoramica e demo

Due approcci per abilitare la protezione da malware per S3

Puoi abilitare Malware Protection for S3 quando attivi il GuardDuty servizio e utilizzi Malware Protection for S3 come parte dell' GuardDuty esperienza complessiva, oppure quando desideri utilizzare la funzionalità Malware Protection for S3 da sola senza abilitare il servizio. Account AWS GuardDuty Quando attivi da sola Malware Protection for S3, nella GuardDuty documentazione si fa riferimento all'utilizzo di Malware Protection for S3 come funzionalità indipendente.

Considerazioni sull'utilizzo indipendente di Malware Protection for S3

- GuardDuty risultati di sicurezza: Detector ID è un identificatore univoco associato al tuo account in una regione. Quando abiliti GuardDuty in una o più regioni in un account, viene creato automaticamente un ID rilevatore per questo account in ogni regione in cui attivi. GuardDuty Per ulteriori informazioni, consulta Detector nel Concetti e terminologia documento.

  Quando abiliti Malware Protection for S3 in modo indipendente in un account, a quell'account non sarà associato un ID rilevatore. Ciò influisce sulle GuardDuty funzionalità che potresti avere a tua disposizione. Ad esempio, quando una scansione antimalware di S3 rileva la presenza di malware, non viene generato alcun GuardDuty risultato Account AWS perché tutti i GuardDuty risultati sono associati a un ID del rilevatore.
- Verifica se l'oggetto scansionato è dannoso: per impostazione predefinita, GuardDuty pubblica i risultati della scansione del malware sul bus di EventBridge eventi Amazon predefinito e su un namespace Amazon CloudWatch . Quando abiliti il tagging al momento dell'attivazione di Malware Protection for S3 per un bucket, l'oggetto S3 scansionato riceve un tag che riporta il risultato della scansione. Per ulteriori informazioni sull'assegnazione di tag, consulta Etichettatura opzionale degli oggetti in base al risultato della scansione.

Considerazioni generali per abilitare Malware Protection for S3

Le seguenti considerazioni generali valgono sia che si utilizzi Malware Protection for S3 in modo indipendente o come parte dell'esperienza: GuardDuty

- Puoi abilitare Malware Protection for S3 per un bucket Amazon S3 che appartiene al tuo account. Come account GuardDuty amministratore delegato non puoi abilitare questa funzionalità in un bucket Amazon S3 che appartiene a un account membro.
- Puoi abilitare questa funzionalità nei bucket S3 che appartengono alla stessa regione attualmente selezionata nella console. GuardDuty GuardDuty non supporta l'attivazione di questa funzionalità nei bucket S3 interregionali.
- In qualità di account GuardDuty amministratore delegato, riceverai una EventBridge notifica Amazon ogni volta che si verifica una modifica in un bucket S3 che uno Stato delle risorse del piano di protezione antimalware degli account membri della tua organizzazione ha configurato per questa funzionalità.

Indice

Prezzi di Malware Protection for S3

Piano Free Tier (costo di scansione)

Ciascuno Account AWS riceve un piano gratuito di 12 mesi che include l'utilizzo fino a un limite mensile specifico per ciascuna regione. Se l'utilizzo supera il limite specificato, inizierai a sostenere il costo di utilizzo per il limite superato. Per informazioni sui limiti specificati e un esempio di prezzo, consulta i prezzi dei piani di GuardDuty protezione.

- Tutti Account AWS gli esistenti possono utilizzare il piano gratuito di 12 mesi per questa funzionalità che inizia dall'11 giugno 2024 e termina l'11 giugno 2025. Questo piano gratuito esteso di 12 mesi per il tuo account si applica all'utilizzo di Malware Protection for S3 e a nessun'altra o altra funzionalità. AWS servizio GuardDuty

  Se un utente esistente Account AWS inizia a utilizzare Malware Protection for S3 dopo l'11 giugno 2025 o dopo la scadenza del piano gratuito di 12 mesi dell'account, inizierai a sostenere i costi di utilizzo associati.
- Se hai un nuovo piano gratuito di 12 mesi Account AWS e inizia dopo la disponibilità generale (11 giugno 2024) di Malware Protection for S3, il periodo del piano gratuito di 12 mesi per questa funzionalità sarà lo stesso del periodo di 12 mesi del piano gratuito del tuo account.

Per informazioni sui costi di utilizzo dopo l'attivazione di Malware Protection for S3, consulta. Visualizzazione dell'utilizzo e dei costi di Malware Protection for S3

Costo di utilizzo di S3 Object Tagging

Quando abiliti Malware Protection for S3, è facoltativo abilitare i tag per gli oggetti S3 scansionati. Quando scegli di abilitare S3 Object Tagging, è associato un costo di utilizzo. Per ulteriori informazioni sui costi, consulta la scheda Management & Insights nella pagina dei prezzi di Amazon S3.

Il costo di utilizzo di S3 Object Tagging non è incluso nel piano Free Tier.

Amazon S3 APIs GET e PUT costi di utilizzo

L' GuardDuty esecuzione di Amazon APIs S3 comporta costi di utilizzo in base al ruolo. IAM Ad esempio, dopo aver assunto il IAM ruolo, GuardDuty esegue il comando `PutObject` API per aggiungere l'oggetto di test al bucket selezionato. Questo aiuta a GuardDuty valutare lo stato di attivazione della funzionalità.

Per informazioni sui prezzi delle API chiamate S3 nella tua Regione AWS, consulta Richieste e recupero dati nella scheda Storage e richieste nella pagina dei prezzi di Amazon S3.

Come funziona Malware Protection for S3?

Questa sezione descrive i componenti di Malware Protection for S3 e come funziona dopo averlo abilitato per un bucket S3.

Panoramica

Puoi abilitare Malware Protection for S3 per un bucket Amazon S3 che appartiene al tuo. Account AWS GuardDutyti offre la flessibilità necessaria per abilitare questa funzionalità per l'intero bucket o limitare l'ambito della scansione antimalware a prefissi di oggetti specifici, in cui GuardDuty analizza ogni oggetto caricato che inizia con uno dei prefissi selezionati. È possibile aggiungere fino a 5 prefissi. Quando abiliti la funzionalità per un bucket S3, quel bucket viene chiamato bucket protetto.

IAMautorizzazioni di ruolo

Malware Protection for S3 utilizza un IAM ruolo che consente di GuardDuty eseguire le azioni di scansione del malware per tuo conto. Queste azioni includono la notifica degli oggetti appena caricati nel bucket selezionato, la scansione di tali oggetti e, facoltativamente, l'aggiunta di tag agli oggetti scansionati. Questo è un prerequisito per configurare il bucket S3 con questa funzionalità.

È possibile aggiornare un IAM ruolo esistente o creare un nuovo ruolo per questo scopo. Quando abiliti Malware Protection for S3 per più di un bucket, puoi aggiornare il IAM ruolo esistente per includere il nome dell'altro bucket, se necessario. Per ulteriori informazioni, consulta Prerequisito: creare o aggiornare i criteri relativi ai IAM ruoli.

Etichettatura opzionale degli oggetti in base al risultato della scansione

Al momento di abilitare Malware Protection for S3 per il tuo bucket, è disponibile un passaggio opzionale per abilitare l'etichettatura per gli oggetti S3 scansionati. Il IAM ruolo include già l'autorizzazione ad aggiungere tag all'oggetto dopo la scansione. Tuttavia, GuardDuty aggiungerà tag solo quando abiliti questa opzione al momento della configurazione.

È necessario abilitare questa opzione prima che un oggetto venga caricato. Al termine della scansione, GuardDuty aggiunge un tag predefinito all'oggetto S3 scansionato con la seguente coppia chiave:valore:

```
GuardDutyMalwareScanStatus:Potential scan result
```

I potenziali valori dei tag dei risultati della scansione includonoNO_THREATS_FOUND,,, eTHREATS_FOUND. UNSUPPORTED ACCESS_DENIED FAILED Per ulteriori informazioni su questi valori, consulta S3 object potential scan result values.

L'abilitazione dei tag è uno dei modi per conoscere i risultati della scansione degli oggetti S3. Puoi utilizzare ulteriormente questi tag per aggiungere una politica di risorse S3 basata su tag access control (TBAC) in modo da poter intraprendere azioni sugli oggetti potenzialmente dannosi. Per ulteriori informazioni, consulta Aggiungendo TBAC una risorsa bucket S3.

Ti consigliamo di abilitare i tag al momento della configurazione di Malware Protection for S3 per il tuo bucket. Se abiliti l'etichettatura dopo il caricamento di un oggetto e potenzialmente l'avvio della scansione, non GuardDuty sarà possibile aggiungere tag all'oggetto scansionato. Per informazioni sui costi associati all'etichettatura degli oggetti S3, consulta. Prezzi di Malware Protection for S3

Procedura dopo aver abilitato Malware Protection for S3 per un bucket

Dopo aver abilitato Malware Protection for S3, viene creata una risorsa del piano Malware Protection esclusivamente per il bucket S3 selezionato. Questa risorsa è associata a un ID del piano Malware Protection, un identificatore univoco per la risorsa protetta. Utilizzando una delle IAM autorizzazioni GuardDuty , crea e gestisce una regola EventBridge gestita denominata. `DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*`

Come GuardDuty gestisce i tuoi dati: guardrails per la protezione dei dati

Malware Protection for S3 ascolta le notifiche di Amazon EventBridge . Quando un oggetto viene caricato nel bucket selezionato o in uno dei prefissi, GuardDuty scarica quell'oggetto dal bucket S3 utilizzando un bucket, quindi lo legge, lo decrittografa AWS PrivateLinke scansiona in un ambiente isolato nella stessa regione. L'ambiente di scansione viene eseguito in un cloud privato virtuale bloccato () senza accesso a Internet. VPC VPCÈ collegato a un gruppo di regole DNS del firewall che consente la comunicazione solo con i domini consentiti elencati di cui è proprietario. AWS Per tutta la durata della scansione, memorizza GuardDuty temporaneamente l'oggetto S3 scaricato all'interno dell'ambiente di scansione crittografato con AWS Key Management Service chiavi ().AWS KMS

Per informazioni sulla metodologia di rilevamento del GuardDuty malware e sui motori di scansione utilizzati, consulta. GuardDuty motore di scansione per il rilevamento di malware

Al termine della scansione antimalware, GuardDuty elabora i metadati di scansione con lo stato della scansione e quindi elimina la copia scaricata dell'oggetto.

GuardDuty pulisce l'ambiente di scansione ogni volta prima che inizi una nuova scansione. GuardDuty utilizza l'autorizzazione contingente per l'accesso dell'operatore all'ambiente di scansione e ogni richiesta di accesso viene esaminata, approvata e verificata.

Revisione dei risultati della scansione degli oggetti S3

GuardDuty pubblica l'evento del risultato della scansione degli oggetti S3 sul bus eventi EventBridge predefinito di Amazon. GuardDuty invia anche i parametri di scansione, come il numero di oggetti scansionati e i byte scansionati, ad Amazon. CloudWatch Se hai abilitato l'etichettatura, GuardDuty aggiungerà il tag predefinito `GuardDutyMalwareScanStatus` e un potenziale risultato della scansione come valore del tag.

Per ulteriori informazioni, consulta Monitoraggio nella protezione da malware per S3.

Revisione dei risultati generati

La revisione dei risultati dipende dal fatto che tu stia utilizzando o meno Malware Protection for S3 con GuardDuty. Considerare i seguenti scenari:

Utilizzo di Malware Protection for S3 quando il GuardDuty servizio è abilitato (detector ID)

> Se la scansione antimalware rileva un file potenzialmente dannoso in un oggetto S3, GuardDuty genererà un risultato associato. È possibile visualizzare i dettagli del risultato e utilizzare i passaggi consigliati per correggere potenzialmente il risultato. In base alla frequenza di esportazione dei risultati, i risultati generati vengono esportati in un bucket S3 e in un bus di eventi. EventBridge

Utilizzo di Malware Protection for S3 come funzionalità indipendente (nessun ID di rilevamento)

> GuardDuty non sarà in grado di generare risultati perché non esiste un ID del rilevatore associato. Per conoscere lo stato della scansione antimalware degli oggetti S3, puoi visualizzare il risultato della scansione che GuardDuty viene pubblicato automaticamente sul tuo bus eventi predefinito. Puoi anche visualizzare le CloudWatch metriche per valutare il numero di oggetti e byte che GuardDuty hanno tentato di scansionare. È possibile impostare CloudWatch allarmi per ricevere notifiche sui risultati della scansione. Se hai abilitato S3 Object Tagging, puoi anche visualizzare lo stato della scansione antimalware controllando l'oggetto S3 per la chiave del tag e il valore del `GuardDutyMalwareScanStatus` tag dei risultati della scansione.

Funzionalità di protezione da malware per S3

L'elenco seguente fornisce una panoramica di ciò che puoi aspettarti o fare dopo aver abilitato Malware Protection for S3 per il tuo bucket:

- Scegli cosa scansionare: scansiona i file man mano che vengono caricati su tutti i prefissi o su alcuni prefissi specifici (fino a 5) associati al bucket S3 selezionato.
- Scansioni automatiche degli oggetti caricati: dopo aver abilitato Malware Protection for S3 per un bucket, GuardDuty avvierà automaticamente una scansione per rilevare potenziali malware in un oggetto appena caricato.
- Abilita tramite console, utilizzandoAPI/AWS CLI, oppure AWS CloudFormation: scegli un metodo preferito per abilitare Malware Protection for S3.

  Puoi abilitare Malware Protection for S3 utilizzando piattaforme Infrastructure as code (IaC) come Terraform. Per ulteriori informazioni, consulta Resource:. `aws_guardduty_malware_protection_plan`
- Formati di file supportati, quote Malware Protection per S3 e funzionalità di Amazon S3: Malware Protection for S3 supporta tutti i formati di file che puoi caricare nei bucket S3. Se il file caricato è protetto da password, salterà la scansione del file. GuardDuty Per informazioni sulle quote relative alla dimensione degli oggetti, al livello massimo di profondità di archiviazione e ad altri dettagli, consulta. Quote nella protezione da malware per S3

  Per informazioni sul supporto o meno di una funzionalità di Amazon S3, consulta. Supportabilità delle funzionalità di Amazon S3
- Supporta l'etichettatura degli oggetti S3 scansionati: se abilitiEtichettatura opzionale degli oggetti in base al risultato della scansione, dopo ogni scansione antimalware, GuardDuty aggiungerai un tag che indica lo stato della scansione. Puoi usare questo tag per configurare il controllo degli accessi basato su tag (TBAC) per gli oggetti S3. Ad esempio, puoi limitare l'accesso agli oggetti S3 che sono indicati come dannosi e il cui valore del tag è pari a. `THREATS_FOUND`
- EventBridge Notifiche Amazon: GuardDuty invia eventi ad Amazon EventBridge quando lo stato delle risorse del piano Malware Protection cambia o viene completata una scansione antimalware dell'oggetto S3. Questi eventi vengono inviati al bus degli eventi predefinito. È possibile utilizzare EventBridge questi eventi per scrivere regole che intraprendono azioni, come il monitoraggio del verificarsi di questi eventi. Per ulteriori informazioni, consulta Monitoraggio con Amazon EventBridge.

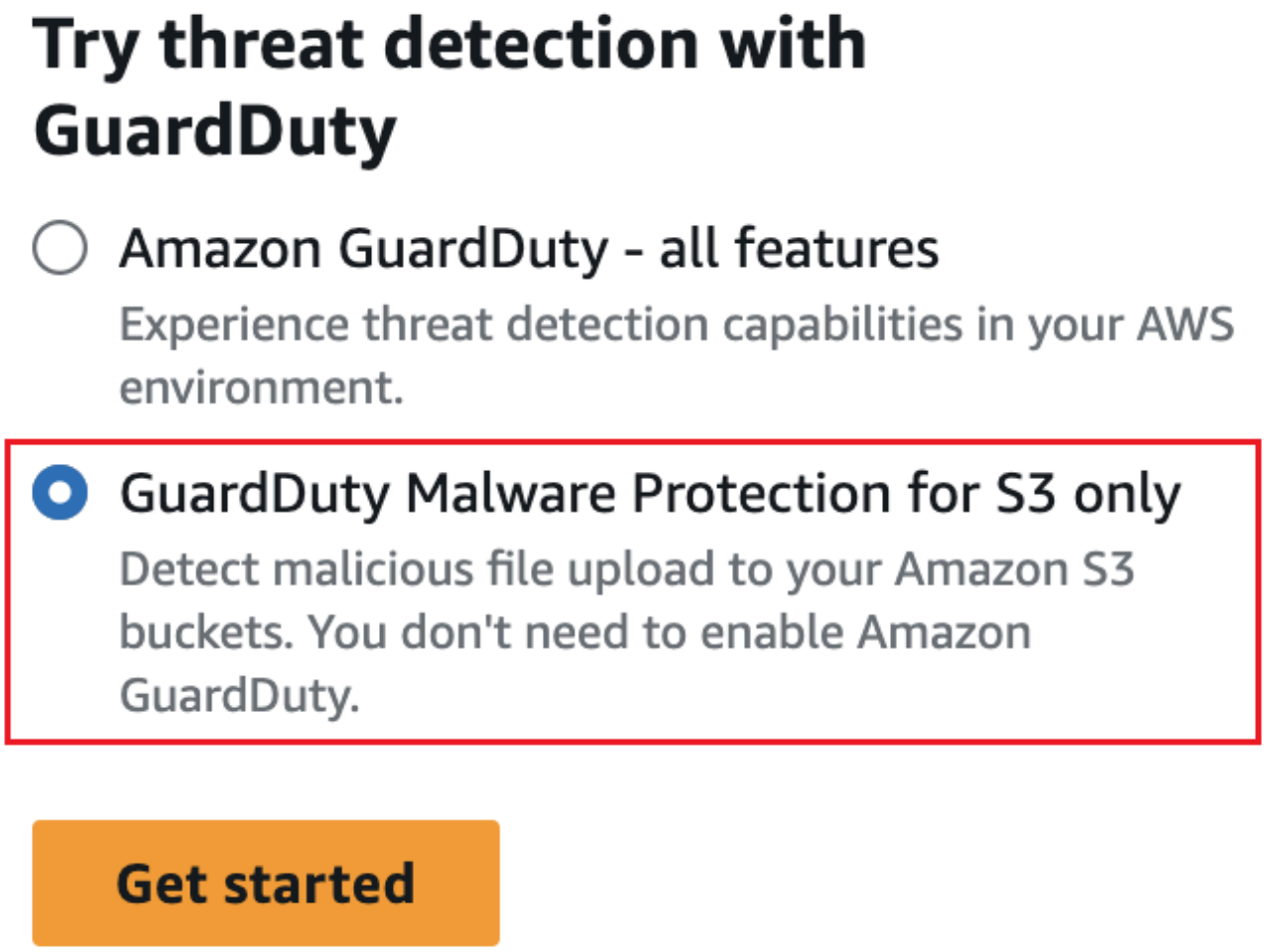
- CloudWatch metriche: visualizza le CloudWatch metriche per abilitare gli allarmi su determinati stati di scansione del malware. Per ulteriori informazioni, consulta Monitoraggio delle metriche dello stato della scansione tramite Amazon CloudWatch.

(Facoltativo) Inizia a usare GuardDuty Malware Protection for S3 in modo indipendente (solo console)

Utilizza questo passaggio facoltativo per iniziare a utilizzare l'opzione di rilevamento delle minacce di Malware Protection for S3 indipendentemente GuardDuty dallo stato del tuo. Account AWS Se l'hai già abilitata GuardDuty nel tuo account, puoi saltare questo passaggio e continuare. Configurazione della protezione da malware per S3 per il tuo bucket

Passaggi per iniziare a utilizzare solo il rilevamento delle minacce da parte di Malware Protection for S3

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Seleziona Protezione GuardDuty da malware solo per S3. Questo ti aiuta a rilevare se un file appena caricato nel tuo bucket Amazon Simple Storage Service (Amazon S3) contiene potenzialmente malware.



3. Scegli Avvia. Ora puoi continuare con i passaggi indicati Configurazione della protezione da malware per S3 per il tuo bucket di seguito.

Configurazione della protezione da malware per S3 per il tuo bucket

Questa sezione include i passaggi per aggiungere i prerequisiti e abilitare Malware Protection for S3 per un bucket Amazon S3 che appartiene al tuo account. I passaggi descritti nelle sezioni seguenti rimangono invariati sia che tu inizi a usare Malware Protection for S3 in modo indipendente sia che tu lo abiliti come parte del servizio. GuardDuty

Utilizza i seguenti passaggi ogni volta che desideri aggiungere questo rilevamento delle minacce a un bucket S3.

1. Prerequisito: creare o aggiornare i criteri relativi ai IAM ruoli
2. Abilita la protezione da malware per S3 per il tuo bucket

Prerequisito: creare o aggiornare i criteri relativi ai IAM ruoli

Affinché Malware Protection for S3 esegua la scansione e (facoltativamente) aggiunga tag agli oggetti S3, devi creare e assegnare un IAM ruolo che includa le seguenti autorizzazioni richieste per:

- Consenti ad Amazon EventBridge Actions di creare e gestire la regola EventBridge gestita in modo che Malware Protection for S3 possa ascoltare le notifiche degli oggetti S3.

  Per ulteriori informazioni, consulta Amazon EventBridge managed rules nella Amazon EventBridge User Guide.
- Consenti ad Amazon S3 e alle EventBridge azioni di inviare notifiche per tutti gli eventi in questo bucket EventBridge

  Per ulteriori informazioni, consulta Enabling Amazon EventBridge nella Amazon S3 User Guide.
- Consenti alle azioni di Amazon S3 di accedere all'oggetto S3 caricato e aggiungi un tag predefinito all'oggetto S3 `GuardDutyMalwareScanStatus` scansionato. Quando usi un prefisso di oggetto, aggiungi una `s3:prefix` condizione solo sui prefissi di destinazione. Ciò GuardDuty impedisce l'accesso a tutti gli oggetti S3 nel bucket.
- Consenti alle azioni KMS chiave di accedere all'oggetto prima di scansionare e inserire un oggetto di test sui bucket con la crittografia supportata DSSE KMS eSSE. KMS

> **Note**
>
> Questo passaggio è necessario ogni volta che attivi Malware Protection for S3 per un bucket nel tuo account. Se disponi già di un IAM ruolo, puoi aggiornarne la policy per includere i dettagli di un'altra risorsa del bucket S3. L'Aggiungere le autorizzazioni IAM relative alle policyargomento fornisce un esempio su come eseguire questa operazione.

Utilizza le seguenti politiche per creare o aggiornare un IAM ruolo.

Policy

- Aggiungere le autorizzazioni IAM relative alle policy
- Aggiungere una politica di relazione di fiducia

Aggiungere le autorizzazioni IAM relative alle policy

Puoi scegliere di aggiornare la politica in linea di un IAM ruolo esistente o creare un nuovo IAM ruolo. Per informazioni sui passaggi, consulta Creazione di un IAM ruolo o Modifica dei criteri di autorizzazione di un ruolo nella Guida per l'IAMutente.

Aggiungi il seguente modello di autorizzazioni al tuo ruolo preferito. IAM Sostituisci i seguenti valori segnaposto con i valori appropriati associati al tuo account:

- In *amzn-s3-demo-bucket*, sostituiscilo con il nome del tuo bucket Amazon S3.

  Per utilizzare lo stesso IAM ruolo per più di una risorsa bucket S3, aggiorna una policy esistente come mostrato nell'esempio seguente:

  ```
  ...
  ...
  "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "arn:aws:s3:::amzn-s3-demo-bucket2/*"
  ],
  ...
  ...
  ```

  Assicurati di aggiungere una virgola (,) prima di aggiungerne una nuova ARN associata al bucket S3. Esegui questa operazione ogni volta che fai riferimento a un bucket S3 `Resource` nel modello di policy.
- In *111122223333*, sostituiscilo con il tuo ID. Account AWS
- In *us-east-1*, sostituiscilo con il tuo Regione AWS.
- In *APKAEIBAERJR2EXAMPLE*, sostituiscilo con il tuo ID chiave gestito dal cliente. Se il bucket è crittografato utilizzando un AWS KMS key, sostituisci il valore segnaposto con un*, come mostrato nell'esempio seguente:

  ```
  "Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
  ```

IAMmodello di politica dei ruoli

```
{
    "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"
                }
            }
        }
    ]
}
```

Aggiungere una politica di relazione di fiducia

Allega la seguente politica di fiducia al tuo IAM ruolo. Per informazioni sui passaggi, vedere Modifica di una politica di attendibilità dei ruoli.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection-plan.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Abilita la protezione da malware per S3 per il tuo bucket

Questa sezione fornisce passaggi dettagliati su come abilitare Malware Protection for S3 per un bucket selezionato nei tuoi account.

Passaggi per abilitare Malware Protection for S3 per un bucket

- Inserisci i dettagli del bucket S3
- Abilita l'etichettatura per gli oggetti scansionati
- Autorizzazioni
- (Facoltativo) Contrassegna l'ID del piano di protezione da malware

Inserisci i dettagli del bucket S3

Utilizza i seguenti passaggi per fornire i dettagli del bucket Amazon S3:

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri abilitare Malware Protection for S3.
3. Nel pannello di navigazione, scegli Malware Protection for S3.
4. Nella sezione Bucket protetti, scegli Abilita per abilitare la protezione da malware per S3 per un bucket S3 che appartiene al tuo. Account AWS
5. In Inserisci i dettagli del bucket S3, inserisci il nome del bucket Amazon S3. In alternativa, scegli Browse S3 per selezionare un bucket S3.

   Il Regione AWS bucket S3 e il Account AWS punto in cui abiliti Malware Protection for S3 devono coincidere. Ad esempio, se il tuo account appartiene alla `us-east-1` regione, deve esserlo anche la tua regione del bucket Amazon S3. `us-east-1`
6. In Prefisso, puoi selezionare Tutti gli oggetti nel bucket S3 o Oggetti che iniziano con un prefisso specifico.

   - Seleziona Tutti gli oggetti nel bucket S3 quando vuoi GuardDuty puoi scansionare tutti gli oggetti appena caricati nel bucket selezionato.
   - Seleziona Oggetti che iniziano con un prefisso specifico quando desideri scansionare gli oggetti appena caricati che appartengono a un prefisso specifico. Questa opzione consente

di concentrare l'ambito della scansione antimalware solo sui prefissi degli oggetti selezionati. Per ulteriori informazioni sull'uso dei prefissi, consulta Organizzare gli oggetti nella console Amazon S3 utilizzando le cartelle nella Amazon S3 User Guide.

Scegli Aggiungi prefisso e inserisci il prefisso. Puoi aggiungere fino a cinque prefissi.

Abilita l'etichettatura per gli oggetti scansionati

Si tratta di un passaggio facoltativo. Quando abiliti l'opzione di etichettatura prima che un oggetto venga caricato nel tuo bucket, dopo aver completato la scansione, GuardDuty aggiungerai un tag predefinito con chiave as `GuardDutyMalwareScanStatus` e il valore come risultato della scansione. Per utilizzare Malware Protection for S3 in modo ottimale, consigliamo di abilitare l'opzione per aggiungere tag agli oggetti S3 al termine della scansione. Si applica il costo standard di S3 Object Tagging. Per ulteriori informazioni, consulta Prezzi di Malware Protection for S3.

Perché dovresti abilitare il tagging?

- L'attivazione dei tag è uno dei modi per conoscere i risultati della scansione antimalware. Per informazioni sui risultati di una scansione antimalware S3, consulta. Monitoraggio nella protezione da malware per S3
- Imposta una politica di controllo degli accessi basata su tag (TBAC) sul tuo bucket S3 che contiene l'oggetto potenzialmente dannoso. Per informazioni sulle considerazioni e su come implementare il controllo degli accessi basato su tag (), consulta. TBAC Utilizzo del controllo degli accessi basato su tag (TBAC) con Malware Protection for S3

Considerazioni sull'aggiunta GuardDuty di un tag all'oggetto S3:

- Per impostazione predefinita, puoi associare fino a 10 tag a un oggetto. Per ulteriori informazioni, consulta Categorizzazione dello storage mediante tag nella Guida per l'utente di Amazon S3.

  Se tutti e 10 i tag sono già in uso, non è GuardDuty possibile aggiungere il tag predefinito all'oggetto scansionato. GuardDuty pubblica inoltre il risultato della scansione nel bus degli eventi predefinito EventBridge . Per ulteriori informazioni, consulta Monitoraggio con Amazon EventBridge.
- Se il IAM ruolo selezionato non include l'autorizzazione GuardDuty per taggare l'oggetto S3, anche se il tagging è abilitato per il bucket protetto, non GuardDuty sarà possibile aggiungere tag a questo oggetto S3 scansionato. Per ulteriori informazioni sull'autorizzazione del IAM ruolo richiesta per l'etichettatura, consulta. Prerequisito: creare o aggiornare i criteri relativi ai IAM ruoli

GuardDuty pubblica inoltre il risultato della scansione nel bus EventBridge degli eventi predefinito. Per ulteriori informazioni, consulta Monitoraggio con Amazon EventBridge.

Per selezionare un'opzione in Etichetta gli oggetti scansionati

- GuardDuty Per aggiungere tag agli oggetti S3 scansionati, seleziona Etichetta gli oggetti.
- Se non desideri aggiungere tag GuardDuty agli oggetti S3 scansionati, seleziona Non etichettare gli oggetti.

Autorizzazioni

Utilizza i seguenti passaggi per scegliere un IAM ruolo che disponga delle autorizzazioni necessarie per eseguire azioni di scansione antimalware per tuo conto. Queste azioni possono includere la scansione degli oggetti S3 appena caricati e (facoltativamente) l'aggiunta di tag a tali oggetti.

Per scegliere il nome di un ruolo IAM

1. Se hai già eseguito i passaggi seguentiPrerequisito: creare o aggiornare i criteri relativi ai IAM ruoli, procedi come segue:
   - Nella sezione Autorizzazioni, per il nome del IAM ruolo, scegli un nome di IAM ruolo che includa le autorizzazioni necessarie.
2. Se non hai già eseguito i passaggi seguentiPrerequisito: creare o aggiornare i criteri relativi ai IAM ruoli, procedi come segue:
   a. Scegli Visualizza autorizzazioni.
   b. In Dettagli di autorizzazione, scegli la scheda Politica. Questo mostra un modello delle IAM autorizzazioni richieste.

      Copia questo modello, quindi scegli Chiudi alla fine della finestra dei dettagli delle autorizzazioni.
   c. Scegli Allega policy che apre la IAM console in una nuova scheda. Puoi scegliere di creare un nuovo IAM ruolo o aggiornare un IAM ruolo esistente con le autorizzazioni del modello copiato.

      Questo modello include valori segnaposto che devi sostituire con i valori appropriati associati al tuo bucket e. Account AWS

d. Torna alla scheda del browser con la console. GuardDuty Scegli nuovamente Visualizza autorizzazioni.

e. In Dettagli di autorizzazione, scegli la scheda Relazione di fiducia. Questo mostra un modello della politica sulle relazioni di fiducia per il tuo IAM ruolo.

   Copia questo modello, quindi scegli Chiudi alla fine della finestra dei dettagli dell'autorizzazione.

f. Vai alla scheda del browser con la IAM console aperta. Al tuo IAM ruolo preferito, aggiungi questa politica sulle relazioni di fiducia.

3. Per aggiungere tag all'ID del piano di protezione da malware che viene creato per questa risorsa protetta, continua con la sezione successiva; altrimenti, scegli Abilita alla fine di questa pagina per aggiungere il bucket S3 come risorsa protetta.

(Facoltativo) Contrassegna l'ID del piano di protezione da malware

Si tratta di un passaggio facoltativo che consente di aggiungere tag alla risorsa del piano Malware Protection che verrebbe creata per la risorsa del bucket S3.

Ogni tag è composto da due parti: una chiave di tag e un valore di tag opzionale. Per ulteriori informazioni sull'etichettatura e sui relativi vantaggi, consulta Risorse per l'etichettatura AWS.

Per aggiungere tag alla risorsa del piano Malware Protection

1. Inserisci la chiave e un valore opzionale per il tag. Sia la chiave che il valore del tag fanno distinzione tra maiuscole e minuscole. Per informazioni sui nomi della chiave e del valore del tag, consulta Limiti e requisiti di denominazione dei tag.
2. Per aggiungere altri tag alla risorsa del piano Malware Protection, scegli Aggiungi nuovo tag e ripeti il passaggio precedente. Puoi aggiungere fino a 50 tag per ciascuna risorsa .
3. Scegli Abilita .

Passaggi dopo aver abilitato Malware Protection for S3

Dopo aver abilitato Malware Protection for S3 per un bucket (o prefissi di oggetti specifici), esegui i seguenti passaggi nell'ordine elencato:

1. Aggiungi una politica delle risorse di controllo degli accessi (TBAC) basata su tag: quando abiliti il tagging, prima che un oggetto venga caricato nel bucket selezionato, assicurati di aggiungere la

policy alla risorsa del TBAC bucket S3. Per ulteriori informazioni, consulta Aggiungendo TBAC una risorsa bucket S3.

2. Monitora lo stato del piano Malware Protection: monitora la colonna Status per ogni bucket protetto. Per informazioni sui potenziali stati e sul loro significato, consulta. Stato delle risorse del piano di protezione antimalware
3. Carica un oggetto:

    1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
    2. Carica un file nel bucket S3 o nel prefisso dell'oggetto per cui hai abilitato questa funzionalità. Per istruzioni su come caricare un file, consulta Caricare un oggetto nel bucket nella Amazon S3 User Guide.
4. Monitora lo stato di scansione degli oggetti S3: questo passaggio include informazioni su come controllare lo stato della scansione antimalware dell'oggetto S3.

Sono abilitati entrambi GuardDuty e Malware Protection for S3	Protezione da malware abilitata solo per S3
• Quando GuardDuty è abilitata, può generare un messaggio Protezione da malware per tipo di ricerca S3 che indica la presenza di malware nell'oggetto S3 scansionato. • Puoi potenzialmente controllare il risultato della scansione degli oggetti S3 utilizzan do una o più opzioni sotto. Monitoraggio nella protezione da malware per S3 Questi includono l'utilizzo di Amazon EventBrid ge, le CloudWatch metriche per il piano Malware Protection e l'etichettatura degli oggetti scansionati.	È possibile verificare il risultato della scansione degli oggetti S3 utilizzando una o più opzioni riportate di seguito. Monitoraggio nella protezione da malware per S3 Questi includono l'utilizzo di Amazon EventBridge, le CloudWatch metriche per il piano Malware Protection e l'etichettatura degli oggetti scansionati.

Stato delle risorse del piano di protezione antimalware

Questa sezione descrive vari valori dello stato di protezione associati alla risorsa del piano Malware Protection.

Stato	Descrizione
Attivo	Il bucket S3 è stato configurato con successo con Malware Protection for S3.
Avvertenza *	Malware Protection for S3 è progettato per non essere influenzato dalla visualizzazione di un avviso. Quando GuardDuty rileva un nuovo oggetto S3, avvierà una scansione antimalware. Dopo aver avviato la scansione con successo, il valore della colonna Status potrebbe impiegare alcuni minuti per passare ad Attivo. Riceverai una EventBridge notifica dopo l'aggiornamento del valore della colonna Status.
Errore *	Il tuo bucket non è protetto. Nessuna delle scansioni antimalware associate a questo bucket S3 verrà completata. Potrebbero esserci una o più cause potenziali.

* Per informazioni sui potenziali problemi e sui passaggi corrispondenti per risolverli, vedereRisoluzione dei problemi relativi allo stato del piano Malware Protection.

Risoluzione dei problemi relativi allo stato del piano Malware Protection

Per ogni bucket protetto, GuardDuty visualizza lo stato in base alla classifica. Ad esempio, se un bucket protetto presenta problemi nelle categorie Errore e Avviso, GuardDuty visualizza innanzitutto il problema associato allo stato di errore.

L'elenco seguente include gli errori e gli avvisi relativi allo stato del piano Malware Protection.

Errori

- EventBridge la notifica è disabilitata per questo bucket S3
- EventBridge manca una regola gestita per ricevere gli eventi del bucket S3
- Il bucket S3 non esiste più

Attenzione

- Impossibile inserire l'oggetto di prova

EventBridge la notifica è disabilitata per questo bucket S3

Il codice del motivo dello stato associato è.
`EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED`

Dettagli sullo stato

GuardDuty utilizza EventBridge per ricevere una notifica quando un nuovo oggetto viene caricato in questo bucket S3. Questa autorizzazione non è presente nel tuo IAM ruolo.

Passaggi per la risoluzione dei problemi

Opzione 1: aggiungi la seguente dichiarazione di autorizzazione al tuo IAM ruolo:

```
{
          "Sid": "AllowEnableS3EventBridgeEvents",
          "Effect": "Allow",
          "Action": [
             "s3:PutBucketNotification",
             "s3:GetBucketNotification"
             ],
          "Resource": [
             "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
}
```

Replace (Sostituisci) *amzn-s3-demo-bucket* con il nome del tuo bucket Amazon S3.

Opzione 2: abilitare le EventBridge notifiche utilizzando la console Amazon S3

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Nella pagina Bucket, nella scheda General purpose buckets, seleziona il nome del bucket associato a questo errore.
3. In questa pagina del bucket, scegli la scheda Proprietà.
4. Nella EventBridge sezione Amazon, seleziona Modifica.
5. Nella EventBridge pagina Modifica Amazon, per Invia notifica ad Amazon EventBridge per tutti gli eventi in questo bucket, seleziona Attiva.
6. Scegli Save changes (Salva modifiche).

Potrebbero essere necessari alcuni minuti prima che il valore della colonna Status diventi Attivo.

EventBridge manca una regola gestita per ricevere gli eventi del bucket S3

Il codice del motivo dello stato associato è. `EVENTBRIDGE_MANAGED_RULE_DISABLED`

Dettagli sullo stato

Mancano le autorizzazioni EventBridge gestite per gestire la configurazione delle EventBridge regole.

Passaggi per la risoluzione dei problemi

Aggiungi la seguente dichiarazione di autorizzazione al tuo IAM ruolo:

```
{
         "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"
              }
           }
}
```

Potrebbero essere necessari alcuni minuti prima che il valore della colonna Status diventi Attivo.

Il bucket S3 non esiste più

Il codice del motivo dello stato associato è. `PROTECTED_RESOURCE_DELETED`

Dettagli sullo stato

Questo bucket S3 è stato eliminato dal tuo account e non esiste più.

Passaggio per la risoluzione dei problemi

Se l'eliminazione del bucket S3 non è stata intenzionale, puoi creare un nuovo bucket utilizzando la console Amazon S3.

Dopo aver creato il bucket con successo, abilita Malware Protection for S3 seguendo i passaggi indicati nella pagina. Configurazione della protezione da malware per S3 per il tuo bucket

Impossibile inserire l'oggetto di prova

Il codice del motivo dello stato associato è`INSUFFICIENT_TEST_OBJECT_PERMISSIONS`.

> **Note**
>
> L'autorizzazione ad aggiungere un oggetto di test è facoltativa. La mancanza di questa autorizzazione nel tuo IAM ruolo non impedisce a Malware Protection for S3 di avviare una scansione antimalware su un oggetto appena caricato. Una volta avviata correttamente una scansione, potrebbero essere necessari alcuni minuti prima che lo stato del piano di protezione da malware passi da Avviso ad Attivo.
> Se il IAM ruolo include già questa autorizzazione, questo avviso indica una politica restrittiva per i bucket di Amazon S3 che non consente IAM al ruolo di includere questa autorizzazione.

Dettagli sullo stato

Per convalidare la configurazione del bucket selezionato, GuardDuty inserisce un oggetto di test nel bucket.

Passaggi per la risoluzione dei problemi

Puoi scegliere di aggiornare il IAM ruolo per includere le autorizzazioni mancanti. Al IAM ruolo selezionato, aggiungi le seguenti autorizzazioni in modo da GuardDuty poter inserire l'oggetto di test nella risorsa selezionata:

```
{
        "Sid": "AllowPutValidationObject",
        "Effect": "Allow",
        "Action": [
          "s3:PutObject"
          ],
```

```
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-
object"
          ]
}
```

Replace (Sostituisci) *amzn-s3-demo-bucket* con il nome del tuo bucket Amazon S3. Per informazioni sulle autorizzazioni dei IAM ruoli, consulta. Prerequisito: creare o aggiornare i criteri relativi ai IAM ruoli

Potrebbero essere necessari alcuni minuti prima che il valore della colonna Status diventi Attivo.

Monitoraggio nella protezione da malware per S3

Quando si utilizza Malware Protection for S3 con un ID GuardDuty rilevatore, se l'oggetto Amazon S3 è potenzialmente dannoso GuardDuty , viene generato. Protezione da malware per tipo di ricerca S3 Utilizzando la GuardDuty console eAPIs, puoi visualizzare i risultati generati. Per informazioni sulla comprensione di questo tipo di risultato, vedereDettagli degli esiti.

Quando si utilizza Malware Protection for S3 senza attivarlo GuardDuty (nessun ID rilevatore), anche quando l'oggetto Amazon S3 scansionato è potenzialmente dannoso, non è GuardDuty possibile generare alcun risultato.

L'elenco seguente fornisce i potenziali valori di stato dei risultati della scansione degli oggetti S3:

- `NO_THREATS_FOUND`— non ha GuardDuty rilevato alcuna potenziale minaccia associata all'oggetto scansionato.
- `THREATS_FOUND`— GuardDuty ha rilevato una potenziale minaccia associata all'oggetto scansionato.
- `UNSUPPORTED`— Esistono alcuni motivi per cui Malware Protection for S3 salterà una scansione. Le possibili ragioni includono file protetti da password, quote Malware Protection for S3 e alcune funzionalità di Amazon S3. Per ulteriori informazioni, consulta Funzionalità di protezione da malware per S3.
- `ACCESS_DENIED`— non è GuardDuty possibile accedere a questo oggetto per la scansione. Controlla i permessi di IAM ruolo associati a questo bucket. Per ulteriori informazioni, consulta Prerequisito: creare o aggiornare i criteri relativi ai IAM ruoli.
- `FAILED`— impossibile GuardDuty eseguire la scansione antimalware su questo oggetto a causa di un errore interno.

L'elenco seguente fornisce i potenziali valori dello stato di scansione degli oggetti S3 e la loro mappatura al risultato della scansione degli oggetti S3:

- Completata: la scansione è stata completata correttamente e indica se l'oggetto S3 contiene malware. In questo caso, il potenziale valore del risultato della scansione degli oggetti S3 potrebbe essere uno dei dueTHREATS_FOUND. NO_THREATS_FOUND
- Ignorato: GuardDuty salta una scansione antimalware quando i dettagli dell'oggetto S3 non sono allineati con l'Quote nella protezione da malware per S3oggetto S3 caricato nel bucket selezionato o GuardDuty non hanno accesso all'oggetto S3 caricato.

  In questo caso, il potenziale valore del risultato della scansione degli oggetti S3 potrebbe essere uno dei due. UNSUPPORTED ACCESS_DENIED
- Fallito: analogamente al valore del risultato della scansione degli oggetti S3FAILED, questo stato di scansione indica che non GuardDuty è stato possibile eseguire la scansione antimalware sull'oggetto S3 a causa di un errore interno.

Argomenti

Monitoraggio con Amazon EventBridge

Amazon EventBridge è un servizio di bus eventi senza server che semplifica la connessione delle applicazioni con dati provenienti da una varietà di fonti. EventBridge fornisce un flusso di dati in tempo reale dalle tue applicazioni, dalle applicazioni oftware-as-a S-Service (SaaS) e dai servizi AWS e indirizza tali dati verso destinazioni come Lambda. In questo modo puoi monitorare gli eventi che si verificano nei servizi e creare architetture basate su eventi. Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

In qualità di account proprietario di un bucket S3 protetto con Malware Protection for S3, GuardDuty pubblica EventBridge notifiche sul bus degli eventi predefinito nei seguenti scenari:

- Modifiche allo stato delle risorse del piano Malware Protection per tutti i bucket protetti. Per informazioni sui vari stati, consulta. Stato delle risorse del piano di protezione antimalware
- Si è verificato un errore nell'evento tag per i seguenti motivi:

- Al tuo IAM ruolo mancano le autorizzazioni per etichettare l'oggetto.

  Il Aggiungere le autorizzazioni IAM relative alle policy modello include l'autorizzazione per GuardDuty etichettare un oggetto.
- La risorsa o l'oggetto bucket specificato nel IAM ruolo non esiste più.
- L'oggetto S3 associato ha già raggiunto il limite massimo di tag. Per ulteriori informazioni sul limite dei tag, consulta Categorizzazione dello storage utilizzando i tag nella Guida per l'utente di Amazon S3.

- Il risultato della scansione degli oggetti S3 viene pubblicato sul bus eventi predefinito EventBridge .

Imposta le regole EventBridge

Puoi impostare EventBridge delle regole nel tuo account per inviare lo stato delle risorse, gli eventi di errore dei tag post-scansione o il risultato della scansione degli oggetti S3 a un altro. AWS servizio In qualità di account GuardDuty amministratore delegato, riceverai la notifica sullo stato delle risorse del piano Malware Protection in caso di modifica dello stato.

Verranno applicate le EventBridge tariffe standard. Per ulteriori informazioni, consulta i EventBridge prezzi di Amazon.

Tutti i valori che compaiono in *red* sono segnaposto per l'esempio. Questi valori cambieranno in base ai valori del tuo account e al fatto che venga rilevato o meno malware.

Stato delle risorse del piano Malware Protection

È possibile creare uno schema di EventBridge eventi basato sui seguenti scenari:

`detail-type`Valori potenziali

- `"GuardDuty Malware Protection Resource Status Active"`
- `"GuardDuty Malware Protection Resource Status Warning"`
- `"GuardDuty Malware Protection Resource Status Error"`

Schema dell'evento

```
{
      "detail-type": ["potential detail-type"],
      "source": ["aws.guardduty"]
```

```
}
```

Schema di notifica di esempio per **`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"
    }
}
```

Schema di notifica di esempio per **`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"
         }
        ]
    }
}
```

Schema di notifica di esempio per **`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"
        }
       ]
    }
}
```

In base al motivo alla base di `resourceStatusERROR`, il `statusReasons` valore verrà compilato.

Per informazioni sulla procedura di risoluzione dei problemi relativi ai seguenti avvisi ed errori, vedereRisoluzione dei problemi relativi allo stato del piano Malware Protection.

Risultato della scansione degli oggetti S3

```
{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}
```

Schema di notifica di esempio per **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
        }
    }
}
```

Schema di notifica di esempio per **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)"
                }
            ]
        }
    }
}
```

Schema di notifica di esempio per lo stato dei risultati della scansione **UNSUPPORTED** (Ignorato):

```
{
    "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
        }
    }
}
```

Schema di notifica di esempio per lo stato dei risultati della scansione **`ACCESS_DENIED`** (Ignorato):

```
{
    "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
        }
    }
}
```

Schema di notifica di esempio per lo stato **`FAILED`** dei risultati della scansione:

```
{
    "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
        }
    }
}
```

Eventi di errore dei tag successivi alla scansione

Schema dell'evento:

```
{
      "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
      "source": "aws.guardduty"
 }
```

Schema di notifica di esempio per **`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"
        }]
    }
}
```

Schema di notifica di esempio per **`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"
        }]
    }
}
```

Per risolvere questi motivi di errore, vedere. Risoluzione dei problemi relativi agli errori dei tag post-scansione degli oggetti S3

Monitoraggio delle metriche dello stato della scansione tramite Amazon CloudWatch

È possibile monitorare GuardDuty l'utilizzo CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili e quasi in tempo reale. Queste statistiche vengono conservate per 15 mesi, in modo da poter accedere alle informazioni storiche e avere una prospettiva migliore sulle prestazioni di Malware Protection for S3. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Le CloudWatch metriche per Malware Protection for S3 sono disponibili a livello di risorsa. Puoi interrogare queste metriche per ogni risorsa protetta separatamente. Le metriche sono riportate nel namespace. `AWS/GuardDuty/MalwareProtection` È possibile impostare allarmi su risorse specifiche per monitorare il livello di sicurezza.

Metriche dello stato della scansione antimalware

Parametro	Descrizione
`CompletedScanCount`	Il numero di scansioni antimalware di oggetti S3 completate in un determinato periodo di tempo. Dimensioni valide: • `Malware Protection Plan Id` `Resource Name`

	Unità: numero
`FailedScanCount`	Il numero di scansioni antimalware di oggetti S3 completate in un determinato periodo di tempo. Dimensioni valide: • `Malware Protection Plan Id` `Resource Name` Unità: numero

`SkippedScanCount`	Il numero di scansioni di malware a oggetti S3 che sono state ignorate in un determinato periodo di tempo.
	Dimensioni valide:
	• `Malware Protection Plan Id`
	`Resource Name`
	`Skipped Reason`
	Valori potenziali
	• `UnSupported`
	• `MissingPermissions`
	Unità: numero

Metriche dei risultati della scansione del malware

`InfectedScanCount`	Il numero di scansioni di malware su oggetti S3 che hanno rilevato oggetti potenzialmente dannosi in un determinato periodo di tempo. Dimensioni valide: • `Malware Protection Plan Id` `Resource Name` Unità: numero
`CompletedScanBytes`	Il numero di byte di oggetti S3 scansionati in un determinato periodo di tempo. Dimensioni valide: • `Malware Protection Plan Id` `Resource Name` Unità: numero

> **Note**
>
> Per impostazione predefinita, le statistiche nelle CloudWatch metriche sonoAVG.

Le seguenti dimensioni sono supportate per le metriche Malware Protection for S3.

Dimensione	Descrizione
`Malware Protection Plan Id`	L'identificatore univoco associato alla risorsa del piano Malware Protection GuardDuty creata per la risorsa protetta.
`Resource Name`	Il nome della risorsa protetta.

`Skipped Reason`	Il motivo per cui una scansione antimalware di oggetti S3 è stata ignorata. Valori potenziali • `UnSupported` • `MissingPermissions`

Per informazioni sull'accesso e sull'interrogazione di questi parametri, consulta Use Amazon CloudWatch metrics nella Amazon CloudWatch User Guide.

Per informazioni sulla configurazione degli allarmi, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

Monitoraggio con tag di oggetti S3

Utilizza l'opzione di abilitazione dei tag in modo da GuardDuty poter aggiungere tag al tuo oggetto Amazon S3 dopo aver completato la scansione del malware.

Considerazioni sull'abilitazione dei tag

- È previsto un costo di utilizzo associato all'etichettatura degli GuardDuty oggetti S3. Per ulteriori informazioni, consulta Prezzi di Malware Protection for S3.
- È necessario mantenere le autorizzazioni di etichettatura richieste per il IAM ruolo preferito associato a questo bucket; in caso contrario, non è GuardDuty possibile aggiungere tag agli oggetti scansionati. Il IAM ruolo include già le autorizzazioni per aggiungere tag agli oggetti S3 scansionati. Per ulteriori informazioni, consulta Prerequisito: creare o aggiornare i criteri relativi ai IAM ruoli.
- Per impostazione predefinita, puoi associare fino a 10 tag a un oggetto S3. Per ulteriori informazioni, consulta Utilizzo del controllo degli accessi basato su tag () TBAC.

Dopo aver abilitato il tagging per un bucket S3 o per prefissi specifici, a ogni oggetto appena caricato che viene scansionato verrà associato un tag nel seguente formato di coppia chiave-valore:

`GuardDutyMalwareScanStatus:`*`Scan-Status`*

Per informazioni sui potenziali valori dei tag, consulta. Utilizzo del controllo degli accessi basato su tag () TBAC

Risoluzione degli errori dei tag post-scansione degli oggetti S3 in Malware Protection for S3

Questa sezione si applica solo agli utenti che utilizzano il Abilita l'etichettatura per gli oggetti scansionati bucket protetto.

Quando si GuardDuty tenta di aggiungere un tag all'oggetto S3 scansionato, l'azione di tagging può avere esito negativo. I potenziali motivi per cui ciò può accadere al tuo bucket sono e. `ACCESS_DENIED` `MAX_TAG_LIMIT_EXCEEDED` Utilizza i seguenti argomenti per comprendere i potenziali motivi di questi motivi di errore dei tag post-scansione e risolverli.

ACCESS_DENIED

L'elenco seguente fornisce i potenziali motivi che possono causare questo problema:

- Il IAM ruolo utilizzato per questo bucket S3 protetto non dispone dell'AllowPostScanTagautorizzazione. Verifica che il IAM ruolo associato utilizzi questa policy del bucket. Per ulteriori informazioni, consulta Prerequisito: creare o aggiornare i criteri relativi ai IAM ruoli.
- La policy protetta del bucket S3 non consente di aggiungere tag GuardDuty a questo oggetto.
- L'oggetto S3 scansionato non esiste più.

MAX_TAG_LIMIT_EXCEEDED

Per impostazione predefinita, puoi associare fino a 10 tag a un oggetto S3. Per ulteriori informazioni, consulta Considerazioni sull'aggiunta GuardDuty di un tag all'oggetto S3 nella sezione. Abilita l'etichettatura per gli oggetti scansionati

Utilizzo del controllo degli accessi basato su tag (TBAC) con Malware Protection for S3

Quando attivi Malware Protection for S3 per il tuo bucket, puoi facoltativamente scegliere di abilitare i tag. Dopo aver tentato di scansionare un oggetto S3 appena caricato nel bucket selezionato, GuardDuty aggiunge un tag all'oggetto scansionato per indicare lo stato della scansione del malware. Quando si abilita il tagging, viene associato un costo di utilizzo diretto. Per ulteriori informazioni, consulta Prezzi di Malware Protection for S3.

GuardDuty utilizza un tag predefinito con la chiave as `GuardDutyMalwareScanStatus` e il valore come uno degli stati di scansione del malware. Per informazioni su questi valori, vedere. S3 object potential scan result values

Considerazioni sull'aggiunta GuardDuty di un tag all'oggetto S3:

- Per impostazione predefinita, puoi associare fino a 10 tag a un oggetto. Per ulteriori informazioni, consulta Categorizzazione dello storage mediante tag nella Guida per l'utente di Amazon S3.

  Se tutti e 10 i tag sono già in uso, non è GuardDuty possibile aggiungere il tag predefinito all'oggetto scansionato. GuardDuty pubblica inoltre il risultato della scansione nel bus degli eventi predefinito EventBridge . Per ulteriori informazioni, consulta Monitoraggio con Amazon EventBridge.
- Se il IAM ruolo selezionato non include l'autorizzazione GuardDuty per taggare l'oggetto S3, anche se il tagging è abilitato per il bucket protetto, non GuardDuty sarà possibile aggiungere tag a questo oggetto S3 scansionato. Per ulteriori informazioni sull'autorizzazione del IAM ruolo richiesta per l'etichettatura, consulta. Prerequisito: creare o aggiornare i criteri relativi ai IAM ruoli

  GuardDuty pubblica inoltre il risultato della scansione nel bus EventBridge degli eventi predefinito. Per ulteriori informazioni, consulta Monitoraggio con Amazon EventBridge.

Aggiungendo TBAC una risorsa bucket S3

Puoi utilizzare le policy delle risorse del bucket S3 per gestire il controllo degli accessi basato su tag (TBAC) per i tuoi oggetti S3. Puoi fornire l'accesso a utenti specifici per accedere e leggere l'oggetto S3. Se hai un'organizzazione creata utilizzando AWS Organizations, devi fare in modo che nessuno possa modificare i tag aggiunti da. GuardDuty Per ulteriori informazioni, consulta Impedire che i tag vengano modificati se non da soggetti autorizzati nella Guida per l'AWS Organizations utente. L'esempio utilizzato nell'argomento collegato cita`ec2`. Quando usi questo esempio, sostituisci *`ec2`* con`s3`.

L'elenco seguente spiega cosa è possibile fare utilizzandoTBAC:

- Impedisci a tutti gli utenti tranne il responsabile del servizio Malware Protection for S3 di leggere gli oggetti S3 che non sono ancora etichettati con la seguente coppia chiave-valore di tag:

  `GuardDutyMalwareScanStatus:`*`Potential key value`*

- Consenti solo GuardDuty di aggiungere la chiave del tag `GuardDutyMalwareScanStatus` con valore come risultato della scansione a un oggetto S3 scansionato. Il seguente modello di policy può consentire a utenti specifici che dispongono dell'accesso di sovrascrivere potenzialmente la coppia chiave-valore del tag.

Esempio di policy sulle risorse del bucket S3:

Replace (Sostituisci) *IAM-role-name* con il IAM ruolo che hai usato per configurare Malware Protection for S3 nel tuo bucket.

```
{
    "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/*"
            ]
        }
    ]
}
```

Per ulteriori informazioni sull'etichettatura delle risorse S3, consulta le politiche di tagging e controllo degli accessi.

Modifica di Malware Protection for S3 per un bucket protetto

Utilizza i seguenti passaggi per modificare la configurazione esistente del tuo bucket S3 protetto:

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione, scegli Malware Protection for S3.
3. In Bucket protetti, seleziona il bucket per il quale desideri modificare la configurazione esistente.
4. Scegli Modifica.
5. Aggiorna la configurazione e le impostazioni esistenti per il tuo bucket e conferma le modifiche. Per informazioni sulla descrizione e sui passaggi per ogni sezione, consultaAbilita la protezione da malware per S3 per il tuo bucket.

   Monitora la colonna Status per questo bucket protetto. Se appare come Avviso o Errore, vediRisoluzione dei problemi relativi allo stato del piano Malware Protection.

Visualizzazione dell'utilizzo e dei costi di Malware Protection for S3

Il tuo account inizia a sostenere costi di utilizzo quando utilizzi Malware Protection for S3 oltre il limite specifico del piano Free Tier o quando scade il piano Free Tier di 12 mesi del tuo account. Per informazioni sul piano Free Tier, consulta. Prezzi di Malware Protection for S3

Per visualizzare il costo di utilizzo, accedi a Cost Explorer nella console https://console.aws.amazon.com/billing/. Per informazioni sulla Account AWS fatturazione, consulta la Guida per l'AWS Billing utente.

Disattiva la protezione da malware per S3 per un bucket protetto

Quando disabiliti Malware Protection for S3 per un bucket protetto, GuardDuty elimina l'ID del piano Malware Protection associato a quel bucket. GuardDuty non avvierà più una scansione antimalware quando un nuovo oggetto viene caricato in questo bucket o in uno dei prefissi dell'oggetto selezionati.

Se lo hai abilitato GuardDuty e ora desideri sospenderlo o disabilitarlo, consulta. GuardDuty Sospensione o disabilitazione GuardDuty Poiché in Malware Protection for S3 non esiste il concetto di ID di rilevamento, la disabilitazione o la sospensione GuardDuty non influiscono sullo stato di un bucket protetto nel tuo account. Puoi continuare a utilizzare la funzionalità Malware Protection for S3 indipendentemente dai prezzi standard associati. Per ulteriori informazioni, consulta Visualizzazione dell'utilizzo e dei costi di Malware Protection for S3. Per smettere di usare Malware Protection for S3, dovrai disabilitarla per tutti i bucket protetti del tuo account. Se desideri continuare a utilizzare GuardDuty e disabilitare solo Malware Protection for S3 per un bucket, i passaggi seguenti non influiranno sulla configurazione del GuardDuty servizio e sugli altri piani di protezione che potresti aver abilitato.

Per disabilitare Malware Protection for S3 per un bucket protetto

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione, scegli Malware Protection for S3.
3. In Bucket protetti, seleziona il bucket per il quale desideri disabilitare Malware Protection for S3.

   Puoi selezionare solo un bucket protetto alla volta. Per disabilitare Malware Protection for S3 per più di un bucket, segui nuovamente questi passaggi per un altro bucket S3.
4. Scegliere Disabilita.

5. Scegli Disabilita per confermare la selezione.

Supportabilità delle funzionalità di Amazon S3

La tabella seguente specifica se Malware Protection for S3 supporta o meno le funzionalità di Amazon S3 elencate.

Il supporto è disponibile?	Descrizione
Sì	Gli oggetti S3 possono essere recuperati senza eseguire il ripristino in modo asincrono.

Il supporto è disponibile?	Descrizione
Condizionale	• Il supporto Intelligent Tiering è disponibile per gli oggetti S3 nei livelli Frequent, Infrequent e Archive Instance Access. • I livelli opt-in Archive e Deep Archive non sono supportati. • Intelligent Tiering crea sempre un nuovo oggetto nel livello Frequent Access. Pertanto, è supportata la scansione degli oggetti durante la creazione. • Le future funzionalità di Intelligent Tiering potrebbero avviare gli oggetti in Archive. Pertanto, questa funzionalità non è supportata.

Il supporto è disponibile?	Descrizione
No	GuardDuty supporta solo bucket generici per Malware Protection for S3.

Il supporto è disponibile?	Descrizione
No	Gli oggetti S3 devono essere ripristinati prima di poter accedervi.
No	La protezione da malware per S3 non è supportata su Outposts.

Il supporto è disponibile?	Descrizione
Sì	Tutti gli oggetti S3 caricati vengono scansionati alla ricerca di malware. Se hai caricato un oggetto con la versione del file v1 e hai immediatamente caricato un'altra versione sostituita con v2, GuardDuty eseguirà la scansione di entrambe le versioni del file oggetto v1 e v2. Tuttavia, l'ora di inizio della scansione potrebbe non essere nello stesso ordine.
Sì	Se il bucket di destinazione è una risorsa protetta, GuardDuty eseguirà la scansione di tutti gli oggetti S3 replicati nei prefissi protetti e monitorati.
No	Non è possibile definire una regola di replica basata sul tag dei risultati della scansione. Amazon S3 non supporta la replica per i tag, ad eccezione di on create.

Il supporto è disponibile?	Descrizione
Sì	GuardDuty supporta scansioni antimalware per oggetti S3 crittografati con chiavi gestite e gestite dal cliente. Assicurati che il IAM ruolo includa l'autorizzazione all'uso della chiave. Per ulteriori informazioni, consulta Aggiungere le autorizzazioni IAM relative alle policy.

Il supporto è disponibile?	Descrizione
No	Malware Protection for S3 non supporta la scansione di oggetti S3 crittografati con chiavi non accessibili.
No	Quando i tuoi oggetti S3 vengono crittografati utilizzando Amazon S3 Encryption Client, i tuoi oggetti non vengono esposti a terze parti, inclusi. AWS Per ulteriori informazioni sul motivo per cui questa funzionalità non è supportata, consulta Proteggere i dati utilizzando la crittografia lato client nella Amazon S3 User Guide.
Sì	Gli oggetti S3 bloccati sono bloccati in base a WORM - Write Once Read Many. Malware Protection for S3 può accedere e scansionare gli oggetti.

Il supporto è disponibile?	Descrizione
Sì	Malware Protection for S3 può scansionare i bucket configurati con Requester Pays. Il richiedente pagherà le chiamate S3. Per ulteriori informazioni, consulta la sezione Utilizzo dei bucket con pagamento a carico del richiedente per i trasferimenti e l'utilizzo dello storage nella Guida per l'utente di Amazon S3.
Sì	È possibile definire le politiche del ciclo di vita in base al tag dei risultati della scansione. Ad esempio, elimina automaticamente gli oggetti dannosi. Per ulteriori informazioni sulla configurazione del ciclo di vita, consulta Managing your storage lifecycle nella Amazon S3 User Guide.
Sì	Puoi definire le politiche relative alle risorse del bucket in base al tag dei risultati della scansione degli oggetti S3. Ad esempio, impedisci l'accesso agli oggetti S3 che non sono ancora stati scansionati o alle minacce rilevate. GuardDuty Per ulteriori informazioni, consulta Utilizzo del controllo degli accessi basato su tag (TBAC) con Malware Protection for S3.

Quote nella protezione da malware per S3

Questa sezione fornisce quote predefinite, spesso denominate limiti. Se non diversamente specificato, ogni quota è specifica della regione. Per visualizzare le quote predefinite specifiche per l'utilizzo del servizio di base (o di base) GuardDuty , vedere. GuardDuty Quote Amazon

Le tabelle seguenti descrivono le quote multiple che verranno applicate al tuo. Account AWS

AWS valore di quota predefinito	È regolabile?	Descrizione
5 GB	No	La dimensione massima dell'oggetto S3 che GuardDuty tenterà di eseguire la scansione alla ricerca di malware.
5 GB	No	La quantità massima di dati (in GB) che è GuardDuty possibile estrarre e analizzare da un file di archivio. Anche se un file di archivio contiene più di 5 GB, GuardDuty ignorerà il contenuto oltre questo valore.
1.000	No	Il numero massimo di file che è GuardDuty possibile estrarre e analizzare in un file di archivio. Se il file contiene più di 1.000 file, GuardDuty sarà necessario saltare il file archiviato.
5	No	I livelli massimi di archivi annidati che è GuardDuty possibile estrarre. Se l'archivio include file nidificati oltre questo valore, GuardDuty ignorerà tali file nidificati.
25	No	Il numero massimo di bucket S3 per i quali è possibile abilitare Malware Protection for S3. Questo limite di quota è per account in ogni regione.

AWS valore di quota predefinito	È regolabile?	Descrizione
25	A livello di regione	Il numero massimo di operazioni sul piano di controllo che possono essere avviate al secondo in ciascuna regione. Le API operazioni includono la creazione, la lettura, l'aggiornamento e l'eliminazione delle risorse. Questo valore di quota si applica a livello di regione.

GuardDuty RDSProtezione

RDSLa protezione in Amazon GuardDuty analizza e profila l'attività di RDS accesso per potenziali minacce di accesso ai tuoi database Amazon Aurora (Amazon Aurora My -Compatible Edition e Aurora Postgre SQL -Compatible Edition) e Amazon for SQL Postgre. RDS SQL La funzionalità consente di identificare comportamenti di accesso potenzialmente sospetti. RDSLa protezione non richiede un'infrastruttura aggiuntiva; è progettata in modo da non influire sulle prestazioni delle istanze di database.

Quando RDS Protection rileva un tentativo di accesso potenzialmente sospetto o anomalo che indica una minaccia per il database, GuardDuty genera una nuova scoperta con dettagli sul database potenzialmente compromesso.

Puoi abilitare o disabilitare la funzione di RDS protezione per qualsiasi account in qualsiasi Regione AWS luogo in cui questa funzione è disponibile in Amazon GuardDuty, in qualsiasi momento. Un GuardDuty account esistente può abilitare RDS Protection con un periodo di prova di 30 giorni. Per un nuovo GuardDuty account, RDS la protezione è già abilitata e inclusa nel periodo di prova gratuito di 30 giorni. Per ulteriori informazioni, consulta Stima del costo.

> **Note**
>
> Quando la funzionalità di RDS protezione non è abilitata, GuardDuty non raccoglie le attività di RDS accesso dell'utente né rileva comportamenti di accesso anomali o sospetti.

Per informazioni su Regioni AWS dove GuardDuty non supporta ancora la protezione, consulta. RDS Disponibilità di funzionalità specifiche per ogni regione

Database Amazon Aurora e Amazon supportati RDS

La tabella seguente mostra le versioni dei RDS database Aurora e Amazon supportate.

Amazon Aurora e motore Amazon DB RDS	Versioni del motore supportate
Aurora Mia SQL	• 2.10.2 o versioni successive • 3.02.1 o versioni successive

Amazon Aurora e motore Amazon DB RDS	Versioni del motore supportate
Aurora Postger SQL	• 10.17 o versioni successive • 11.12 o versioni successive • 12.7 o versioni successive • 13.3 o versioni successive • 14.3 o versioni successive • 15.2 o versione successiva • 16.1 o versione successiva
RDSper Postgre SQL	• 14.5 o versione successiva • 13.8 o versione successiva • 12.12 o versione successiva • 11.17 o versione successiva • 10.22 o versione successiva • RDSper la versione 15 di Postgre SQL • RDSper SQL Postgre versione 16

In che modo RDS Protection utilizza il monitoraggio delle attività RDS di accesso

RDSLa protezione in Amazon ti GuardDuty aiuta a proteggere i database Amazon Aurora (Aurora) e SQL Postgre RDS supportati nel tuo account. Dopo aver abilitato la funzionalità di RDS protezione, inizia GuardDuty immediatamente a monitorare l'attività di RDS accesso dai database Aurora e Amazon RDS nel tuo account. GuardDuty monitora e profila continuamente l'attività di RDS accesso per attività sospette, ad esempio l'accesso non autorizzato al database Aurora nel tuo account, da parte di un attore esterno invisibile in precedenza. Quando si attiva la RDS protezione per la prima volta o si dispone di un'istanza di database appena creata, è necessario un periodo di apprendimento per definire il comportamento normale. Per questo motivo, alle istanze di database appena abilitate o appena create potrebbero non essere associati esiti relativi a un accesso anomalo per un massimo di due settimane. Per ulteriori informazioni, consulta RDSmonitoraggio delle attività di accesso.

Quando RDS Protection rileva una potenziale minaccia, ad esempio uno schema insolito in una serie di tentativi di accesso riusciti, falliti o incompleti, GuardDuty genera una nuova scoperta con dettagli

sull'istanza di database potenzialmente compromessa. Per ulteriori informazioni, consulta Tipi di esiti della Protezione RDS. Se si disabilita RDS la protezione, interrompe GuardDuty immediatamente il monitoraggio dell'attività di RDS accesso e non è in grado di rilevare alcuna potenziale minaccia per le istanze di database supportate.

> **Note**
>
> GuardDuty non gestisce la tua attività Database supportati o quella di RDS accesso né ti rende disponibile l'attività di RDS accesso.

Funzionalità di RDS protezione

RDSmonitoraggio delle attività di accesso

RDSl'attività di accesso registra sia i tentativi di accesso riusciti che quelli non riusciti effettuati Database Amazon Aurora e Amazon supportati RDS nell' AWS ambiente dell'utente. Per aiutarvi a proteggere i database, GuardDuty RDS Protection monitora continuamente l'attività di accesso alla ricerca di tentativi di accesso potenzialmente sospetti. Ad esempio, un avversario potrebbe tentare un accesso di forza bruta a un database Amazon Aurora cercando di indovinarne la password.

Quando abiliti la funzionalità di RDS protezione, inizia GuardDuty automaticamente a monitorare l'attività di RDS accesso per i tuoi database direttamente dai servizi Aurora e AmazonRDS. Se c'è un'indicazione di un comportamento di accesso anomalo, GuardDuty genera un risultato con dettagli sul database potenzialmente compromesso. Quando si attiva la RDS protezione per la prima volta o si dispone di un'istanza di database appena creata, è necessario un periodo di apprendimento per definire il comportamento normale. Per questo motivo, alle istanze di database appena abilitate o appena create potrebbero non essere associati esiti relativi a un accesso anomalo per un massimo di due settimane.

La funzionalità di RDS protezione non richiede alcuna configurazione aggiuntiva; non influisce su alcun database Amazon Aurora esistente o sulle configurazioni Amazon AmazonRDS. GuardDuty non gestisce i database o le attività di RDS accesso supportati né rende disponibile l'attività di RDS accesso.

Se scegli di abilitare automaticamente la funzionalità di RDS protezione per i nuovi account membro quando entrano a far parte dell'organizzazione, questa azione si attiva automaticamente GuardDuty per quei nuovi account membro. Per ulteriori informazioni sulla configurazione del monitoraggio delle attività di RDS accesso come funzionalità, consulta. GuardDuty RDSProtezione

Configurazione della RDS protezione per un account autonomo

Console

1. Apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/
2. Nel riquadro di navigazione, scegli RDSProtezione.
3. La pagina RDSProtezione mostra lo stato attuale del tuo account. Puoi abilitare o disabilitare la funzionalità in qualsiasi momento selezionando Abilita o Disabilita. Conferma la selezione.

API/CLI

Eseguite l'updateDetectorAPIoperazione utilizzando il vostro ID regionale del rilevatore e passando l'`features`oggetto `name` come `RDS_LOGIN_EVENTS` e `status` come `ENABLED` o`DISABLED`.

È inoltre possibile abilitare o disabilitare RDS la protezione eseguendo il AWS CLI comando seguente. Assicurati di usare il tuo codice valido *`detector ID`*.

> **Note**
>
> Il codice di esempio seguente abilita RDS la protezione. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

Configurazione della RDS protezione in ambienti con più account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di abilitare o disabilitare la funzionalità di RDS protezione per gli account dei membri della propria organizzazione. GuardDutyGli account dei membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce i propri account membro

utilizzando AWS Organizations. Questo account GuardDuty amministratore delegato può scegliere di abilitare automaticamente il monitoraggio delle attività di RDS accesso per tutti i nuovi account quando entrano a far parte dell'organizzazione. Per ulteriori informazioni sugli ambienti con più account, consulta Gestione di più account in Amazon. GuardDuty

Configurazione della RDS protezione per l'account amministratore delegato GuardDuty

Scegli il metodo di accesso preferito per configurare il monitoraggio delle attività di RDS accesso per l'account amministratore delegato. GuardDuty

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali dell'account di gestione.
2. Nel riquadro di navigazione, scegli RDSProtezione.
3. Nella pagina RDSProtezione, scegli Modifica.
4. Esegui una di queste operazioni:

   Utilizzando Abilita per tutti gli account

   - Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi nell' AWS organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
   - Seleziona Salva.

   Utilizzando Configura gli account manualmente

   - Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
   - Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
   - Seleziona Salva.

API/CLI

Esegui l'updateDetectorAPIoperazione utilizzando il tuo ID regionale del rilevatore e passando l'`features`oggetto `name` come `RDS_LOGIN_EVENTS` e `status` come `ENABLED` o. `DISABLED`

È possibile abilitare o disabilitare RDS la protezione eseguendo il AWS CLI comando seguente. Assicurati di utilizzare un account GuardDuty amministratore delegato valido *detector ID*.

> **Note**
>
> Il codice di esempio seguente abilita RDS la protezione. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

Abilita automaticamente RDS la protezione per tutti gli account dei membri

Scegli il tuo metodo di accesso preferito per abilitare la funzione di RDS protezione per tutti gli account dei membri. inclusi gli account membri esistenti e i nuovi account che entrano a far parte dell'organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una di queste operazioni:

   Utilizzo della pagina Protezione RDS

   1. Nel riquadro di navigazione, scegli RDSProtezione.
   2. Scegli Abilita per tutti gli account. Questa azione abilita automaticamente RDS la protezione sia per gli account esistenti che per quelli nuovi dell'organizzazione.
   3. Seleziona Salva.

> **Note**
>
> L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

Utilizzando la pagina Account

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
3. Nella finestra Gestisci le preferenze di attivazione automatica, scegli Abilita per tutti gli account in Monitoraggio delle attività di RDS accesso.
4. Seleziona Salva.

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta Abilita o disabilita in modo selettivo RDS la protezione per gli account dei membri.

API/CLI

- Per abilitare o disabilitare in modo selettivo RDS la protezione per i tuoi account membro, richiama l'updateMemberDetectorsAPIoperazione utilizzando la tua *`detector ID`*.
- L'esempio seguente mostra come abilitare la RDS protezione per un account con un solo membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

> **Note**
>
> Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita RDS la protezione per tutti gli account dei membri attivi esistenti

Scegli il metodo di accesso preferito per abilitare la RDS protezione per tutti gli account membri attivi esistenti nella tua organizzazione.

Console

Per configurare RDS la protezione per tutti gli account dei membri attivi esistenti

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, scegli RDS Protezione.
3. Nella pagina RDSProtezione, puoi visualizzare lo stato corrente della configurazione. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Conferma.

API/CLI

- Per abilitare o disabilitare in modo selettivo la RDS protezione per i tuoi account membro, richiama l'updateMemberDetectorsAPIoperazione utilizzando la tua *`detector ID`*.
- L'esempio seguente mostra come abilitare la RDS protezione per un account con un solo membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

> **Note**
>
> Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita automaticamente RDS la protezione per gli account dei nuovi membri

Scegli il metodo di accesso preferito per abilitare l'attività di RDS accesso per i nuovi account che entrano a far parte della tua organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare nuovi account membro in un'organizzazione tramite la console, utilizzando la pagina RDSProtezione o Account.

Per abilitare automaticamente la RDS protezione per gli account dei nuovi membri

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Esegui una di queste operazioni:
   - Utilizzo della pagina RDSProtezione:

     1. Nel riquadro di navigazione, scegli RDSProtezione.
     2. Nella pagina RDSProtezione, scegli Modifica.
     3. Scegli Configura gli account manualmente.

4. Seleziona Abilita automaticamente per i nuovi account membri. Questo passaggio garantisce che ogni volta che un nuovo account si unisce alla tua organizzazione, RDS la protezione venga automaticamente abilitata per l'account. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
5. Seleziona Salva.

- Utilizzando la pagina Account:

1. Dal riquadro di navigazione, selezionare Accounts (Account).
2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.
3. Nella finestra Gestisci le preferenze di attivazione automatica, seleziona Abilita per nuovi account in Monitoraggio delle attività di RDS accesso.
4. Seleziona Salva.

API/CLI

- Per abilitare o disabilitare in modo selettivo RDS la protezione per i tuoi account membro, richiama l'UpdateOrganizationConfigurationAPIoperazione utilizzando la tua *`detector ID`*.
- L'esempio seguente mostra come abilitare la RDS protezione per un account con un solo membro. Per disabilitarlo, consulta Abilita o disabilita in modo selettivo RDS la protezione per gli account dei membri. Se non desideri abilitarlo per tutti i nuovi account che entrano a far parte dell'organizzazione, imposta `autoEnable` su `NONE`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilita o disabilita in modo selettivo RDS la protezione per gli account dei membri

Scegli il metodo di accesso preferito per abilitare o disabilitare in modo selettivo il monitoraggio delle attività di RDS accesso per gli account dei membri.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Dal riquadro di navigazione, selezionare Accounts (Account).

   Nella pagina Account, consulta la colonna relativa all'attività di RDS accesso per verificare lo stato del tuo account membro.
3. Per abilitare o disabilitare in modo selettivo l'attività di RDS accesso

   Seleziona l'account per il quale desideri configurare la RDS protezione. Puoi selezionare più account alla volta. Nel menu a discesa Modifica piani di protezione, scegli Attività di RDS accesso, quindi scegli l'opzione appropriata.

API/CLI

Per abilitare o disabilitare in modo selettivo RDS la protezione per i tuoi account membro, richiama l'updateMemberDetectorsAPIoperazione utilizzando la tua *`detector ID`*.

L'esempio seguente mostra come abilitare la RDS protezione per un account con un solo membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

> **Note**
>
> Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

GuardDuty Protezione Lambda

La Protezione Lambda è utile per identificare potenziali minacce alla sicurezza quando una funzione AWS Lambda viene richiamata nel tuo ambiente AWS . Quando abiliti Lambda Protection, GuardDuty inizia a monitorare i registri delle attività di rete Lambda, a partire da Log di flusso VPC tutte le funzioni Lambda per account, inclusi i registri che non utilizzano la reteVPC, e vengono generati quando viene richiamata la funzione Lambda. Se GuardDuty identifica un traffico di rete sospetto che è indicativo della presenza di un codice potenzialmente dannoso nella funzione Lambda, GuardDuty genererà un risultato.

> **Note**
>
> Il monitoraggio delle attività di rete Lambda non include i log per le funzioni Lambda @Edge.

Puoi configurare Lambda Protection per qualsiasi account o disponibile Regioni AWS, in qualsiasi momento. Per impostazione predefinita, un GuardDuty account esistente può abilitare Lambda Protection con un periodo di prova di 30 giorni. Per un nuovo GuardDuty account, Lambda Protection è già abilitata e inclusa nel periodo di prova di 30 giorni. Per informazioni sulle statistiche di utilizzo, consulta Stima del costo.

GuardDuty monitora i registri delle attività di rete generati richiamando le funzioni Lambda. Attualmente, Lambda Network Activity Monitoring include i log di flusso VPC Amazon di tutte le funzioni Lambda del tuo account, compresi i log che non VPC utilizzano la rete e sono soggetti a modifiche, inclusa l'espansione ad altre attività di rete DNS come i dati di query generati richiamando le funzioni Lambda. L'espansione ad altre forme di monitoraggio delle attività di rete aumenterà il volume di dati che GuardDuty verranno elaborati per Lambda Protection. il che avrà un impatto diretto sul costo di utilizzo di questa protezione. Ogni volta che GuardDuty inizia a monitorare un registro delle attività di rete aggiuntivo, fornirà un avviso agli account che hanno attivato Lambda Protection, almeno 30 giorni prima del rilascio.

Funzionalità della Protezione Lambda

Monitoraggio delle attività di rete Lambda

Quando abiliti Lambda Protection, GuardDuty monitora i registri delle attività di rete Lambda generati quando viene richiamata una funzione Lambda associata al tuo account. Ciò consente di rilevare

potenziali minacce alla sicurezza della funzione Lambda. GuardDuty monitora i log di VPC flusso di tutte le funzioni Lambda, comprese quelle che non utilizzano la rete. VPC Per le funzioni Lambda configurate per utilizzare la VPC rete, non è necessario abilitare i log di VPC flusso per le interfacce di rete elastiche () ENI create da Lambda for. GuardDuty GuardDuty addebita solo la quantità di dati dei registri delle attività di rete Lambda elaborati (in GB) per generare un risultato. GuardDuty ottimizza i costi applicando filtri intelligenti e analizzando un sottoinsieme di registri delle attività di rete Lambda rilevanti per il rilevamento delle minacce. Per informazioni sui prezzi, consulta la pagina GuardDuty dei prezzi di Amazon.

GuardDuty non gestisce i registri delle attività della rete Lambda (inclusi VPC i registri non di VPC flusso) né li rende accessibili nel tuo account.

Configurazione della Protezione Lambda

Configurazione della Protezione Lambda per un account autonomo

Per gli account associati a AWS Organizations, puoi automatizzare questo processo tramite la GuardDuty console o API le istruzioni, come descritto nella sezione successiva.

Scegli il metodo di accesso che preferisci per abilitare o disabilitare la Protezione Lambda per un account autonomo.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, in Impostazioni, scegli Protezione Lambda.
3. La pagina della Protezione Lambda mostra lo stato attuale del tuo account. Puoi abilitare o disabilitare la funzionalità in qualsiasi momento selezionando Abilita o Disabilita.
4. Seleziona Salva.

API/CLI

Eseguite l'updateDetectorAPIoperazione utilizzando il vostro ID regionale del rilevatore e passando l'`features`oggetto `name` come `LAMBDA_NETWORK_LOGS` e `status` come `ENABLED` o`DISABLED`.

Puoi anche abilitare o disabilitare il monitoraggio dell'attività di rete Lambda eseguendo il comando seguente AWS CLI . Assicurati di usare il tuo codice valido *`detector ID`*.

> **Note**
>
> Il codice di esempio seguente abilita il monitoraggio delle attività di rete Lambda. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

Configurazione della Protezione Lambda in ambienti multi-account

In un ambiente con più account, solo l'account GuardDuty amministratore delegato ha la possibilità di abilitare o disabilitare Lambda Protection per gli account dei membri della propria organizzazione. GuardDuty Gli account membri non possono modificare questa configurazione dai propri account. L'account GuardDuty amministratore delegato gestisce gli account dei membri utilizzando AWS Organizations. L'account GuardDuty amministratore delegato può scegliere di abilitare automaticamente il monitoraggio dell'attività di rete Lambda per tutti i nuovi account quando entrano a far parte dell'organizzazione. Per ulteriori informazioni sugli ambienti con più account, consulta Gestione di più account in Amazon GuardDuty.

Configurazione di Lambda Protection per GuardDuty l'account amministratore delegato

Scegli il tuo metodo di accesso preferito per abilitare o disabilitare il monitoraggio dell'attività di rete Lambda per l'account amministratore delegato GuardDuty .

Console

1. Apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/

   Assicurati di utilizzare le credenziali dell'account di gestione.
2. Nel riquadro di navigazione, in Impostazioni, scegli Protezione Lambda.
3. Nella pagina Protezione Lambda, scegli Modifica.
4. Esegui una di queste operazioni:

Utilizzando Abilita per tutti gli account

- Scegli Abilita per tutti gli account. Ciò abiliterà il piano di protezione per tutti gli GuardDuty account attivi AWS dell'organizzazione, inclusi i nuovi account che entrano a far parte dell'organizzazione.
- Seleziona Salva.

Utilizzando Configura gli account manualmente

- Per abilitare il piano di protezione solo per l'account GuardDuty amministratore delegato, scegli Configura gli account manualmente.
- Scegli Abilita nella sezione Account GuardDuty amministratore delegato (questo account).
- Seleziona Salva.

API/CLI

Esegui l'updateDetectorAPIoperazione utilizzando il tuo ID regionale del rilevatore e passando l'`features`oggetto `name` come `LAMBDA_NETWORK_LOGS` e `status` come `ENABLED` o. `DISABLED`

È possibile abilitare o disabilitare il monitoraggio dell'attività di rete Lambda eseguendo il comando seguente AWS CLI . Assicurati di utilizzare un account di GuardDuty amministratore delegato valido *`detector ID`*.

> **Note**
>
> Il codice di esempio seguente abilita il monitoraggio delle attività di rete Lambda. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare l'`detectorId`account e la regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

```
aws guardduty update-detector --detector-
id 12abc34d567e8fa901bc2d34e56789f0 555555555555 --features '[{"Name":
 "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

Abilitare automaticamente il monitoraggio delle attività di rete Lambda per tutti gli account membri

Scegli il metodo di accesso che preferisci per abilitare la funzionalità di monitoraggio delle attività di rete Lambda per tutti gli account membri, inclusi gli account membri esistenti e i nuovi account che entrano a far parte dell'organizzazione.

Console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Esegui una di queste operazioni:

   Utilizzando la pagina Protezione Lambda

   1. Nel riquadro di navigazione, scegli Protezione Lambda.
   2. Scegli Abilita per tutti gli account. Questa operazione abilita automaticamente il monitoraggio delle attività di rete Lambda per gli account dell'organizzazione esistenti e per quelli nuovi.
   3. Seleziona Salva.

   > **Note**
   >
   > L'aggiornamento della configurazione per gli account membri può richiedere fino a 24 ore.

   Utilizzando la pagina Account

   1. Dal riquadro di navigazione, selezionare Accounts (Account).
   2. Nella pagina Account, scegli le preferenze di Abilitazione automatica, quindi Aggiungi account tramite invito.
   3. Nella finestra Gestisci le preferenze di abilitazione automatica, scegli Abilita per tutti gli account in Monitoraggio delle attività di rete Lambda.

> **Note**
>
> Per impostazione predefinita, questa azione attiva automaticamente l'opzione Attivazione automatica GuardDuty per nuovi account membro.

4. Seleziona Salva.

Se non puoi utilizzare l'opzione Abilita per tutti gli account, consulta Abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri.

API/CLI

- Per abilitare o disabilitare selettivamente il monitoraggio dell'attività di rete Lambda per i tuoi account membro, richiama l'operazione utilizzando updateMemberDetectorsAPIil tuo *`detector ID`*.
- L'esempio seguente mostra come abilitare il monitoraggio delle attività di rete Lambda per un singolo account membro. Per disabilitare un account membro, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

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

  Puoi anche passare un elenco di account IDs separati da uno spazio.
- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare il monitoraggio delle attività di rete Lambda per tutti gli account membri attivi esistenti

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio delle attività di rete Lambda per tutti gli account membri attivi esistenti dell'organizzazione.

Console

Per configurare il monitoraggio delle attività di rete Lambda per tutti gli account membri attivi esistenti

1. Accedi a AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Accedi utilizzando le credenziali GuardDuty dell'account amministratore delegato.
2. Nel riquadro di navigazione, scegli Protezione Lambda.
3. Nella pagina Protezione Lambda, puoi visualizzare lo stato attuale della configurazione. Nella sezione Account membri attivi, scegli Operazioni.
4. Dal menu a discesa Operazioni, scegli Abilita per tutti gli account membri attivi esistenti.
5. Scegli Conferma.

API/CLI

- Per abilitare o disabilitare selettivamente il monitoraggio dell'attività di rete Lambda per i tuoi account membro, richiama l'operazione utilizzando updateMemberDetectorsAPIil tuo *`detector ID`*.
- L'esempio seguente mostra come abilitare il monitoraggio delle attività di rete Lambda per un singolo account membro. Per disabilitare un account membro, sostituisci `ENABLED` con `DISABLED`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

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

  Puoi anche passare un elenco di account IDs separati da uno spazio.

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare automaticamente il monitoraggio delle attività di rete Lambda per i nuovi account membri

Scegli il metodo di accesso che preferisci per abilitare il monitoraggio delle attività di rete Lambda per i nuovi account che entrano a far parte dell'organizzazione.

Console

L'account GuardDuty amministratore delegato può abilitare il monitoraggio dell'attività di rete Lambda per i nuovi account membro di un'organizzazione, utilizzando la pagina Lambda Protection o Account.

Per abilitare automaticamente il monitoraggio delle attività di rete Lambda per i nuovi account membri

1. Apri la console all' GuardDuty indirizzo. https://console.aws.amazon.com/guardduty/

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.
2. Esegui una di queste operazioni:
   - Utilizzando la pagina Protezione Lambda:
     1. Nel riquadro di navigazione, scegli Protezione Lambda.
     2. Nella pagina Protezione Lambda, scegli Modifica.
     3. Scegli Configura gli account manualmente.
     4. Seleziona Abilita automaticamente per i nuovi account membri. Questa fase garantisce l'abilitazione automatica della Protezione Lambda per ogni nuovo account che entra a far parte dell'organizzazione. Solo l'account GuardDuty amministratore delegato dell'organizzazione può modificare questa configurazione.
     5. Seleziona Salva.
   - Utilizzando la pagina Account:
     1. Dal riquadro di navigazione, selezionare Accounts (Account).
     2. Nella pagina Account, scegli le preferenze di Abilitazione automatica.

3. Nella finestra Gestisci le preferenze di abilitazione automatica, seleziona Abilita per nuovi account in Monitoraggio delle attività di rete Lambda.
4. Seleziona Salva.

API/CLI

- Per abilitare o disabilitare il monitoraggio dell'attività di rete Lambda per i nuovi account membro, richiama l'UpdateOrganizationConfigurationAPIoperazione utilizzando il tuo *detector ID*.
- L'esempio seguente mostra come abilitare il monitoraggio delle attività di rete Lambda per un singolo account membro. Per disabilitarlo, consulta Abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri. Se non desideri abilitarlo per tutti i nuovi account che entrano a far parte dell'organizzazione, imposta `AutoEnable` su `NONE`.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

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

- Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri

Scegli il metodo di accesso che preferisci per abilitare o disabilitare in modo selettivo il monitoraggio delle attività di rete Lambda per gli account membri.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare le credenziali GuardDuty dell'account amministratore delegato.

2. Nel riquadro di navigazione, in Settings (Impostazioni), scegliere Accounts (Account).

   Nella pagina Account, consulta la colonna Monitoraggio delle attività di rete Lambda, che indica se il monitoraggio delle attività di rete Lambda è abilitato o meno.
3. Scegli l'account per il quale desideri configurare la Protezione Lambda. Puoi scegliere più account alla volta.
4. Dal menu a discesa Modifica piani di protezione, scegli Monitoraggio delle attività di rete Lambda, quindi scegli l'operazione appropriata.

API/CLI

Invoca usando le tue updateMemberDetectorsAPI *`detector ID`*.

L'esempio seguente mostra come abilitare il monitoraggio delle attività di rete Lambda per un singolo account membro. Per disabilitarla, sostituisci `ENABLED` con `DISABLED`.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

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

Puoi anche passare un elenco di account IDs separati da uno spazio.

Se il codice viene eseguito correttamente, restituisce un elenco vuoto di `UnprocessedAccounts`. Se si verifica qualsiasi problema durante la modifica delle impostazioni del rilevatore di un account, l'ID dell'account viene elencato insieme a un riepilogo del problema.

Protezione dei carichi di lavoro AI con GuardDuty

Amazon GuardDuty Foundational Threat Detection e Lambda Protection ti aiutano a proteggere e rilevare meglio le minacce ai carichi di lavoro di intelligenza artificiale su cui si basano. AWS

Il rilevamento fondamentale delle GuardDuty minacce monitora gli eventi di AWS CloudTrail gestione per rilevare attività sospette e dannose nei carichi di lavoro di intelligenza artificiale generativi creati utilizzando servizi AWS , tra cui Amazon Bedrock e Amazon. SageMaker Ad esempio, può identificare attività come GuardDuty :

- Rimozione insolita dei parapetti di sicurezza di Amazon Bedrock
- Modifica della fonte dei dati di addestramento del modello che può potenzialmente portare a un attacco di data poisoning
- Richiamata sospetta del modello Amazon Bedrock
- Istanza insolita di un notebook o creazione di posti di lavoro di formazione in SageMaker
- Credenziali Amazon Elastic Compute Cloud esfiltrate che potrebbero essere state utilizzate per richiamare APIs Amazon Bedrock, Amazon o carichi di lavoro AI autogestiti su EC2 istanze SageMaker, cluster o attività. EKS ECS

GuardDuty Lambda Protection può aiutare a rilevare potenziali minacce legate agli agenti Amazon Bedrock. Ciò può includere attività di rete sospette, come il cryptomining, e la comunicazione con server di comando e controllo malevoli, che possono essere causate da attacchi alla catena di fornitura o richieste complesse.

Il video seguente mostra come apparirebbero i risultati associati.

Il video seguente mostra come apparirebbero i risultati associati. Utilizzo GuardDuty di Amazon per monitorare e proteggere i carichi di lavoro di intelligenza artificiale basati su AWS

Gestione di più account in Amazon GuardDuty

Se AWS l'ambiente dispone di più account, è possibile gestirli designandone uno Account AWS come account amministratore. È quindi possibile associare i multipli Account AWS a questo account amministratore come account membro. Con questa configurazione, un account GuardDuty amministratore designato può valutare e monitorare la sicurezza generale dell'organizzazione. L'account amministratore può anche eseguire attività di gestione degli account, come la revisione di tutti i risultati generati e la configurazione dei piani di protezione interni GuardDuty.

In GuardDuty, un'organizzazione è composta da un account GuardDuty amministratore delegato e da uno o più account membro associati. È possibile associare gli account in due modi: mediante l'integrazione o utilizzando un metodo legacy di invio e accettazione degli inviti di iscrizione nella console. AWS Organizations GuardDuty GuardDuty consiglia l'integrazione con. AWS Organizations

AWS Organizations è un servizio globale di gestione degli account che consente AWS agli amministratori di consolidare e gestire centralmente più account. Account AWS Fornisce funzionalità di gestione degli account e fatturazione consolidata progettate per supportare le esigenze di budget, sicurezza e conformità. È offerto senza costi aggiuntivi e si integra con più piattaforme AWS servizi, tra cui Macie e Amazon. AWS Security Hub GuardDuty Per ulteriori informazioni, consulta la Guida per l'utente AWS Organizations.

Indice

Comprensione della relazione tra account GuardDuty amministratore e account membro

Quando si utilizza GuardDuty in un ambiente con più account, l'account amministratore può gestire determinati aspetti per GuardDuty conto degli account dei membri. Un account amministratore può svolgere le seguenti funzioni principali:

- Aggiungere e rimuovere gli account membri associati. Il processo con cui un account amministratore può eseguire questa operazione varia in base alla modalità di gestione degli account, tramite organizzazioni o tramite invito.

- Attivazione GuardDuty dell'account amministratore delegato GuardDuty nell'account di gestione

  Se l'account di AWS Organizations gestione viene disabilitato GuardDuty, l'account GuardDuty amministratore delegato può essere abilitato GuardDuty nell'account di gestione. Tuttavia, è necessario che l'account di gestione non abbia eliminato in modo esplicito il. Autorizzazioni di ruolo collegate ai servizi per GuardDuty
- Gestisci lo stato degli GuardDuty account dei membri associati, incluse l'attivazione e la sospensione GuardDuty.

  > **Note**
  >
  > Account amministrativi delegati gestiti con attivazione AWS Organizations GuardDuty automatica degli account aggiunti come membri.

- Personalizza i risultati all'interno della GuardDuty rete attraverso la creazione e la gestione di regole di soppressione, elenchi di IP affidabili ed elenchi di minacce. In un ambiente con più account, la configurazione di queste funzionalità è disponibile solo per un account amministratore delegato. GuardDuty Un account membro non può aggiornare questa configurazione.

La tabella seguente descrive in dettaglio la relazione tra account GuardDuty amministratore e account membro.

In questa tabella:

- Autonomo: un account può eseguire l'azione elencata solo per il proprio account.
- Qualsiasi: un account può eseguire l'azione elencata per qualsiasi account associato.
- Tutti: un account può eseguire l'azione elencata e questa si applica a tutti gli account associati. In genere, l'account che esegue questa azione è un account GuardDuty amministratore designato

Le celle della tabella con un trattino (—) indicano che l'account non può eseguire l'azione elencata.

Action	Tramite AWS Organizations		Su invito	
	Account GuardDuty amministratore delegato	Account membro associato	Account GuardDuty amministratore delegato	Account membro associato

Abilita GuardDuty	Qualsiasi	–	Personale	Personale
Abilita GuardDuty automaticamente per l'intera organizzazione (`ALL`,`NEW`,`NONE`)	Tutti	–	–	–
Visualizza tutti gli account dei membri di Organizations indipendentemente GuardDuty dallo stato	Qualsiasi	–	–	–
Genera risultati campione	Personale	Personale	Personale	Personale
Visualizza tutti i GuardDuty risultati	Qualsiasi	Personale	Qualsiasi	Personale
Archivia GuardDuty i risultati	Qualsiasi	–	Qualsiasi	–
Applica regole di soppressione	Tutti	–	Tutti	–
Crea un elenco di IP o elenchi di minacce affidabili	Tutti	–	Tutti	–

Aggiorna l'elenco di IP attendibili o gli elenchi di minacce	Tutti	–	Tutti	–
Eliminare l'elenco di IP attendibili o gli elenchi di minacce	Tutti	–	Tutti	–
Imposta la frequenza di EventBridge notifica	Tutti	–	Tutti	Personale
Imposta la posizione Amazon S3 per l'esportazione degli esiti	Tutti	–	Tutti	Personale
Abilita uno o più piani di protezione opzionali per l'intera organizzazione (`ALL`,`NEW`,`NONE`) Questo non include Malware Protection for S3.	Tutti	–	–	–

Abilita qualsiasi piano di GuardDuty protezione per i singoli account Ciò non include Malware Protection for EC2 e Malware Protection for S3.	Qualsiasi	–	Qualsiasi	–
Protezione da malware per EC2	Qualsiasi	–	Personale	Personale
Protezione da malware per S3	–	Personale	–	Personale
Annulla l'associazione di un account membro	Qualsiasi	–	Qualsiasi	–
Dissociarsi da un account amministratore	–	Self +	–	Personale
Eliminare un account membro dissociato	Qualsiasi	–	Qualsiasi	–
Sospendere GuardDuty	Qualunque *	–	Qualunque *	–
Disabilita GuardDuty	Qualunque *	–	Qualunque *	–

[+] Indica che l'account può eseguire questa azione solo se l'account GuardDuty amministratore delegato non ha impostato la preferenza di attivazione automatica per `ALL` i membri dell'organizzazione.

[*] Indica che un account GuardDuty amministratore delegato non può essere disabilitato direttamente GuardDuty in un account membro. L'account GuardDuty amministratore delegato deve prima dissociare l'account membro e quindi eliminarlo. Dopodiché, ogni account membro può essere disattivato GuardDuty nei propri account. Per ulteriori informazioni sull'esecuzione di queste attività all'interno dell'organizzazione, consultaMantenere la propria organizzazione all'interno GuardDuty.

Gestione GuardDuty degli account con AWS Organizations

In un' AWS organizzazione, l'account di gestione può designare qualsiasi account all'interno di questa organizzazione come account amministratore delegato. GuardDuty Per questo account amministratore, GuardDuty viene abilitato automaticamente solo nell'account corrente. Regione AWS Per impostazione predefinita, l'account amministratore può abilitare e gestire tutti GuardDuty gli account dei membri dell'organizzazione all'interno di quella regione. L'account amministratore può visualizzare e aggiungere membri a questa AWS organizzazione.

Le seguenti sezioni illustreranno le varie attività che è possibile eseguire come account GuardDuty amministratore delegato.

Considerazioni e consigli per l'utilizzo con GuardDuty AWS Organizations

Le considerazioni e i consigli seguenti possono aiutarti a capire come funziona un account GuardDuty amministratore delegato in: GuardDuty

Un account GuardDuty amministratore delegato può gestire un massimo di 50.000 membri.

- È previsto un limite di 50.000 account membro per account amministratore delegato GuardDuty . Ciò include gli account membro aggiunti tramite AWS Organizations o quelli che hanno accettato l'invito dell'account GuardDuty amministratore a entrare a far parte della propria organizzazione. Tuttavia, nella tua AWS organizzazione potrebbero esserci più di 50.000 account.

  Se superi il limite di 50.000 account membri, riceverai una notifica e un'e-mail all'account amministratore delegato designato GuardDuty . CloudWatch AWS Health Dashboard

Un account GuardDuty amministratore delegato è regionale.

- Al contrario AWS Organizations, GuardDuty è un servizio regionale. Gli account di GuardDuty amministratore delegato e i relativi account membro devono essere aggiunti AWS Organizations

in ogni regione desiderata in cui è stata GuardDuty abilitata. Se l'account di gestione dell'organizzazione designa un account GuardDuty amministratore delegato solo negli Stati Uniti orientali (Virginia settentrionale), l'account GuardDuty amministratore delegato gestirà solo gli account dei membri aggiunti all'organizzazione in quella regione. Per ulteriori informazioni sulla parità di funzionalità nelle regioni in cui GuardDuty è disponibile, consulta. Regioni ed endpoint

Casi speciali per le regioni che hanno aderito

- Quando un account GuardDuty amministratore delegato disattiva un'area di attivazione, anche se l'organizzazione ha la configurazione di GuardDuty attivazione automatica impostata su Solo nuovi account membro (`NEW`) o su tutti gli account membro (`ALL`), GuardDuty non può essere abilitata per nessun account membro dell'organizzazione attualmente disabilitato. GuardDuty Per informazioni sulla configurazione degli account membro, apri Account nel riquadro di navigazione della GuardDuty console o utilizza il. ListMembersAPI
- Quando lavori con la configurazione di GuardDuty attivazione automatica impostata su`NEW`, assicurati che sia soddisfatta la seguente sequenza:

  1. Gli account dei membri aderiscono a una regione opt-in.
  2. Aggiungi gli account dei membri alla tua organizzazione in. AWS Organizations

  Se modifichi l'ordine di questi passaggi, l'impostazione di GuardDuty attivazione automatica con non **`NEW`** funzionerà nella regione di attivazione specifica perché l'account membro non è più nuovo per l'organizzazione. GuardDuty offre due soluzioni alternative:

  - Imposta la configurazione di GuardDuty attivazione automatica su`ALL`, che include account membri nuovi ed esistenti. In questo caso, l'ordine di questi passaggi non è rilevante.
  - Se un account membro fa già parte dell'organizzazione, gestisci la GuardDuty configurazione di questo account singolarmente nella regione di attivazione specifica utilizzando la GuardDuty console o ilAPI.

È necessario che un' AWS organizzazione disponga dello stesso account GuardDuty amministratore delegato in tutti i. Regioni AWS

È necessario designare un account membro come account GuardDuty amministratore delegato per tutti gli account where abilitati Regioni AWS . GuardDuty Ad esempio, se si designa un account membro *`111122223333`* in *`Europe (Ireland)`*, non puoi designare un altro account membro *`555555555555`* in *`Canada (Central)`*. È necessario utilizzare lo stesso account dell'account GuardDuty amministratore delegato in tutte le altre regioni.

È possibile designare un nuovo account GuardDuty amministratore delegato in qualsiasi momento. Per ulteriori informazioni sulla rimozione dell'account GuardDuty amministratore delegato esistente, consulta. Modifica dell'account amministratore delegato GuardDuty

Non è consigliabile impostare l'account di gestione dell'organizzazione come account GuardDuty amministratore delegato.

L'account di gestione dell'organizzazione può essere l'account GuardDuty amministratore delegato. Tuttavia, le best practice di sicurezza AWS seguono il principio del privilegio minimo e sconsigliano questa configurazione.

La modifica di un account GuardDuty amministratore delegato non disabilita gli account GuardDuty dei membri.

Se rimuovi un account GuardDuty amministratore delegato, GuardDuty rimuove tutti gli account membro associati a tale account amministratore delegato GuardDuty . GuardDuty rimane comunque abilitato per tutti questi account membro.

Autorizzazioni necessarie per designare un account amministratore delegato GuardDuty

Per iniziare a utilizzare Amazon GuardDuty con AWS Organizations, l'account di AWS Organizations gestione dell'organizzazione designa un account come account GuardDuty amministratore delegato. Ciò consente GuardDuty come servizio affidabile in. AWS Organizations Abilita inoltre GuardDuty l'account GuardDuty amministratore delegato e consente inoltre all'account amministratore delegato di abilitare e gestire GuardDuty altri account dell'organizzazione nella regione corrente. Per informazioni su come vengono concesse queste autorizzazioni, vedere Utilizzo AWS Organizations con altri servizi. AWS

Come account di AWS Organizations gestione, prima di designare l'account GuardDuty amministratore delegato per l'organizzazione, verificate di poter eseguire le seguenti GuardDuty azioni:. `guardduty:EnableOrganizationAdminAccount` Questa azione consente di designare l'account GuardDuty amministratore delegato per l'organizzazione utilizzando. GuardDuty È inoltre necessario assicurarsi di avere il permesso di eseguire le AWS Organizations azioni che consentono di recuperare informazioni sulla propria organizzazione.

Per concedere queste autorizzazioni, includi la seguente dichiarazione in una politica AWS Identity and Access Management (IAM) per il tuo account:

```
{
```

```
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

Se desideri designare il tuo account di AWS Organizations gestione come account GuardDuty amministratore delegato, anche il tuo account richiederà l'IAMazione:. `CreateServiceLinkedRole` Questa azione consente di inizializzare l'account GuardDuty di gestione. Tuttavia, controlla Considerazioni e consigli per l'utilizzo con GuardDuty AWS Organizations prima di procedere con l'aggiunta delle autorizzazioni.

Per continuare a designare l'account di gestione come account GuardDuty amministratore delegato, aggiungi la seguente dichiarazione alla politica e sostituisci IAM *111122223333* con l' Account AWS ID dell'account di gestione della tua organizzazione:

```
{
 "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"
  }
 }
}
```

Designazione di un account amministratore delegato GuardDuty

Scegli un metodo di accesso preferito per designare un account GuardDuty amministratore delegato per la tua organizzazione. Solo un account di gestione può eseguire questo passaggio.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Per accedere, utilizza le credenziali dell'account di gestione della tua AWS Organizations organizzazione.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri designare l'account amministratore delegato GuardDuty per la tua organizzazione.
3. Effettua una delle seguenti operazioni, a seconda che GuardDuty sia abilitato per il tuo account di gestione nella regione corrente:

   - Se GuardDuty è abilitato, seleziona Amazon GuardDuty - tutte le funzionalità e scegli Inizia. Questa azione ti porterà alla GuardDuty pagina Benvenuto.
   - Se GuardDuty è abilitata, scegli Impostazioni nel riquadro di navigazione.
4. In Amministratore delegato, inserisci l' Account AWS ID a 12 cifre dell'account che desideri designare come account GuardDuty amministratore delegato per l'organizzazione.

   Assicurati di abilitarlo GuardDuty per il tuo account GuardDuty amministratore delegato appena designato, altrimenti non sarà in grado di intraprendere alcuna azione.
5. Scegli Delega.
6. (Consigliato) Ripeti i passaggi precedenti per designare l'account GuardDuty amministratore delegato in ogni account in Regione AWS cui hai abilitato. GuardDuty

API/CLI

1. Esegui enableOrganizationAdminAccountutilizzando le credenziali dell'account di gestione Account AWS dell'organizzazione.
   - In alternativa, è possibile utilizzare AWS Command Line Interface per eseguire questa operazione. Il AWS CLI comando seguente designa un account GuardDuty amministratore delegato solo per la regione corrente. Esegui il AWS CLI comando

seguente e assicurati di sostituirlo *111111111111* con l' Account AWS ID dell'account che desideri designare come account GuardDuty amministratore delegato:

```
aws guardduty enable-organization-admin-account --admin-account-
id 111111111111
```

Per designare l'account GuardDuty amministratore delegato per altre regioni, specifica la regione nel comando. AWS CLI L'esempio seguente mostra come abilitare un account GuardDuty amministratore delegato negli Stati Uniti occidentali (Oregon). Assicurati di sostituirlo *us-west-2* con la regione a cui desideri assegnare l' GuardDuty account amministratore delegato.

```
aws guardduty enable-organization-admin-account --admin-account-
id 111111111111 --region us-west-2
```

Per informazioni su Regioni AWS dove GuardDuty è disponibile, consulta. Regioni ed endpoint

Se non GuardDuty è abilitato per il tuo account GuardDuty amministratore delegato, non sarà in grado di eseguire alcuna azione. Se non l'hai già fatto, assicurati di abilitarlo GuardDuty per il nuovo GuardDuty account amministratore delegato designato.

2. (Consigliato) Ripeti i passaggi precedenti per designare l'account GuardDuty amministratore delegato in ogni account in Regione AWS cui hai abilitato. GuardDuty

Aggiornamento delle preferenze di attivazione automatica dell'organizzazione

La funzionalità di attivazione automatica dell'organizzazione GuardDuty consente di impostare lo stesso stato GuardDuty e i piani di protezione per `NEW` gli account `ALL` esistenti o membri dell'organizzazione, in un unico passaggio. Allo stesso modo, puoi anche specificare quando non desideri intraprendere alcuna azione sugli account dei membri, `NEW` selezionando. I passaggi seguenti spiegano queste impostazioni e indicano anche quando si desidera utilizzare un'impostazione specifica.

Scegli un metodo di accesso preferito per aggiornare le preferenze di attivazione automatica per l'organizzazione.

Console

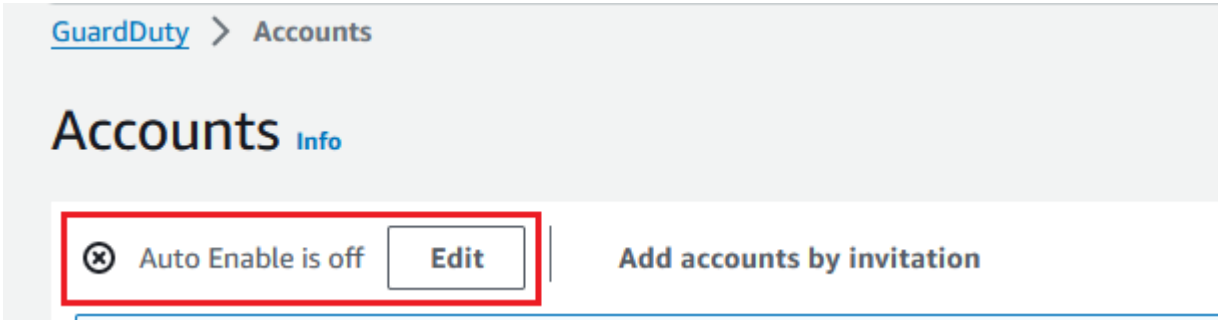
1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Per accedere, utilizza le credenziali GuardDuty dell'account amministratore.

2. Dal riquadro di navigazione, selezionare Accounts (Account).

   La pagina Account fornisce opzioni di configurazione per l'account GuardDuty amministratore da abilitare automaticamente GuardDuty e i piani di protezione opzionali per conto degli account membri che appartengono all'organizzazione.

3. Per aggiornare le impostazioni di attivazione automatica esistenti, scegli Modifica.



   Questo supporto è disponibile per la configurazione GuardDuty e per tutti i piani di protezione opzionali supportati dal tuo. Regione AWS Puoi selezionare una delle seguenti opzioni di configurazione per GuardDuty conto dei tuoi account membro:

   - Abilita per tutti gli account (**`ALL`**): seleziona questa opzione per abilitare l'opzione corrispondente per tutti gli account di un'organizzazione. inclusi i nuovi account che entrano a far parte dell'organizzazione e gli account che potrebbero essere stati sospesi o rimossi dall'organizzazione. Ciò include anche l'account GuardDuty amministratore delegato.

     > **Note**
     >
     > Potrebbero essere necessarie fino a 24 ore per aggiornare la configurazione di tutti gli account membri.

   - Attivazione automatica per nuovi account (**`NEW`**): seleziona questa opzione per abilitare GuardDuty automaticamente i piani di protezione opzionali solo per i nuovi account membri quando entrano a far parte dell'organizzazione.

- Non abilitare (**NONE**): seleziona questa opzione per impedire l'attivazione dell'opzione corrispondente per i nuovi account dell'organizzazione. In questo caso, l'account GuardDuty amministratore gestirà ogni account singolarmente.

  Quando aggiorni l'impostazione di attivazione automatica da `ALL` o `NEW` versoNONE, questa azione non disattiva l'opzione corrispondente per i tuoi account esistenti. Questa configurazione verrà applicata ai nuovi account che entrano a far parte dell'organizzazione. Dopo aver aggiornato le impostazioni di attivazione automatica, nessun nuovo account avrà l'opzione corrispondente abilitata.

> **Note**
>
> Quando un account GuardDuty amministratore delegato disattiva un'area di attivazione, anche se l'organizzazione ha la configurazione di GuardDuty attivazione automatica impostata su Solo nuovi account membro (`NEW`) o su tutti gli account membro (`ALL`), GuardDuty non può essere abilitata per nessun account membro dell'organizzazione attualmente disabilitato. GuardDuty Per informazioni sulla configurazione degli account membro, apri Account nel riquadro di navigazione della GuardDuty console o utilizza il. ListMembersAPI

4. Scegli Save changes (Salva modifiche).
5. (Facoltativo) se desideri utilizzare le stesse preferenze in ogni regione, aggiorna le preferenze in ciascuna delle regioni supportate separatamente.

   Alcuni dei piani di protezione opzionali potrebbero non essere disponibili in tutti i paesi in Regioni AWS cui GuardDuty sono disponibili. Per ulteriori informazioni, consulta Regioni ed endpoint.

API/CLI

1. Esegui UpdateOrganizationConfigurationutilizzando le credenziali dell'account GuardDuty amministratore delegato, per configurare automaticamente GuardDuty e i piani di protezione opzionali in quella regione per la tua organizzazione. Per informazioni sulle varie configurazioni di attivazione automatica, vedere autoEnableOrganization Membri.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

Per impostare le preferenze di abilitazione automatica per uno qualsiasi dei piani di protezione facoltativi supportati nella tua regione, segui i passaggi riportati nelle sezioni della documentazione corrispondenti a ciascun piano di protezione.

2. Puoi convalidare le preferenze per la tua organizzazione nella regione attuale. Esegui describeOrganizationConfiguration. Assicurati di specificare l'ID del rilevatore dell' GuardDuty account amministratore delegato.

> **Note**
>
> L'aggiornamento della configurazione per tutti gli account membri può richiedere fino a 24 ore.

1. In alternativa, esegui il AWS CLI comando seguente per impostare le preferenze da abilitare o disabilitare automaticamente GuardDuty in quella regione per i nuovi account (`NEW`) che entrano a far parte dell'organizzazione, per tutti gli account (`ALL`) o per nessuno degli account (`NONE`) dell'organizzazione. Per ulteriori informazioni, consulta autoEnableOrganizationMembri. In base alle tue preferenze, potrebbe essere necessario sostituire `NEW` con `ALL` o `NONE`. Se si configura il piano di protezione con`ALL`, il piano di protezione verrà abilitato anche per l'account GuardDuty amministratore delegato. Assicurati di specificare l'ID del rilevatore dell'account GuardDuty amministratore delegato che gestisce la configurazione dell'organizzazione.

   Per trovare il nome del `detectorId` tuo account e della regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

2. Puoi convalidare le preferenze per la tua organizzazione nella regione attuale. Esegui il AWS CLI comando seguente utilizzando l'ID del rilevatore dell' GuardDuty account amministratore delegato.

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0
```

(Consigliato) ripeti i passaggi precedenti in ogni regione utilizzando l'ID di rilevamento dell'account GuardDuty amministratore delegato.

> **Note**
>
> Quando un account GuardDuty amministratore delegato disattiva un'area di attivazione, anche se l'organizzazione ha la configurazione di GuardDuty attivazione automatica impostata su Solo nuovi account membro (`NEW`) o su tutti gli account membro (`ALL`), GuardDuty non può essere abilitata per nessun account membro dell'organizzazione attualmente disabilitato. GuardDuty Per informazioni sulla configurazione degli account membro, apri Account nel riquadro di navigazione della GuardDuty console o utilizza il. ListMembersAPI

Aggiungere membri all'organizzazione

Scegli un metodo di accesso preferito per aggiungere membri alla tua organizzazione.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Per accedere, utilizza le credenziali GuardDuty dell'account amministratore delegato.

2. Dal riquadro di navigazione, selezionare Accounts (Account).

   La tabella degli account mostra tutti gli account aggiunti Tramite l'organizzazione (AWS Organizations) o Tramite invito. Se un account membro non è associato all'account GuardDuty amministratore dell'organizzazione, lo stato di tale account membro è Non membro.

3. Seleziona uno o più account IDs che desideri aggiungere come membri. Questi account IDs devono avere il tipo come Via Organizations.

Gli account aggiunti tramite invito non fanno parte dell'organizzazione. Puoi gestire tali account singolarmente. Per ulteriori informazioni, consulta Gestione degli account tramite invito.

4. Scegli il menu a discesa Operazioni, quindi Aggiungi membro. Dopo aver aggiunto questo account come membro, verrà applicata la GuardDuty configurazione di attivazione automatica. In base alle impostazioni diAggiornamento delle preferenze di attivazione automatica dell'organizzazione, la GuardDuty configurazione di questi account potrebbe cambiare.
5. Puoi selezionare la freccia rivolta verso il basso della colonna Stato per ordinare gli account in base allo stato Non sono un membro e quindi scegliere ogni account che non è GuardDuty abilitato nella Regione corrente.

   Se nessuno degli account elencati nella tabella degli account è stato ancora aggiunto come membro, puoi abilitarlo GuardDuty nella regione corrente per tutti gli account dell'organizzazione. Scegli Abilita nel banner nella parte superiore della pagina. Questa azione attiva automaticamente la GuardDuty configurazione di attivazione automatica in modo che GuardDuty venga abilitata per ogni nuovo account che si unisce all'organizzazione.
6. Scegli Conferma per aggiungere gli account come membri. Questa azione si attiva anche GuardDuty per tutti gli account selezionati. Lo Stato degli account cambia in Abilitato.
7. (Consigliato) Ripeti questi passaggi in ciascuno di essi Regione AWS. Ciò garantisce che l'account GuardDuty amministratore delegato possa gestire i risultati e altre configurazioni per gli account dei membri in tutte le regioni in cui è stata GuardDuty abilitata.

   La funzionalità di attivazione automatica abilita tutti GuardDuty i futuri membri della tua organizzazione. Ciò consente GuardDuty all'account amministratore delegato di gestire tutti i nuovi membri creati all'interno o aggiunti all'organizzazione. Quando il numero di account membri raggiunge il limite di 50.000, la funzione di attivazione automatica viene disattivata automaticamente. Se rimuovi un account membro e il numero totale di membri scende a meno di 50.000, la funzione di attivazione automatica si riattiva.

API/CLI

- Esegui CreateMembersutilizzando le credenziali dell'account GuardDuty amministratore delegato indicato nel passaggio precedente.

È necessario specificare l'ID del rilevatore regionale dell'account GuardDuty amministratore delegato e i dettagli dell'account (Account AWS IDse gli indirizzi e-mail corrispondenti) degli account che si desidera aggiungere come membri. GuardDuty È possibile creare uno o più membri con questa API operazione.

Quando lavori CreateMembers nella tua organizzazione, le preferenze di attivazione automatica per i nuovi membri verranno applicate quando nuovi account membro entrano a far parte dell'organizzazione. Se utilizzi CreateMembers un account membro esistente, la configurazione dell'organizzazione verrà applicata anche ai membri esistenti. Ciò potrebbe modificare la configurazione attuale degli account dei membri esistenti.

Esegui ListAccountsnel AWS Organizations APIReference, per visualizzare tutti gli account dell' AWS organizzazione.

> **Important**
>
> Quando aggiungi un account come GuardDuty membro, questo verrà automaticamente GuardDuty abilitato in quella regione. Esiste un'eccezione relativamente all'account di gestione dell'organizzazione. Prima che l'account dell'account di gestione venga aggiunto come GuardDuty membro, deve essere GuardDuty abilitato.

- In alternativa, puoi usare AWS Command Line Interface. Esegui il comando AWS CLI seguente e assicurati di utilizzare il tuo ID rilevatore, l'ID Account AWS e l'indirizzo e-mail validi associati all'ID account.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

  ```
  aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
   --account-details AccountId=111122223333,Email=guardduty-member-
  name@amazon.com
  ```

  È possibile visualizzare un elenco di tutti i membri dell'organizzazione eseguendo il AWS CLI comando seguente:

```
aws organizations list-accounts
```

Dopo aver aggiunto questo account come membro, verrà applicata la GuardDuty configurazione di attivazione automatica.

(Facoltativo) Abilita i piani di protezione per gli account dei membri esistenti

La procedura seguente include i passaggi per abilitare i piani di protezione per gli account dei membri esistenti utilizzando la pagina Account. Per istruzioni su come eseguire questa operazione utilizzando API o AWS CLI, consulta i documenti relativi al piano di protezione specifico.

È possibile abilitare i piani di protezione per singoli account tramite la pagina Account.

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Utilizza le credenziali GuardDuty dell'account amministratore delegato.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Seleziona uno o più account per i quali desideri configurare un piano di protezione. Ripeti i seguenti passaggi per ogni piano di protezione da configurare:

   a. Scegli Modifica piani di protezione.

   b. Dall'elenco dei piani di protezione, scegli quello da configurare.

   c. Scegli una delle operazioni che desideri eseguire per questo piano di protezione, quindi scegli Conferma.

   d. Per l'account selezionato, la colonna corrispondente al piano di protezione configurato mostrerà la configurazione aggiornata come Abilitata o Non abilitata.

Mantenere la propria organizzazione all'interno GuardDuty

In qualità di account GuardDuty amministratore delegato, sei responsabile del mantenimento della configurazione GuardDuty e dei relativi piani di protezione opzionali per tutti gli account dell'organizzazione supportati. Regione AWS Le seguenti sezioni forniscono le opzioni relative al mantenimento dello stato di configurazione GuardDuty o di uno qualsiasi dei relativi piani di protezione opzionali:

Per mantenere lo stato di configurazione dell'intera organizzazione in ogni regione

- Imposta le preferenze di attivazione automatica per l'intera organizzazione utilizzando la GuardDuty console: puoi abilitarla GuardDuty automaticamente per tutti (`ALL`) i membri dell'organizzazione o per i nuovi (`NEW`) membri che si uniscono all'organizzazione, oppure scegliere di non (`NONE`) abilitare automaticamente nessuno dei membri dell'organizzazione.

  Puoi anche configurare le stesse impostazioni o impostazioni diverse per tutti i piani di protezione inclusi. GuardDuty

  Potrebbero essere necessarie fino a 24 ore per aggiornare la configurazione di tutti gli account membri dell'organizzazione.
- Aggiorna le preferenze di attivazione automatica utilizzando API — Run UpdateOrganizationConfigurationto configura automaticamente GuardDuty e i relativi piani di protezione opzionali per l'organizzazione. Quando corri CreateMembersad aggiungere nuovi account membro nella tua organizzazione, le impostazioni configurate verranno applicate automaticamente. Se utilizzi CreateMembers un account membro esistente, la configurazione dell'organizzazione verrà applicata anche ai membri esistenti. Ciò potrebbe modificare la configurazione attuale degli account dei membri esistenti.

  Per visualizzare tutti gli account della tua organizzazione, ListAccountsesegui il comando AWS Organizations APIReference.

Per mantenere lo stato di configurazione per i singoli account dei membri in ciascuna regione

- Per visualizzare tutti gli account della tua organizzazione, ListAccountsesegui il comando AWS Organizations APIReference.
- Se desideri che gli account membro selettivi abbiano uno stato di configurazione diverso, esegui l'operazione UpdateMemberDetectorsper ogni account membro singolarmente.

  Puoi utilizzare la GuardDuty console per eseguire la stessa operazione accedendo alla pagina Account della console. GuardDuty

  Per informazioni sull'attivazione dei piani di protezione per singoli account utilizzando la console oAPI, consulta la pagina di configurazione per il piano di protezione corrispondente.

Modifica dell'account amministratore delegato GuardDuty

Puoi modificare l'account GuardDuty amministratore delegato per la tua organizzazione in ogni regione e quindi delegare un nuovo amministratore in ogni regione. Per mantenere un livello di sicurezza per gli account dei membri dell'organizzazione in una regione, è necessario disporre di un account GuardDuty amministratore delegato in quella regione.

Rimozione dell'account amministratore delegato GuardDuty esistente

Fase 1 - Rimuovere l'account GuardDuty amministratore delegato esistente in ogni regione

1. Come account GuardDuty amministratore delegato esistente, elenca tutti gli account membro associati al tuo account amministratore. Corri ListMembersconOnlyAssociated=false.
2. Se la preferenza di attivazione automatica per GuardDuty o per uno qualsiasi dei piani di protezione opzionali è impostata suALL, esegui UpdateOrganizationConfigurationper aggiornare la configurazione dell'organizzazione su NEW oNONE. Questa azione eviterà che si verifichi un errore quando si dissociano tutti gli account dei membri nel passaggio successivo.
3. Esegui DisassociateMembersper dissociare tutti gli account membro associati all'account amministratore.
4. Esegui DeleteMembersper eliminare le associazioni tra l'account amministratore e gli account dei membri.
5. Come account di gestione dell'organizzazione, esegui DisableOrganizationAdminAccountper rimuovere l'account GuardDuty amministratore delegato esistente.
6. Ripeti questi passaggi in ognuno dei Regione AWS paesi in cui hai questo GuardDuty account amministratore delegato.

Fase 2 - Annullare la registrazione GuardDuty dell'account amministratore delegato esistente in AWS Organizations (azione globale una tantum)

- Esegui DeregisterDelegatedAdministratornel AWS Organizations APIReference, per annullare la registrazione dell'account amministratore delegato GuardDuty esistente in. AWS Organizations

  In alternativa, puoi eseguire il seguente AWS CLI comando:

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --
service-principal guardduty.amazonaws.com
```

Assicurati di sostituire *111122223333* con l'account GuardDuty amministratore delegato esistente.

Dopo aver annullato la registrazione del vecchio account GuardDuty amministratore delegato, puoi aggiungerlo come account membro al nuovo account amministratore delegato GuardDuty .

Designazione di un nuovo account amministratore delegato GuardDuty in ogni regione

1. Designate un nuovo account GuardDuty amministratore delegato in ogni regione utilizzando il metodo di accesso preferito: GuardDuty console o o. API AWS CLI Per ulteriori informazioni, consulta Designazione di un account amministratore delegato GuardDuty .
2. Esegui DescribeOrganizationConfigurationper visualizzare l'attuale configurazione di attivazione automatica per la tua organizzazione.

   > **Important**
   >
   > Prima di aggiungere membri al nuovo account GuardDuty amministratore delegato, è necessario verificare la configurazione di attivazione automatica per l'organizzazione. Questa configurazione è specifica del nuovo account GuardDuty amministratore delegato e della regione selezionata e non si riferisce a. AWS Organizations Quando si aggiunge un account membro dell'organizzazione (nuovo o esistente) al nuovo account GuardDuty amministratore delegato, la configurazione di attivazione automatica del nuovo account GuardDuty amministratore delegato verrà applicata al momento dell'attivazione GuardDuty o di uno qualsiasi dei suoi piani di protezione opzionali.

   Modifica la configurazione dell'organizzazione per il nuovo account GuardDuty amministratore delegato utilizzando il metodo di accesso preferito: GuardDuty console o o. API AWS CLI Per ulteriori informazioni, consulta Aggiornamento delle preferenze di attivazione automatica dell'organizzazione.

Gestione GuardDuty degli account su invito

Per gestire gli account esterni all'organizzazione, è possibile utilizzare il metodo di invito legacy. Quando utilizzi questo metodo, il tuo account viene designato come account amministratore nel momento in cui un altro account accetta l'invito a diventare un account membro.

Se il tuo account non è un account amministratore, puoi accettare un invito da un altro account. Quando accetti l'invito, il tuo account diventa un account membro. Un AWS account non può essere contemporaneamente un account GuardDuty amministratore e un account membro.

Quando accetti un invito da un account, non puoi accettare un invito da un altro account. Per accettare un invito da un altro account, devi prima dissociare il tuo account dall'account amministratore esistente. In alternativa, l'account amministratore può anche dissociare e rimuovere il tuo account dalla sua organizzazione.

Gli account associati su invito hanno lo stesso account-to-member rapporto di amministratore complessivo degli account associati da AWS Organizations, come descritto inComprensione della relazione tra account GuardDuty amministratore e account membro. Tuttavia, gli utenti con account amministratore a inviti non possono GuardDuty attivare gli account dei membri associati o visualizzare altri account non membri all'interno della propria AWS Organizations organizzazione.

> **Important**
>
> Quando si GuardDuty creano account membri utilizzando questo metodo, può verificarsi un trasferimento di dati interregionale. Per verificare gli indirizzi e-mail degli account dei membri, GuardDuty utilizza un servizio di verifica e-mail che opera solo nella regione degli Stati Uniti orientali (Virginia settentrionale).

Aggiunta e gestione degli account tramite invito

Scegli uno dei metodi di accesso per aggiungere e invitare account a diventare account GuardDuty membro come account GuardDuty amministratore.

Console

Fase 1: aggiunta di un account

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Scegli Aggiungi account tramite invito nel riquadro superiore.
4. Nella pagina Aggiungi account membro, in Inserisci i dettagli dell'account, inserisci l' Account AWS ID e l'indirizzo email associati all'account che desideri aggiungere.

5. Per aggiungere un'altra riga in cui immettere i dettagli dell'account uno alla volta, scegli Aggiungi un altro account. Puoi anche scegliere Carica il file .csv con i dettagli dell'account per aggiungere account in blocco.

   > **Important**
   >
   > La prima riga del file csv deve contenere l'intestazione, come illustrato nell'esempio seguente: `Account ID,Email`. Ogni riga successiva deve contenere un unico Account AWS ID valido e l'indirizzo e-mail associato. Il formato di una riga è valido se contiene un solo Account AWS ID e l'indirizzo e-mail associato separati da una virgola.
   >
   > ```
   > Account ID,Email
   > 555555555555,user@example.com
   > ```

6. Dopo aver aggiunto tutti i dettagli degli account, scegli Successivo. Puoi visualizzare gli account appena aggiunti nella tabella Account. Lo Stato di questi account sarà Invito non inviato. Per informazioni sull'invio di un invito a uno o più account aggiunti, consulta Step 2 - Invite an account.

Fase 2: invito di un account

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Dal riquadro di navigazione, selezionare Accounts (Account).
3. Seleziona uno o più account che desideri invitare su Amazon GuardDuty.
4. Scegli il menu a discesa Operazioni, quindi Invita.
5. Nella GuardDuty finestra di dialogo Invito a, inserisci un messaggio di invito (opzionale).

   Se l'account invitato non ha accesso all'e-mail, seleziona la casella di controllo Invia anche una notifica e-mail all'utente root nell' Account AWS dell'invitato e genera un avviso nel AWS Health Dashboard.
6. Selezionare Send invitation (Invia invito). Se gli invitati hanno accesso all'indirizzo e-mail specificato, possono visualizzare l'invito aprendo la GuardDuty console all'https://console.aws.amazon.com/guardduty/indirizzo.
7. Quando un invitato accetta l'invito, il valore nella colonna Stato cambia in Invitato. Per informazioni sull'accettazione di un invito, consulta Step 3 - Accept an invitation.

Fase 3: accettazione di un invito

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   > **Important**
   >
   > È necessario abilitarla GuardDuty prima di poter visualizzare o accettare un invito all'iscrizione.

2. Effettua le seguenti operazioni solo se non l'hai GuardDuty ancora abilitato; in caso contrario, puoi saltare questo passaggio e continuare con il passaggio successivo.

   Se non l'hai ancora abilitato GuardDuty, scegli Get Started sulla GuardDuty pagina Amazon.

   Nella GuardDuty pagina Benvenuto, scegli Abilita GuardDuty.

3. Dopo aver abilitato GuardDuty il tuo account, segui la procedura seguente per accettare l'invito all'iscrizione:

   a. Nel pannello di navigazione scegli Impostazioni.

   b. Scegli Account.

   c. In Account, assicurati di verificare il proprietario dell'account dal quale accetti l'invito. Attiva Accetta per accettare l'invito.

4. Dopo aver accettato l'invito, il tuo account diventa un account GuardDuty membro. L'account il cui proprietario ha inviato l'invito diventa l'account GuardDuty amministratore. L'account amministratore saprà che hai accettato l'invito. La tabella Account GuardDuty del relativo account verrà aggiornata. Il valore nella colonna Stato corrispondente all'ID del tuo account membro cambierà in Abilitato. Il proprietario dell'account amministratore può ora visualizzare GuardDuty e gestire le configurazioni del piano di protezione per conto del tuo account. L'account amministratore può anche visualizzare e gestire i GuardDuty risultati generati per il tuo account membro.

API/CLI

Puoi designare un account GuardDuty amministratore e creare o aggiungere account GuardDuty membro su invito tramite le API operazioni. Esegui le seguenti GuardDuty API operazioni per designare l'account amministratore e gli account membro in. GuardDuty

Completare la procedura seguente utilizzando le credenziali dell' Account AWS account che si desidera designare come amministratore. GuardDuty

Creazione o aggiunta di account membri

1. Esegui l'CreateMembersAPIoperazione utilizzando le credenziali dell' AWS account che hai abilitato. GuardDuty Questo è l'account che desideri utilizzare come GuardDuty account amministratore.

   È necessario specificare l'ID del rilevatore dell' AWS account corrente e l'ID account e l'indirizzo e-mail degli account di cui si desidera diventare GuardDuty membri. È possibile creare uno o più membri con questa API operazione.

   È inoltre possibile utilizzare gli strumenti della riga di AWS comando per designare un account amministratore eseguendo il CLI comando seguente. Assicurati di utilizzare il tuo ID rilevatore valido, l'ID account e l'e-mail.

   Per trovare il nome del `detectorId` tuo account e della regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

   ```
   aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-details AccountId=111122223333,Email=guardduty-member@organization.com
   ```

2. Esegui InviteMembersutilizzando le credenziali dell' AWS account che hai GuardDuty abilitato. Questo è l'account che desideri utilizzare come GuardDuty account amministratore.

   È necessario specificare l'ID del rilevatore dell' AWS account corrente e l'account IDs degli account di cui si desidera diventare GuardDuty membri. È possibile invitare uno o più membri con questa API operazione.

   > **Note**
   >
   > È anche possibile specificare un messaggio di invito facoltativo tramite il parametro di richiesta `message`.

È inoltre possibile utilizzare AWS Command Line Interface per designare gli account dei membri eseguendo il comando seguente. Assicurati di utilizzare un ID rilevatore valido e un account valido IDs per gli account che desideri invitare.

Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 111122223333
```

Accettazione degli inviti

Completa la procedura seguente utilizzando le credenziali di ogni AWS account che desideri designare come account GuardDuty membro.

1. Esegui l'CreateDetectorAPIoperazione per ogni AWS account che è stato invitato a diventare un account GuardDuty membro e per il quale desideri accettare un invito.

   È necessario specificare se la risorsa del rilevatore deve essere abilitata utilizzando il GuardDuty servizio. Un rilevatore deve essere creato e abilitato per GuardDuty diventare operativo. È necessario abilitarlo GuardDuty prima di accettare un invito.

   È inoltre possibile eseguire questa operazione utilizzando gli strumenti della riga di AWS comando utilizzando il seguente CLI comando.

   ```
   aws guardduty create-detector --enable
   ```

2. Esegui l'AcceptAdministratorInvitationAPIoperazione per ogni AWS account di cui desideri accettare l'invito all'iscrizione, utilizzando le credenziali di quell'account.

   Devi specificare l'ID rilevatore di questo AWS account per l'account membro, l'ID account dell'account amministratore che ha inviato l'invito e l'ID dell'invito che stai accettando. Puoi trovare l'ID dell'account amministratore nell'e-mail di invito o utilizzando il ListInvitationscomando di. API

È inoltre possibile accettare un invito utilizzando gli strumenti della riga di AWS comando eseguendo il CLI comando seguente. Assicurati di utilizzare ID rilevatore, ID account amministratore e ID invito validi.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadcf5
```

Consolidamento degli account di GuardDuty amministratore in un unico account di amministratore delegato GuardDuty dell'organizzazione

GuardDuty consiglia di utilizzare l'associazione attraverso AWS Organizations per gestire gli account dei membri con un account amministratore delegato. GuardDuty È possibile utilizzare il processo di esempio descritto di seguito per consolidare l'account amministratore e il membro associato su invito in un'organizzazione in un unico account amministratore GuardDuty delegato GuardDuty .

> **Note**
>
> Gli account che sono già gestiti da un account GuardDuty amministratore delegato o gli account dei membri attivi associati all'account GuardDuty amministratore delegato non possono essere aggiunti a un altro account amministratore delegato. GuardDuty Ogni organizzazione può avere un solo account GuardDuty amministratore delegato per regione e ogni account membro può avere un solo account amministratore delegato. GuardDuty

Scegli uno dei metodi di accesso per consolidare gli account GuardDuty amministratore in un unico account amministratore delegato GuardDuty .

Console

1. Apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/

   Per accedere, utilizza le credenziali dell'account di gestione dell'organizzazione.

2. Tutti gli account che desideri gestire GuardDuty devono far parte della tua organizzazione. Per informazioni sull'aggiunta di un account alla tua organizzazione, vedi Invitare un utente Account AWS a entrare a far parte della tua organizzazione.
3. Assicurati che tutti gli account membro siano associati all'account che desideri designare come unico account amministratore delegato GuardDuty . Disassocia qualsiasi account membro che è ancora associato agli account amministratore preesistenti.

   I seguenti passaggi sono utili per disassociare gli account membri dall'account amministratore preesistente:

   a. Apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/
   b. Per accedere, utilizza le credenziali dell'account amministratore preesistente.
   c. Dal riquadro di navigazione, selezionare Accounts (Account).
   d. Nella pagina Account, seleziona uno o più account che desideri disassociare dall'account amministratore.
   e. Scegli Operazioni, quindi Disassocia account.
   f. Scegli Conferma per completare il passaggio.
4. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Per accedere, utilizza le credenziali dell'account di gestione.
5. Nel pannello di navigazione scegli Impostazioni. Nella pagina Impostazioni, designa l'account GuardDuty amministratore delegato per l'organizzazione.
6. Accedere all'account amministratore delegato designato. GuardDuty
7. Aggiungi membri dall'organizzazione. Per ulteriori informazioni, consulta Gestione GuardDuty degli account con AWS Organizations.

API/CLI

1. Tutti gli account che desideri gestire GuardDuty devono far parte della tua organizzazione. Per informazioni sull'aggiunta di un account alla tua organizzazione, vedi Invitare un utente Account AWS a entrare a far parte della tua organizzazione.
2. Assicurati che tutti gli account membro siano associati all'account che desideri designare come unico account amministratore delegato GuardDuty .

   a. Esegui DisassociateMembersper dissociare qualsiasi account membro ancora associato agli account amministratore preesistenti.

b. In alternativa, puoi usare AWS Command Line Interface per eseguire il seguente comando e sostituirlo *777777777777* con l'ID del rilevatore dell'account amministratore preesistente da cui desideri dissociare l'account membro. Replace (Sostituisci) *666666666666* con l' Account AWS ID dell'account membro da cui desideri dissociare.

```
aws guardduty disassociate-members --detector-id 777777777777 --account-
ids 666666666666
```

3. Esegui EnableOrganizationAdminAccountper delegare un Account AWS account come amministratore delegato. GuardDuty

   In alternativa, puoi usare AWS Command Line Interface per eseguire il seguente comando per delegare un account amministratore delegato GuardDuty :

```
aws guardduty enable-organization-admin-account --admin-account-id 777777777777
```

4. Aggiungi membri dall'organizzazione. Per ulteriori informazioni, consulta Create or add member member accounts using API.

> **Important**
>
> Per massimizzare l'efficacia di un servizio regionale GuardDuty, ti consigliamo di designare il tuo account GuardDuty amministratore delegato e aggiungere tutti gli account membro in ogni regione.

Abilita più account GuardDuty contemporaneamente

Utilizza il seguente metodo per abilitare GuardDuty più account contemporaneamente.

Usa gli script Python per abilitare più account GuardDuty contemporaneamente

Puoi automatizzare l'attivazione o la disabilitazione di GuardDuty su più account utilizzando gli script del repository di esempio negli script multiaccount di Amazon GuardDuty . Utilizza la procedura descritta in questa sezione GuardDuty per abilitare un elenco di account membri che utilizzano AmazonEC2. Per informazioni sull'utilizzo dello script di disabilitazione o sulla configurazione dello script localmente, consulta le istruzioni contenute nel link condiviso.

Lo `enableguardduty.py` script abilita GuardDuty, invia gli inviti dall'account amministratore e accetta gli inviti in tutti gli account dei membri. Il risultato è un GuardDuty account amministratore che contiene tutti i risultati di sicurezza per tutti gli account dei membri. Poiché GuardDuty è isolato per regione, i risultati di ogni account membro vengono aggregati alla regione corrispondente nell'account amministratore. Ad esempio, la regione us-east-1 nell' GuardDuty account amministratore contiene i risultati di sicurezza per tutti i risultati us-east-1 di tutti gli account membro associati.

Questi script dipendono da un IAM ruolo condiviso con la politica gestita:. AWS politica gestita: AmazonGuardDutyFullAccess Questa politica consente alle entità di accedere GuardDuty e deve essere presente nell'account amministratore e in ogni account per il quale si desidera abilitare. GuardDuty

Il seguente processo è abilitato per impostazione predefinita GuardDuty in tutte le regioni disponibili. È possibile GuardDuty abilitarlo solo nelle regioni specificate utilizzando l'`--enabled_regions`argomento opzionale e fornendo un elenco di regioni separate da virgole. È inoltre possibile personalizzare facoltativamente il messaggio di invito inviato agli account membri aprendo `enableguardduty.py` e modificando la stringa `gd_invite_message`.

1. Crea un IAM ruolo nell'account GuardDuty amministratore e allega la AWS politica gestita: AmazonGuardDutyFullAccess politica da abilitare. GuardDuty
2. Crea un IAM ruolo in ogni account membro che desideri venga gestito dal tuo account GuardDuty amministratore. Questo ruolo deve avere lo stesso nome del ruolo creato nel passaggio 1, deve consentire l'accesso all'account amministratore come entità attendibile e deve avere la stessa politica di AmazonGuardDutyFullAccess gestione descritta in precedenza.
3. Avviare una nuova istanza di Amazon Linux con un ruolo allegato che abbia la seguente relazione di trust per consentire all'istanza di assumere un ruolo di servizio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Accedere alla nuova istanza ed eseguire i seguenti comandi per configurarla.

```
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. Crea un CSV file contenente un elenco di account IDs e di e-mail degli account dei membri a cui hai aggiunto un ruolo nel passaggio 2. Gli account devono essere visualizzati uno per riga e l'ID account e l'indirizzo di posta elettronica devono essere separati da una virgola, come nell'esempio seguente.

```
111122223333,guardduty-member@organization.com
```

> **Note**
>
> Il CSV file deve trovarsi nella stessa posizione `enableguardduty.py` dello script. Puoi copiare un CSV file esistente da Amazon S3 nella directory corrente con il seguente metodo.
>
> ```
> aws s3 cp s3://my-bucket/my_key_name example.csv
> ```

6. Eseguire lo script Python. Assicurati di fornire come argomenti l'ID del tuo account GuardDuty amministratore, il nome del ruolo creato nei primi passaggi e il nome del CSV file.

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

Comprendere i GuardDuty risultati di Amazon

Un GuardDuty risultato rappresenta un potenziale problema di sicurezza rilevato all'interno della rete. GuardDutygenera un risultato ogni volta che rileva attività impreviste e potenzialmente dannose nell' AWS ambiente in uso.

È possibile visualizzare e gestire i GuardDuty risultati nella pagina Findings della GuardDuty console o utilizzando le API operazioni AWS CLI or. Per una panoramica dei modi in cui puoi gestire gli esiti, consulta Gestione dei GuardDuty risultati di Amazon.

Argomenti:

Formato degli esiti di GuardDuty

Comprendi il formato dei tipi di GuardDuty ricerca e i diversi scopi delle minacce seguiti GuardDuty.

Risultati di esempio

Prova a generare risultati di esempio per testare e comprendere GuardDuty i risultati e i dettagli associati. Questi risultati sono contrassegnati con un prefisso [SAMPLE].

GuardDuty Risultati dei test in account dedicati

Eseguite uno `guardduty-tester` script in un ambiente non di produzione dedicato Account AWS per generare GuardDuty risultati selezionati nel vostro AWS ambiente.

Dettagli degli esiti

Scopri i dettagli associati ai GuardDuty risultati generati nel tuo account.

Tipi di esiti

Visualizza e cerca tutti i GuardDuty risultati disponibili per tipo. Ogni voce del tipo di esito include una spiegazione di tale esito, nonché consigli e suggerimenti per la correzione.

Formato degli esiti di GuardDuty

GuardDuty genera un esito se rileva un comportamento sospetto o non previsto nel tuo ambiente AWS. Un esito è una notifica che contiene i dettagli su un potenziale problema di sicurezza rilevato

da GuardDuty. I dettagli degli esiti includono informazioni su quanto è accaduto, sulle risorse AWS coinvolte nell'attività sospetta, sul momento in cui questa è avvenuta e molto altro.

Una delle informazioni più utili di questi dettagli è il tipo di risultato. La funzione del tipo di risultato è di fornire una descrizione concisa ma intelligibile del potenziale problema di sicurezza. Ad esempio, il tipo di esito di GuardDuty Recon:EC2/PortProbeUnprotectedPort ti informa rapidamente che una porta non protetta di un'istanza EC2 nel tuo ambiente AWS è sottoposta a probing da parte di un potenziale utente malintenzionato.

GuardDuty utilizza il formato seguente per nominare i vari tipi di esiti che genera:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism!Artifact

Ogni parte di questo formato rappresenta un aspetto di un tipo di esito. Di seguito le spiegazioni di questi aspetti:

- ThreatPurpose: descrive l'obiettivo principale di una minaccia, di un tipo di attacco o della fase di un potenziale attacco. Consulta la sezione seguente per un elenco completo degli scopi delle minacce GuardDuty.
- ResourceTypeAffected: descrive il tipo di risorse AWS identificate in questo esito come potenziali destinazioni di un attacco. Attualmente, GuardDuty è in grado di generare esiti per le risorse EC2, S3, IAM ed EKS.
- ThreatFamilyName: descrive la minaccia o la potenziale attività dannosa globale in corso di rilevamento da parte di GuardDuty. Ad esempio, il valore NetworkPortUnusual indica che un'istanza EC2 identificata nell'esito di GuardDuty non ha mai comunicato su una determinata porta remota (anch'essa identificata nell'esito) in precedenza.
- DetectionMechanism: descrive il metodo con cui GuardDuty ha rilevato l'esito. Questo aspetto può essere utilizzato per indicare la variazione di un tipo di esito comune o un esito che GuardDuty ha rilevato utilizzando un meccanismo specifico. Ad esempio, Backdoor:EC2/DenialOfService.Tcp indica che il Denial of Service (DoS) è stato rilevato tramite TCP. La variante UDP è Backdoor:EC2/DenialOfService.Udp.

  Il valore .Custom indica che GuardDuty ha rilevato l'esito in base agli elenchi minacce personalizzati, mentre .Reputation indica che GuardDuty ha rilevato l'esito utilizzando un modello di punteggio di reputazione del dominio.
- Artefatto: descrive una risorsa specifica di proprietà di uno strumento utilizzato nell'attività dannosa. Ad esempio, DNS nel tipo di risultato CryptoCurrency:EC2/BitcoinTool.B!DNS indica che un'istanza EC2 sta comunicando con un noto dominio correlato al bitcoin.

Scopi delle minacce

In GuardDuty, lo scopo della minaccia descrive l'obiettivo principale di una minaccia, di un tipo di attacco o della fase di un potenziale attacco. Ad esempio, alcuni scopi delle minacce, come Backdoor, indicano un tipo di attacco. Tuttavia, alcuni scopi delle minacce, come Impatto, sono in linea con le Tattiche MITRE ATT&CK. Le tattiche MITRE ATT&CK indicano diverse fasi del ciclo di attacco di un avversario. Nella versione corrente di GuardDuty, ThreatPurpose può avere i valori seguenti:

Backdoor

Questo valore indica che un avversario ha compromesso una risorsa AWS e l'ha alterata in modo da riuscire a contattare il relativo server di comando e controllo (C&C) per ricevere ulteriori istruzioni a fini dannosi.

Comportamento

Questo valore indica che GuardDuty ha rilevato un'attività o modelli di attività che differiscono dalla linea di base stabilita per la risorsa AWS coinvolta.

CredentialAccess

Questo valore indica che GuardDuty ha rilevato modelli di attività che un avversario potrebbe utilizzare per rubare credenziali, come ID account o password, dal tuo ambiente. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK

Criptovalute

Questo valore indica che GuardDuty ha rilevato che una risorsa AWS nel tuo ambiente ospita un software associato a criptovalute (ad esempio, Bitcoin).

DefenseEvasion

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per non essere rilevato mentre si infiltra nel tuo ambiente. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK

Individuazione

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per ampliare la propria conoscenza dei sistemi e delle reti interne. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK.

Esecuzione

Questo valore indica che GuardDuty ha rilevato che un avversario potrebbe tentare di eseguire codice dannoso per esplorare la rete o rubare dati. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK .

Esfiltrazione

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per tentare di rubare dati dalla rete. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK.

Impatto

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che suggeriscono il tentativo di un avversario di manipolare, interrompere o distruggere i sistemi e i dati. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK

InitialAccess

Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK

Test di penetrazione (pen-test)

A volte i proprietari di risorse AWS o i loro rappresentanti autorizzati eseguono intenzionalmente dei test su determinate applicazioni AWS per identificarne le vulnerabilità, come gruppi di sicurezza aperti o chiavi di accesso troppo permissive. Questi test di penetrazione vengono eseguiti nel tentativo di identificare e bloccare le risorse vulnerabili prima che siano individuate dagli avversari. Tuttavia, alcuni degli strumenti utilizzati dai tester autorizzati sono disponibili gratuitamente e quindi possono essere utilizzati da utenti non autorizzati o malintenzionati per eseguire test di probing. Sebbene GuardDuty non sia in grado di identificare il vero scopo di tale attività, il valore Test di penetrazione (pen-test) indica che GuardDuty rileva un'attività simile a quella generata da strumenti di test di penetrazione noti, attività che potrebbe indicare un'azione di probing dannosa della rete.

Persistence

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per cercare di mantenere l'accesso ai sistemi anche se la loro via di accesso iniziale è interrotta. Ad esempio, ciò potrebbe includere la creazione di un nuovo utente IAM dopo aver ottenuto l'accesso tramite le credenziali compromesse di un utente esistente. Quando le credenziali dell'utente esistente vengono eliminate, l'avversario manterrà l'accesso al nuovo

utente che non è stato rilevato come parte dell'evento originale. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK.

Policy

Questo valore indica che il tuo account Account AWS ha un comportamento che va contro le best practice di sicurezza consigliate.

PrivilegeEscalation

Questo valore indica che il principale coinvolto nel tuo ambiente AWS ha un comportamento che un avversario potrebbe utilizzare per ottenere autorizzazioni di livello superiore per accedere alla rete. Questo scopo di minaccia si basa sulle Tattiche MITRE ATT&CK.

Recon

Questo valore indica che GuardDuty ha rilevato attività o modelli di attività che un avversario potrebbe utilizzare per eseguire la ricognizione della rete in modo da capire come ampliare il proprio accesso o utilizzare le tue risorse. Ad esempio, questa attività può includere l'individuazione delle vulnerabilità presenti nel tuo ambiente AWS controllando le porte, elencando gli utenti e le tabelle del database e così via.

Stealth

Questo valore indica che un avversario cerca attivamente di nascondere le proprie operazioni. Ad esempio, potrebbe utilizzare un server proxy anonimo, il che rende estremamente difficile valutare la vera natura dell'attività.

Trojan

Questo valore indica che un attacco utilizza programmi Trojan per svolgere attività dannose di nascosto. A volte questo software assume l'aspetto di un programma legittimo che gli utenti eseguono quindi involontariamente. In altre, questo software si esegue automaticamente sfruttando una vulnerabilità.

UnauthorizedAccess

Questo valore indica che GuardDuty rileva un'attività o un modello di attività sospetto da parte di un individuo non autorizzato.

GuardDuty motore di scansione per il rilevamento di malware

Amazon GuardDuty dispone di un motore di scansione integrato e gestito internamente e di un fornitore terzo. Entrambi utilizzano indicatori di compromissione (IoCs) provenienti da vari feed interni

che hanno visibilità sui diversi tipi di malware che potrebbero colpire. AWS GuardDuty include anche definizioni di rilevamento basate su YARA regole aggiunte dai nostri tecnici di sicurezza e rilevamenti basati su modelli euristici e di apprendimento automatico (ML). Il rilevamento basato sulla firma non include solo la corrispondenza dei byte, ma anche un frammento di codice potenzialmente complesso e lo scanner può analizzare il contenuto e prendere decisioni.

Il motore di scansione antimalware non esegue analisi comportamentali in tempo reale, mentre la detonazione del malware monitora il campione mentre viene eseguito in un sistema reale. La GuardDuty soluzione è principalmente un rilevamento basato su file. Per rilevare malware senza file, GuardDuty fornisce una soluzione basata su agenti, ad esempio per Amazon, Monitoraggio del runtime Amazon EC2 e EKS Amazon (incluso). ECS AWS Fargate

Senza alcuna restrizione sui formati di file utilizzati per la GuardDuty scansione alla ricerca di malware, i motori di scansione che utilizza sono in grado di rilevare diversi tipi di malware, come cryptominer, ransomware e webshell. Il motore di GuardDuty scansione completamente gestito aggiorna continuamente l'elenco delle firme dei malware ogni 15 minuti.

Il motore di scansione fa parte del sistema di intelligence GuardDuty sulle minacce che utilizza un componente interno per la detonazione del malware. Ciò genera nuove informazioni sulle minacce raccogliendo in modo indipendente malware e campioni benigni da più fonti. Il tipo di file hash IoC del sistema di intelligence sulle minacce alimenta ulteriormente il motore di scansione antimalware per rilevare il malware sulla base di hash di file dannosi noti.

Generazione di risultati campionari in GuardDuty

Puoi generare risultati di esempio con Amazon GuardDuty per aiutarti a visualizzare e comprendere i vari tipi di risultati che GuardDuty possono generare. Quando generi risultati di esempio, GuardDuty compila l'elenco dei risultati attuali con un risultato di esempio per ogni tipo di risultato supportato.

Gli esempi generati sono approssimazioni compilate con valori segnaposto. Questi esempi possono apparire diversi dai risultati reali relativi all'ambiente in uso, ma è possibile utilizzarli per testare varie configurazioni GuardDuty, ad esempio EventBridge eventi o filtri. Per un elenco dei valori disponibili per la ricerca dei tipi, consultate la Tipi di esiti tabella.

Generazione di risultati di esempio tramite la GuardDuty console o API

Scegli il metodo di accesso che preferisci per generare esiti di esempio.

> **Note**
>
> Utilizzando la console puoi generare un esito per ogni tipo, I risultati di un singolo campione possono essere generati solo tramiteAPI.

Console

Utilizza la procedura seguente per generare esiti di esempio. Questo processo genera un campione di risultati per ogni tipo di GuardDuty risultato.

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella pagina Settings (Impostazioni), in Sample findings (Risultati di esempio), selezionare Generate sample findings (Genera risultati di esempio).
4. Nel riquadro di navigazione, seleziona Esiti. I risultati di esempio vengono visualizzati nella pagina Risultati correnti con il prefisso [SAMPLE].

API/CLI

È possibile generare un singolo risultato di esempio corrispondente a qualsiasi tipo di GuardDuty risultato tramite CreateSampleFindingsAPI, i valori disponibili per la ricerca dei tipi sono elencati nella Tipi di esiti tabella.

Ciò è utile per testare le regole o l'automazione degli CloudWatch eventi in base ai risultati. L'esempio seguente mostra come generare un singolo esempio di esito del tipo `Backdoor:EC2/DenialOfService.Tcp` utilizzando la AWS CLI.

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

Il titolo dei risultati di esempio generati con questi metodi inizia sempre con [SAMPLE] nella console. I risultati di esempio hanno un valore pari `"sample": true` a nella additionalInfosezione dei JSON dettagli del risultato.

Per generare alcuni risultati comuni basati su un'attività simulata in un ambiente dedicato e isolato Account AWS all'interno del proprio ambiente, vedere GuardDuty Risultati dei test in account dedicati.

GuardDuty Risultati dei test in account dedicati

Utilizzate questo documento per eseguire uno script di tester che genera GuardDuty risultati in un Account AWS ambiente utilizzato specificamente per questo scopo. È possibile eseguire questi passaggi quando si desidera comprendere e apprendere determinati tipi di GuardDuty risultati. Questa esperienza è diversa dalla generazioneRisultati di esempio. Per ulteriori informazioni sull'esperienza acquisita con GuardDuty i risultati dei test, vedereConsiderazioni.

Indice

Considerazioni

Prima di procedere, tenete conto delle seguenti considerazioni:

- GuardDuty consiglia di distribuire lo script del tester in un ambiente dedicato, non di produzione Account AWS o isolato. Eseguendo lo script tester, GuardDuty distribuirà determinate AWS risorse in questo account. Questo ti aiuterà anche a identificare questi risultati simulati.
- Lo script tester genera oltre 100 GuardDuty risultati con diverse combinazioni di AWS risorse. Attualmente, questo non include tutti i. Tipi di esiti Per un elenco dei tipi di ricerca che puoi generare con questo script di test, vedi. GuardDuty lo script del tester dei risultati può generare
- Lo script tester convalida lo stato della GuardDuty configurazione nel tuo account dedicato. Se questo account non è GuardDuty abilitato, lo script richiederà di abilitarlo al momento

dell'esecuzione. Fase 3 - Esegui gli script dei tester Lo script tester richiederà l'autorizzazione dell'utente per abilitare determinati piani di protezione necessari per generare i risultati.

Attivazione GuardDuty per la prima volta

Quando GuardDuty viene abilitato per la prima volta nel tuo account dedicato in una regione specifica, il tuo account verrà automaticamente registrato a una prova gratuita di 30 giorni.

GuardDuty offre piani di protezione opzionali. Al momento dell'attivazione GuardDuty, vengono attivati anche alcuni piani di protezione, inclusi nella versione di prova gratuita di GuardDuty 30 giorni. Per ulteriori informazioni, consulta Utilizzo della GuardDuty prova gratuita di 30 giorni.

GuardDuty è già abilitato nel tuo account prima di eseguire lo script tester

Se GuardDuty è già abilitato, in base ai parametri, lo script tester controllerà lo stato di configurazione di determinati piani di protezione e altre impostazioni a livello di account necessarie per generare i risultati.

Eseguendo questo script di test, alcuni piani di protezione potrebbero essere abilitati per la prima volta nell'account dedicato in una regione. Verrà così avviata la prova gratuita di 30 giorni per quel piano di protezione. Per informazioni sulla prova gratuita associata a ciascun piano di protezione, consultaUtilizzo della GuardDuty prova gratuita di 30 giorni.

- Al termine dello script del tester, l'account dedicato ripristinerà la configurazione e le impostazioni originali del piano di protezione.

GuardDuty lo script del tester dei risultati può generare

Attualmente, lo script tester genera i seguenti tipi di risultati relativi ad Amazon, AmazonEKS, EC2 Amazon S3 e ai log di IAM controllo: EKS

- 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

Fase 1 - Prerequisiti

Per preparare l'ambiente di test, sono necessari i seguenti elementi:

- Git: installa lo strumento da riga di comando git in base al sistema operativo che utilizzi. Questo è necessario per clonare il `amazon-guardduty-tester`repository.
- AWS Command Line Interface— Uno strumento open source che consente di interagire AWS servizi utilizzando i comandi della shell della riga di comando. Per ulteriori informazioni, consulta la Guida introduttiva AWS CLI nella Guida per l'AWS Command Line Interface utente.
- AWS Systems Manager— Per avviare sessioni di Session Manager con i nodi gestiti utilizzando, AWS CLI è necessario installare il plug-in Session Manager sul computer locale. Per ulteriori informazioni, consulta Installa il plug-in Session Manager AWS CLI nella Guida per l'AWS Systems Manager utente.
- Node Package Manager (NPM) — NPM Installa per installare tutte le dipendenze.
- Docker: è necessario che Docker sia installato. Per istruzioni sull'installazione, consulta il sito Web Docker.

  Per verificare che Docker sia stato installato, esegui il comando seguente e conferma che esista un output simile al seguente:

  ```
  $ docker --version
  Docker version 19.03.1
  ```
- Iscriviti all'immagine di Kali Linux in. Marketplace AWS

Fase 2 - Implementazione delle risorse AWS

Questa sezione fornisce un elenco di concetti chiave e i passaggi per distribuire determinate AWS risorse nel tuo account dedicato.

Concetti

L'elenco seguente fornisce i concetti chiave relativi ai comandi che consentono di distribuire le risorse:

- AWS Cloud Development Kit (AWS CDK)— CDK è un framework di sviluppo software open source per definire l'infrastruttura cloud in codice e fornirla tramite. AWS CloudFormation CDKsupporta un paio di linguaggi di programmazione per definire componenti cloud riutilizzabili noti come costrutti. Puoi comporli insieme in pile e app. Quindi, puoi distribuire CDK le tue applicazioni per AWS CloudFormation fornire o aggiornare le tue risorse. Per ulteriori informazioni, consulta Cos'è il AWS CDK? nella Guida per gli AWS Cloud Development Kit (AWS CDK) sviluppatori.

- Bootstrap: è il processo di preparazione dell' AWS ambiente per l'utilizzo con. AWS CDK Prima di distribuire uno CDK stack in un AWS ambiente, è necessario avviare l'ambiente. Questo processo di provisioning di AWS risorse specifiche nell'ambiente utilizzate da AWS CDK fa parte dei passaggi che verranno eseguiti nella prossima sezione -. Passaggi per distribuire le risorse AWS

  Per ulteriori informazioni su come funziona il bootstrap, consulta Bootstrapping nella Developer Guide.AWS Cloud Development Kit (AWS CDK)

Passaggi per distribuire le risorse AWS

Esegui i passaggi seguenti per iniziare a distribuire le risorse:

1. Configura l'account e la regione AWS CLI predefiniti, a meno che le variabili Region dell'account dedicato non vengano impostate manualmente nel `bin/cdk-gd-tester.ts` file. Per ulteriori informazioni, consulta Environments nella AWS Cloud Development Kit (AWS CDK) Developer Guide.
2. Esegui i seguenti comandi per distribuire le risorse:

```
git clone https://github.com/awslabs/amazon-guardduty-tester && cd amazon-guardduty-tester
npm install
cdk bootstrap
cdk deploy
```

   L'ultimo comando (`cdk deploy`) crea uno AWS CloudFormation stack per tuo conto. Il nome di questo stack è. GuardDutyTesterStack

   Come parte di questo script, GuardDuty crea nuove risorse per generare GuardDuty risultati nel tuo account. Aggiunge inoltre la seguente coppia di tag key:value alle istanze AmazonEC2:

   `CreatedBy:GuardDuty Test Script`

   Le EC2 istanze Amazon includono anche le EC2 istanze che ospitano EKS nodi e ECS cluster.

   > **Tipi di istanza**
   >
   > GuardDuty crea `t3.micro` per tutte le risorse ad eccezione del gruppo di EKS nodi Amazon. Poiché EKS richiede almeno 2 core, il EKS nodo ha un tipo di `t3.medium`

istanza. Per ulteriori informazioni sui tipi di istanze, consulta le dimensioni disponibili nella Amazon EC2 Instances Types Guide.

Fase 3 - Esegui gli script dei tester

Si tratta di un processo in due fasi in cui è necessario prima avviare una sessione con il test driver e quindi eseguire script per generare GuardDuty risultati con combinazioni di risorse specifiche.

Parte A - Inizia la sessione con il test driver

1. Dopo aver distribuito le risorse, salvate il codice regionale in una variabile nella sessione di terminale corrente. Utilizzate il seguente comando e sostituite *us-east-1* con il codice regionale in cui hai distribuito le risorse:

```
$ REGION=us-east-1
```

2. Lo script tester è disponibile solo tramite AWS Systems Manager ()SSM. Per avviare una shell interattiva sull'istanza dell'host del tester, interroga l'host. InstanceId
3. Utilizzate il seguente comando per iniziare la sessione per lo script tester:

```
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)
```

Parte B - Generazione di risultati

Lo script tester è un programma basato su Python che crea dinamicamente uno script bash per generare risultati in base al tuo input. Hai la flessibilità necessaria per generare risultati basati su uno o più tipi di AWS risorse, piani di GuardDuty protezione, (tattiche) o. Scopi delle minacce Origini dati fondamentali the section called “GuardDuty lo script del tester dei risultati può generare”

Utilizza i seguenti esempi di comandi come riferimento ed esegui uno o più comandi per generare risultati da esplorare:

```
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'
```

Per ulteriori informazioni sui parametri validi, puoi eseguire il seguente comando help:

```
python3 guardduty_tester.py --help
```

Parte C - Esamina i risultati generati

Scegli un metodo preferito per visualizzare i risultati generati nel tuo account.

GuardDuty console

1. Accedi AWS Management Console e apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, seleziona Esiti.
3. Dalla tabella dei risultati, seleziona un risultato di cui desideri visualizzare i dettagli. Si aprirà il pannello dei dettagli del risultato. Per informazioni, consultare Comprendere i GuardDuty risultati di Amazon.
4. Se desideri filtrare questi risultati, usa la chiave e il valore del tag di risorsa. Ad esempio, per filtrare i risultati generati per le EC2 istanze Amazon, usa`CreatedBy: GuardDuty Test Script` tag key:value pair per Instance tag key e Instance tag key.

API

- Esegui ListFindingsper visualizzare i risultati relativi a uno specifico ID del rilevatore. È possibile filtrare i risultati con parametri specifici.

Per trovare i `detectorId` dati relativi al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

AWS CLI

- Esegui il AWS CLI comando seguente per visualizzare i risultati generati e sostituirli *us-east-1* e *12abc34d567e8fa901bc2d34EXAMPLE* con valori adeguati:

```
aws guardduty list-findings --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34EXAMPLE
```

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

Per ulteriori informazioni sui parametri che puoi utilizzare per filtrare i risultati, consulta list-findings nel AWS CLI Command Reference.

Fase 4 - Pulisci le risorse di test AWS

Le impostazioni a livello di account e gli altri aggiornamenti dello stato di configurazione effettuati durante il Fase 3 - Esegui gli script dei tester ripristino dello stato originale al termine dello script del tester.

Dopo aver eseguito lo script del tester, puoi scegliere di ripulire le risorse del test. AWS Puoi scegliere di eseguire questa operazione utilizzando uno dei seguenti metodi:

- Esegui il comando seguente:

```
cdk destroy
```

- Eliminare lo AWS CloudFormation stack con il nome GuardDutyTesterStack. Per informazioni sui passaggi, vedi Eliminazione di uno stack sulla console. AWS CloudFormation

Risoluzione dei problemi più comuni

GuardDuty ha identificato i problemi più comuni e consiglia le procedure per la risoluzione dei problemi:

- `Cloud assembly schema version mismatch`— Esegui l'aggiornamento AWS CDK CLI a una versione compatibile con la versione di cloud assembly richiesta o all'ultima versione disponibile. Per ulteriori informazioni, vedi AWS CDK CLIcompatibilità.
- `Docker permission denied`— Aggiungi l'utente dell'account dedicato agli utenti docker in modo che l'account dedicato possa eseguire i comandi. Per ulteriori informazioni sui passaggi, vedi Accesso negato a Docker.
- `Your requested instance type is not supported in your requested Availability Zone`— Alcune zone di disponibilità non supportano particolari tipi di istanze. Per identificare quali zone di disponibilità supportano il tipo di istanza preferito e tentare nuovamente di distribuire AWS le risorse, procedi nel seguente modo:

  1. Scegli un metodo preferito per determinare quali zone di disponibilità supportano il tuo tipo di istanza:

     Console

     Per identificare le zone di disponibilità che supportano il tipo di istanza preferito

     1. Accedi a AWS Management Console e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
     2. Utilizzando il selettore AWS della regione nell'angolo in alto a destra della pagina, scegli la regione in cui desideri avviare l'istanza.
     3. Nel riquadro di navigazione, in Istanze, scegli Tipi di istanze.
     4. Dalla tabella Tipi di istanze, scegli un tipo di istanza preferito.
     5. In Rete, visualizza le regioni elencate in Zone di disponibilità.

        In base a queste informazioni, potrebbe essere necessario scegliere una nuova regione in cui distribuire le risorse.

     AWS CLI

     Esegui il comando seguente per visualizzare un elenco di zone di disponibilità. Assicurati di specificare il tipo di istanza preferito e la regione (*`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
```

Per ulteriori informazioni su questo comando, vedete describe-instance-type-offeringsnella Guida di riferimento ai AWS CLI comandi.

Quando esegui questo comando, se ricevi un errore, assicurati di utilizzare la versione più recente di AWS CLI. Per ulteriori informazioni, consulta la sezione Risoluzione dei problemi nella Guida per l'utente di AWS Command Line Interface .

2. Prova a distribuire nuovamente le AWS risorse e specifica una zona di disponibilità che supporti il tipo di istanza preferito.

   Per riprovare a distribuire le risorse AWS

   1. Imposta la regione predefinita nel file. `bin/cdk-gd-tester.ts`
   2. Per specificare la zona di disponibilità, apri il `amazon-guardduty-tester/lib/common/network/vpc.ts` file.
   3. In questo file, `maxAzs: 2,` sostituiscilo con `availabilityZones: ['us-east-1a', 'us-east-1c'],` dove devi specificare le zone di disponibilità per il tipo di istanza.
   4. Continua con i passaggi rimanenti riportati di seguitoPassaggi per distribuire le risorse AWS.

Livelli di gravità dei GuardDuty risultati

A ogni GuardDuty rilevazione è assegnato un livello di gravità e un valore che riflettono il rischio potenziale che la scoperta potrebbe comportare per la rete, secondo quanto stabilito dai nostri tecnici di sicurezza. Il valore della gravità può rientrare ovunque nell'intervallo da 1,0 a 8,9, con valori più alti che indicano un rischio maggiore per la sicurezza. Per aiutarti a determinare una risposta a un potenziale problema di sicurezza evidenziato da un risultato GuardDuty , suddividi questo intervallo in livelli di gravità alto, medio e basso.

> **Note**
>
> I valori 0 e quelli compresi tra 9,0 e 10,0 sono riservati per l'utilizzo futuro.

Di seguito sono riportati i livelli e i valori di gravità attualmente definiti per i GuardDuty risultati, nonché le raccomandazioni generali per ciascuno di essi:

Livello di gravità	Intervallo di valori
Elevate	7,0 - 8,9

Un livello di severità elevato indica che la risorsa in questione (un'EC2istanza o un set di credenzia li di accesso IAM utente) è compromessa e viene utilizzata attivamente per scopi non autorizzati.

Si consiglia di considerare prioritario qualsiasi problema di sicurezza di individuazione di gravità elevata e di adottare misure immediate per prevenire un ulteriore utilizzo non autorizzato delle risorse. Ad esempio, pulisci l'EC2istanza o chiudila o ruota le credenziali. IAM Per ulteriori dettagli, vedere Procedure di correzione .

Medio	4,0 - 6,9

Un livello di gravità medio indica un'attività sospetta che si discosta dal comportamento normalmente osservato e, a seconda del caso d'uso, può essere indicativa di una compromissione delle risorse.

Ti consigliamo di esaminare le risorse coinvolte appena possibile. I passaggi di correzione variano in base alla risorsa e alla famiglia Ricerca, ma in generale, dovresti verificare che l'attività sia autorizzata e coerente con il tuo caso d'uso. Se non è possibile identificare la causa o confermar e che l'attività è stata autorizzata, è necessario considerare la risorsa compromessa e seguire le Procedure di correzione per proteggere la risorsa.

Ecco alcune cose da considerare quando si esamina una ricerca di livello medio:

- Controlla se un utente autorizzato ha installato un nuovo software che ha modificato il comportamento di una risorsa (ad esempio, consentito un traffico da alto a normale o abilitato le comunicazioni su una nuova porta).
- Controlla se un utente autorizzato ha modificato le impostazioni del pannello di controllo, per esempio, o ha cambiato le impostazioni del gruppo di sicurezza
- Esegui una scansione antivirus sulla risorsa coinvolta per rilevare il software non autorizzato.
- Verifica le autorizzazioni associate al IAM ruolo, all'utente, al gruppo o al set di credenziali implicati. Queste potrebbero essere modificate o ruotate.

Livello di gravità	Intervallo di valori
Bassa	1,0 - 3,9

Un livello di gravità basso indica un tentativo di attività sospetta che non ha compromesso la rete, ad esempio una scansione della porta o un tentativo di intrusione non riuscito.

Non vi è alcuna operazione consigliata immediata, ma vale la pena prendere nota di queste informazioni in quanto ciò potrebbe indicare che qualcuno sta cercando punti deboli nella rete.

Revisione GuardDuty dei risultati

Utilizza la procedura seguente per esaminare e comprendere i GuardDuty risultati.

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Scegliere Risultati e quindi scegliere un risultato specifico per visualizzarne i dettagli.

   I dettagli per ogni esito variano a seconda del tipo di esito, delle risorse coinvolte e della natura dell'attività. Per ulteriori informazioni sui campi di ricerca disponibili, vedere Dettagli degli esiti.
3. (Facoltativo) Se desideri archiviare un esito, selezionalo dall'elenco degli esiti e seleziona il menu Operazioni. Quindi scegli Archivia.

   Gli esiti archiviati possono essere visualizzati scegliendo Archiviati dall'elenco a discesa Attuali.

   Attualmente gli GuardDuty utenti degli account dei GuardDuty membri non possono archiviare i risultati.

   > **Important**
   >
   > Se si archivia una ricerca manualmente utilizzando la procedura qui sopra, tutte le successive occorrenze di questo risultato (generato dopo l'archiviazione) vengono aggiunte all'elenco dei risultati disponibili. Per non visualizzare mai questo risultato nell'elenco corrente, è possibile archiviarlo automaticamente. Per ulteriori informazioni, consulta Regole di eliminazione.

4. Per archiviare o scaricare un risultato, selezionarlo dall'elenco dei risultati, quindi scegliere il menu Operazioni. Quindi scegliere Esporta. Quando esporti un risultato, puoi visualizzarne il JSON documento completo.

> **Note**
>
> In alcuni casi, GuardDuty si rende conto che alcuni risultati sono falsi positivi dopo che sono stati generati. GuardDuty fornisce un campo Confidenza nei risultati e ne imposta il valore su zero. JSON In questo GuardDuty modo saprai che puoi tranquillamente ignorare tali risultati.

Dettagli degli esiti

Nella GuardDuty console Amazon, puoi visualizzare i dettagli della ricerca nella sezione di riepilogo dei risultati. I dettagli degli esiti variano in base al tipo di esito.

Esistono due dettagli principali che determinano il tipo di informazioni disponibili per qualsiasi esito. Il primo è il tipo di risorsa, che può essere `InstanceAccessKey`,`S3Bucket`,`S3Object`,`Kubernetes cluster`,`ECS cluster`,`Container`,`RDSDBInstance`, `oLambda`. Il secondo dettaglio che determina le informazioni sull'esito è Ruolo risorsa. Il ruolo risorsa può essere `Target` per le chiavi di accesso, che indica che la risorsa è stata la destinazione di attività sospette. Per gli esiti del tipo istanza, il ruolo risorsa può anche essere `Actor`, che indica che la risorsa è stata l'attore che svolgeva attività sospette. In questo argomento vengono descritti alcuni dei dettagli degli esiti comunemente disponibili.

Panoramica degli esiti

La sezione Panoramica di un esito ne contiene le caratteristiche identificative di base, incluse le informazioni seguenti:

- ID account: l'ID dell' AWS account in cui si è svolta l'attività che ha richiesto la generazione GuardDuty di questo risultato.
- Conteggio: il numero di volte in cui GuardDuty è stata aggregata un'attività che corrisponde a questo schema a questo risultato ID.
- Ora creazione: la data e l'ora di creazione di questo esito. Se questo valore è diverso da Ora aggiornamento significa che l'attività si è verificata più volte e si tratta di un problema in corso.

> **Note**
>
> I timestamp dei risultati nella GuardDuty console vengono visualizzati nel fuso orario locale, mentre le JSON esportazioni e gli CLI output visualizzano i timestamp in. UTC

- ID risultato: un identificatore univoco per questo tipo di esito e insieme di parametri. Le nuove occorrenze di attività corrispondenti a questo modello verranno aggregate allo stesso ID.
- Tipo di esito: una stringa formattata che rappresenta il tipo di attività che ha attivato l'esito. Per ulteriori informazioni, consulta Formato degli esiti di GuardDuty.
- Regione: la AWS regione in cui è stato generato il risultato. Per ulteriori informazioni sulle regioni supportate, consulta Regioni ed endpoint.
- ID risorsa: l'ID della AWS risorsa in base alla quale si è svolta l'attività che ha portato GuardDuty alla generazione del risultato.
- Scan ID: applicabile ai risultati quando GuardDuty Malware Protection for EC2 è abilitata, si tratta di un identificatore della scansione antimalware eseguita sui EBS volumi collegati al carico di lavoro dell'EC2istanza o del container potenzialmente compromessi. Per ulteriori informazioni, consulta Protezione da malware per la EC2 ricerca di dettagli.
- Gravità: a un esito viene assegnato un livello di gravità, che può essere alto, medio o basso. Per ulteriori informazioni, consulta Livelli di gravità dei GuardDuty risultati.
- Aggiornato il: l'ultima volta che questo risultato è stato aggiornato con una nuova attività che corrisponde allo schema che ha portato GuardDuty alla generazione di questo risultato.

Risorsa

La risorsa interessata fornisce dettagli sulla AWS risorsa presa di mira dall'attività iniziale. Le informazioni disponibili variano in base al tipo di risorsa e al tipo di operazione.

Ruolo della risorsa: il ruolo della AWS risorsa che ha avviato la ricerca. Questo valore può essere TARGETo ACTORe indica se la risorsa era l'obiettivo dell'attività sospetta o l'attore che ha eseguito l'attività sospetta.

Tipo di risorsa: il tipo di risorsa interessata. Un esito può includere diversi tipi di risorse se sono state coinvolte più risorse. I tipi di risorse sono Instance AccessKey, S3Bucket, S3Object,,, Container KubernetesClustere ECSClusterLambda. RDSDBInstance A seconda del tipo di risorsa sono

disponibili diversi dettagli degli esiti. Seleziona una scheda delle opzioni di risorsa per scoprire i dettagli disponibili per la risorsa interessata.

Instance

Dettagli dell'istanza:

> **Note**
>
> Alcuni dettagli sull'istanza potrebbero mancare se l'istanza è già stata interrotta o se la API chiamata sottostante ha avuto origine da un'EC2istanza in una regione diversa durante una chiamata interregionale. API

- ID istanza: l'ID dell'EC2istanza coinvolta nell'attività che ha richiesto GuardDuty la generazione del risultato.
- Tipo di istanza: il tipo di EC2 istanza coinvolta nel risultato.
- Ora di avvio: la data e l'ora in cui l'istanza è stata avviata.
- Outpost ARN: il nome della risorsa Amazon (ARN) di AWS Outposts. Applicabile solo alle AWS Outposts istanze. Per ulteriori informazioni, consulta What is AWS Outposts?
- Nome del gruppo di sicurezza: il nome del gruppo di sicurezza collegato all'istanza interessata.
- ID gruppo di sicurezza: l'ID del gruppo di sicurezza collegato all'istanza interessata.
- Stato dell'istanza: lo stato attuale dell'istanza di destinazione.
- Zona di disponibilità: la zona di disponibilità della regione AWS in cui si trova l'istanza coinvolta.
- ID immagine: l'ID dell'Amazon Machine Image utilizzato per creare l'istanza coinvolta nell'attività.
- Descrizione immagine: una descrizione dell'ID dell'Amazon Machine Image utilizzato per creare l'istanza coinvolta nell'attività.
- Tag: un elenco di tag collegati a questa risorsa elencati nel formato `key:value`.

AccessKey

Dettagli chiave di accesso:

- ID chiave di accesso: l'ID della chiave di accesso dell'utente impegnato nell'attività che ha richiesto GuardDuty la generazione del risultato.

- ID principale: l'ID principale dell'utente impegnato nell'attività che ha richiesto GuardDuty la generazione del risultato.
- Tipo di utente: il tipo di utente impegnato nell'attività che ha richiesto GuardDuty la generazione del risultato. Per ulteriori informazioni, consulta CloudTrail userIdentity element.
- Nome utente: il nome dell'utente impegnato nell'attività che ha portato GuardDuty alla generazione del risultato.

S3Bucket

Dettagli bucket Amazon S3:

- Nome: il nome del bucket coinvolto nell'esito.
- ARN— Il contenuto ARN del secchio utilizzato per il ritrovamento.
- Proprietario: l'ID utente canonico dell'utente proprietario del bucket coinvolto nell'esito. Per ulteriori informazioni sugli utenti canonici, IDs consulta AWS gli identificatori dell'account.
- Tipo: il tipo di esito del bucket può essere Destinazione o Origine.
- Crittografia lato server predefinita: i dettagli di crittografia per il bucket.
- Tag bucket: un elenco dei tag collegati a questa risorsa, elencati nel formato di `key:value`.
- Autorizzazioni valide: una valutazione di tutte le autorizzazioni e le policy valide nel bucket che indica se il bucket interessato è esposto pubblicamente. I valori possono essere Pubblico o Non pubblico.

S3Object

- Dettagli dell'oggetto S3: include le seguenti informazioni sull'oggetto S3 scansionato:
  - ARN— Amazon Resource Name (ARN) dell'oggetto S3 scansionato.
  - Chiave: il nome assegnato al file quando è stato creato nel bucket S3.
  - ID versione: se hai abilitato il controllo delle versioni del bucket, questo campo indica l'ID della versione associato all'ultima versione dell'oggetto S3 scansionato. Per ulteriori informazioni, consulta Using versioning in bucket S3 nella Amazon S3 User Guide.
  - eTag— Rappresenta la versione specifica dell'oggetto S3 scansionato.
  - Hash: hash della minaccia rilevata in questo risultato.
- Dettagli sul bucket S3: include le seguenti informazioni sul bucket Amazon S3 associato all'oggetto S3 scansionato:

  - Nome: indica il nome del bucket S3 che contiene l'oggetto.
  - ARN— Amazon Resource Name (ARN) del bucket S3.
- Proprietario: ID canonico del proprietario del bucket S3.

EKSCluster

Dettagli del cluster Kubernetes:

- Nome: il nome del cluster Kubernetes.
- ARN— Il ARN che identifica il cluster.
- Ora creazione: la data e l'ora di creazione di questo cluster.

> **Note**
>
> I timestamp dei risultati nella GuardDuty console vengono visualizzati nel fuso orario locale, mentre le JSON esportazioni e gli CLI output visualizzano i timestamp in. UTC

- VPCID: l'ID di VPC che è associato al cluster.
- Stato: lo stato attuale del cluster.
- Tag: i metadati applicati al cluster utili per catalogarli e organizzarli. Ciascun tag è formato da una chiave e da un valore facoltativo, elencati nel formato `key:value`. Puoi definire sia la chiave che il valore.

  I tag del cluster non si propagano ad altre risorse associate al cluster.

Dettagli del carico di lavoro Kubernetes:

- Tipo: il tipo di carico di lavoro Kubernetes, ad esempio pod, implementazione e processo.
- Nome: il nome del carico di lavoro Kubernetes.
- Uid: l'ID univoco del carico di lavoro Kubernetes.
- Ora creazione: la data e l'ora di creazione di questo carico di lavoro.
- Etichette: le coppie chiave-valore collegate al carico di lavoro Kubernetes.
- Container: i dettagli del container in esecuzione come parte del carico di lavoro Kubernetes.
- Spazio dei nomi: il carico di lavoro appartiene a questo spazio dei nomi Kubernetes.
- Volumi: i volumi utilizzati dal carico di lavoro Kubernetes.

    - Percorso host: rappresenta un file o una directory preesistente sulla macchina host a cui è mappato il volume.
    - Nome: il nome del volume.
- Contesto di sicurezza del pod: definisce i privilegi e le impostazioni di controllo degli accessi per tutti i container in un pod.
- Rete host: impostata su `true` se i pod sono inclusi nel carico di lavoro Kubernetes.

Dettagli utente Kubernetes:

- Gruppi: gruppi Kubernetes RBAC (controllo basato sull'accesso ai ruoli) dell'utente coinvolto nell'attività che ha generato il risultato.
- ID: l'ID univoco dell'utente Kubernetes.
- Nome utente: nome dell'utente Kubernetes coinvolto nell'attività che ha generato l'esito.
- Nome sessione: entità che ha assunto il ruolo con le autorizzazioni KubernetesIAM. RBAC

ECSCluster

ECSdettagli del cluster:

- ARN— Il ARN che identifica il cluster.
- Nome: il nome del cluster.
- Stato: lo stato attuale del cluster.
- Numero di servizi attivi: il numero dei servizi in esecuzione sul cluster con stato `ACTIVE`. È possibile visualizzare questi servizi con ListServices
- Numero di istanze di container registrate: il numero delle istanze di container registrate nel cluster, incluse sia le istanza di container con stato `ACTIVE` che quelle con stato `DRAINING`.
- Numero di attività in esecuzione: il numero di attività con stato `RUNNING` nel cluster.
- Tag: i metadati applicati al cluster utili per catalogarli e organizzarli. Ciascun tag è formato da una chiave e da un valore facoltativo, elencati nel formato `key:value`. Puoi definire sia la chiave che il valore.
- Container: i dettagli sul container associato all'attività.
    - Nome container: il nome del container.
    - Immagine del container: l'immagine del container.

- Dettagli dell'attività: i dettagli di un'attività in un cluster.
  - ARN— L'Amazon Resource Name (ARN) dell'attività.
  - Definizione ARN: Amazon Resource Name (ARN) della definizione dell'attività che crea l'attività.
  - Versione: il contatore delle versioni per l'attività.
  - Ora creazione attività: il timestamp Unix al momento della creazione dell'attività.
  - Ora inizio attività: il timestamp Unix all'inizio dell'attività.
  - Attività iniziata da: il tag specificato all'avvio di un'attività.

Container

Dettagli container:

- Runtime del container: il runtime del container (ad esempio `docker` o `containerd`) utilizzato per eseguire il container.
- ID: l'ID dell'istanza del contenitore o ARN le voci complete per l'istanza del contenitore.
- Nome: il nome del container.

  Se disponibile, questo campo mostra il valore dell'etichetta `io.kubenetes.container.name`.
- Immagine: l'immagine dell'istanza di container.
- Montaggi volume: elenco dei montaggi del volume del container. Un container può montare un volume nel proprio file system.
- Contesto di sicurezza: il contesto di sicurezza del container definisce i privilegi e le impostazioni di controllo degli accessi per un container.
- Dettagli del processo: descrive i dettagli del processo associato all'esito.

RDSDBInstance

RDSDBInstancedettagli:

> **Note**
>
> Questa risorsa è disponibile nei risultati di RDS protezione relativi all'istanza del database.

- ID dell'istanza del database: l'identificatore associato all'istanza di database coinvolta nel GuardDuty risultato.
- Motore: il nome del motore di database dell'istanza di database coinvolta nell'esito. I valori possibili sono Aurora My SQL -Compatible o Aurora Postgre -Compatible. SQL
- Versione del motore: la versione del motore di database coinvolta nella ricerca. GuardDuty
- ID del cluster di database: l'identificatore del cluster di database che contiene l'ID dell'istanza di database coinvolta nel GuardDuty risultato.
- Istanza di database ARN: ARN identifica l'istanza di database coinvolta nel GuardDuty risultato.

Lambda

Dettagli della funzione Lambda

- Nome funzione: il nome della funzione Lambda coinvolta nell'esito.
- Versione della funzione: la versione della funzione Lambda coinvolta nell'esito.
- Descrizione della funzione: una descrizione della funzione Lambda coinvolta nell'esito.
- Funzione ARN: Amazon Resource Name (ARN) della funzione Lambda coinvolta nella ricerca.
- ID revisione: l'ID di revisione della versione della funzione Lambda.
- Ruolo: il ruolo di esecuzione della funzione Lambda coinvolta nell'esito.
- VPCconfigurazione: la VPC configurazione di Amazon, inclusi l'VPCID, il gruppo di sicurezza e la sottorete IDs associati alla funzione Lambda.
- VPCID: l'ID di Amazon VPC associato alla funzione Lambda coinvolta nella ricerca.
- Subnet IDs: l'ID delle sottoreti associate alla funzione Lambda.
- Gruppo di sicurezza: il gruppo di sicurezza collegato alla funzione Lambda coinvolta. Sono inclusi il nome e l'ID del gruppo di sicurezza.
- Tag: un elenco di tag collegati a questa risorsa, elencati nel formato della coppia `key:value`.

RDSdettagli utente del database (DB)

> **Note**
>
> Questa sezione è applicabile ai risultati quando si abilita la funzionalità di RDS protezione in GuardDuty. Per ulteriori informazioni, consulta GuardDuty RDSProtezione.

La GuardDuty scoperta fornisce i seguenti dettagli sull'utente e sull'autenticazione del database potenzialmente compromesso.

- Utente: il nome utente utilizzato per effettuare il tentativo di accesso anomalo.
- Applicazione: il nome dell'applicazione utilizzata per effettuare il tentativo di accesso anomalo.
- Database: il nome dell'istanza di database coinvolta nel tentativo di accesso anomalo.
- SSL— La versione del Secure Socket Layer (SSL) utilizzata per la rete.
- Metodo di autenticazione: il metodo di autenticazione utilizzato dall'utente coinvolto nell'esito.

Runtime Monitoring: dettagli relativi

> **Note**
>
> Questi dettagli possono essere disponibili solo se GuardDuty genera uno deiTipi di risultati del monitoraggio del runtime.

Questa sezione contiene i dettagli del runtime, inclusi i dettagli del processo e qualsiasi contesto richiesto. I dettagli del processo descrivono le informazioni sul processo osservato e il contesto di runtime descrive qualsiasi informazione aggiuntiva sull'attività potenzialmente sospetta.

Dettagli del processo

- Nome: il nome del processo.
- Percorso eseguibile: il percorso assoluto del file eseguibile del processo.
- Executable SHA -256: l'`SHA256`hash del processo eseguibile.
- Namespace PID: l'ID del processo in uno spazio dei PID nomi secondario diverso dallo spazio dei nomi a livello di host. PID Per i processi all'interno di un container, corrisponde all'ID processo osservabile nel container.
- Directory di lavoro presente: la directory di lavoro presente del processo.
- ID processo: l'ID che il sistema operativo assegna al processo.
- startTime— L'ora in cui è iniziato il processo. È in formato stringa di UTC data (`2023-03-22T19:37:20.168Z`).
- UUID— L'ID univoco assegnato al processo da GuardDuty.

- Genitore UUID: l'ID univoco del processo principale. Questo ID viene assegnato al processo principale da GuardDuty.
- Utente: l'utente che ha eseguito il processo.
- ID utente: l'ID dell'utente che ha eseguito il processo.
- ID utente effettivo: l'ID utente effettivo del processo al momento dell'evento.
- Eredità: informazioni sugli antenati del processo.
  - ID processo: l'ID che il sistema operativo assegna al processo.
  - UUID— L'ID univoco assegnato al processo da GuardDuty.
  - Percorso eseguibile: il percorso assoluto del file eseguibile del processo.
  - ID utente effettivo: l'ID utente effettivo del processo al momento dell'evento.
  - Genitore UUID: l'ID univoco del processo principale. Questo ID viene assegnato al processo principale da GuardDuty.
  - Ora di inizio: l'ora in cui è iniziato il processo.
  - Namespace PID: l'ID del processo in uno spazio dei PID nomi secondario diverso dallo spazio dei nomi a livello di host. PID Per i processi all'interno di un container, corrisponde all'ID processo osservabile nel container.
  - ID utente: l'ID utente dell'utente che ha eseguito il processo.
  - Nome: il nome del processo.

Contesto di runtime

Un esito generato può includere, tra i campi seguenti, solo quelli pertinenti al tipo di esito.

- Origine di montaggio: il percorso sull'host montato dal container.
- Destinazione di montaggio: il percorso nel container mappato alla directory host.
- Tipo di file system: rappresenta il tipo di file system montato.
- Flag: rappresenta le opzioni che controllano il comportamento dell'evento coinvolto in questo esito.
- Processo di modifica: informazioni sul processo che in fase di runtime ha creato o modificato un file binario, uno script o una libreria all'interno di un container.
- Ora della modifica: il timestamp in cui il processo ha creato o modificato un file binario, uno script o una libreria all'interno di un container in fase di runtime. Questo campo è nel formato della stringa di data (). UTC `2023-03-22T19:37:20.168Z`
- Percorso libreria: il percorso della nuova libreria che è stata caricata.

- Valore LD Preload: il valore della variabile di ambiente `LD_PRELOAD`.
- Percorso socket: il percorso del socket Docker a cui è stato effettuato l'accesso.
- Percorso binario runc: il percorso del file binario `runc`.
- Percorso agente di rilascio: il percorso del file dell'agente di rilascio `cgroup`.
- Esempio di riga di comando: l'esempio della riga di comando coinvolta nell'attività potenzialmente sospetta.
- Categoria utensile: categoria a cui appartiene lo strumento. Alcuni esempi sono Backdoor Tool, Pentest Tool, Network Scanner e Network Sniffer.
- Nome dello strumento: il nome dello strumento potenzialmente sospetto.
- Percorso dello script: il percorso dello script eseguito che ha generato il risultato.
- Threat File Path: il percorso sospetto per il quale sono stati trovati i dettagli di intelligence sulle minacce.
- Nome del servizio: il nome del servizio di sicurezza che è stato disabilitato.

EBSdettagli di scansione dei volumi

> **Note**
>
> Questa sezione è applicabile ai risultati rilevati quando si attiva la scansione antimalware GuardDuty avviata. Protezione da malware per EC2

La scansione EBS dei volumi fornisce dettagli sul EBS volume collegato al carico di lavoro dell'EC2istanza o del contenitore potenzialmente compromesso.

- ID scansione: l'identificatore della scansione malware.
- Ora inizio scansione: la data e l'ora di inizio della scansione malware.
- Ora completamento scansione: la data e l'ora di completamento della scansione malware.
- Trigger Finding ID: l'ID di ricerca del GuardDuty risultato che ha avviato questa scansione antimalware.
- Fonti: i valori potenziali sono `Bitdefender` e`Amazon`.
- Rilevamenti scansione: la visualizzazione completa dei dettagli e degli esiti di ogni scansione malware.

- Numero elementi scansionati: il numero totale di file scansionati. Fornisce dettagli come `totalGb`, `files` e `volumes`.
- Numero elementi rilevati come minacce: il numero totale di `files` dannosi rilevati durante la scansione.
- Dettagli sulla minaccia con gravità più alta: i dettagli sulla minaccia di gravità più alta rilevata durante la scansione e sul numero di file dannosi. Fornisce dettagli come `severity`, `threatName` e `count`.
- Minacce rilevate per nome: l'elemento container che raggruppa le minacce di tutti i livelli di gravità. Fornisce dettagli come `itemCount`, `uniqueThreatNameCount`, `shortened` e `threatNames`.

Protezione da malware per la EC2 ricerca di dettagli

> **Note**
>
> Questa sezione è applicabile ai risultati ottenuti quando si attiva la scansione antimalware GuardDuty avviata. Protezione da malware per EC2

Quando la EC2 scansione Malware Protection for Scan rileva un malware, puoi visualizzare i dettagli della scansione selezionando il risultato corrispondente nella pagina Findings della console. https://console.aws.amazon.com/guardduty/ La gravità della protezione antimalware da EC2 individuare dipende dalla gravità del GuardDuty rilevamento.

> **Note**
>
> Il tag `GuardDutyFindingDetected` specifica che gli snapshot contengono malware.

Le seguenti informazioni sono disponibili nella sezione Minacce rilevate nel pannello dei dettagli.

- Nome: il nome della minaccia, ottenuto raggruppando i file in base al rilevamento.
- Gravità: la gravità della minaccia rilevata.
- Hash: il SHA -256 del file.
- Percorso del file: la posizione del file dannoso nel EBS volume.
- Nome file: il nome del file in cui è stata rilevata la minaccia.

- Volume ARN: ARN i EBS volumi scansionati.

Le seguenti informazioni sono disponibili nella sezione Dettagli della scansione malware nel pannello dei dettagli.

- ID scansione: l'ID di scansione della scansione malware.
- Ora inizio scansione: la data e l'ora di inizio della scansione.
- Ora completamento scansione: la data e l'ora di completamento della scansione.
- File scansionati: il numero totale di file e directory scansionati.
- GB totali scansionati: la quantità di spazio di archiviazione scansionato durante il processo.
- Trigger finding ID: l'ID di ricerca del GuardDuty risultato che ha avviato questa scansione antimalware.
- Le seguenti informazioni sono disponibili nella sezione Dettagli del volume nel pannello dei dettagli.
  - Volume ARN: il nome della risorsa Amazon (ARN) del volume.
  - Istantanea ARN: ARN l'istantanea del EBS volume.
  - Stato: lo stato della scansione del volume, ad esempio, `Running`, `Skipped` e `Completed`.
  - Tipo di crittografia: il tipo di crittografia utilizzato per crittografare il volume. Ad esempio `CMCMK`.
  - Nome dispositivo: il nome del dispositivo. Ad esempio `/dev/xvda`.

Informazioni sulla ricerca di Malware Protection for S3

I seguenti dettagli di scansione antimalware sono disponibili quando attivi GuardDuty sia Malware Protection for S3 su: Account AWS

- Minacce: un elenco di minacce rilevate durante la scansione del malware.

  Per informazioni sul numero di minacce che la scoperta può includere, consultaQuote nella protezione da malware per S3.
- Percorso dell'elemento: un elenco del percorso dell'elemento annidato e dei dettagli dell'hash dell'oggetto S3 scansionato.
  - Percorso dell'elemento annidato: percorso dell'elemento dell'oggetto S3 scansionato in cui è stata rilevata la minaccia.

    Il valore di questo campo è disponibile solo se l'oggetto di primo livello è un archivio e se la minaccia viene rilevata all'interno di un archivio.

  - Hash: hash della minaccia rilevata in questo risultato.
- Fonti: i valori potenziali sono `Bitdefender` e. `Amazon`

Azione

L'Operazione di un esito fornisce dettagli sul tipo di attività che l'ha attivato. Le informazioni disponibili variano in base al tipo di operazione.

Tipo di operazione: il tipo di attività dell'esito. Questo valore può essere NETWORKPORT_ CONNECTION PROBE, DNS_ REQUEST, AWS_ API _ CALL o RDS_ LOGIN _ ATTEMPT. Le informazioni disponibili variano in base al tipo di operazione:

- NETWORK_ CONNECTION — Indica che il traffico di rete è stato scambiato tra l'EC2istanza identificata e l'host remoto. Questo tipo di operazione include le seguenti informazioni aggiuntive:
  - Direzione della connessione: la direzione della connessione di rete osservata nell'attività che ha richiesto GuardDuty la generazione del risultato. Può essere uno dei seguenti valori:
    - INBOUND— Indica che un host remoto ha avviato una connessione a una porta locale sull'EC2istanza identificata nell'account.
    - OUTBOUND— Indica che l'EC2istanza identificata ha avviato una connessione a un host remoto.
    - UNKNOWN— Indica che non è GuardDuty stato possibile determinare la direzione della connessione.
  - Protocollo: il protocollo di connessione di rete osservato nell'attività che ha richiesto GuardDuty la generazione del risultato.
  - IP locale: il primo indirizzo IP di origine del traffico che ha attivato l'esito. Queste informazioni possono essere utilizzate per distinguere tra indirizzo IP di un livello intermedio su cui fluisce il traffico e il primo indirizzo IP di origine del traffico. Ad esempio, l'indirizzo IP di un EKS pod rispetto all'indirizzo IP dell'istanza su cui il EKS pod è in esecuzione.
  - Bloccata: indica se la porta di destinazione è bloccata.
- PORT_ PROBE — Indica che un host remoto ha sondato l'EC2istanza identificata su più porte aperte. Questo tipo di operazione include le seguenti informazioni aggiuntive:
  - IP locale: il primo indirizzo IP di origine del traffico che ha attivato l'esito. Queste informazioni possono essere utilizzate per distinguere tra indirizzo IP di un livello intermedio su cui fluisce il traffico e il primo indirizzo IP di origine del traffico. Ad esempio, l'indirizzo IP di un EKS pod rispetto all'indirizzo IP dell'istanza su cui il EKS pod è in esecuzione.

- Bloccata: indica se la porta di destinazione è bloccata.

- DNS_ REQUEST — Indica che l'EC2istanza identificata ha richiesto un nome di dominio. Questo tipo di operazione include le seguenti informazioni aggiuntive:
  - Protocollo: il protocollo di connessione di rete osservato nell'attività che ha richiesto la generazione del GuardDuty risultato.
  - Bloccata: indica se la porta di destinazione è bloccata.
- AWS_ API _ CALL — Indica che AWS API è stato richiamato un. Questo tipo di operazione include le seguenti informazioni aggiuntive:
  - API— Il nome dell'APIoperazione che è stata richiamata e quindi richiesta GuardDuty per generare questo risultato.

    > **Note**
    >
    > Queste operazioni possono includere anche API eventi diversi da. AWS CloudTrail Per ulteriori informazioni, vedere APIEventi non acquisiti da CloudTrail.

  - Agente utente: l'agente utente che ha effettuato la API richiesta. Questo valore indica se la chiamata è stata effettuata da AWS Management Console, un AWS servizio, da o da AWS CLI. AWS SDKs
  - ERRORCODE— Se il risultato è stato attivato da una API chiamata fallita, viene visualizzato il codice di errore relativo a quella chiamata.
  - Nome del servizio: il DNS nome del servizio che ha tentato di effettuare la API chiamata che ha attivato il risultato.
- RDS_ LOGIN _ ATTEMPT — Indica che è stato effettuato un tentativo di accesso al database potenzialmente compromesso da un indirizzo IP remoto.
  - Indirizzo IP: l'indirizzo IP remoto utilizzato per effettuare il tentativo di accesso potenzialmente sospetto.

Attore o destinazione

Un esito ha una sezione Attore se il Ruolo risorsa era `TARGET`. Ciò indica che la risorsa è stata la destinazione di attività sospette e la sezione Attore contiene dettagli sull'entità che ha scelto come destinazione la risorsa.

Un esito ha una sezione Destinazione se il Ruolo risorsa era `ACTOR`. Ciò indica che la risorsa è stata coinvolta in attività sospette nei confronti di un host remoto e questa sezione contiene informazioni sull'IP o sul dominio di destinazione della risorsa.

Le informazioni disponibili nella sezione Attore o Destinazione possono includere quanto segue:

- Affiliato: indica se l' AWS account del API chiamante remoto è correlato all'ambiente in uso. GuardDuty Se questo valore è`true`, il API chiamante è in qualche modo affiliato all'account dell'utente; in caso contrario`false`, proviene da un ambiente API esterno all'utente.
- ID account remoto: l'ID dell'account proprietario dell'indirizzo IP in uscita utilizzato per accedere alla risorsa sulla rete finale.
- Indirizzo IP: l'indirizzo IP coinvolto nell'attività che ha richiesto GuardDuty la generazione del risultato.
- Posizione: informazioni sulla posizione dell'indirizzo IP coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- Organizzazione: informazioni sull'ISPorganizzazione dell'indirizzo IP coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- Porta: il numero di porta coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- Dominio: il dominio coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- Dominio con suffisso: il dominio di secondo e primo livello coinvolto in un'attività che potenzialmente ha richiesto GuardDuty la generazione del risultato. Per un elenco dei domini di primo e secondo livello, consulta l'elenco dei suffissi pubblici.

Informazioni aggiuntive

Tutti gli esiti hanno una sezione Informazioni aggiuntive che può includere le informazioni seguenti:

- Nome dell'elenco delle minacce: il nome dell'elenco delle minacce che include l'indirizzo IP o il nome di dominio coinvolto nell'attività che ha richiesto GuardDuty la generazione del risultato.
- Esempio: un valore vero o falso che indica se si tratta di un esito di esempio.
- Archiviato: un valore vero o falso che indica se l'esito è stato archiviato.
- Insolito: dettagli dell'attività che non sono stati osservati in precedenza. Questi possono includere un utente insolito (non osservato in precedenza), la posizione, l'ora, il bucket, il comportamento di accesso o ASN l'organizzazione.

- Protocollo insolito: il protocollo di connessione di rete coinvolto nell'attività che ha portato GuardDuty alla generazione del risultato.
- Dettagli dell'agente: dettagli sul security agent attualmente distribuito nel EKS cluster del tuo. Account AWS Questo è applicabile solo ai tipi di risultati di EKS Runtime Monitoring.
  - Versione dell'agente: la versione del GuardDuty security agent.
  - ID agente: l'identificatore univoco del GuardDuty security agent.

Evidenza

Gli esiti basati sull'intelligence sulle minacce hanno una sezione Evidenza che include le informazioni seguenti:

- Dettagli di intelligence sulle minacce: il nome dell'elenco delle minacce in cui `Threat name` compaiono le minacce riconosciute.
- Nome della minaccia: il nome della famiglia di malware o altro identificatore associato alla minaccia.
- File di minaccia SHA256: SHA256 del file che ha generato la scoperta.

Comportamento anomalo

I tipi di risultati che terminano con AnomalousBehaviorindicano che il risultato è stato generato dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello ML valuta tutte le API richieste inviate all'account e identifica gli eventi anomali associati alle tattiche utilizzate dagli avversari. Il modello ML tiene traccia di vari fattori della API richiesta, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e lo specifico richiesto. API

I dettagli su quali fattori della API richiesta sono insoliti per l'identità CloudTrail dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato. Le identità sono definite dall' CloudTrail userIdentity Elemento e i valori possibili sono:`Root`,,`IAMUser`, `AssumedRole` `FederatedUserAWSAccount`, o. `AWSService`

Oltre ai dettagli disponibili per tutti i GuardDuty risultati associati all'APIattività, AnomalousBehaviori risultati hanno dettagli aggiuntivi descritti nella sezione seguente. Questi dettagli possono essere visualizzati nella console e sono disponibili anche nei risultati. JSON

- Anomala APIs: un elenco di API richieste che sono state richiamate dall'identità dell'utente in prossimità della API richiesta principale associata al risultato. Questo riquadro suddivide ulteriormente i dettagli dell'APIevento nei seguenti modi.
  - La prima API elencata è la principaleAPI, ovvero la API richiesta associata all'attività osservata con il rischio più elevato. Questa è API quella che ha innescato la scoperta ed è correlata alla fase di attacco del tipo di scoperta. Questa è anche API la descrizione dettagliata nella sezione Azione della console e nei risultati. JSON
  - Tutte le altre identità APIs elencate sono ulteriori anomale APIs rispetto all'identità utente elencata osservata in prossimità della principale. API Se ce n'è solo una API nell'elenco, il modello ML non ha identificato come anomale alcuna API richiesta aggiuntiva proveniente da quell'identità utente.
  - L'elenco di APIs viene suddiviso in base al fatto che una chiamata sia API stata effettuata correttamente o meno, ovvero che sia API stata ricevuta una risposta di errore. Il tipo di risposta di errore ricevuta è elencato sopra ogni chiamata non riuscita. API I possibili tipi di risposta di errore sono: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` e `operation not permitted`.
  - APIssono classificati in base al servizio associato.
  - Per maggiori informazioni, scegli Cronologico APIs per visualizzare i dettagli relativi alla parte superioreAPIs, fino a un massimo di 20, in genere relativi all'identità dell'utente e a tutti gli utenti all'interno dell'account. APIsSono contrassegnati come Rari (meno di una volta al mese), Non frequenti (alcune volte al mese) o Frequenti (da giornalieri a settimanali), a seconda della frequenza con cui vengono utilizzati nell'account.
- Comportamento insolito (account): questa sezione fornisce ulteriori dettagli sul comportamento profilato del tuo account.

> **Comportamento profilato**
>
> GuardDuty impara continuamente sulle attività all'interno del tuo account in base agli eventi organizzati. Queste attività e la loro frequenza osservata sono note come comportamenti profilati.

Le informazioni registrate in questo pannello includono:

- ASNOrg: l'ASNorganizzazione da cui è stata effettuata la API chiamata anomala.

- Nome utente: il nome dell'utente che ha effettuato la chiamata anomalaAPI.
- Agente utente: l'agente utente utilizzato per effettuare la chiamata anomalaAPI. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `aws-cli` o `Botocore`.
- Tipo di utente: il tipo di utente che ha effettuato la chiamata anomalaAPI. I valori possibili sono `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.
- Bucket: il nome del bucket S3 a cui viene effettuato l'accesso.

- Comportamento insolito (identità utente): questa sezione fornisce ulteriori dettagli sul comportamento profilato dell'Identità utente coinvolta nell'esito. Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non aveva mai visto questa identità utente effettuare questa API chiamata in questo modo durante il periodo di formazione. Sono disponibili i seguenti dettagli aggiuntivi sull'Identità utente:
  - ASNOrg: l'ASNOrg da cui è stata effettuata la API chiamata anomala.
  - User Agent: l'agente utente utilizzato per effettuare la chiamata anomalaAPI. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `aws-cli` o `Botocore`.
  - Bucket: il nome del bucket S3 a cui viene effettuato l'accesso.
- Comportamento insolito (bucket): questa sezione fornisce ulteriori dettagli sul comportamento profilato del bucket S3 associato all'esito Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non aveva mai visto in precedenza API chiamate effettuate in questo modo a questo bucket durante il periodo di formazione. Le informazioni registrate in questa sezione includono:
  - ASNOrg: l'ASNOrg da cui è stata effettuata la API chiamata anomala.
  - Nome utente: il nome dell'utente che ha effettuato la chiamata anomalaAPI.
  - Agente utente: l'agente utente utilizzato per effettuare la chiamata anomalaAPI. L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `aws-cli` o `Botocore`.
  - Tipo di utente: il tipo di utente che ha effettuato la chiamata anomalaAPI. I valori possibili sono `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.

> **Note**
>
> Per maggiori informazioni sui comportamenti storici, scegli Comportamento storico nella sezione Comportamento insolito (account), ID utente o Bucket per visualizzare i dettagli sul comportamento previsto nel tuo account per ciascuna delle seguenti categorie: Raro (meno di una volta al mese), Poco frequente (alcune volte al mese) o Frequente (da giornaliero

a settimanale), a seconda della frequenza con cui vengono utilizzati all'interno del tuo account.

- Comportamento insolito (database): questa sezione fornisce ulteriori dettagli sul comportamento profilato dell'istanza di database associata all'esito Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non ha mai visto in precedenza un tentativo di accesso effettuato in questo modo a questa istanza di database durante il periodo di formazione. Le informazioni registrate nel pannello dell'esito per questa sezione includono:
  - Nome utente: il nome utente utilizzato per effettuare il tentativo di accesso anomalo.
  - ASNOrg: l'ASNorganizzazione da cui è stato effettuato il tentativo di accesso anomalo.
  - Nome applicazione: il nome dell'applicazione utilizzata per effettuare il tentativo di accesso anomalo.
  - Nome database: il nome dell'istanza di database coinvolta nel tentativo di accesso anomalo.

  La sezione Cronologia del comportamento fornisce ulteriori informazioni sui nomi utente, le ASN organizzazioni, i nomi delle applicazioni e i nomi dei database osservati in precedenza per il database associato. A ogni valore univoco è associato un conteggio che rappresenta il numero di volte in cui questo valore è stato osservato in un evento di accesso riuscito.
- Comportamento insolito (account cluster Kubernetes, spazio dei nomi Kubernetes e nome utente Kubernetes): questa sezione fornisce ulteriori dettagli sul comportamento profilato per il cluster e lo spazio dei nomi Kubernetes associati all'esito. Quando un comportamento non è identificato come storico, significa che il modello GuardDuty ML non ha mai osservato in precedenza questo account, cluster, namespace o nome utente in questo modo. Le informazioni registrate nel pannello dell'esito per questa sezione includono:
  - Nome utente: l'utente che ha chiamato Kubernetes API associato al risultato.
  - Nome utente impersonato: l'utente impersonato da `username`.
  - Namespace: lo spazio dei nomi Kubernetes all'interno del cluster Amazon in cui si è verificata l'azione. EKS
  - User Agent: l'agente utente associato alla chiamata Kubernetes. API L'agente utente è il metodo utilizzato per effettuare la chiamata, ad esempio `kubectl`.
  - API— I Kubernetes API richiamati `username` all'interno del cluster Amazon. EKS
  - ASNInformazioni: le ASN informazioni, ad esempio Organizzazione eISP, associate all'indirizzo IP dell'utente che effettua questa chiamata.

- Giorno della settimana: il giorno della settimana in cui è stata effettuata la API chiamata Kubernetes.
- Autorizzazione: il verbo e la risorsa Kubernetes di cui viene verificata l'accesso per indicare se possono utilizzare Kubernetes o meno. `username` API
- Nome dell'account di servizio: l'account di servizio associato al carico di lavoro Kubernetes che fornisce un'identità al carico di lavoro.
- Registro: il registro del contenitore associato all'immagine del contenitore che viene distribuito nel carico di lavoro Kubernetes.
- Immagine: l'immagine del contenitore, senza i tag e il digest associati, che viene distribuita nel carico di lavoro Kubernetes.
- Image Prefix Config: il prefisso dell'immagine con la configurazione di sicurezza del contenitore e del carico di lavoro abilitata, ad esempio `hostNetwork` `privileged` o, per il contenitore che utilizza l'immagine.
- Nome del soggetto: i soggetti, ad esempio a `usergroup`, o `serviceAccountName` che sono associati a un ruolo di riferimento in un o. `RoleBinding` `ClusterRoleBinding`
- Nome del ruolo: il nome del ruolo coinvolto nella creazione o nella modifica dei ruoli o di `roleBinding`API.

Anomalie basate sul volume S3

Questa sezione descrive in dettaglio le informazioni contestuali per le anomalie basate sul volume S3. Il volume-based finding (Exfiltration:S3/AnomalousBehavior) monitora il numero insolito di API chiamate S3 effettuate dagli utenti ai bucket S3, indicando una potenziale esfiltrazione di dati. Le seguenti chiamate S3 vengono monitorate per il rilevamento di anomalie basate sul volume. API

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Le seguenti metriche aiuterebbero a creare una linea di base del comportamento abituale quando un'entità accede a un bucket S3. IAM Per identificare un'eventuale esfiltrazione di dati, l'esito del rilevamento delle anomalie basato sul volume valuta tutte le attività rispetto alla consueta linea di base comportamentale. Scegli Comportamento storico nelle sezioni Comportamento insolito

(identità utente), Volume osservato (identità utente) e Volume osservato (Bucket) per visualizzare rispettivamente le metriche seguenti.

- Numero di `s3-api-name` API chiamate richiamate dall'IAMutente o dal IAM ruolo (dipende da quale sia stata emessa) associate al bucket S3 interessato nelle ultime 24 ore.
- Numero di `s3-api-name` API chiamate richiamate dall'IAMutente o dal IAM ruolo (dipende da quale sia stata emessa) associate a tutti i bucket S3 nelle ultime 24 ore.
- Numero di `s3-api-name` API chiamate tra tutti gli IAM utenti o i IAM ruoli (dipende da quale sia stato emesso) associate al bucket S3 interessato nelle ultime 24 ore.

RDSanomalie basate sull'attività di accesso

Questa sezione descrive in dettaglio il conteggio dei tentativi di accesso eseguiti dall'attore insolito ed è raggruppata in base al risultato dei tentativi di accesso. Tipi di esiti della Protezione RDS identifica comportamenti anomali monitorando gli eventi di accesso alla ricerca di schemi insoliti di `successfulLoginCount`, `failedLoginCount` e `incompleteConnectionCount`.

- successfulLoginCount— Questo contatore rappresenta la somma delle connessioni riuscite (combinazione corretta di attributi di accesso) effettuate all'istanza del database dall'attore insolito. Gli attributi di accesso includono nome utente, password e nome del database.
- failedLoginCount— Questo contatore rappresenta la somma dei tentativi di accesso falliti (non riusciti) effettuati per stabilire una connessione all'istanza del database. Ciò indica che uno o più attributi della combinazione di accesso, ad esempio nome utente, password o nome del database, erano errati.
- incompleteConnectionCount— Questo contatore rappresenta il numero di tentativi di connessione che non possono essere classificati come riusciti o falliti. Queste connessioni vengono chiuse prima che il database fornisca una risposta. Ad esempio, la scansione delle porte viene effettuata dove è connessa la porta del database, ma al database non viene inviata alcuna informazione oppure la connessione è stata interrotta prima del completamento di un tentativo di accesso riuscito o fallito.

GuardDuty trovare l'aggregazione

Tutti i risultati sono dinamici, il che significa che, se GuardDuty rileva una nuova attività correlata allo stesso problema di sicurezza, aggiornerà il risultato originale con le nuove informazioni, invece di generare un nuovo risultato. Questo comportamento consente di identificare i problemi in corso senza

dover esaminare più report simili e riduce il rumore complessivo causato da problemi di sicurezza di cui sei già a conoscenza.

Ad esempio, per un esito `UnauthorizedAccess:EC2/SSHBruteForce`, più tentativi di accesso contro l'istanza verranno aggregati allo stesso ID esito, aumentando il numero di conteggio nei dettagli dell'esito. Questo perché tale risultato rappresenta un unico problema di sicurezza: l'istanza indica che la SSH porta sull'istanza non è adeguatamente protetta contro questo tipo di attività. Tuttavia, se GuardDuty rileva un'attività di SSH accesso rivolta a una nuova istanza nell'ambiente in uso, creerà una nuova scoperta con un ID di ricerca univoco per avvisare l'utente del fatto che esiste un problema di sicurezza associato alla nuova risorsa.

Quando un esito viene aggregato, viene aggiornato con le informazioni relative all'ultima occorrenza di tale attività, il che significa che nell'esempio precedente se la tua istanza è la destinazione di un tentativo di forza bruta da un nuovo attore, i dettagli dell'esito verranno aggiornati per riflettere l'IP remoto dell'origine più recente e le precedenti informazioni saranno sostituite. Le informazioni complete sui singoli tentativi di attività saranno ancora disponibili nei tuoi log CloudTrail o in VPC Flow.

I criteri che avvisano GuardDuty di generare un nuovo risultato invece di aggregarne uno esistente dipendono dal tipo di risultato. I criteri di aggregazione per ogni tipo di ricerca sono determinati dai nostri tecnici di sicurezza per offrirti la migliore panoramica dei problemi di sicurezza distinti all'interno del tuo account.

Tipi di esiti

Per informazioni sulle modifiche importanti ai tipi di risultati, inclusi i tipi di GuardDuty risultati appena aggiunti o ritirati, vedere. Cronologia dei documenti per Amazon GuardDuty

Per informazioni sui tipi di esiti che sono stati ritirati, consulta Tipi di esiti ritirati.

GuardDuty Tipi di ricerca EC2

Gli esiti seguenti sono specifici per le risorse Amazon EC2 e hanno sempre un Tipo risorsa di `Instance`. La gravità e i dettagli degli esiti variano in base al ruolo risorsa, che indica se la risorsa EC2 è stata la destinazione di attività sospette o l'attore che le ha eseguite.

Gli esiti qui elencati includono le origini dati e i modelli utilizzati per generare quel tipo di esito. Per ulteriori informazioni sulle origini dati e sui modelli, consulta GuardDuty fonti di dati fondamentali.

> **Note**
>
> Per alcuni esiti EC2 potrebbero mancare i dettagli dell'istanza se quest'ultima è già stata terminata o se la chiamata API sottostante faceva parte di una chiamata API tra regioni originata da un'istanza EC2 in una regione diversa.

Per tutti gli esiti EC2, ti consigliamo di esaminare la risorsa in questione per determinare se si comporta nel modo previsto. Se l'attività è autorizzata, puoi utilizzare le regole di eliminazione o gli elenchi di indirizzi IP affidabili per prevenire notifiche false positive per quella risorsa. Se l'attività non è prevista, la best practice di sicurezza consiste nel presupporre che l'istanza sia stata compromessa e intraprendere le azioni dettagliate in Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Argomenti

- 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

Un'istanza EC2 esegue una query su un IP associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza elencata all'interno del tuo ambiente AWS esegue una query su un IP associato a un server di comando e controllo (C&C) noto. L'istanza elencata potrebbe essere compromessa. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è una raccolta di dispositivi connessi a Internet, come PC, server, dispositivi mobili e dispositivi Internet of Things, che sono infettati e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche inviare comandi per lanciare un attacco DDoS (Distributed Denial of Service).

> **Note**
>
> Se l'IP su cui viene eseguita una query è correlato a log4j, determinati campi dell'esito associato includeranno i valori seguenti:
>
> - Servizio. Informazioni aggiuntive. threatListName = Amazon
> - service.additionalInfo.threatName = Log4j Related

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Backdoor:EC2/C&CActivity.B!DNS

Un'istanza EC2 esegue una query su un nome di dominio associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio associato a un server di comando e controllo (C&C) noto. L'istanza elencata potrebbe essere compromessa. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è una raccolta di dispositivi connessi a Internet, come PC, server, dispositivi mobili e dispositivi Internet of Things, che sono infettati e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche inviare comandi per lanciare un attacco DDoS (Distributed Denial of Service).

> **Note**
>
> Se il nome di dominio su cui è stata eseguita la query è relativo a log4j, i campi dell'esito associato includeranno i valori seguenti:
>
> - Servizio. Informazioni aggiuntive. threatListName = Amazon
> - service.additionalInfo.threatName = Log4j Related

> **Note**
>
> Per verificare come GuardDuty genera questo tipo di risultato, puoi effettuare una richiesta DNS dalla tua istanza (utilizzando `dig` per Linux o `nslookup` per Windows) su un dominio `guarddutyc2activityb.com` di test.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Backdoor:EC2/DenialOfService.Dns

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo DNS.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico DNS in uscita. Ciò può indicare che l'istanza elencata è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo DNS.

> **Note**
>
> Questo risultato rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Backdoor:EC2/DenialOfService.Tcp

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo TCP.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico TCP in uscita. Ciò può indicare che l'istanza è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo TCP.

> **Note**
>
> Questo risultato rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Backdoor:EC2/DenialOfService.Udp

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo UDP.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico UDP in uscita. Ciò può indicare che l'istanza elencata è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo UDP.

> **Note**
>
> Questo risultato rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando il protocollo UDP sulla porta TCP.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata all'interno del tuo ambiente AWS genera un grande volume di traffico UDP in uscita indirizzato a una porta utilizzata di solito per le comunicazioni TCP. Ciò può indicare che l'istanza elencata è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando il protocollo UDP su una porta TCP.

> **Note**
>
> Questo risultato rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Backdoor:EC2/DenialOfService.UnusualProtocol

Un'istanza EC2 si sta comportando in un modo che potrebbe indicare che viene utilizzata per eseguire un attacco Denial of Service (DoS) utilizzando un protocollo insolito.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS genera un grande volume di traffico in uscita da un tipo di protocollo insolito che normalmente non è utilizzato dalle istanze EC2, ad esempio, l'Internet Group Management Protocol. Ciò può indicare che l'istanza è compromessa e viene utilizzata per eseguire attacchi denial-of-service (DoS) utilizzando un protocollo insolito. Questo risultato rileva attacchi DoS solo contro indirizzi IP instradabili pubblicamente, che sono gli obiettivi principali degli attacchi DoS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Backdoor:EC2/Spambot

Un'istanza EC2 presenta un comportamento insolito in quanto comunica con un host remoto sulla porta 25.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS comunica con un host remoto sulla porta 25. Questo comportamento è inusuale in quanto l'istanza EC2 non ha mai comunicato sulla porta 25 in precedenza. La porta 25 è tradizionalmente utilizzata dai server di posta per le comunicazioni SMTP. Questo risultato indica che l'istanza EC2 potrebbe essere compromessa per l'uso nell'invio di spam.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Behavior:EC2/NetworkPortUnusual

Un'istanza EC2 sta comunicando con un host remoto su una porta server inusuale.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. Questa istanza EC2 non ha mai comunicato su questa porta remota in precedenza.

> **Note**
>
> Se l'istanza EC2 ha comunicato sulla porta 389 o sulla porta 1389, la gravità dell'esito associata verrà modificata in "alta" e i campi dell'esito includeranno il valore seguente:
>
> - service.additionalInfo.context = Possible log4j callback

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Behavior:EC2/TrafficVolumeUnusual

Un'istanza EC2 sta generando un volume di traffico di rete insolitamente elevato verso un host remoto.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. L'istanza EC2 non ha mai inviato una tale quantità di traffico a questo host remoto in precedenza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

CryptoCurrency:EC2/BitcoinTool.B

Un'istanza EC2 sta eseguendo una query su un indirizzo IP associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue una query su un indirizzo IP associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Il Bitcoin è una criptovaluta e un sistema di pagamento digitale utilizzato in tutto il mondo che può essere scambiato con altre valute, prodotti e servizi. Il Bitcoin è una ricompensa per il mining di Bitcoin ed è molto ricercato dagli autori delle minacce.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 per estrarre o gestire criptovaluta o se questa istanza è altrimenti coinvolta nell'attività di blockchain, questo esito potrebbe essere un'attività prevista per il tuo ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `CryptoCurrency:EC2/BitcoinTool.B`. Il secondo criterio di filtro dovrebbe essere l'ID istanza dell'istanza coinvolta nell'attività di blockchain. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere Regole di eliminazione.

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

CryptoCurrency:EC2/BitcoinTool.B!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue una query su un nome di dominio associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Il Bitcoin è una criptovaluta e un sistema di pagamento digitale utilizzato in tutto il mondo che può essere scambiato

con altre valute, prodotti e servizi. Il Bitcoin è una ricompensa per il mining di Bitcoin ed è molto ricercato dagli autori delle minacce.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 per estrarre o gestire criptovaluta o se questa istanza è altrimenti coinvolta nell'attività di blockchain, questo esito potrebbe essere un'attività prevista per il tuo ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `CryptoCurrency:EC2/BitcoinTool.B!DNS`. Il secondo criterio di filtro dovrebbe essere l'ID istanza dell'istanza coinvolta nell'attività di blockchain. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere Regole di eliminazione.

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

DefenseEvasion:EC2/UnusualDNSResolver

Un'istanza Amazon EC2 comunica con un resolver DNS pubblico insolito.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza Amazon EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dal comportamento di base. L'istanza EC2 in questione non ha alcuna storia recente di comunicazioni con questo resolver DNS pubblico. Il campo Unusual nel pannello dei dettagli di ricerca della GuardDuty console può fornire informazioni sul resolver DNS richiesto.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

DefenseEvasion:EC2/UnusualDoHActivity

Un'istanza Amazon EC2 esegue una comunicazione DNS su HTTPS (DoH) insolita.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. L'istanza EC2 in questione non ha alcuna storia recente di comunicazioni DNS su HTTPS (DoH) con questo server DoH pubblico. Il campo Insolito nei dettagli degli esiti può fornire informazioni sul server DoH su cui è stata effettuata la query.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

DefenseEvasion:EC2/UnusualDoTActivity

Un'istanza Amazon EC2 esegue una comunicazione DNS su TLS (DoT) insolita.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS si comporta in un modo che differisce dalla linea di base stabilita. L'istanza EC2 in questione non ha alcuna storia recente di comunicazioni DNS su TLS (DoT) con questo server DoT pubblico. Il campo Insolito nel pannello dei dettagli dell'esito può fornire informazioni sul server DoT su cui è stata effettuata la query.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Impact:EC2/AbusedDomainRequest.Reputation

Un'istanza EC2 esegue una query su un nome di dominio a bassa reputazione associato a domini noti in abuso.

Gravità predefinita: media

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione associato a domini o indirizzi IP noti in abuso. Esempi di domini in abuso sono i nomi di dominio di primo livello (TLD) e i nomi di dominio di secondo livello (2LD) che offrono registrazioni gratuite di sottodomini e provider DNS dinamici. Gli autori delle minacce tendono a utilizzare questi servizi per registrare domini gratuitamente o a basso costo. I domini a bassa reputazione di questa categoria possono anche essere domini scaduti che vengono sostituiti con l'indirizzo IP di parcheggio di un registrar e quindi potrebbero non essere più attivi. Un IP di parcheggio è il luogo in cui un registrar indirizza il traffico verso domini che non sono stati collegati ad alcun servizio. L'istanza Amazon EC2 elencata potrebbe essere compromessa poiché gli autori delle minacce utilizzano comunemente questi registrar o servizi per la distribuzione di malware e C&C.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Impact:EC2/BitcoinDomainRequest.Reputation

Un'istanza EC2 esegue una query su un nome di dominio a bassa reputazione associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Il Bitcoin è una criptovaluta e un sistema di pagamento digitale utilizzato in tutto il mondo che può essere scambiato con altre valute, prodotti e servizi. Il Bitcoin è una ricompensa per il mining di Bitcoin ed è molto ricercato dagli autori delle minacce.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se utilizzi questa istanza EC2 per estrarre o gestire criptovaluta o se questa istanza è altrimenti coinvolta nell'attività di blockchain, questo esito potrebbe rappresentare un'attività prevista per il tuo ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `Impact:EC2/BitcoinDomainRequest.Reputation`. Il secondo criterio di filtro dovrebbe essere l'ID istanza dell'istanza coinvolta nell'attività di blockchain. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere Regole di eliminazione.

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Impact:EC2/MaliciousDomainRequest.Reputation

Un'istanza EC2 esegue una query su un dominio a bassa reputazione associato a domini dannosi noti.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata all'interno del tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione associato a domini o indirizzi IP dannosi noti. Ad esempio, i domini possono essere associati a un indirizzo IP sinkhole noto. I domini sinkhole sono domini che sono stati precedentemente controllati da un autore di minacce e se vengono inoltrate richieste a questi domini può significare che l'istanza è compromessa. Questi domini possono anche essere correlati a campagne dannose note o algoritmi di generazione di domini.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Impact:EC2/PortSweep

Su un gran numero di indirizzi IP è in corso il probing di una porta da parte di un'istanza EC2.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS effettua il probing di una porta su un gran numero di indirizzi IP instradabili pubblicamente. Questo tipo di attività viene in genere utilizzato per trovare host vulnerabili da sfruttare. Nel pannello dei dettagli di ricerca della GuardDuty console, viene visualizzato solo l'indirizzo IP remoto più recente

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Impact:EC2/SuspiciousDomainRequest.Reputation

Un'istanza EC2 esegue una query su un nome di dominio a bassa reputazione di natura sospetta a causa della sua età o della scarsa popolarità.

Gravità predefinita: bassa

- Origine dati: log DNS

Questo esito segnala che l'istanza Amazon EC2 elencata nel tuo ambiente AWS esegue una query su un nome di dominio a bassa reputazione sospettato di essere dannoso. Abbiamo notato che le caratteristiche di questo dominio sono coerenti con i domini dannosi osservati in precedenza, ma il nostro modello di reputazione non è stato in grado di collegarlo in modo definitivo a una minaccia nota. Questi domini vengono in genere osservati per la prima volta o ricevono una quantità di traffico ridotta.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Impact:EC2/WinRMBruteForce

Un'istanza EC2 esegue un attacco di forza bruta di Windows Remote Management in uscita.

Gravità predefinita: bassa*

> **Note**
>
> La gravità di questo esito è bassa se l'istanza EC2 era la destinazione di un attacco di forza bruta. La gravità di questo esito è alta se l'istanza EC2 è l'attore viene utilizzato per eseguire l'attacco di forza bruta.

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue un attacco di forza bruta di Windows Remote Management (WinRM) volto a ottenere l'accesso al servizio Windows Remote Management su sistemi basati su Windows.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Recon:EC2/PortProbeEMRUnprotectedPort

Una porta non protetta EMR di un'istanza EC2 è sottoposta a probing da parte di un host dannoso noto.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo risultato indica che una porta sensibile relativa all'EMR sull'istanza EC2 elencata che fa parte di un cluster nel AWS tuo ambiente non è bloccata da un gruppo di sicurezza, da una lista di controllo degli accessi (ACL) o da un firewall on-host come Linux IPTables. Questa scoperta indica inoltre che scanner noti su Internet stanno sondando attivamente questa porta. Le porte che possono attivare questo esito, ad esempio la porta 8088 (porta dell'interfaccia utente Web YARN), potrebbero potenzialmente essere utilizzate per l'esecuzione di codice in modalità remota.

Raccomandazioni per la correzione:

Ti consigliamo di bloccare l'accesso aperto alle porte su cluster da Internet e limitare l'accesso solo a indirizzi IP specifici che richiedono l'accesso a queste porte. Per ulteriori informazioni, consultare Gruppi di sicurezza per cluster EMR.

Recon:EC2/PortProbeUnprotectedPort

Una porta non protetta di un'istanza EC2 è sottoposta a probing da parte di un host dannoso noto.

Gravità predefinita: bassa*

> **Note**
>
> La gravità predefinita di questi esiti è bassa. Tuttavia, se la porta che viene esaminata viene utilizzata da Elasticsearch (9200 o 9300), la gravità del risultato è elevata.

- Origine dati: log di flusso VPC

Questo esito segnala che una porta sull'istanza EC2 elencata nel tuo ambiente AWS non è bloccata da un gruppo di sicurezza, una lista di controllo degli accessi (ACL) o un firewall su host, ad esempio, Linux IPTables, e che è sottoposta attivamente a probing da parte di scanner noti.

Se la porta non protetta identificata è 22 o 3389 e si utilizzano queste porte per connettersi all'istanza, è comunque possibile limitare l'esposizione consentendo l'accesso a queste porte solo agli indirizzi

IP dello spazio degli indirizzi IP della rete aziendale. Per limitare l'accesso alla porta 22 su Linux, consulta Authorizing Inbound Traffic for Your Linux Instance. Per limitare l'accesso alla porta 3389 su Windows, consulta Authorizing Inbound Traffic for Your Windows Instances.

GuardDuty non genera questo risultato per le porte 443 e 80.

Raccomandazioni per la correzione:

Tuttavia, ci possono essere casi in cui le istanze sono intenzionalmente esposte, ad esempio se ospitano server web. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `Recon:EC2/PortProbeUnprotectedPort`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da bastion host. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. Per ulteriori informazioni sulla creazione di regole di eliminazione, consulta Regole di eliminazione.

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Recon:EC2/Portscan

Un'istanza EC2 sta eseguendo la scansione delle porte in uscita verso un host remoto.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS è coinvolta in un possibile attacco port scan in quanto sta effettuando più tentativi di connessione a diverse porte in un breve periodo di tempo. Lo scopo di un attacco port scan è di individuare le porte aperte per determinare quali servizi sono in esecuzione sulla macchina e per identificarne il sistema operativo.

Raccomandazioni per la correzione:

Questo esito può essere un falso positivo se nel tuo ambiente vengono implementate applicazioni di valutazione della vulnerabilità su istanze EC2. Queste applicazioni, infatti, eseguono scansioni

delle porte per avvisarti in caso di porte aperte configurate in modo errato. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `Recon:EC2/Portscan`. Il secondo criterio di filtro dovrebbe corrispondere all'istanza o alle istanze che ospitano questi strumenti di valutazione della vulnerabilità. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda dei criteri identificabili con le istanze che ospitano questi strumenti. Per ulteriori informazioni sulla creazione di regole di eliminazione, consulta Regole di eliminazione.

Se questa attività non è prevista, è probabile che l'istanza sia compromessa, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Trojan:EC2/BlackholeTraffic

Un'istanza EC2 sta tentando di comunicare con un indirizzo IP di un host remoto che è un noto buco nero.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che l'istanza EC2 nel tuo ambiente AWS potrebbe essere compromessa in quanto tenta di comunicare con l'indirizzo IP di un buco nero (o sinkhole). I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario. L'indirizzo IP di un buco nero designa un computer host non in esecuzione o un indirizzo a cui non è stato assegnato alcun host.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Trojan:EC2/BlackholeTraffic!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio che è reindirizzato a un indirizzo IP di un buco nero.

Gravità predefinita: media

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS potrebbe essere compromessa in quanto esegue una query su un nome di dominio che è reindirizzato all'indirizzo IP di un buco nero. I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Trojan:EC2/DGADomainRequest.B

Un'istanza EC2 sta eseguendo una query su domini generati da algoritmi. Tali domini sono in genere utilizzati da malware e potrebbero essere un'indicazione di un'istanza EC2 compromessa.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 nel tuo ambiente AWS tenta di eseguire una query su domini DGA. L'istanza EC2 potrebbe essere compromessa.

I DGA sono utilizzati periodicamente per generare un gran numero di nomi di dominio che possono essere utilizzati come punti di incontro con i relativi server di comando e controllo (C&C). I server di comando e controllo sono computer che inviano comandi a membri di una botnet, ovvero una raccolta di dispositivi connessi a Internet infettati e controllati da un tipo comune di malware. Il numero elevato di punti di rendez-vous potenziali rende difficile l'arresto delle botnet in quanto i computer infettati tentano di contattare quotidianamente alcuni di questi nomi di dominio per ricevere aggiornamenti o comandi.

> **Note**
>
> L'esito è basato sull'analisi dei nomi di dominio tramite un'euristica avanzata e può quindi identificare nuovi domini DGA che non sono presenti nei feed di intelligence sulle minacce.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Trojan:EC2/DGADomainRequest.C!DNS

Un'istanza EC2 sta eseguendo una query su domini generati da algoritmi. Tali domini sono in genere utilizzati da malware e potrebbero essere un'indicazione di un'istanza EC2 compromessa.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 nel tuo ambiente AWS tenta di eseguire una query su domini DGA. L'istanza EC2 potrebbe essere compromessa.

I DGA sono utilizzati periodicamente per generare un gran numero di nomi di dominio che possono essere utilizzati come punti di incontro con i relativi server di comando e controllo (C&C). I server di comando e controllo sono computer che inviano comandi a membri di una botnet, ovvero una raccolta di dispositivi connessi a Internet infettati e controllati da un tipo comune di malware. Il numero elevato di punti di rendez-vous potenziali rende difficile l'arresto delle botnet in quanto i computer infettati tentano di contattare quotidianamente alcuni di questi nomi di dominio per ricevere aggiornamenti o comandi.

> **Note**
>
> Questo risultato si basa su domini DGA noti tratti dai feed GuardDuty di intelligence sulle minacce.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Trojan:EC2/DNSDataExfiltration

Un'istanza EC2 sta eseguendo l'esfiltrazione di dati tramite query DNS.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS esegue un malware che utilizza query DNS per trasferire dati in uscita. Questo tipo di trasferimento di dati è indicativo di un'istanza compromessa e potrebbe comportare l'esfiltrazione di dati. Di solito, il traffico DNS non è bloccato dai firewall. Ad esempio, il malware in un'istanza EC2 compromessa può codificare i dati (ad esempio i numeri di carte di credito) in una query DNS e inviarli a un server DNS remoto controllato da un utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Trojan:EC2/DriveBySourceTraffic!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio di un host remoto che è l'origine nota di attacchi di download drive-by.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che l'istanza EC2 elencata nel tuo ambiente AWS potrebbe essere compromessa in quanto esegue una query su un nome di dominio di un host remoto che è un'origine nota di attacchi di download drive-by. Si tratta di download di software non voluti da Internet che possono attivare l'installazione automatica di virus, spyware o malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Trojan:EC2/DropPoint

Un'istanza EC2 sta tentando di comunicare con un indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS tenta di comunicare con l'indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Trojan:EC2/DropPoint!DNS

Un'istanza EC2 sta eseguendo una query su un nome di dominio di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Origine dati: log DNS

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS esegue una query su un nome di dominio di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Trojan:EC2/PhishingDomainRequest!DNS

Un'istanza EC2 sta eseguendo una query su domini implicati in attacchi di phishing. L'istanza EC2 potrebbe essere compromessa.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che nel tuo ambiente AWS è presente un'istanza EC2 che tenta di eseguire una query su un dominio implicato in attacchi di phishing. I domini di phishing sono configurati da individui che fingono di essere un'istituzione legittima allo scopo di indurre gli utenti a fornire dati sensibili come informazioni personali, coordinate bancarie, informazioni di carte di credito e password. L'istanza EC2 potrebbe tentare di recuperare dati sensibili archiviati su un sito Web di phishing oppure di configurare un sito Web di phishing. L'istanza EC2 potrebbe essere compromessa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Un'istanza EC2 stabilisce connessioni a un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: media

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS comunica con un indirizzo IP incluso in un elenco minacce che hai caricato. In GuardDuty, un elenco di minacce è costituito da indirizzi IP dannosi noti. GuardDuty genera i risultati in base agli elenchi di minacce caricati. L'elenco delle minacce utilizzato per generare questo risultato verrà elencato nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

UnauthorizedAccess:EC2/MetadataDNSRebind

Un'istanza EC2 esegue ricerche DNS che vengono risolte nel servizio di metadati dell'istanza.

Gravità predefinita: alta

- Origine dati: log DNS

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS esegue una query su un dominio che restituisce l'indirizzo IP dei metadati EC2 (169.254.169.254). Una query DNS di questo tipo può indicare che l'istanza è la destinazione di una tecnica di rebinding DNS. Questa tecnica può essere utilizzata per ottenere metadati da un'istanza EC2, incluse le credenziali IAM a essa associate.

Il rebinding DNS implica l'inganno di un'applicazione in esecuzione sull'istanza EC2 per caricare i dati restituiti da un URL, dove il nome di dominio nell'URL si risolve nell'indirizzo IP dei metadati EC2 (169.254.169.254). In questo modo l'applicazione accede ai metadati EC2 e, possibilmente, li rende disponibili all'utente malintenzionato.

Puoi accedere ai metadati EC2 utilizzando il rebinding DNS solo se l'istanza EC2 esegue un'applicazione vulnerabile che consente l'iniezione di URL oppure se qualcuno accede all'URL in un browser Web in esecuzione sull'istanza EC2.

Raccomandazioni per la correzione:

In risposta a questo esito, devi valutare se è presente un'applicazione vulnerabile in esecuzione sull'istanza EC2 o se qualcuno ha utilizzato un browser per accedere al dominio identificato nell'esito. Se la causa principale è un'applicazione vulnerabile, è necessario correggere la vulnerabilità. Se qualcuno ha navigato nel dominio identificato, è necessario bloccare il dominio o impedire agli utenti di accedervi. Se ritieni che l'esito sia correlato a uno dei due casi precedenti, revoca la sessione associata all'istanza EC2.

Alcuni clienti AWS mappano intenzionalmente l'indirizzo IP dei metadati a un nome di dominio sui server DNS autorevoli. Se questo è il caso del tuo ambiente , ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `UnauthorizedAccess:EC2/MetaDataDNSRebind`. Il secondo criterio di filtro deve essere il dominio di richiesta DNS e il valore deve corrispondere al dominio mappato all'indirizzo IP dei

metadati (169.254.169.254). Per ulteriori informazioni sulla creazione di regole di soppressione, vedere Regole di eliminazione.

UnauthorizedAccess:EC2/RDPBruteForce

Un'istanza EC2 è stata implicata in attacchi forza bruta RDP.

Gravità predefinita: bassa*

> **Note**
>
> La gravità di questo esito è bassa se l'istanza EC2 era la destinazione di un attacco di forza bruta. La gravità di questo esito è alta se l'istanza EC2 è l'attore viene utilizzato per eseguire l'attacco di forza bruta.

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS è stata coinvolta in un attacco forza bruta che mirava a ottenere le password dei servizi RDP su sistemi basati su Windows. Ciò può indicare un accesso non autorizzato alle risorse AWS.

Raccomandazioni per la correzione:

Se il Ruolo risorsa dell'istanza è `ACTOR`, significa che l'istanza è stata utilizzata per eseguire gli attacchi di forza bruta RDP. A meno che questa istanza non abbia un motivo legittimo per contattare l'indirizzo IP elencato come `Target`, ti consigliamo di presumere che l'istanza sia stata compromessa e di intraprendere le azioni elencate in Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Se il Ruolo risorsa dell'istanza è `TARGET`, questo esito può essere risolto proteggendo la porta RDP, consentendo l'accesso solo agli IP affidabili tramite gruppi di sicurezza, ACL o firewall. Per ulteriori informazioni, consulta Suggerimenti per la protezione delle istanze EC2 (Linux).

UnauthorizedAccess:EC2/SSHBruteForce

Un'istanza EC2 è stata implicata in attacchi forza bruta SSH.

Gravità predefinita: bassa*

> **Note**
>
> La gravità di questo esito è bassa se un attacco di forza bruta è rivolto a una delle istanze EC2. La gravità di questo esito è alta se l'istanza EC2 viene utilizzata per eseguire l'attacco di forza bruta.

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS è stata coinvolta in un attacco forza bruta che mirava a ottenere le password dei servizi SSH su sistemi basati su Linux. Ciò può indicare un accesso non autorizzato alle risorse AWS.

> **Note**
>
> Questo risultato viene generato solo dal monitoraggio del traffico di sulla porta 22. Se i servizi SSH sono configurati per utilizzare altre porte, questo risultato non viene generato.

Raccomandazioni per la correzione:

Se la destinazione del tentativo di attacco forza bruta è un host bastione, questo comportamento potrebbe essere previsto per l'ambiente AWS. In questo caso, si consiglia di impostare una regola di eliminazione per questa individuazione. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `UnauthorizedAccess:EC2/SSHBruteForce`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da bastion host. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. Per ulteriori informazioni sulla creazione di regole di eliminazione, consulta Regole di eliminazione.

Se questa attività non è prevista per il tuo ambiente e il Ruolo risorsa dell'istanza è `TARGET`, questo esito può essere risolto proteggendo la porta SSH, consentendo l'accesso solo a IP affidabili tramite gruppi di sicurezza, ACL o firewall. Per ulteriori informazioni, consulta Suggerimenti per la protezione delle istanze EC2 (Linux).

Se il Ruolo risorsa dell'istanza è `ACTOR`, questo indica che l'istanza è stata utilizzata per eseguire gli attacchi di forza bruta SSH. A meno che questa istanza non abbia un motivo legittimo per contattare l'indirizzo IP elencato come `Target`, ti consigliamo di presumere che l'istanza sia stata compromessa e di intraprendere le azioni elencate in Correzione di un'istanza Amazon potenzialmente compromessa EC2.

UnauthorizedAccess:EC2/TorClient

L'istanza EC2 sta stabilendo connessioni a un Tor Guard o a un nodo Authority.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS stabilisce connessioni a un Tor Guard o a un nodo Authority. Tor è un software che consente la comunicazione anonima. I Tor Guard e i nodi fungono da gateway iniziali per una rete Tor. Questo traffico può indicare che l'istanza EC2 è stata compromessa e funge da client su una rete Tor. L'esito potrebbe indicare un accesso non autorizzato alle risorse AWS con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

UnauthorizedAccess:EC2/TorRelay

L'istanza EC2 sta stabilendo connessioni a una rete Tor come relay Tor.

Gravità predefinita: alta

- Origine dati: log di flusso VPC

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS stabilisce connessioni a una rete Tor in un modo che suggerisce che funga da relè Tor. Tor è un software che consente la comunicazione anonima. Tor aumenta l'anonimato della comunicazione inoltrando il traffico potenzialmente illecito del client da un relè Tor a un altro.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

GuardDuty IAMtipi di ricerca

I seguenti risultati sono specifici per le IAM entità e le chiavi di accesso e hanno sempre un tipo di risorsa pari a. `AccessKey` La gravità e i dettagli degli esiti variano in base al tipo di esito.

Gli esiti qui elencati includono le origini dati e i modelli utilizzati per generare quel tipo di esito. Per ulteriori informazioni, consulta GuardDuty fonti di dati fondamentali.

Per tutti i risultati IAM correlati, ti consigliamo di esaminare l'entità in questione e assicurarti che le relative autorizzazioni seguano la migliore pratica del privilegio minimo. Se l'attività non è prevista, le credenziali potrebbero essere compromesse. Per informazioni su come correggere gli esiti, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Argomenti

- 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

Un utente API per accedere a un AWS ambiente è stato richiamato in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che è stata rilevata una API richiesta anomala nel tuo account. Questo risultato può includere una API o una serie di API richieste correlate effettuate in prossimità di un'unica identità utente. L'APIosservazione è comunemente associata alla fase di accesso alle credenziali di un attacco, quando un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per l'ambiente in uso. APIsIn questa categoria ci sono,, e. `GetPasswordData` `GetSecretValue` `BatchGetSecretValue` `GenerateDbAuthToken`

Questa API richiesta è stata identificata come anomala dal modello ML (Anomaly GuardDuty Detection Machine Learning) di Anomaly Detection. Il modello ML valuta tutte le API richieste nell'account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello ML tiene traccia di vari fattori della API richiesta, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e lo specifico richiesto. API I dettagli su quali fattori della API richiesta sono insoliti per l'identità dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

DefenseEvasion:IAMUser/AnomalousBehavior

Un dispositivo API usato per eludere le misure difensive è stato invocato in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che è stata rilevata una API richiesta anomala nel tuo account. Questo risultato può includere una API o una serie di API richieste correlate effettuate in prossimità di un'unica identità utente. L'APIosservazione è comunemente associata a tattiche di evasione difensiva in cui un avversario cerca di coprire le proprie tracce ed evitare di essere scoperto. APIsin questa categoria si trovano in genere operazioni di eliminazione, disabilitazione o interruzione, come, o. `DeleteFlowLogs` `DisableAlarmActions` `StopLogging`

Questa API richiesta è stata identificata come anomala dal modello GuardDuty di machine learning (ML) per il rilevamento delle anomalie. Il modello ML valuta tutte le API richieste nell'account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello ML tiene traccia di vari fattori della API richiesta, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e lo specifico richiesto. API I dettagli su quali fattori della API richiesta sono insoliti per l'identità dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Discovery:IAMUser/AnomalousBehavior

Un comando API comunemente usato per scoprire risorse è stato invocato in modo anomalo.

Gravità predefinita: bassa

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che è stata rilevata una API richiesta anomala nel tuo account. Questo risultato può includere una API o una serie di API richieste correlate effettuate in prossimità di un'unica identità utente. L'APIosservazione è generalmente associata alla fase di scoperta di un attacco, quando un avversario raccoglie informazioni per determinare se l' AWS ambiente è suscettibile a un attacco più ampio. APIsin questa categoria rientrano in genere le operazioni di recupero, descrizione o elenco, ad esempio, `DescribeInstances` o. `GetRolePolicy` `ListAccessKeys`

Questa API richiesta è stata identificata come anomala dal modello ML (Anomaly GuardDuty Detection Machine Learning) di Anomaly Detection. Il modello ML valuta tutte le API richieste nell'account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello ML tiene traccia di vari fattori della API richiesta, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e lo specifico richiesto. API I dettagli su quali fattori della API richiesta sono insoliti per l'identità dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Exfiltration:IAMUser/AnomalousBehavior

Un API comando comunemente usato per raccogliere dati da un AWS ambiente è stato richiamato in modo anomalo.

Gravità predefinita: alta

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che è stata rilevata una API richiesta anomala nel tuo account. Questo risultato può includere una API o una serie di API richieste correlate effettuate in prossimità di un'unica identità utente. Quanto API osservato è comunemente associato a tattiche di esfiltrazione in cui un avversario tenta di raccogliere dati dalla rete utilizzando pacchetti e crittografia per evitare il rilevamento. APIsper questo tipo di risultato si tratta solo di operazioni di gestione (piano di controllo) e sono in genere correlate a S3, alle istantanee e ai database, come,, o. `PutBucketReplication` `CreateSnapshot` `RestoreDBInstanceFromDBSnapshot`

Questa API richiesta è stata identificata come anomala dal modello di machine learning (ML) GuardDuty di anomaly detection. Il modello ML valuta tutte le API richieste nell'account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello ML tiene traccia di vari fattori della API richiesta, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e lo specifico richiesto. API I dettagli su quali fattori della API richiesta sono insoliti per l'identità dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Impact:IAMUser/AnomalousBehavior

Un comando API comunemente usato per manomettere dati o processi in un AWS ambiente è stato invocato in modo anomalo.

Gravità predefinita: alta

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che è stata rilevata una API richiesta anomala nel tuo account. Questo risultato può includere una API o una serie di API richieste correlate effettuate in prossimità di un'unica identità utente. Quanto API osservato è comunemente associato a tattiche di impatto in cui un avversario cerca di interrompere le operazioni e manipolare, interrompere o distruggere i dati del tuo account. APIsper questo tipo di risultato sono in genere operazioni di eliminazione, aggiornamento o invio, come, o. `DeleteSecurityGroup` `UpdateUser` `PutBucketPolicy`

Questa API richiesta è stata identificata come anomala dal modello GuardDuty di machine learning (ML) per il rilevamento delle anomalie. Il modello ML valuta tutte le API richieste nell'account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello ML tiene traccia di vari fattori della API richiesta, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e lo specifico richiesto. API I dettagli su quali fattori della API richiesta sono insoliti per l'identità dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

InitialAccess:IAMUser/AnomalousBehavior

Un comando API comunemente usato per ottenere l'accesso non autorizzato a un AWS ambiente è stato invocato in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che è stata rilevata una API richiesta anomala nel tuo account. Questo risultato può includere una API o una serie di API richieste correlate effettuate in prossimità di un'unica identità utente. Quanto API osservato è comunemente associato alla fase di accesso iniziale di un attacco, quando un avversario tenta di stabilire l'accesso all'ambiente dell'utente. APIsin questa categoria rientrano in genere operazioni get token o di sessione, come,`GetFederationToken`, `StartSession` o. `GetAuthorizationToken`

Questa API richiesta è stata identificata come anomala dal modello GuardDuty di machine learning (ML) per il rilevamento delle anomalie. Il modello ML valuta tutte le API richieste nell'account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello ML tiene traccia di vari fattori della API richiesta, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e lo specifico richiesto. API I dettagli su quali fattori della API richiesta sono insoliti per l'identità dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

PenTest:IAMUser/KaliLinux

An API è stato richiamato da una macchina Kali Linux.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che una macchina che esegue Kali Linux sta effettuando API chiamate utilizzando credenziali che appartengono all' AWS account elencato nel tuo ambiente. Kali Linux è un popolare strumento di test di penetrazione che i professionisti della sicurezza utilizzano per identificare i punti deboli nei casi che richiedono l'applicazione di patch. EC2 Gli aggressori utilizzano questo strumento anche per trovare punti deboli di EC2 configurazione e ottenere l'accesso non autorizzato all'ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

PenTest:IAMUser/ParrotLinux

An API è stato richiamato da una macchina Parrot Security Linux.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta indica che una macchina che esegue Parrot Security Linux sta effettuando API chiamate utilizzando credenziali che appartengono all' AWS account elencato nell'ambiente in uso. Parrot Security Linux è un popolare strumento di test di penetrazione che i professionisti della sicurezza utilizzano per identificare i punti deboli nelle istanze che richiedono l'applicazione di patch. EC2 Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della EC2 configurazione e ottenere l'accesso non autorizzato all'ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

PenTest:IAMUser/PentooLinux

An API è stato richiamato da una macchina Pentoo Linux.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che una macchina che esegue Pentoo Linux sta effettuando API chiamate utilizzando credenziali che appartengono all' AWS account elencato nel tuo ambiente. Pentoo Linux è un popolare strumento di test di penetrazione che i professionisti della sicurezza utilizzano per identificare i punti deboli nei casi che richiedono l'applicazione di patch. EC2 Gli aggressori utilizzano questo strumento anche per trovare punti deboli di EC2 configurazione e ottenere l'accesso non autorizzato all'ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Persistence:IAMUser/AnomalousBehavior

Uno strumento API comunemente usato per mantenere l'accesso non autorizzato a un AWS ambiente è stato invocato in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: evento di gestione CloudTrail

Questa scoperta ti informa che è stata rilevata una API richiesta anomala nel tuo account. Questo risultato può includere una API o una serie di API richieste correlate effettuate in prossimità di un'unica identità utente. L'APIosservazione è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso all'ambiente dell'utente e sta tentando di mantenere tale accesso. APIsin questa categoria rientrano in genere operazioni di creazione, importazione o modifica, come, o. `CreateAccessKey` `ImportKeyPair` `ModifyInstanceAttribute`

Questa API richiesta è stata identificata come anomala dal modello ML (Anomaly GuardDuty Detection Machine Learning) di Anomaly Detection. Il modello ML valuta tutte le API richieste nell'account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello ML tiene traccia di vari fattori della API richiesta, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e lo specifico richiesto. API I dettagli su quali fattori della API richiesta sono insoliti per l'identità dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Policy:IAMUser/RootCredentialUsage

An API è stato richiamato utilizzando le credenziali di accesso dell'utente root.

Gravità predefinita: bassa

- Fonte dati: eventi di CloudTrail gestione o eventi relativi ai dati CloudTrail

Questo esito segnala che le credenziali di accesso dell'utente root dell' Account AWS elencato nel tuo ambiente vengono utilizzate per effettuare richieste ai servizi AWS . Si consiglia agli utenti di non utilizzare mai le credenziali di accesso dell'utente root per accedere ai servizi AWS . È invece necessario accedere AWS ai servizi utilizzando le credenziali temporanee con privilegi minimi di (). AWS Security Token Service STS Per le situazioni in cui non AWS STS è supportata, si consigliano le credenziali IAM utente. Per ulteriori informazioni, consulta IAMBest Practices.

> **Note**
>
> Se il rilevamento delle minacce di S3 è abilitato per l'account, questo esito può essere generato in risposta ai tentativi di eseguire operazioni del piano dati S3 sulle risorse S3 utilizzando le credenziali di accesso dell'utente root di Account AWS. La API chiamata utilizzata verrà elencata nei dettagli del risultato. Se il rilevamento delle minacce S3 non è abilitato, questo risultato può essere attivato solo dal registro eventi. APIs Per maggiori informazioni sul rilevamento delle minacce di S3, consulta Protezione S3.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

PrivilegeEscalation:IAMUser/AnomalousBehavior

Un comando API comunemente usato per ottenere autorizzazioni di alto livello per un AWS ambiente è stato richiamato in modo anomalo.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questa scoperta ti informa che è stata rilevata una API richiesta anomala nel tuo account. Questo risultato può includere una API o una serie di API richieste correlate effettuate in prossimità di un'unica identità utente. L'APIosservazione è comunemente associata a tattiche di escalation dei privilegi in cui un avversario tenta di ottenere autorizzazioni di livello superiore per un ambiente. APIsin questa categoria si tratta in genere di operazioni che modificano le IAM politiche, i ruoli e gli utenti, ad esempio, o. `AssociateIamInstanceProfile` `AddUserToGroup` `PutUserPolicy`

Questa API richiesta è stata identificata come anomala dal modello GuardDuty di machine learning (ML) per il rilevamento delle anomalie. Il modello ML valuta tutte le API richieste nell'account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello ML tiene traccia di vari fattori della API richiesta, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e lo specifico richiesto. API I dettagli su quali fattori della API richiesta sono insoliti per l'identità dell'utente che ha richiamato la richiesta sono disponibili nei dettagli del risultato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/MaliciousIPCaller

An API è stato richiamato da un indirizzo IP malevolo noto.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta indica che un'APIoperazione in grado di elencare o descrivere AWS le risorse in un account all'interno dell'ambiente è stata richiamata da un indirizzo IP incluso in un elenco di minacce. Un utente malintenzionato può utilizzare credenziali rubate per eseguire questo tipo di ricognizione delle AWS risorse dell'utente al fine di trovare credenziali più preziose o determinare le funzionalità delle credenziali di cui già dispone.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/MaliciousIPCaller.Custom

An è API stato richiamato da un indirizzo IP malevolo noto.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta indica che un'APIoperazione in grado di elencare o descrivere AWS le risorse in un account all'interno dell'ambiente è stata richiamata da un indirizzo IP incluso in un elenco di minacce personalizzato. L'elenco delle minacce utilizzato sarà elencato nei dettagli del risultato. Un utente malintenzionato potrebbe utilizzare credenziali rubate per eseguire questo tipo di ricognizione delle AWS risorse dell'utente al fine di trovare credenziali più preziose o determinare le funzionalità delle credenziali già in suo possesso.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/TorIPCaller

Un API è stato richiamato da un indirizzo IP del nodo di uscita Tor.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta ti informa che un'APIoperazione in grado di elencare o descrivere AWS le risorse in un account all'interno del tuo ambiente è stata richiamata da un indirizzo IP del nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Un utente malintenzionato può usare Tor per mascherare la propria identità.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail la registrazione è stata disabilitata.

Gravità predefinita: bassa

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta indica che una CloudTrail traccia all'interno AWS dell'ambiente in uso è stata disattivata. Può trattarsi di un tentativo di un utente malintenzionato di disabilitare la registrazione per eliminare le tracce della sua attività accedendo nel contempo alle risorse AWS per scopi dannosi. Questo risultato può essere generato dall'eliminazione o dall'aggiornamento riuscito di un trail Questo risultato può essere innescato anche dall'eliminazione riuscita di un bucket S3 che memorizza i log di un trail associato a. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Stealth:IAMUser/PasswordPolicyChange

La policy delle password dell'account è stata indebolita.

Gravità predefinita: bassa*

> **Note**
>
> La gravità di questo esito può essere bassa, media o alta a seconda della gravità delle modifiche apportate alla policy delle password.

- Fonte dei dati: eventi di gestione CloudTrail

La politica relativa alle password degli AWS account è stata indebolita nell'account elencato nell' AWS ambiente in uso. Ad esempio, è stata eliminata o aggiornata per richiedere un numero minore di caratteri, non richiedere simboli e numeri o per prolungare l'estensione del periodo di scadenza delle password. Questo risultato può essere causato anche dal tentativo di aggiornare o eliminare la politica relativa alle password AWS dell'account. La politica sulle password degli AWS account definisce le regole che regolano i tipi di password che possono essere impostati per gli utenti. IAM Un policy delle password indebolita consente la creazione di password facili da ricordare e potenzialmente più facili da indovinare, creando di fatto un rischio per la sicurezza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Molteplici connessioni riuscite alla console sono state osservate in tutto il mondo.

Gravità predefinita: media

- Fonte dei dati: eventi di gestione CloudTrail

Questo risultato indica che più accessi riusciti alla console per lo stesso IAM utente sono stati rilevati più o meno nello stesso periodo in diverse aree geografiche. Questi modelli di posizione di accesso anomali e rischiosi indicano un potenziale accesso non autorizzato alle risorse dell'utente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Le credenziali create esclusivamente per un'EC2istanza tramite un ruolo di avvio dell'istanza vengono utilizzate da un altro account all'interno. AWS

Gravità predefinita: alta*

> **Note**
>
> La gravità predefinita di questi esiti è alta. Tuttavia, se API è stato richiamato da un account affiliato al tuo AWS ambiente, la gravità è Media.

- Fonte dei dati: eventi di CloudTrail gestione o eventi relativi ai dati S3

Questo risultato indica quando le credenziali dell'EC2istanza vengono utilizzate per richiamare l'istanza APIs da un indirizzo IP di proprietà di un AWS account diverso da quello su cui è in esecuzione l'EC2istanza associata.

AWS non consiglia di ridistribuire le credenziali temporanee all'esterno dell'entità che le ha create (ad esempio, AWS applicazioni EC2 o Lambda). Tuttavia, gli utenti autorizzati possono esportare le credenziali dalle proprie EC2 istanze per effettuare chiamate legittime. API Se il `remoteAccountDetails.Affiliated` campo è `True` API stato richiamato da un account associato al tuo ambiente. AWS Per escludere un potenziale attacco e verificare la legittimità dell'attività, contatta l'IAMutente a cui sono assegnate queste credenziali.

> **Note**
>
> Se GuardDuty rileva un'attività continua da un account remoto, il relativo modello di machine learning (ML) la identificherà come un comportamento previsto. Pertanto, GuardDuty smetterà di generare questo risultato per l'attività da quell'account remoto. GuardDuty continuerà a generare risultati relativi a nuovi comportamenti provenienti da altri account remoti e rivaluterà gli account remoti appresi man mano che il comportamento cambia nel tempo.

Raccomandazioni per la correzione:

In risposta a questo esito, puoi utilizzare il seguente flusso di lavoro per determinare una linea d'azione:

1. Identifica l'account remoto coinvolto tramite il campo `service.action.awsApiCallAction.remoteAccountDetails.accountId`.

2. Successivamente, stabilisci direttamente sul campo se quell'account è affiliato al tuo GuardDuty ambiente. `service.action.awsApiCallAction.remoteAccountDetails.affiliated`
3. Se l'account è affiliato, contatta il proprietario dell'account remoto e il proprietario delle credenziali dell'EC2istanza per verificare.
4. Se l'account non è affiliato, per prima cosa valuta se è associato alla tua organizzazione ma non fa parte della configurazione GuardDuty multiaccount o se non GuardDuty è ancora stato abilitato nell'account. Altrimenti contatta il proprietario delle EC2 credenziali per determinare se esiste un caso d'uso per un account remoto in cui utilizzare tali credenziali.
5. Se il proprietario non riconosce l'account remoto, allora le credenziali potrebbero essere state compromesse da un autore di minacce che opera all'interno di AWS. Segui i passaggi consigliati in Correzione di un'istanza Amazon potenzialmente compromessa EC2 per proteggere il tuo ambiente.

   Inoltre, puoi inviare una segnalazione di abuso al team AWS Trust and Safety per avviare un'indagine sull'account remoto. Quando invii la segnalazione a AWS Trust and Safety, includi tutti JSON i dettagli della scoperta.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Le credenziali create esclusivamente per un'EC2istanza tramite un ruolo di avvio dell'istanza vengono utilizzate da un indirizzo IP esterno.

Gravità predefinita: alta

- Fonte dei dati: eventi CloudTrail di gestione o eventi relativi ai dati S3

Questo risultato ti informa che un host esterno AWS ha tentato di eseguire AWS API operazioni utilizzando AWS credenziali temporanee create su un'EC2istanza del tuo ambiente. AWS L'EC2istanza elencata potrebbe essere compromessa e le credenziali temporanee di questa istanza potrebbero essere state esfiltrate su un host remoto esterno a. AWS AWS non consiglia di ridistribuire le credenziali temporanee all'esterno dell'entità che le ha create (ad esempio, AWS applicazioni EC2 o Lambda). Tuttavia, gli utenti autorizzati possono esportare le credenziali dalle proprie EC2 istanze per effettuare chiamate legittime. API Per escludere un potenziale attacco e verificare la legittimità dell'attività, verifica se nell'esito è previsto l'uso di credenziali di istanza provenienti dall'IP remoto.

> **Note**
>
> Se GuardDuty rileva un'attività continua da un account remoto, il relativo modello di machine learning (ML) la identificherà come un comportamento previsto. Pertanto, GuardDuty smetterà di generare questo risultato per l'attività da quell'account remoto. GuardDuty continuerà a generare risultati relativi a nuovi comportamenti provenienti da altri account remoti e rivaluterà gli account remoti appresi man mano che il comportamento cambia nel tempo.

Raccomandazioni per la correzione:

Questo risultato viene generato quando la rete è configurata per instradare il traffico Internet in modo che esca da un gateway locale anziché da un VPC Internet Gateway ()IGW. Le configurazioni comuni, ad esempio l'utilizzo o le VPC VPN connessioni AWS Outposts, possono far sì che il traffico venga instradato in questo modo. Se questo comportamento è previsto, ti consigliamo di utilizzare le regole di eliminazione e creare una regola composta da due criteri di filtro. Il primo criterio è trovare il tipo, che dovrebbe essere `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. Il secondo criterio di filtro è l'IPv4indirizzo del API chiamante con l'indirizzo IP o l'CIDRintervallo del gateway Internet locale. Per ulteriori informazioni sulla creazione di regole di soppressione, vedere Regole di eliminazione.

> **Note**
>
> Se GuardDuty rileva un'attività continua proveniente da una fonte esterna, il suo modello di apprendimento automatico identificherà questo comportamento come previsto e smetterà di generare questo risultato per l'attività proveniente da quella fonte. GuardDuty continuerà a generare risultati per nuovi comportamenti da altre fonti e rivaluterà le fonti apprese man mano che il comportamento cambia nel tempo.

Se questa attività non è prevista, le credenziali potrebbero essere compromesse, vedere Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

An API è stato richiamato da un indirizzo IP malevolo noto.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta indica che un'APIoperazione (ad esempio, un tentativo di avviare un'EC2istanza, creare un nuovo IAM utente o modificare AWS i privilegi) è stata richiamata da un indirizzo IP dannoso noto. Ciò può indicare un accesso non autorizzato alle AWS risorse all'interno dell'ambiente.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

An API è stato richiamato da un indirizzo IP in un elenco di minacce personalizzato.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta ti informa che un'APIoperazione (ad esempio, un tentativo di avviare un'EC2istanza, creare un nuovo IAM utente o modificare AWS i privilegi) è stata richiamata da un indirizzo IP incluso in un elenco di minacce che hai caricato. In GuardDuty, un elenco minacce include indirizzi IP dannosi noti. Ciò può indicare un accesso non autorizzato alle AWS risorse all'interno dell'ambiente.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/TorIPCaller

An API è stato richiamato da un indirizzo IP del nodo di uscita Tor.

Gravità predefinita: media

- Fonte dei dati: eventi CloudTrail di gestione

Questa scoperta ti informa che un'APIoperazione (ad esempio, un tentativo di avviare un'EC2istanza, creare un nuovo IAM utente o modificare AWS i tuoi privilegi) è stata richiamata da un indirizzo IP del nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse AWS con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

GuardDuty Tipi di ricerca S3

I seguenti risultati sono specifici per le risorse di Amazon S3 e avranno un tipo di risorsa **`S3Bucket`** se l'origine CloudTrail dati è data events per S3 o **`AccessKey`** se l'origine dati è CloudTrail un evento di gestione. La gravità e i dettagli dei risultati saranno diversi in base al tipo di ricerca e all'autorizzazione associata al bucket.

Gli esiti qui elencati includono le origini dati e i modelli utilizzati per generare quel tipo di esito. Per ulteriori informazioni sulle origini dati e sui modelli, consulta GuardDuty fonti di dati fondamentali.

> **Important**
>
> I risultati con una fonte di dati sugli eventi di CloudTrail dati per S3 vengono generati solo se la protezione S3 è abilitata per. GuardDuty La Protezione S3 è abilitata per impostazione predefinita in tutti gli account creati dopo il 31 luglio 2020. Per informazioni su come abilitare o disabilitare la Protezione S3, consulta GuardDuty Protezione S3

Per tutti i tipi di esiti `S3Bucket`, ti consigliamo di esaminare le autorizzazioni sul bucket in questione e le autorizzazioni di tutti gli utenti coinvolti nell'esito. Se l'attività è non è prevista, consulta le raccomandazioni per la correzione descritte in dettaglio in Riparazione di un bucket S3 potenzialmente compromesso.

Argomenti

- 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

Un'API comunemente utilizzata per scovare gli oggetti S3 è stata richiamata in modo anomalo.

Gravità predefinita: bassa

- Fonte dati: eventi relativi CloudTrail ai dati per S3

Questo esito indica che un'entità IAM ha richiamato un'API S3 per scoprire i bucket S3 nel tuo ambiente, ad esempio `ListObjects`. Questo tipo di attività è associata alla fase di scoperta di un

attacco, in cui un aggressore raccoglie informazioni per determinare se l' AWS ambiente in uso è suscettibile a un attacco più ampio. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello di machine learning (ML) GuardDuty di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta Dettagli sui risultati.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Discovery:S3/MaliciousIPCaller

Un'API S3 comunemente utilizzata per scoprire risorse in un AWS ambiente è stata richiamata da un indirizzo IP malevolo noto.

Gravità predefinita: alta

- Fonte dei dati: eventi CloudTrail relativi ai dati per S3

Questo esito segnala che un'operazione API S3 è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è generalmente associata alla fase di scoperta di un attacco, quando un avversario sta raccogliendo informazioni sull'ambiente in uso. AWS A titolo di esempio si possono menzionare `GetObjectAcl` e `ListObjects`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Discovery:S3/MaliciousIPCaller.Custom

Un'API S3 è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'API S3, come `GetObjectAcl` o `ListObjects`, è stata richiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. Questo tipo di attività è associato alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il tuo ambiente AWS è suscettibile a un attacco più ampio.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Discovery:S3/TorIPCaller

Un'API S3 è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: media

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'API S3, come `GetObjectAcl` o `ListObjects`, è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. Questo tipo di attività è associata alla fase di scoperta di un attacco, in cui un aggressore raccoglie informazioni per determinare se l' AWS ambiente in uso è suscettibile a un attacco più ampio. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle AWS risorse dell'utente con l'intento di nascondere la vera identità dell'aggressore.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Exfiltration:S3/AnomalousBehavior

Un'entità IAM ha richiamato un'API S3 in modo sospetto.

Gravità predefinita: alta

- Fonte dei dati: CloudTrail eventi relativi ai dati per S3

Questo esito segnala che un'entità IAM effettua chiamate API che coinvolgono un bucket S3 e questa attività differisce dalla linea di base stabilita per tale entità. La chiamata API utilizzata in questa attività è associata alla fase di esfiltrazione di un attacco, in cui un utente malintenzionato tenta di raccogliere dati. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello ML (Anomaly Detection Machine Learning) GuardDuty di Anomaly Detection. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta Dettagli sui risultati.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Exfiltration:S3/MaliciousIPCaller

Un'API S3 comunemente utilizzata per raccogliere dati da un AWS ambiente è stata richiamata da un indirizzo IP malevolo noto.

Gravità predefinita: alta

- Fonte dei dati: eventi CloudTrail relativi ai dati per S3

Questo esito segnala che un'operazione API S3 è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di esfiltrazione in cui un avversario cerca di raccogliere dati dalla tua rete. A titolo di esempio si possono menzionare `GetObject` e `CopyObject`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Impact:S3/AnomalousBehavior.Delete

Un'entità IAM ha richiamato un'API S3 che tenta di eliminare i dati in modo sospetto.

Gravità predefinita: alta

- Fonte dati: eventi di CloudTrail dati per S3

Questo risultato indica che un'entità IAM nel tuo AWS ambiente sta effettuando chiamate API che coinvolgono un bucket S3 e questo comportamento è diverso dalla linea di base stabilita da tale entità. La chiamata API utilizzata in questa attività è associata a un attacco che tenta di eliminare i dati. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello di machine learning (ML) per GuardDuty il rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta Dettagli sui risultati.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Ti consigliamo di controllare il contenuto del tuo bucket S3 per determinare se la versione precedente dell'oggetto può o deve essere ripristinata.

Impact:S3/AnomalousBehavior.Permission

Un'API comunemente utilizzata per impostare le autorizzazioni della lista di controllo degli accessi (ACL) è stata richiamata in modo anomalo.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo risultato ti informa che un'entità IAM nel tuo AWS ambiente ha modificato una policy o un ACL sui bucket S3 elencati. Questa modifica può esporre pubblicamente i bucket S3 a tutti gli utenti autenticati. AWS

Questa API è stata identificata come anomala dal modello di apprendimento automatico (ML) GuardDuty di rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta Dettagli sui risultati.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Ti consigliamo di controllare il contenuto del tuo bucket S3 per assicurarti che a nessun oggetto sia stato inaspettatamente consentito l'accesso pubblico.

Impact:S3/AnomalousBehavior.Write

Un'entità IAM ha richiamato un'API S3 che tenta di scrivere i dati in modo sospetto.

Gravità predefinita: media

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo risultato indica che un'entità IAM nel tuo AWS ambiente sta effettuando chiamate API che coinvolgono un bucket S3 e questo comportamento è diverso dalla linea di base stabilita da tale entità. La chiamata API utilizzata in questa attività è associata a un attacco che tenta di scrivere i dati. Questa attività è sospetta perché l'entità IAM ha richiamato l'API in un modo insolito. Ad esempio, un'entità IAM senza cronologia precedente richiama un'API S3 o un'entità IAM richiama un'API S3 da una posizione insolita.

Questa API è stata identificata come anomala dal modello di machine learning (ML) per GuardDuty il rilevamento delle anomalie. Il modello di ML valuta tutte le richieste API nel tuo account e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Tiene traccia di vari fattori delle richieste API, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata, l'API specifica e il bucket richiesti e il numero di chiamate API effettuate. Per ulteriori informazioni su quali fattori della richiesta API sono insoliti per l'identità utente che ha richiamato la richiesta, consulta Dettagli sui risultati.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Ti consigliamo di controllare il contenuto del tuo bucket S3 per assicurarti che questa chiamata API non abbia scritto dati dannosi o non autorizzati.

Impact:S3/MaliciousIPCaller

Un'API S3 comunemente utilizzata per manomettere dati o processi in un AWS ambiente è stata richiamata da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Fonte dei dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'operazione API S3 è stata richiamata da un indirizzo IP associato ad attività dannose note. L'API osservata è comunemente associata a tattiche di impatto in cui un avversario cerca di manipolare, interrompere o distruggere i dati all'interno dell'ambiente. AWS A titolo di esempio si possono menzionare `PutObject` e `PutObjectAcl`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

PenTest:S3/KaliLinux

Un'API S3 è stata richiamata da una macchina Kali Linux.

Gravità predefinita: media

- Fonte dei dati: eventi relativi ai dati per S3 CloudTrail

Questa scoperta ti informa che una macchina che esegue Kali Linux sta effettuando chiamate all'API S3 utilizzando credenziali che appartengono al tuo account. AWS Le tue credenziali potrebbero essere compromesse. Kali Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della configurazione EC2 e ottenere l'accesso non autorizzato al tuo ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

PenTest:S3/ParrotLinux

Un'API S3 è stata richiamata da una macchina Parrot Security Linux.

Gravità predefinita: media

- Fonte dei dati: eventi relativi ai dati per S3 CloudTrail

Questa scoperta indica che una macchina su cui è in esecuzione Parrot Security Linux sta effettuando chiamate all'API S3 utilizzando credenziali che appartengono al vostro account. AWS Le tue credenziali potrebbero essere compromesse. Parrot Security Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Questo strumento è utilizzato anche dagli utenti malintenzionati per identificare le vulnerabilità nella configurazione EC2 e ottenere accesso non autorizzato all'ambiente AWS .

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

PenTest:S3/PentooLinux

Un'API S3 è stata richiamata da una macchina Pentoo Linux.

Gravità predefinita: media

- Fonte dei dati: CloudTrail eventi di dati per S3

Questa scoperta ti informa che una macchina su cui è in esecuzione Pentoo Linux sta effettuando chiamate all'API S3 utilizzando credenziali che appartengono al tuo account. AWS Le tue credenziali potrebbero essere compromesse. Pentoo Linux è uno noto strumento per l'esecuzione di test di intrusione utilizzato dai professionisti della sicurezza informatica per identificare le vulnerabilità nelle istanze EC2 che richiedono l'applicazione di patch. Gli aggressori utilizzano questo strumento anche per individuare i punti deboli della configurazione EC2 e ottenere l'accesso non autorizzato al tuo ambiente. AWS

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Policy:S3/AccountBlockPublicAccessDisabled

Un'entità IAM ha richiamato un'API utilizzata per disabilitare il blocco dell'accesso pubblico S3 su un account.

Gravità predefinita: bassa

- Fonte dei dati: eventi di gestione CloudTrail

Questo esito segnala che il blocco dell'accesso pubblico Amazon S3 è stato disabilitato a livello di account. Quando le impostazioni relative al blocco dell'accesso pubblico S3 sono abilitate, vengono utilizzate per filtrare le policy o le liste di controllo degli accessi (ACL) sui bucket come misura di sicurezza per evitare l'esposizione pubblica accidentale dei dati.

In genere, il blocco dell'accesso pubblico S3 è disattivato nell'account per consentire l'accesso pubblico a un bucket o agli oggetti al suo interno. Quando il blocco dell'accesso pubblico S3 è disabilitato per un account, l'accesso ai bucket è controllato dalle policy, dalle ACL o dalle impostazioni di blocco dell'accesso pubblico a livello di bucket applicate ai singoli bucket. Questo non significa per forza che i bucket sono condivisi pubblicamente, ma che è necessario controllare le autorizzazioni applicate ai bucket per verificare che forniscano il livello di accesso appropriato.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Policy:S3/BucketAnonymousAccessGranted

Un principale IAM ha concesso l'accesso a Internet a un bucket S3 modificando le policy o le ACL del bucket.

Gravità predefinita: alta

- Fonte dei dati: eventi CloudTrail di gestione

Questo esito segnala che il bucket S3 elencato è stato reso accessibile pubblicamente su Internet perché un'entità IAM ha modificato una policy o un'ACL per il bucket in questione. Una volta rilevata

una modifica alla policy o all'ACL, viene utilizzato il ragionamento automatico fornito da Zelkova per determinare se il bucket è accessibile pubblicamente.

> **Note**
>
> Se le ACL o le policy del bucket sono configurate per negare esplicitamente o negare tutto, questo esito potrebbe non riflettere lo stato attuale del bucket. Questo esito non rifletterà alcuna impostazione di Blocco dell'accesso pubblico S3 che potrebbe essere stata abilitata per il tuo bucket S3. In questi casi, il valore `effectivePermission` dell'esito verrà contrassegnato come `UNKNOWN`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Policy:S3/BucketBlockPublicAccessDisabled

Un'entità IAM ha richiamato un'API utilizzata per disabilitare il blocco dell'accesso pubblico S3 su un bucket.

Gravità predefinita: bassa

- Fonte dei dati: eventi CloudTrail di gestione

Questo esito segnala che il blocco dell'accesso pubblico è stato disabilitato per il bucket S3 elencato. Quando sono abilitate, le impostazioni relative al blocco dell'accesso pubblico S3 vengono utilizzate per filtrare le policy o le liste di controllo degli accessi (ACL) applicate ai bucket come misura di sicurezza per evitare l'esposizione pubblica accidentale dei dati.

In genere, il blocco dell'accesso pubblico S3 è disattivato su un bucket per consentire l'accesso pubblico al bucket in questione o agli oggetti al suo interno. Quando il blocco dell'accesso pubblico S3 è disabilitato per un bucket, l'accesso al bucket stesso è controllato dalle relative policy o ACL. Questo non significa che il bucket è condiviso pubblicamente, ma è necessario controllare le policy e le ACL applicate al bucket per verificare che vengano applicate le autorizzazioni appropriate.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Policy:S3/BucketPublicAccessGranted

Un responsabile IAM ha concesso l'accesso pubblico a un bucket S3 a tutti AWS gli utenti modificando le policy o gli ACL dei bucket.

Gravità predefinita: alta

- Fonte dei dati: eventi di gestione CloudTrail

Questo risultato indica che il bucket S3 elencato è stato esposto pubblicamente a tutti AWS gli utenti autenticati perché un'entità IAM ha modificato una policy del bucket o ACL su quel bucket S3. Una volta rilevata una modifica alla policy o all'ACL, viene utilizzato il ragionamento automatico fornito da Zelkova per determinare se il bucket è accessibile pubblicamente.

> **Note**
>
> Se le ACL o le policy del bucket sono configurate per negare esplicitamente o negare tutto, questo esito potrebbe non riflettere lo stato attuale del bucket. Questo esito non rifletterà alcuna impostazione di Blocco dell'accesso pubblico S3 che potrebbe essere stata abilitata per il tuo bucket S3. In questi casi, il valore `effectivePermission` dell'esito verrà contrassegnato come `UNKNOWN`.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Stealth:S3/ServerAccessLoggingDisabled

La registrazione degli accessi al server S3 è stata disabilitata per un bucket.

Gravità predefinita: bassa

- Fonte dei datiCloudTrail : eventi di gestione

Questa scoperta ti informa che la registrazione degli accessi al server S3 è disabilitata per un bucket all'interno del tuo ambiente. AWS Se disabilitata, non viene creato alcun registro delle richieste Web per i tentativi di accesso al bucket S3 identificato, tuttavia, le chiamate API di gestione S3 al bucket, ad esempio, vengono comunque tracciate. DeleteBucket Se la registrazione degli eventi dei dati S3 è abilitata CloudTrail per questo bucket, le richieste web per gli oggetti all'interno del bucket verranno comunque tracciate. La disabilitazione della registrazione è una tecnica utilizzata da utenti non autorizzati per evitare il rilevamento. Per ulteriori informazioni sui log S3, consulta Registrazione degli accessi al server S3 e Opzioni di registrazione S3 .

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Un'API S3 è stata richiamata da un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: alta

- Fonte dati: eventi di dati per S3 CloudTrail

Questo esito segnala che un'operazione API S3, ad esempio, `PutObject` o `PutObjectAcl`, è stata richiamata da un indirizzo IP incluso in un elenco minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

UnauthorizedAccess:S3/TorIPCaller

Un'API S3 è stata richiamata dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Fonte dati: eventi di CloudTrail dati per S3

Questo esito segnala che un'operazione API S3, come `PutObject` o `PutObjectAcl`, è stata richiamata dall'indirizzo IP di un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Questa scoperta può indicare un accesso non autorizzato alle tue AWS risorse con l'intento di nascondere la vera identità dell'aggressore.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

EKStipi di ricerca dei registri di controllo

I seguenti esiti sono specifici per le risorse Kubernetes e hanno un resource_type di `EKSCluster`. La gravità e i dettagli degli esiti variano in base al tipo di esito.

Per tutti i tipi di esiti di Kubernetes, ti consigliamo di esaminare la risorsa in questione per determinare se l'attività è prevista o potenzialmente dannosa. Per indicazioni su come correggere una risorsa Kubernetes compromessa identificata da un risultato, consulta. GuardDuty Correzione degli esiti del monitoraggio dei log di audit EKS

> **Note**
>
> Se questi esiti vengono generati a causa di un'attività prevista, valuta la possibilità di aggiungere una Regole di eliminazione per evitare avvisi futuri.

Argomenti

- 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**
>
> Prima della versione 1.14 di Kubernetes, il gruppo era associato a e per impostazione predefinita. `system:unauthenticated` `system:discovery` `system:basic-user` ClusterRoles Questa associazione potrebbe consentire l'accesso non intenzionale a utenti anonimi. Gli aggiornamenti del cluster non revocano queste autorizzazioni. Anche se hai aggiornato il cluster alla versione 1.14 o successiva, le autorizzazioni in questione potrebbero essere ancora abilitate. Ti consigliamo di disassociare queste autorizzazioni dal gruppo `system:unauthenticated`. Per indicazioni sulla revoca di queste autorizzazioni, consulta le best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide.

CredentialAccess:Kubernetes/MaliciousIPCaller

Un indirizzo API comunemente usato per accedere a credenziali o segreti in un cluster Kubernetes è stato richiamato da un indirizzo IP malevolo noto.

Gravità predefinita: alta

- EKSFunzionalità: registri di controllo

Questo risultato indica che un'APIoperazione è stata richiamata da un indirizzo IP associato ad attività dannose note. L'APIosservazione è comunemente associata alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *`KubernetesUserDetails`* sezione lo è*`system:anonymous`*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di

sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Un codice API comunemente usato per accedere a credenziali o segreti in un cluster Kubernetes è stato richiamato da un indirizzo IP presente in un elenco di minacce personalizzato.

Gravità predefinita: alta

- Funzionalità: registri di controllo EKS

Questa scoperta ti informa che un'APIoperazione è stata richiamata da un indirizzo IP incluso in un elenco di minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'APIosservazione è comunemente associata alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di invocare API e revoca le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Un comando API comunemente usato per accedere a credenziali o segreti in un cluster Kubernetes è stato richiamato da un utente non autenticato.

Gravità predefinita: alta

- EKSFunzionalità: registri di controllo

Questo risultato indica che un'APIoperazione è stata richiamata con successo dall'utente. `system:anonymous` APIIle chiamate effettuate da non `system:anonymous` sono autenticate. Ciò che API viene osservato è comunemente associato alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes. Questa attività indica che l'accesso anonimo o non autenticato è consentito all'azione riportata nel risultato e può essere consentito ad altre API azioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

CredentialAccess:Kubernetes/TorIPCaller

Un indirizzo API IP comunemente usato per accedere a credenziali o segreti in un cluster Kubernetes è stato richiamato da un indirizzo IP del nodo di uscita Tor.

Gravità predefinita: alta

- EKSFunzionalità: registri di controllo

Questa scoperta ti informa che un indirizzo IP API è stato richiamato da un indirizzo IP del nodo di uscita Tor. Quanto API osservato è comunemente associato alle tattiche di accesso alle credenziali in cui un avversario tenta di raccogliere password, nomi utente e chiavi di accesso per il cluster Kubernetes. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse del cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *KubernetesUserDetails* sezione lo è*system:anonymous*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller

Una delle misure difensive API comunemente utilizzate per eludere le misure difensive è stata invocata da un indirizzo IP malevolo noto.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo risultato indica che un'APIoperazione è stata richiamata da un indirizzo IP associato ad attività dannose note. L'APIosservazione è comunemente associata a tattiche di evasione difensiva in cui un avversario cerca di nascondere le proprie azioni per evitare di essere scoperto.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *KubernetesUserDetails* sezione lo è*system:anonymous*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Una delle misure difensive API comunemente utilizzate per eludere le misure difensive veniva invocata da un indirizzo IP presente in un elenco di minacce personalizzato.

Gravità predefinita: alta

- Funzionalità: registri di controllo EKS

Questa scoperta ti informa che un'APIoperazione è stata richiamata da un indirizzo IP incluso in un elenco di minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'APIosservazione è comunemente associata a tattiche di evasione difensiva in cui un avversario cerca di nascondere le proprie azioni per evitare di essere scoperto.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *`KubernetesUserDetails`* sezione lo è*`system:anonymous`*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Una misura API comunemente usata per eludere le misure difensive è stata invocata da un utente non autenticato.

Gravità predefinita: alta

- EKSCaratteristica: registri di controllo

Questo risultato indica che un'APIoperazione è stata richiamata con successo dall'utente. `system:anonymous` APIIle chiamate effettuate da non `system:anonymous` sono autenticate. L'osservazione API è comunemente associata a tattiche di evasione difensiva in cui un avversario cerca di nascondere le proprie azioni per evitare di essere scoperto. Questa attività indica che l'accesso anonimo o non autenticato è consentito all'APIazione segnalata nella rilevazione e può essere consentito per altre azioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

DefenseEvasion:Kubernetes/TorIPCaller

Un indirizzo API IP comunemente usato per eludere le misure difensive è stato invocato da un indirizzo IP del nodo di uscita Tor.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questa scoperta ti informa che un indirizzo IP API è stato richiamato da un indirizzo IP del nodo di uscita Tor. L'APIosservazione è comunemente associata a tattiche di evasione difensiva in cui un avversario cerca di nascondere le proprie azioni per evitare di essere scoperto. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato al cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *`KubernetesUserDetails`* sezione lo è*`system:anonymous`*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Discovery:Kubernetes/MaliciousIPCaller

Un comando API comunemente usato per scoprire risorse in un cluster Kubernetes è stato richiamato da un indirizzo IP.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo risultato indica che un'APIoperazione è stata richiamata da un indirizzo IP associato ad attività dannose note. L'osservazione API viene comunemente utilizzata nella fase di scoperta di un attacco, in cui un utente malintenzionato raccoglie informazioni per determinare se il cluster Kubernetes è suscettibile a un attacco più ampio.

> **Per l'accesso non autenticato**
>
> MaliciousIPCalleri risultati non vengono generati per l'accesso non autenticato. SuccessfulAnonymousAccessi risultati vengono generati per un accesso non autenticato o anonimo.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *`KubernetesUserDetails`* sezione lo è*`system:anonymous`*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Un comando API comunemente usato per scoprire risorse in un cluster Kubernetes è stato richiamato da un indirizzo IP su un elenco di minacce personalizzato.

Gravità predefinita: media

- Funzionalità: registri di controllo EKS

Questa scoperta ti informa che API è stato richiamato un messaggio da un indirizzo IP incluso in un elenco di minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'osservazione API viene comunemente utilizzata nella fase di scoperta di un attacco, in cui un utente malintenzionato raccoglie informazioni per determinare se il cluster Kubernetes è suscettibile a un attacco più ampio.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *`KubernetesUserDetails`* sezione lo è*`system:anonymous`*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Discovery:Kubernetes/SuccessfulAnonymousAccess

Un comando API comunemente usato per scoprire risorse in un cluster Kubernetes è stato richiamato da un utente non autenticato.

Gravità predefinita: media

- Funzionalità: registri di controllo EKS

Questo risultato indica che un'APIoperazione è stata richiamata con successo dall'utente. `system:anonymous` APIle chiamate effettuate da non `system:anonymous` sono autenticate. L'osservazione API è comunemente associata alla fase di scoperta di un attacco, quando un avversario sta raccogliendo informazioni sul cluster Kubernetes. Questa attività indica che l'accesso anonimo o non autenticato è consentito all'APIazione riportata nel risultato e può essere consentito per altre azioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Questo tipo di risultato esclude gli API endpoint per il controllo dello stato di salute come`/healthz`,, `/livez` e. `/readyz` `/version`

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Discovery:Kubernetes/TorIPCaller

Un indirizzo API IP comunemente usato per scoprire risorse in un cluster Kubernetes è stato richiamato da un indirizzo IP del nodo di uscita Tor.

Gravità predefinita: media

- Funzionalità: registri di controllo EKS

Questa scoperta ti informa che un indirizzo IP API è stato richiamato da un indirizzo IP del nodo di uscita Tor. Quanto osservato API viene comunemente utilizzato nella fase di scoperta di un attacco, in cui un aggressore raccoglie informazioni per determinare se il cluster Kubernetes è suscettibile a un attacco più ampio. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato al cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *`KubernetesUserDetails`* sezione lo è*`system:anonymous`*, scopri perché all'utente anonimo è stato consentito di invocare la APIand revoca delle autorizzazioni, se necessario, seguendo le istruzioni contenute nelle migliori pratiche di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un

avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Execution:Kubernetes/ExecInKubeSystemPod

È stato eseguito un comando in un pod all'interno dello spazio dei nomi del **`kube-system`**.

Gravità predefinita: media

- Funzionalità: registri di controllo EKS

Questa scoperta informa che un comando è stato eseguito in un pod all'interno del **`kube-system`** namespace utilizzando Kubernetes exec. API `kube-system`namespace è uno spazio dei nomi predefinito, utilizzato principalmente per componenti a livello di sistema come e. `kube-dns` `kube-proxy` L'esecuzione di comandi in pod o container all'interno dello spazio dei nomi del `kube-system` è molto rara e può indicare attività sospette.

Raccomandazioni per la correzione:

Se l'esecuzione di questo comando non è prevista, le credenziali dell'identità utente utilizzate per eseguirlo potrebbero essere compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Impact:Kubernetes/MaliciousIPCaller

Un indirizzo API comunemente usato per manomettere le risorse in un cluster Kubernetes veniva richiamato da un indirizzo IP malevolo noto.

Gravità predefinita: alta

- EKSFunzionalità: registri di controllo

Questo risultato indica che un'APIoperazione è stata richiamata da un indirizzo IP associato ad attività dannose note. L'osservazione API è comunemente associata a tattiche di impatto in cui un avversario tenta di manipolare, interrompere o distruggere i dati all'interno dell'ambiente. AWS

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *KubernetesUserDetails* sezione lo è*system:anonymous*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Impact:Kubernetes/MaliciousIPCaller.Custom

Un comando API comunemente usato per manomettere le risorse in un cluster Kubernetes è stato richiamato da un indirizzo IP su un elenco di minacce personalizzato.

Gravità predefinita: alta

- Funzionalità: registri di controllo EKS

Questa scoperta ti informa che un'APIoperazione è stata richiamata da un indirizzo IP incluso in un elenco di minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'osservazione API è comunemente associata a tattiche di impatto in cui un avversario cerca di manipolare, interrompere o distruggere i dati all'interno dell'ambiente. AWS

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *KubernetesUserDetails* sezione lo è*system:anonymous*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Impact:Kubernetes/SuccessfulAnonymousAccess

Un comando API comunemente usato per manomettere le risorse in un cluster Kubernetes è stato richiamato da un utente non autenticato.

Gravità predefinita: alta

- Funzionalità: registri di controllo EKS

Questo risultato indica che un'APIoperazione è stata richiamata con successo dall'utente. `system:anonymous` APIIle chiamate effettuate da non `system:anonymous` sono autenticate. Ciò che API viene osservato è in genere associato alla fase di impatto di un attacco, quando un avversario sta manomettendo le risorse del cluster. Questa attività indica che l'accesso anonimo o non autenticato è consentito all'APIazione riportata nel risultato e può essere consentito per altre azioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Impact:Kubernetes/TorIPCaller

Un indirizzo API IP comunemente usato per manomettere le risorse in un cluster Kubernetes è stato richiamato da un indirizzo IP del nodo di uscita Tor.

Gravità predefinita: alta

- Funzionalità: registri di controllo EKS

Questa scoperta ti informa che un indirizzo IP API è stato richiamato da un indirizzo IP del nodo di uscita Tor. Quanto API osservato è comunemente associato a tattiche di impatto in cui un avversario

cerca di manipolare, interrompere o distruggere i dati all'interno dell'ambiente. AWS Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato al cluster Kubernetes con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *`KubernetesUserDetails`* sezione lo è*`system:anonymous`*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Persistence:Kubernetes/ContainerWithSensitiveMount

È stato avviato un container con un percorso host esterno sensibile montato all'interno.

Gravità predefinita: media

- Caratteristica: registri di controllo EKS

Questo esito segnala che un container è stato avviato con una configurazione che includeva un percorso host sensibile con accesso in scrittura nella sezione `volumeMounts`. Ciò rende questo percorso accessibile e scrivibile dall'interno del container. Questa tecnica viene comunemente utilizzata dagli avversari per accedere al file system dell'host.

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione composta da un criterio di filtro basato sul campo

`resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve essere uguale all'`imagePrefix` specificato nell'esito. Per ulteriori informazioni sulla creazione delle regole di eliminazione, consulta Regole di eliminazione.

Persistence:Kubernetes/MaliciousIPCaller

Un indirizzo API comunemente usato per ottenere l'accesso persistente a un cluster Kubernetes veniva richiamato da un indirizzo IP malevolo noto.

Gravità predefinita: media

- Funzionalità: registri di controllo EKS

Questo risultato indica che un'APIoperazione è stata richiamata da un indirizzo IP associato ad attività dannose note. L'APIosservazione è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster Kubernetes e sta tentando di mantenere tale accesso.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *`KubernetesUserDetails`* sezione lo è*`system:anonymous`*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Un comando API comunemente usato per ottenere l'accesso permanente a un cluster Kubernetes è stato richiamato da un indirizzo IP su un elenco di minacce personalizzato.

Gravità predefinita: media

- Funzionalità: registri di controllo EKS

Questa scoperta ti informa che un'APIoperazione è stata richiamata da un indirizzo IP incluso in un elenco di minacce che hai caricato. L'elenco minacce associato a questo esito è elencato nella sezione Informazioni aggiuntive dei dettagli di un esito. L'APIosservazione è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster Kubernetes e sta tentando di mantenere tale accesso.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la *`KubernetesUserDetails`* sezione lo è*`system:anonymous`*, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Persistence:Kubernetes/SuccessfulAnonymousAccess

Un comando API comunemente usato per ottenere autorizzazioni di alto livello per un cluster Kubernetes è stato richiamato da un utente non autenticato.

Gravità predefinita: alta

- Funzionalità: registri di controllo EKS

Questo risultato indica che un'APIoperazione è stata richiamata con successo dall'utente. `system:anonymous` APIIe chiamate effettuate da non `system:anonymous` sono autenticate. L'osservazione API è comunemente associata alle tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster e sta tentando di mantenere tale accesso. Questa attività indica che l'accesso anonimo o non autenticato è consentito all'APIazione riportata nel risultato e può essere consentito per altre azioni. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` sul cluster e assicurati che tutte le autorizzazioni siano necessarie. Se le autorizzazioni sono state concesse erroneamente o

intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Persistence:Kubernetes/TorIPCaller

Un indirizzo API IP comunemente usato per ottenere l'accesso persistente a un cluster Kubernetes è stato richiamato da un indirizzo IP del nodo di uscita Tor.

Gravità predefinita: media

- Funzionalità: registri di controllo EKS

Questa scoperta ti informa che un indirizzo IP API è stato richiamato da un indirizzo IP del nodo di uscita Tor. L'APIosservazione è comunemente associata a tattiche di persistenza in cui un avversario ha ottenuto l'accesso al cluster Kubernetes e sta tentando di mantenere tale accesso. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relay tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle AWS risorse con l'intento di nascondere la vera identità dell'aggressore.

Raccomandazioni per la correzione:

Se l'utente segnalato nella scoperta sotto la `KubernetesUserDetails` sezione lo è`system:anonymous`, scopri perché all'utente anonimo è stato consentito di richiamarlo API e revocare le autorizzazioni, se necessario, seguendo le istruzioni riportate nelle best practice di sicurezza per Amazon EKS nella Amazon User Guide. EKS Se l'utente è autenticato, effettua ulteriori verifiche per determinare se l'attività era legittima o dannosa. Se l'attività era dannosa, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

All'account di servizio predefinito sono stati concessi i privilegi di amministratore su un cluster Kubernetes.

Gravità predefinita: alta

- Caratteristica: registri di controllo EKS

Questo esito segnala che all'account di servizio predefinito per uno spazio dei nomi nel cluster Kubernetes sono stati concessi i privilegi di amministratore. Kubernetes crea un account di servizio predefinito per tutti gli spazi dei nomi del cluster e lo assegna automaticamente come identità ai pod che non sono stati associati esplicitamente a un altro account di servizio. Se l'account di servizio predefinito dispone di privilegi di amministratore, è possibile che vengano lanciati involontariamente pod con privilegi di amministratore. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

Raccomandazioni per la correzione:

Non utilizzare l'account di servizio predefinito per concedere autorizzazioni ai pod. Crea invece un account di servizio dedicato per ogni carico di lavoro e concedi l'autorizzazione a tale account in base alle esigenze. Per risolvere questo problema, crea account di servizio dedicati per tutti i tuoi pod e carichi di lavoro e aggiornali per migrare dall'account di servizio predefinito ai relativi account dedicati. Rimuovi quindi l'autorizzazione di amministratore dall'account di servizio predefinito. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Policy:Kubernetes/AnonymousAccessGranted

All'**`system:anonymous`**utente è stata concessa l'APIautorizzazione su un cluster Kubernetes.

Gravità predefinita: alta

- Funzionalità: registri di controllo EKS

Questo esito segnala che un utente del cluster Kubernetes ha creato correttamente un `ClusterRoleBinding` o `RoleBinding` per associare l'utente `system:anonymous` a un ruolo. Ciò consente l'accesso non autenticato alle API operazioni consentite dal ruolo. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente `system:anonymous` o al gruppo `system:unauthenticated` sul cluster e revoca l'accesso anonimo non necessario. Per ulteriori informazioni, consulta le best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide. Se le autorizzazioni sono state concesse intenzionalmente, revoca l'accesso dell'utente che le ha concesse e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Policy:Kubernetes/ExposedDashboard

Il pannello di un cluster Kubernetes era esposto a Internet

Gravità predefinita: media

- Funzionalità: registri EKS di controllo

Questo esito segnala che il pannello Kubernetes per il cluster è stato esposto a Internet da un servizio del sistema di bilanciamento del carico. Un pannello esposto rende l'interfaccia di gestione del cluster accessibile da Internet e consente agli avversari di sfruttare eventuali lacune nell'autenticazione e nel controllo degli accessi.

Raccomandazioni per la correzione:

Assicurati di applicare autenticazione e autorizzazione avanzate sul pannello Kubernetes. Inoltre, implementa il controllo dell'accesso alla rete per limitare l'accesso al pannello da indirizzi IP specifici.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Policy:Kubernetes/KubeflowDashboardExposed

Il pannello Kubeflow di un cluster Kubernetes era esposto a Internet

Gravità predefinita: media

- Caratteristica: registri EKS di controllo

Questo esito segnala che il pannello Kubeflow per il cluster è stato esposto a Internet da un servizio del sistema di bilanciamento del carico. Un pannello Kubeflow esposto rende l'interfaccia di gestione

dell'ambiente Kubeflow accessibile da Internet e consente agli avversari di sfruttare eventuali lacune nell'autenticazione e nel controllo degli accessi.

Raccomandazioni per la correzione:

Assicurati di applicare autenticazione e autorizzazione avanzate sul pannello Kubeflow. Inoltre, implementa il controllo dell'accesso alla rete per limitare l'accesso al pannello da indirizzi IP specifici.

Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Un container privilegiato con accesso a livello root è stato avviato sul cluster Kubernetes.

Gravità predefinita: media

- Caratteristica: registri EKS di controllo

Questo esito segnala che un container privilegiato è stato avviato sul cluster Kubernetes utilizzando un'immagine che non era mai stata utilizzata per avviare container privilegiati nel cluster. Un container privilegiato ha accesso di livello root all'host. Gli avversari possono avviare container privilegiati come tattica di escalation dei privilegi per accedere all'host e quindi comprometterlo.

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un avversario. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Un Kubernetes API comunemente usato per accedere ai segreti è stato richiamato in modo anomalo.

Gravità predefinita: media

- EKSFunzionalità: registri di controllo

Questa scoperta ti informa che un'APIoperazione anomala per recuperare i segreti sensibili del cluster è stata richiamata da un utente Kubernetes del tuo cluster. Quanto osservato API è comunemente associato a tattiche di accesso alle credenziali che possono portare a un aumento dei privilegi e a ulteriori accessi all'interno del cluster. Se questo comportamento non è previsto, può indicare un errore di configurazione o che le credenziali sono compromesse. AWS

L'osservazione API è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello ML valuta tutte le API attività degli utenti all'interno del EKS cluster e identifica gli eventi anomali associati alle tecniche utilizzate da utenti non autorizzati. Il modello ML tiene traccia di diversi fattori dell'APIoperazione, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta, l'agente utente utilizzato e lo spazio dei nomi utilizzato dall'utente. Puoi trovare i dettagli insoliti della API richiesta nel pannello dei dettagli di ricerca della GuardDuty console.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente Kubernetes nel cluster e assicurati che siano tutte necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Nel cluster RoleBinding ClusterRoleBinding Kubernetes è stato creato o modificato un ruolo o un namespace riservato eccessivamente permissivo.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se un RoleBinding or ClusterRoleBinding coinvolge o, la gravità è Alta. ClusterRoles `admin` `cluster-admin`

- Funzionalità: registri EKS di controllo

Questo esito segnala che un utente del cluster Kubernetes ha creato un `RoleBinding` o un `ClusterRoleBinding` per associare un utente a un ruolo con autorizzazioni di amministratore o spazi dei nomi sensibili. Se questo comportamento non è previsto, può indicare un errore di configurazione o che le AWS credenziali sono compromesse.

L'osservazione API è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello ML valuta tutte le API attività degli utenti all'interno del cluster. EKS Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello ML tiene inoltre traccia di diversi fattori dell'APIoperazione, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta, l'agente utente utilizzato e lo spazio dei nomi utilizzato dall'utente. Puoi trovare i dettagli insoliti della API richiesta nel pannello dei dettagli di ricerca della GuardDuty console.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente Kubernetes. Queste autorizzazioni sono definite nel ruolo e nei soggetti coinvolti nel `RoleBinding` e nel `ClusterRoleBinding`. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Execution:Kubernetes/AnomalousBehavior.ExecInPod

È stato eseguito un comando in un pod in modo anomalo.

Gravità predefinita: media

- Funzionalità: EKS registri di controllo

Questa scoperta ti informa che un comando è stato eseguito in un pod utilizzando Kubernetes exec. API Kubernetes API exec consente l'esecuzione di comandi arbitrari in un pod. Se questo

comportamento non è previsto per l'utente, lo spazio dei nomi o il pod, può indicare un errore di configurazione o che le credenziali sono compromesse. AWS

L'osservazione API è stata identificata come anomala dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello ML valuta tutte le API attività degli utenti all'interno del cluster. EKS Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello ML tiene inoltre traccia di diversi fattori dell'APIoperazione, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta, l'agente utente utilizzato e lo spazio dei nomi utilizzato dall'utente. Puoi trovare i dettagli insoliti della API richiesta nel pannello dei dettagli di ricerca della GuardDuty console.

Raccomandazioni per la correzione:

Se l'esecuzione di questo comando non è prevista, le credenziali dell'identità utente utilizzate per eseguirlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Un carico di lavoro è stato avviato in modo anomalo con un container privilegiato.

Gravità predefinita: alta

- Funzionalità: EKS registri di controllo

Questo risultato ti informa che è stato avviato un carico di lavoro con un contenitore privilegiato nel tuo cluster Amazon. EKS Un container privilegiato ha accesso di livello root all'host. Gli utenti non autorizzati possono avviare container privilegiati come tattica di escalation dei privilegi prima per accedere all'host, poi per comprometterlo.

La creazione o la modifica del contenitore osservata è stata identificata come anomala dal modello di apprendimento automatico per il rilevamento delle GuardDuty anomalie (ML). Il modello ML valuta tutte le attività relative alle immagini degli utenti API e dei contenitori all'interno del cluster. EKS

Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello ML tiene inoltre traccia di diversi fattori dell'APIoperazione, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta, l'agente utente utilizzato, le immagini del contenitore osservate nell'account e lo spazio dei nomi utilizzato dall'utente. Puoi trovare i dettagli insoliti della API richiesta nel pannello dei dettagli di ricerca della GuardDuty console.

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione con un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve avere lo stesso valore del campo `imagePrefix` specificato nell'esito. Per ulteriori informazioni, consulta Regole di eliminazione.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount

Un carico di lavoro è stato implementato in modo anomalo con un percorso host sensibile montato al suo interno.

Gravità predefinita: alta

- Funzionalità: EKS registri di controllo

Questo esito segnala che un carico di lavoro è stato avviato con un container che includeva un percorso host sensibile nella sezione `volumeMounts`. Ciò rende questo percorso potenzialmente accessibile e scrivibile dall'interno del container. Questa tecnica viene comunemente utilizzata dagli utenti non autorizzati per accedere al file system dell'host.

La creazione o la modifica del contenitore osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello ML valuta tutte le attività relative alle immagini degli utenti API e dei contenitori all'interno del cluster. EKS Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello ML tiene inoltre traccia di diversi fattori dell'APIoperazione, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta, l'agente utente utilizzato, le immagini del contenitore osservate nell'account e lo spazio dei nomi utilizzato dall'utente. Puoi trovare i dettagli insoliti della API richiesta nel pannello dei dettagli di ricerca della GuardDuty console.

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione con un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve avere lo stesso valore del campo `imagePrefix` specificato nell'esito. Per ulteriori informazioni, consulta Regole di eliminazione.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Un carico di lavoro è stato avviato in modo anomalo.

Gravità predefinita: bassa*

> **Note**
>
> La gravità predefinita è bassa. Tuttavia, se il carico di lavoro contiene un nome immagine potenzialmente sospetto, ad esempio uno strumento di test di penetrazione (pen-test) noto, o un container che esegue un comando potenzialmente sospetto all'avvio, come i comandi di shell (interprete di comandi) inversa, questo tipo di esito verrà considerato di gravità media.

- Funzionalità: EKS registri di controllo

Questa scoperta ti informa che un carico di lavoro Kubernetes è stato creato o modificato in modo anomalo, ad esempio un'APIattività, nuove immagini di container o una configurazione rischiosa del carico di lavoro, all'interno del tuo cluster Amazon. EKS Gli utenti non autorizzati possono avviare container come tattica per eseguire un codice arbitrario prima per accedere all'host, poi per comprometterlo.

La creazione o la modifica del contenitore osservata è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle anomalie. GuardDuty Il modello ML valuta tutte le attività relative alle immagini degli utenti API e dei contenitori all'interno del cluster. EKS Questo modello di ML identifica anche gli eventi anomali associati alle tecniche utilizzate da un utente non autorizzato. Il modello ML tiene inoltre traccia di diversi fattori dell'APIoperazione, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta, l'agente utente utilizzato, le immagini del contenitore osservate nell'account e lo spazio dei nomi utilizzato dall'utente. Puoi trovare i dettagli insoliti della API richiesta nel pannello dei dettagli di ricerca della GuardDuty console.

Raccomandazioni per la correzione:

Se l'avvio del container non è previsto, le credenziali dell'identità utente utilizzate per avviarlo potrebbero essere state compromesse. Revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Se l'avvio di questo container è previsto, ti consigliamo di utilizzare una regola di eliminazione con un criterio di filtro basato sul campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nei criteri di filtro, il campo `imagePrefix` deve avere lo stesso valore del campo `imagePrefix` specificato nell'esito. Per ulteriori informazioni, consulta Regole di eliminazione.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Un ruolo altamente permissivo o ClusterRole è stato creato o modificato in modo anomalo.

Gravità predefinita: bassa

- Funzionalità: registri di controllo EKS

Questa scoperta ti informa che un'APIoperazione anomala per creare un `Role` o `ClusterRole` con autorizzazioni eccessive è stata chiamata da un utente Kubernetes nel tuo cluster Amazon. EKS Gli attori possono utilizzare la creazione di ruoli con autorizzazioni avanzate per non utilizzare ruoli incorporati simili a quelli di amministratore ed evitare il rilevamento. Le autorizzazioni eccessive possono portare a un'escalation dei privilegi, all'esecuzione di codice in modalità remota e al potenziale controllo di uno spazio dei nomi o di un cluster. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono compromesse.

L'osservazione API è stata identificata come anomala dal modello di apprendimento automatico di rilevamento delle GuardDuty anomalie (ML). Il modello ML valuta tutte le API attività degli utenti all'interno del tuo EKS cluster Amazon e identifica gli eventi anomali associati alle tecniche utilizzate da utenti non autorizzati. Il modello ML tiene inoltre traccia di diversi fattori dell'APIoperazione, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta, lo user agent utilizzato, le immagini dei container osservate nell'account e lo spazio dei nomi utilizzato dall'utente. Puoi trovare i dettagli insoliti della API richiesta nel pannello dei dettagli di ricerca della GuardDuty console.

Raccomandazioni per la correzione:

Esamina le autorizzazioni definite in `Role` o `ClusterRole` per assicurarti che tutte le autorizzazioni siano necessarie e segui i principi del privilegio minimo. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Un utente ha verificato la propria autorizzazione di accesso in modo anomalo.

Gravità predefinita: bassa

- Funzionalità: EKS registri di controllo

Questo esito segnala che un utente del cluster Kubernetes ha verificato correttamente se sono consentite o meno le autorizzazioni avanzate note che possono portare a un'escalation dei privilegi e all'esecuzione di codice in modalità remota. Ad esempio, `kubectl auth can-i` è un comando comune utilizzato per verificare le autorizzazioni di un utente. Se questo comportamento non è previsto, potrebbe indicare un errore di configurazione o che le credenziali sono state compromesse.

L'osservazione API è stata identificata come anomala dal modello di machine learning (ML) per il rilevamento delle GuardDuty anomalie. Il modello ML valuta tutte le API attività degli utenti all'interno del tuo EKS cluster Amazon e identifica gli eventi anomali associati alle tecniche utilizzate da utenti non autorizzati. Il modello ML tiene inoltre traccia di diversi fattori dell'APIoperazione, come l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta, il controllo dell'autorizzazione e lo spazio dei nomi utilizzato dall'utente. Puoi trovare i dettagli insoliti della API richiesta nel pannello dei dettagli di ricerca della GuardDuty console.

Raccomandazioni per la correzione:

Esamina le autorizzazioni concesse all'utente Kubernetes per assicurarti che siano tutte necessarie. Se le autorizzazioni sono state concesse erroneamente o intenzionalmente, revoca l'accesso dell'utente e annulla qualsiasi eventuale modifica che è stata apportata al cluster da un utente non autorizzato. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Se AWS le tue credenziali sono compromesse, consulta. Riparazione delle credenziali potenzialmente compromesse AWS

Tipi di risultati del monitoraggio del runtime

Amazon GuardDuty genera i seguenti risultati di Runtime Monitoring per indicare potenziali minacce in base al comportamento a livello di sistema operativo degli EC2 host e dei container Amazon nei EKS cluster Amazon, nei carichi di lavoro ECS Fargate e Amazon e nelle istanze Amazon. EC2

> **Note**
>
> I tipi di esiti del monitoraggio del runtime EKS si basano sui log di runtime raccolti dagli host. I log contengono campi, come i percorsi dei file, che potrebbero essere controllati da un utente malintenzionato. Questi campi sono inclusi anche nei risultati per fornire un contesto di runtime GuardDuty . Quando si elaborano i risultati del Runtime Monitoring all'esterno della

GuardDuty console, è necessario ripulire i campi di ricerca. Ad esempio, è possibile HTML codificare i campi di ricerca quando li si visualizza su una pagina Web.

Argomenti

- CryptoCurrency:Runtime/BitcoinTool.B
- Backdoor:Runtime/C&CActivity.B
- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Backdoor:Runtime/C&CActivity.B!DNS
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- 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

Un'EC2istanza o un contenitore Amazon sta interrogando un indirizzo IP associato a un'attività correlata alla criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che l'EC2istanza o un contenitore elencato nel tuo AWS ambiente sta interrogando un indirizzo IP associato a un'attività correlata alla criptovaluta. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se utilizzate questa EC2 istanza o un container per estrarre o gestire criptovalute, o se uno di questi è coinvolto in altro modo nell'attività della blockchain, il CryptoCurrency:Runtime/BitcoinTool.B risultato potrebbe rappresentare l'attività prevista per il vostro ambiente. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio di filtro deve utilizzare l'attributo Tipo di risultato con un valore di `CryptoCurrency:Runtime/BitcoinTool.B`. Il secondo criterio di filtro deve essere l'ID istanza dell'istanza o l'ID immagine del container del container coinvolti in attività legate alle criptovalute o alla blockchain. Per ulteriori informazioni, consulta Regole di eliminazione.

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B

Un'EC2istanza o un contenitore Amazon sta interrogando un IP associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che l'EC2istanza o un contenitore elencato all'interno del tuo AWS ambiente sta interrogando un IP associato a un server di comando e controllo (C&C) noto. L'istanza elencata o il container potrebbero essere potenzialmente compromessi. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è un insieme di dispositivi connessi a Internet che possono includere serverPCs, dispositivi mobili e dispositivi Internet of Things, infetti e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche emettere comandi per avviare un attacco denial of service () distribuito. DDoS

> **Note**
>
> Se l'IP su cui viene eseguita una query è correlato a log4j, i campi dell'esito associato includeranno i valori seguenti:

- `service.additionalInfo.threatListName = Amazon`
- `service.additionalInfo.threatName = Log4j Related`

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

UnauthorizedAccess:Runtime/TorRelay

La tua EC2 istanza Amazon o un contenitore sta effettuando connessioni a una rete Tor come relè Tor.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un'EC2istanza o un contenitore nel tuo AWS ambiente sta effettuando connessioni a una rete Tor in un modo che suggerisce che stia agendo come un relè Tor. Tor è un software che consente la comunicazione anonima. Tor aumenta l'anonimato della comunicazione inoltrando il traffico potenzialmente illecito del client da un relè Tor a un altro.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

UnauthorizedAccess:Runtime/TorClient

La tua EC2 istanza Amazon o un container sta effettuando connessioni a un nodo Tor Guard o Authority.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un'EC2istanza o un contenitore nel tuo AWS ambiente sta effettuando connessioni a un nodo Tor Guard o a un nodo Authority. Tor è un software che consente la comunicazione anonima. I Tor Guard e i nodi fungono da gateway iniziali per una rete Tor. Questo traffico può indicare che questa EC2 istanza o il contenitore sono stati potenzialmente compromessi e agiscono come client su una rete Tor. Questa scoperta potrebbe indicare un accesso non autorizzato alle tue AWS risorse con l'intento di nascondere la vera identità dell'aggressore.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic

Un'EC2istanza o un contenitore Amazon sta tentando di comunicare con un indirizzo IP di un host remoto che è un buco nero noto.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questa scoperta indica che l'EC2istanza elencata o un contenitore nel tuo AWS ambiente potrebbero essere compromessi perché sta tentando di comunicare con l'indirizzo IP di un buco nero (o sink hole). I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario. L'indirizzo IP di un buco nero designa un computer host non in esecuzione o un indirizzo a cui non è stato assegnato alcun host.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/DropPoint

Un'EC2istanza o un contenitore Amazon sta tentando di comunicare con un indirizzo IP di un host remoto noto per contenere credenziali e altri dati rubati acquisiti dal malware.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questa scoperta indica che un'EC2istanza o un contenitore nel tuo AWS ambiente sta tentando di comunicare con un indirizzo IP di un host remoto noto per contenere credenziali e altri dati rubati acquisiti dal malware.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Un'EC2istanza o un contenitore Amazon sta interrogando un nome di dominio associato a un'attività di criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che l'EC2istanza o un contenitore elencato nel tuo AWS ambiente sta interrogando un nome di dominio associato a Bitcoin o ad altre attività legate alle criptovalute. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo al fine di riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se utilizzate questa EC2 istanza o questo contenitore per estrarre o gestire criptovalute, o se uno di questi è coinvolto in altro modo nell'attività della blockchain, la CryptoCurrency:Runtime/BitcoinTool.B!DNS scoperta potrebbe essere un'attività prevista per il vostro ambiente. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di eliminazione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. Il secondo criterio di filtro deve essere l'ID istanza dell'istanza o l'ID immagine del container del container coinvolti in attività legate alle criptovalute o alla blockchain. Per ulteriori informazioni, consulta Regole di eliminazione.

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B!DNS

Un'EC2istanza o un contenitore Amazon sta interrogando un nome di dominio associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che l'EC2istanza o il contenitore elencato all'interno del tuo AWS ambiente sta interrogando un nome di dominio associato a un server di comando e controllo (C&C) noto. L'EC2istanza o il contenitore elencati potrebbero essere compromessi. I server di comando e controllo sono computer che inviano comandi ai membri di una botnet.

Una botnet è un insieme di dispositivi connessi a Internet che può includere serverPCs, dispositivi mobili e dispositivi Internet of Things, infetti e controllati da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche emettere comandi per avviare un attacco denial of service () distribuito. DDoS

> **Note**
>
> Se il nome di dominio su cui è stata eseguita la query è relativo a log4j, i campi dell'esito associato includeranno i valori seguenti:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> Per verificare come GuardDuty genera questo tipo di risultato, puoi effettuare una DNS richiesta dalla tua istanza (utilizzando `dig` per Linux o `nslookup` per Windows) rispetto a un dominio di test. `guarddutyc2activityb.com`

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic!DNS

Un'EC2istanza o un contenitore Amazon sta interrogando un nome di dominio che viene reindirizzato a un indirizzo IP nero.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questa scoperta indica che l'EC2istanza o il contenitore elencato nel tuo AWS ambiente potrebbero essere compromessi perché sta interrogando un nome di dominio che viene reindirizzato a un indirizzo IP di buco nero. I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/DropPoint!DNS

Un'EC2istanza o un contenitore Amazon sta interrogando il nome di dominio di un host remoto noto per contenere credenziali e altri dati rubati acquisiti da malware.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questa scoperta indica che un'EC2istanza o un contenitore nel tuo AWS ambiente sta interrogando il nome di dominio di un host remoto noto per contenere credenziali e altri dati rubati acquisiti da malware.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/DGADomainRequest.C!DNS

Un'EC2istanza o un contenitore Amazon sta interrogando domini generati algoritmicamente. Tali domini sono comunemente utilizzati dal malware e potrebbero essere un'indicazione di un'istanza o di un contenitore compromessi. EC2

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo risultato indica che l'EC2istanza o il contenitore elencati nell' AWS ambiente in uso sta tentando di interrogare i domini dell'algoritmo di generazione del dominio ()DGA. La risorsa potrebbe essere stata compromessa.

DGAsvengono utilizzati per generare periodicamente un gran numero di nomi di dominio che possono essere utilizzati come punti di incontro con i relativi server di comando e controllo (C&C). I server di comando e controllo sono computer che inviano comandi a membri di una botnet, ovvero una raccolta di dispositivi connessi a Internet infettati e controllati da un tipo comune di malware. Il numero elevato di punti di rendez-vous potenziali rende difficile l'arresto delle botnet in quanto i computer infettati tentano di contattare quotidianamente alcuni di questi nomi di dominio per ricevere aggiornamenti o comandi.

> **Note**
>
> Questa scoperta si basa su domini noti provenienti dai feed di intelligence sulle minacceDGA. GuardDuty

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/DriveBySourceTraffic!DNS

Un'EC2istanza o un contenitore Amazon sta interrogando il nome di dominio di un host remoto che è una fonte nota di attacchi di download Drive-By.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che l'EC2istanza o il contenitore elencati nel tuo AWS ambiente potrebbero essere compromessi perché sta interrogando il nome di dominio di un host remoto che è una fonte nota di attacchi drive-by download. Si tratta di download di software non voluti da Internet che possono avviare l'installazione automatica di virus, spyware o malware.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Trojan:Runtime/PhishingDomainRequest!DNS

Un'EC2istanza o un contenitore Amazon interroga i domini coinvolti negli attacchi di phishing.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta indica che nel tuo AWS ambiente è presente un'EC2istanza o un contenitore che sta cercando di interrogare un dominio coinvolto in attacchi di phishing. I domini di phishing sono

configurati da individui che fingono di essere un'istituzione legittima allo scopo di indurre gli utenti a fornire dati sensibili come informazioni personali, coordinate bancarie, informazioni di carte di credito e password. L'EC2istanza o il contenitore potrebbero tentare di recuperare dati sensibili archiviati su un sito Web di phishing oppure di configurare un sito Web di phishing. L'EC2istanza o il contenitore potrebbero essere compromessi.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Impact:Runtime/AbusedDomainRequest.Reputation

Un'EC2istanza o un contenitore Amazon sta interrogando un nome di dominio a bassa reputazione associato a domini noti di abuso.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che l'EC2istanza o il contenitore elencato all'interno del tuo AWS ambiente sta interrogando un nome di dominio a bassa reputazione associato a domini o indirizzi IP noti per abuso. Esempi di domini abusati sono i nomi di dominio di primo livello (TLDs) e i nomi di dominio di secondo livello (2LDs) che offrono registrazioni gratuite di sottodomini e provider dinamici. DNS Gli autori delle minacce tendono a utilizzare questi servizi per registrare domini gratuitamente o a basso costo. I domini a bassa reputazione di questa categoria possono anche essere domini scaduti che vengono sostituiti con l'indirizzo IP di parcheggio di un registrar e quindi potrebbero non essere più attivi. Un IP di parcheggio è il luogo in cui un registrar indirizza il traffico verso domini che non sono stati collegati ad alcun servizio. L'EC2istanza Amazon o il contenitore elencati potrebbero essere compromessi poiché gli autori delle minacce utilizzano comunemente questi registrar o servizi per C&C e la distribuzione di malware.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Impact:Runtime/BitcoinDomainRequest.Reputation

Un'EC2istanza o un contenitore Amazon sta interrogando un nome di dominio a bassa reputazione associato ad attività legate alle criptovalute.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che l'EC2istanza elencata o il contenitore all'interno del tuo AWS ambiente sta interrogando un nome di dominio a bassa reputazione associato a Bitcoin o ad altre attività legate alle criptovalute. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se utilizzate questa EC2 istanza o il contenitore per estrarre o gestire criptovalute, o se queste risorse sono altrimenti coinvolte nell'attività della blockchain, questo risultato potrebbe rappresentare l'attività prevista per il vostro ambiente. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio di filtro deve utilizzare l'attributo Tipo di risultato con un valore di `Impact:Runtime/BitcoinDomainRequest.Reputation`. Il secondo criterio di filtro

deve essere l'ID istanza dell'istanza o l'ID immagine del container del container coinvolti in attività legate alle criptovalute o alla blockchain. Per ulteriori informazioni, consulta Regole di eliminazione.

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Impact:Runtime/MaliciousDomainRequest.Reputation

Un'EC2istanza o un contenitore Amazon sta interrogando un dominio a bassa reputazione associato a domini dannosi noti.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che l'EC2istanza o il contenitore elencato all'interno del tuo AWS ambiente sta interrogando un nome di dominio a bassa reputazione associato a domini o indirizzi IP dannosi noti. Ad esempio, i domini possono essere associati a un indirizzo IP sinkhole noto. I domini sinkhole sono domini che sono stati precedentemente controllati da un autore di minacce e se vengono inoltrate richieste a questi domini può significare che l'istanza è compromessa. Questi domini possono anche essere correlati a campagne dannose note o algoritmi di generazione di domini.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Un'EC2istanza o un contenitore Amazon sta interrogando un nome di dominio a bassa reputazione di natura sospetta a causa della sua età o della sua scarsa popolarità.

Gravità predefinita: bassa

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che l'EC2istanza o il contenitore elencato all'interno del tuo AWS ambiente sta interrogando un nome di dominio a bassa reputazione sospettato di essere dannoso. Abbiamo notato che le caratteristiche di questo dominio erano coerenti con i domini dannosi osservati in precedenza, tuttavia il nostro modello di reputazione non è stato in grado di collegarlo in modo definitivo a una minaccia nota. Questi domini vengono in genere osservati per la prima volta o ricevono una quantità di traffico ridotta.

I domini a bassa reputazione si basano su un modello di punteggio di reputazione. Questo modello valuta e classifica le caratteristiche di un dominio per determinarne la probabilità di essere dannoso.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Un'EC2istanza o un contenitore Amazon esegue DNS ricerche che si risolvono nel servizio di metadati dell'istanza.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

> **Note**
>
> Attualmente, questo tipo di risultato è supportato solo per l'architettura. AMD64

Questo risultato indica che un'EC2istanza o un contenitore nell' AWS ambiente in uso sta interrogando un dominio che si risolve nell'indirizzo IP dei EC2 metadati (169.254.169.254). Una DNS query di questo tipo può indicare che l'istanza è oggetto di una tecnica di rebinding. DNS Questa

tecnica può essere utilizzata per ottenere metadati da un'EC2istanza, incluse IAM le credenziali associate all'istanza.

DNSIl rebinding consiste nell'indurre un'applicazione in esecuzione sull'EC2istanza a caricare i dati di ritorno da aURL, dove il nome di dominio contenuto nel file si URL risolve nell'indirizzo IP dei metadati (). EC2 `169.254.169.254` Ciò fa sì che l'applicazione acceda ai EC2 metadati e possibilmente li renda disponibili all'aggressore.

È possibile accedere ai EC2 metadati utilizzando il DNS rebinding solo se l'EC2istanza esegue un'applicazione vulnerabile che consente l'iniezione o se qualcuno accede ai metadati URL in un browser Web in esecuzione sull'istanza. URLs EC2

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

In risposta a questo risultato, è necessario valutare se sull'EC2istanza o sul contenitore è in esecuzione un'applicazione vulnerabile o se qualcuno ha utilizzato un browser per accedere al dominio identificato nel risultato. Se la causa principale è un'applicazione vulnerabile, procedi alla correzione della vulnerabilità. Se qualcuno ha navigato nel dominio identificato, blocca il dominio o impedisci agli utenti di accedervi. Se ritieni che questo risultato sia correlato a uno dei casi precedenti, revoca la sessione associata all'EC2istanza.

Alcuni AWS clienti associano intenzionalmente l'indirizzo IP dei metadati a un nome di dominio sui propri server autorevoli. DNS Se questo è il caso del tuo ambiente , ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio di filtro deve utilizzare l'attributo Tipo di risultato con un valore di `UnauthorizedAccess:Runtime/MetaDataDNSRebind`. Il secondo criterio di filtro deve essere il dominio di DNS richiesta o l'ID dell'immagine del contenitore. Il valore del dominio di DNS richiesta deve corrispondere al dominio mappato all'indirizzo IP dei metadati (). `169.254.169.254` Per informazioni sulla creazione di regole di eliminazione, consulta Regole di eliminazione.

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/NewBinaryExecuted

È stato eseguito un file binario appena creato o modificato di recente in un container.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo esito segnala che è stato eseguito un file binario appena creato o modificato di recente in un container. Ti consigliamo di mantenere i container non modificabili in fase di runtime. Inoltre, i file binari, gli script e le librerie non devono essere creati o modificati durante il ciclo di vita del container. Questo comportamento indica che un malintenzionato che ha ottenuto l'accesso al contenitore ha scaricato ed eseguito malware o altro software come parte della potenziale compromissione. Sebbene questo tipo di attività possa essere indice di una compromissione, è anche un modello di utilizzo comune. Pertanto, GuardDuty utilizza meccanismi per identificare i casi sospetti di questa attività e genera questo tipo di risultati solo per i casi sospetti.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/DockerSocketAccessed

Un processo all'interno di un container comunica con il daemon Docker utilizzando il socket Docker.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Il socket Docker è un socket di dominio Unix utilizzato da daemon Docker (`dockerd`) per comunicare con i propri client. Un client può eseguire varie operazioni, come la creazione di container comunicando con il daemon Docker tramite il socket Docker. È sospetto che un processo del container acceda al socket Docker. Un processo del container può sfuggire ad esso e ottenere un accesso a livello di host comunicando con il socket Docker e creando un container privilegiato.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/RuncContainerEscape

È stato rilevato un tentativo di fuga dal contenitore tramite RunC.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

RunC è il runtime di container di basso livello utilizzato dai runtime di container di alto livello, come Docker e Containerd, per generare ed eseguire contenitori. RunC viene sempre eseguito con i privilegi di root perché deve eseguire l'operazione di basso livello di creazione di un contenitore. Un autore di minacce può ottenere l'accesso a livello di host modificando o sfruttando una vulnerabilità nel binario RunC.

Questa scoperta rileva la modifica del binario RunC e i potenziali tentativi di sfruttare le seguenti vulnerabilità RunC:

- CVE-2019-5736— Lo sfruttamento di CVE-2019-5736 implica la sovrascrittura del binario RunC dall'interno di un contenitore. Questa scoperta viene richiamata quando il binario RunC viene modificato da un processo all'interno di un contenitore.
- CVE-2024-21626— Lo sfruttamento di CVE-2024-21626 implica l'impostazione della directory di lavoro corrente (CWD) o di un contenitore su un descrittore di file aperto. `/proc/self/fd/`*`FileDescriptor`* Questo risultato viene richiamato quando viene rilevato un processo contenitore con una directory di lavoro corrente sotto`/proc/self/fd/`, ad esempio. `/proc/self/fd/7`

Questo risultato può indicare che un malintenzionato ha tentato di sfruttare uno dei seguenti tipi di contenitori:

- Un nuovo container con un'immagine controllata dall'utente malintenzionato.
- Un contenitore esistente accessibile all'attore con autorizzazioni di scrittura sul binario RunC a livello di host.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

È stato rilevato un tentativo di fuga dal container tramite il CGroups release agent.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questo esito segnala che è stato rilevato un tentativo di modificare un file dell'agente di rilascio del gruppo di controllo (cgroup). Linux utilizza i gruppi di controllo (cgroup) per limitare, tenere in considerazione e isolare l'utilizzo delle risorse di una raccolta di processi. Ogni cgroup ha un file dell'agente di rilascio (`release_agent`), uno script che Linux esegue quando termina un processo all'interno del cgroup. Il file dell'agente di rilascio viene sempre eseguito a livello di host. Un autore di minacce all'interno di un container può sfuggire all'host scrivendo comandi arbitrari nel file dell'agente di rilascio che appartiene a un cgroup. Al termine di un processo all'interno di questo cgroup, i comandi scritti dall'autore vengono eseguiti.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Proc

È stata rilevata un'iniezione di processo utilizzando il filesystem proc in un contenitore o in un'istanza Amazon. EC2

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

L'iniezione di processo è una tecnica utilizzata dagli autori delle minacce per iniettare codice nei processi in modo da eludere le difese e cercare di aumentare i privilegi. Il file system proc (procfs) è un particolare file system in Linux che presenta la memoria virtuale del processo come file. Il percorso di questo file è `/proc/PID/mem`, in cui `PID` è l'ID univoco del processo. Un autore di minacce può scrivere su questo file per iniettare codice nel processo. Questo esito identifica potenziali tentativi di scrittura sul file in questione.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

È stata rilevata un'iniezione di processo utilizzando la chiamata di sistema ptrace in un contenitore o in un'EC2istanza Amazon.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

L'iniezione di processo è una tecnica utilizzata dagli autori delle minacce per iniettare codice nei processi in modo da eludere le difese e cercare di aumentare i privilegi. Un processo può utilizzare la chiamata di sistema ptrace per iniettare codice in un altro processo. Questo esito identifica un potenziale tentativo di iniettare codice in un processo utilizzando la chiamata di sistema ptrace.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

È stata rilevata un'iniezione di processo tramite scrittura diretta nella memoria virtuale in un contenitore o in un'EC2istanza Amazon.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

L'iniezione di processo è una tecnica utilizzata dagli autori delle minacce per iniettare codice nei processi in modo da eludere le difese e cercare di aumentare i privilegi. Un processo può utilizzare una chiamata di sistema, ad esempio `process_vm_writev`, per iniettare codice direttamente nella memoria virtuale di un altro processo. Questo esito identifica un potenziale tentativo di iniettare codice in un processo utilizzando una chiamata di sistema per scrivere nella memoria virtuale del processo stesso.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/ReverseShell

Un processo in un contenitore o in un'EC2istanza Amazon ha creato una shell inversa.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Una shell (interprete di comandi) inversa è una sessione di shell creata su una connessione avviata dall'host di destinazione all'host dell'attore, ossia l'opposto di una normale shell (interprete di comandi), che viene invece avviata dall'host dell'attore all'host di destinazione. Gli autori delle minacce creano una shell (interprete di comandi) inversa per eseguire comandi sulla destinazione dopo aver ottenuto l'accesso iniziale. Questo esito identifica un potenziale tentativo di creare una shell (interprete di comandi) inversa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il tipo di risorsa potrebbe essere stato compromesso.

DefenseEvasion:Runtime/FilelessExecution

Un processo in un contenitore o in un'EC2istanza Amazon esegue codice dalla memoria.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo esito segnala un processo eseguito utilizzando un file eseguibile in memoria su disco. Si tratta di una tecnica comune di evasione della difesa in cui il file eseguibile dannoso non viene scritto sul disco per eludere il rilevamento basato sulla scansione del file system. Sebbene questa sia una tecnica utilizzata dal malware, presenta anche alcuni casi d'uso legittimi. Uno degli esempi è un compilatore just-in-time (JIT) che scrive codice compilato in memoria e lo esegue dalla memoria.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Impact:Runtime/CryptoMinerExecuted

Un container o un'EC2istanza Amazon sta eseguendo un file binario associato a un'attività di mining di criptovalute.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un contenitore o un'EC2istanza nel tuo AWS ambiente sta eseguendo un file binario associato a un'attività di mining di criptovalute. Gli autori delle minacce potrebbero cercare di assumere il controllo delle risorse di calcolo per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

L'agente di runtime monitora gli eventi provenienti da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza Tipo di risorsa nel pannello dei risultati della GuardDuty console.

Raccomandazioni per la correzione:

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console e vediCorrezione dei risultati del Runtime Monitoring.

Execution:Runtime/NewLibraryLoaded

Una libreria appena creata o modificata di recente è stata caricata da un processo all'interno di un container.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questo esito segnala che una libreria è stata creata o modificata all'interno di un container durante il runtime e caricata da un processo in esecuzione all'interno del container. La best practice è quella di mantenere i container non modificabili in fase di runtime e di non creare o modificare i file binari, gli script e le librerie durante il ciclo di vita del container. Il caricamento di una libreria appena creata o modificata in un container può indicare attività sospette. Questo comportamento indica che un

utente malintenzionato ha potenzialmente ottenuto l'accesso al container e che ha scaricato ed eseguito malware o altro software come parte della potenziale compromissione. Sebbene questo tipo di attività possa essere indice di un compromesso, è anche un modello di utilizzo comune. Pertanto, GuardDuty utilizza meccanismi per identificare i casi sospetti di questa attività e genera questo tipo di risultati solo per i casi sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Un processo all'interno di un container ha montato un file system host in fase di runtime.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Diverse tecniche di evasione da un container prevedono il montaggio di un file system host al suo interno in fase di runtime. Questo esito segnala che un processo all'interno di un container ha potenzialmente tentato di montare un file system host, il che potrebbe indicare un tentativo di sfuggire all'host.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/UserfaultfdUsage

Un processo ha utilizzato chiamate di sistema **`userfaultfd`** per gestire errori di pagina nello spazio utente.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

In genere, gli errori di pagina vengono gestiti dal kernel nello spazio corrispondente. Tuttavia, la chiamata di sistema `userfaultfd` consente a un processo di gestire gli errori di pagina su un file system nello spazio utente. Questa funzionalità è utile perché abilita l'implementazione di file system nello spazio utente. D'altra parte, può anche essere usata da un processo potenzialmente dannoso per interrompere il kernel dallo spazio utente. L'interruzione del kernel tramite la chiamata di sistema `userfaultfd` è una tecnica di sfruttamento comune volta a estendere le finestre di gara durante lo sfruttamento delle condizioni di gara del kernel. L'uso di `userfaultfd` può indicare attività sospette sull'istanza Amazon Elastic Compute Cloud EC2 (Amazon).

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/SuspiciousTool

Un container o un'EC2istanza Amazon esegue un file o uno script binario che viene spesso utilizzato in scenari di sicurezza offensivi come il pentesting engagement.

Gravità predefinita: variabile

La gravità di questo risultato può essere elevata o bassa, a seconda che lo strumento sospetto rilevato sia considerato a duplice uso o destinato esclusivamente a un uso offensivo.

- Funzionalità: monitoraggio del runtime

Questo risultato indica che uno strumento sospetto è stato eseguito su un'EC2istanza o un contenitore all'interno del vostro ambiente. AWS Ciò include gli strumenti utilizzati nelle interazioni di pentesting, noti anche come strumenti di backdoor, scanner di rete e sniffer di rete. Tutti questi strumenti possono essere utilizzati in contesti benigni, ma sono spesso utilizzati anche da autori di

minacce con intenti malevoli. L'osservazione di strumenti di sicurezza offensivi potrebbe indicare che l'EC2istanza o il contenitore associati sono stati compromessi.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/SuspiciousCommand

Un comando sospetto è stato eseguito su un'EC2istanza Amazon o su un contenitore indicativo di una compromissione.

Gravità predefinita: variabile

A seconda dell'impatto del pattern dannoso osservato, la gravità di questo tipo di rilevamento potrebbe essere bassa, media o alta.

- Funzionalità: monitoraggio del runtime

Questo risultato indica che è stato eseguito un comando sospetto e indica che un'EC2istanza Amazon o un contenitore nel tuo AWS ambiente sono stati compromessi. Ciò potrebbe significare che un file è stato scaricato da una fonte sospetta e quindi eseguito oppure che un processo in esecuzione mostra uno schema dannoso noto nella riga di comando. Ciò indica inoltre che sul sistema è in esecuzione del malware.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

DefenseEvasion:Runtime/SuspiciousCommand

Un comando è stato eseguito sull'EC2istanza Amazon o su un contenitore elencato, tenta di modificare o disabilitare un meccanismo di difesa Linux, come un firewall o servizi di sistema essenziali.

Gravità predefinita: variabile

A seconda del meccanismo di difesa modificato o disabilitato, la gravità di questo tipo di risultato può essere alta, media o bassa.

- Funzionalità: monitoraggio del runtime

Questa scoperta indica che è stato eseguito un comando che tenta di nascondere un attacco ai servizi di sicurezza del sistema locale. Ciò include azioni come la disabilitazione del firewall Unix, la modifica delle tabelle IP locali, la rimozione di crontab voci, la disabilitazione di un servizio locale o l'assunzione della funzione. `LDPreload` Qualsiasi modifica è altamente sospetta e rappresenta un potenziale indicatore di compromissione. Pertanto, questi meccanismi rilevano o impediscono ulteriori compromissioni del sistema.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nei dettagli dei risultati nella console. GuardDuty

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

DefenseEvasion:Runtime/PtraceAntiDebugging

Un processo in un contenitore o in un'EC2istanza Amazon ha eseguito una misura anti-debug utilizzando la chiamata di sistema ptrace.

Gravità predefinita: bassa

- Funzionalità: monitoraggio del runtime

Questo risultato mostra che un processo in esecuzione su un'EC2istanza Amazon o su un contenitore all'interno del tuo AWS ambiente ha utilizzato la chiamata di sistema ptrace con l'`PTRACE_TRACEME`opzione. Questa attività provocherebbe il distacco di un debugger collegato dal processo in esecuzione. Se non è collegato alcun debugger, non ha alcun effetto. Tuttavia, l'attività di per sé solleva sospetti. Ciò potrebbe indicare che sul sistema è in esecuzione del malware. Il malware utilizza spesso tecniche anti-debug per eludere l'analisi e queste tecniche possono essere rilevate in fase di esecuzione.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/MaliciousFileExecuted

Un file eseguibile dannoso noto è stato eseguito su un'EC2istanza o un contenitore Amazon.

Gravità predefinita: alta

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un file eseguibile dannoso noto è stato eseguito su un'EC2istanza Amazon o su un contenitore all'interno del tuo AWS ambiente. Si tratta di un forte indicatore del fatto che l'istanza o il contenitore sono stati potenzialmente compromessi e che il malware è stato eseguito.

Il malware utilizza spesso tecniche anti-debugging per eludere l'analisi e queste tecniche possono essere rilevate in fase di esecuzione.

GuardDuty esamina l'attività e il contesto di runtime correlati in modo da generare questo risultato solo quando l'attività e il contesto associati sono potenzialmente sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Execution:Runtime/SuspiciousShellCreated

Un servizio di rete o un processo accessibile dalla rete su un'EC2istanza Amazon o in un contenitore ha avviato un processo shell interattivo.

Gravità predefinita: bassa

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un servizio accessibile in rete su un'EC2istanza Amazon o in un contenitore all'interno del tuo AWS ambiente ha lanciato una shell interattiva. In determinate circostanze, questo scenario può indicare un comportamento successivo allo sfruttamento. Le shell interattive consentono agli aggressori di eseguire comandi arbitrari su un'istanza o un contenitore compromessi.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella console. GuardDuty È possibile visualizzare le informazioni sul processo accessibili dalla rete nei dettagli del processo principale.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

PrivilegeEscalation:Runtime/ElevationToRoot

Un processo in esecuzione sull'EC2istanza o sul contenitore Amazon elencato ha assunto i privilegi di root.

Gravità predefinita: media

- Funzionalità: monitoraggio del runtime

Questa scoperta ti informa che un processo in esecuzione sull'Amazon elencato EC2 o nel contenitore elencato all'interno del tuo AWS ambiente ha assunto i privilegi di root a causa di un'esecuzione binaria insolita o sospetta`setuid`. Ciò indica che un processo in esecuzione è stato potenzialmente compromesso, EC2 ad esempio a causa di un exploit o di uno sfruttamento. `setuid` Utilizzando i privilegi di root, l'aggressore può potenzialmente eseguire comandi sull'istanza o sul contenitore.

Sebbene GuardDuty sia progettato per non generare questo tipo di risultati per attività che richiedono l'uso regolare del `sudo` comando, lo genererà quando identificherà l'attività come insolita o sospetta.

GuardDuty esamina l'attività e il contesto di runtime correlati e genera questo tipo di risultato solo quando l'attività e il contesto associati sono insoliti o sospetti.

L'agente di runtime monitora gli eventi provenienti da più risorse. Per identificare la risorsa interessata, visualizza il tipo di risorsa nei dettagli dei risultati nella GuardDuty console.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la risorsa potrebbe essere stata compromessa. Per ulteriori informazioni, consulta Correzione dei risultati del Runtime Monitoring.

Protezione da malware per tipi di ricerca EC2

GuardDuty Malware Protection for EC2 fornisce un'unica funzionalità di Malware Protection for EC2 che individua tutte le minacce rilevate durante la scansione di un'istanza EC2 o di un carico di lavoro di un container. L'esito include il numero totale di rilevamenti effettuati durante la scansione e, in base alla gravità, fornisce dettagli sulle 32 minacce rilevate principali. A differenza di altri GuardDuty risultati, i risultati di Malware Protection for EC2 non vengono aggiornati quando viene nuovamente scansionata la stessa istanza EC2 o lo stesso carico di lavoro dello stesso container.

Per ogni scansione che rileva il malware viene generato un nuovo risultato di Malware Protection for EC2. I risultati di Malware Protection for EC2 includono informazioni sulla scansione corrispondente che ha prodotto il risultato e sul GuardDuty risultato che ha avviato la scansione. In questo modo, la correlazione tra il comportamento sospetto e il malware rilevato è più semplice.

> **Note**
>
> Quando GuardDuty rileva attività dannose su un carico di lavoro di un container, Malware Protection for EC2 non genera un risultato a livello EC2.

I seguenti risultati sono specifici di GuardDuty Malware Protection for EC2.

Argomenti

Execution:EC2/MaliciousFile

È stato rilevato un file dannoso su un'istanza EC2.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Caratteristica: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file dannosi sull'istanza EC2 elencata all'interno dell'ambiente in uso. AWS Questa istanza elencata potrebbe essere compromessa. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Execution:ECS/MaliciousFile

È stato rilevato un file dannoso su un cluster ECS.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file dannosi su un carico di lavoro di un container che appartiene a un cluster ECS. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il container appartenente al cluster ECS potrebbe essere compromesso. Per ulteriori informazioni, consulta Riparazione di un cluster potenzialmente compromesso ECS.

Execution:Kubernetes/MaliciousFile

È stato rilevato un file dannoso su un cluster Kubernetes.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Caratteristica: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file dannosi su un carico di lavoro di container che appartiene a un cluster Kubernetes. Se questo cluster è gestito da EKS, i dettagli degli esiti forniranno informazioni aggiuntive sulla risorsa EKS interessata. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Execution:Container/MaliciousFile

È stato rilevato un file dannoso in un container autonomo.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file dannosi sul carico di lavoro di un container e non sono state identificate informazioni sul cluster. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta Riparazione di un contenitore autonomo potenzialmente compromesso.

Execution:EC2/SuspiciousFile

È stato rilevato un file sospetto su un'istanza EC2.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file sospetti su un'istanza EC2. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo `SuspiciousFile` indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo

legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se ti aspetti di vederlo nel tuo ambiente. AWS Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Execution:ECS/SuspiciousFile

È stato rilevato un file sospetto su un cluster ECS.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file sospetti su un contenitore che appartiene a un cluster ECS. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo `SuspiciousFile` indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se prevedi di vederlo nel tuo ambiente. AWS Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il container appartenente al cluster ECS potrebbe essere compromesso. Per ulteriori informazioni, consulta Riparazione di un cluster potenzialmente compromesso ECS.

Execution:Kubernetes/SuspiciousFile

È stato rilevato un file sospetto su un cluster Kubernetes.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file sospetti su un contenitore che appartiene a un cluster Kubernetes. Se questo cluster è gestito da EKS, i dettagli degli esiti forniranno informazioni aggiuntive sull'EKS interessato. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo `SuspiciousFile` indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se prevedi di vederlo nel tuo ambiente. AWS Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta Correzione degli esiti del monitoraggio dei log di audit EKS.

Execution:Container/SuspiciousFile

È stato rilevato un file sospetto in un container autonomo.

Gravità predefinita: varia a seconda della minaccia rilevata.

- Funzionalità: EBS Malware Protection

Questo risultato indica che la scansione GuardDuty Malware Protection for EC2 ha rilevato uno o più file sospetti su un contenitore senza informazioni sul cluster. Per ulteriori informazioni, consulta la sezione Minacce rilevate nei dettagli degli esiti.

I rilevamenti di tipo `SuspiciousFile` indicano che su una risorsa interessata sono presenti programmi potenzialmente indesiderati come adware, spyware o strumenti a duplice uso. Questi programmi potrebbero avere un impatto negativo sulla risorsa o essere utilizzati da utenti malintenzionati per scopi dannosi. Ad esempio, gli strumenti di rete possono essere utilizzati in modo legittimo o in modo dannoso dagli avversari come strumenti di hacking per cercare di compromettere le risorse.

Quando viene rilevato un file sospetto, valuta se prevedi di vederlo nel tuo ambiente. AWS Se il file non è previsto, segui la procedura descritta nella sezione successiva.

Raccomandazioni per la correzione:

Se questa attività non è prevista, il carico di lavoro del container potrebbe essere compromesso. Per ulteriori informazioni, consulta Riparazione di un contenitore autonomo potenzialmente compromesso.

Protezione da malware per tipo di ricerca S3

GuardDuty genera un risultato solo quando rileva una potenziale minaccia alla sicurezza nel tuo. Account AWS Un risultato di Malware Protection for S3 indica che l'oggetto caricato che ha avviato la scansione antimalware contiene un file potenzialmente dannoso.

Affinché Amazon GuardDuty generi un risultato nel tuo Account AWS, abilita entrambi GuardDuty e Malware Protection for S3. La migliore pratica è abilitare prima Malware Protection for S3 GuardDuty e poi. Se per te questo ordine è diverso, assicurati di abilitarlo GuardDuty prima che un oggetto S3 venga caricato nel tuo bucket protetto.

> **Note**
>
> GuardDuty non riesco a generare un risultato per un oggetto S3 che è stato scansionato prima dell'attivazione. GuardDuty Per scansionare un oggetto S3 esistente, puoi caricarlo di nuovo.

Object:S3/MaliciousFile

È stato rilevato un file dannoso su un oggetto S3 scansionato.

Gravità predefinita: alta

- Funzionalità: protezione da malware per S3

Questo risultato indica che una scansione antimalware ha rilevato che l'oggetto S3 elencato è dannoso. Per ulteriori informazioni, consulta la sezione Minacce rilevate nel pannello dei dettagli della ricerca.

Correzione dei consigli:

Se questo risultato è inaspettato, l'oggetto S3 è potenzialmente dannoso. Per informazioni sui passaggi di riparazione consigliati, consulta. Correzione di un oggetto S3 potenzialmente dannoso

Tipi di esiti della Protezione RDS di GuardDuty

La Protezione RDS di GuardDuty rileva eventuali comportamenti di accesso anomali sull'istanza di database. Gli esiti seguenti sono specifici per il Database Amazon Aurora e Amazon supportati RDS e avranno un Tipo di risorsa di `RDSDBInstance`. La gravità e i dettagli dei risultati saranno diversi in base al tipo di risultato.

Argomenti

- CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin
- CredentialAccess:RDS/AnomalousBehavior.FailedLogin
- CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce
- CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin
- CredentialAccess:RDS/MaliciousIPCaller.FailedLogin
- Discovery:RDS/MaliciousIPCaller
- CredentialAccess:RDS/TorIPCaller.SuccessfulLogin
- CredentialAccess:RDS/TorIPCaller.FailedLogin
- Discovery:RDS/TorIPCaller

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account in modo anomalo.

Gravità predefinita: variabile

> **Note**
>
> A seconda del comportamento anomalo associato a questo esito, la gravità predefinita può essere bassa, media e alta.
>
> - Bassa: se il nome utente associato a questo esito ha effettuato l'accesso da un indirizzo IP associato a una rete privata.
> - Media: se il nome utente associato a questo esito ha effettuato l'accesso da un indirizzo IP pubblico.
> - Alta: se viene individuata una serie di tentativi di accesso falliti da indirizzi IP pubblici, indicativo di policy di accesso troppo permissive.

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che è stato osservato un accesso anomalo riuscito a un database RDS nel tuo ambiente AWS. Ciò può indicare che un utente che non era mai stato rilevato in precedenza ha effettuato l'accesso a un database RDS per la prima volta. Uno scenario comune consiste nell'accesso da parte di un utente interno a un database a cui accedono le applicazioni a livello di programmazione, ma non i singoli utenti.

Questo accesso riuscito è stato identificato come anomalo dal modello di machine learning (ML) di GuardDuty per il rilevamento delle anomalie. Il modello di ML valuta tutti gli eventi di accesso al database nel tuo Database Amazon Aurora e Amazon supportati RDS e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori dell'attività di accesso RDS, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e i dettagli specifici di connessione al database utilizzati. Per informazioni sugli eventi di accesso potenzialmente insoliti, consulta RDSanomalie basate sull'attività di accesso.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, ti consigliamo di modificare la password dell'utente del database e di esaminare i log di audit disponibili per le attività eseguite dall'utente anomalo. Gli esiti di gravità media e alta possono indicare che la policy di accesso al database è troppo permissiva e che le credenziali dell'utente potrebbero essere state esposte o compromesse. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza

per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Uno o più tentativi di accesso insoliti falliti sono stati osservati su un database RDS del tuo account.

Gravità predefinita: bassa

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che sono stati osservati uno o più accessi anomali falliti su un database RDS nel tuo ambiente AWS. Un tentativo di accesso fallito da indirizzi IP pubblici può indicare che il database RDS del tuo account è stato oggetto di un tentativo di attacco di forza bruta da parte di un utente potenzialmente malintenzionato.

Questi accessi falliti sono stati identificati come anomali dal modello di machine learning (ML) di GuardDuty per il rilevamento delle anomalie. Il modello di ML valuta tutti gli eventi di accesso al database nel tuo Database Amazon Aurora e Amazon supportati RDS e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori dell'attività di accesso RDS, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e i dettagli specifici di connessione al database utilizzati. Per informazioni sulle attività di accesso RDS potenzialmente insolite, consulta RDSanomalie basate sull'attività di accesso.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che il database è esposto pubblicamente o che la policy di accesso al database è troppo permissiva. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account da un indirizzo IP pubblico in modo anomalo dopo una serie di tentativi di accesso insoliti falliti.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che su un database RDS nel tuo ambiente AWS è stato osservato un accesso anomalo indicativo di un attacco di forza bruta riuscito. Prima di un accesso anomalo riuscito, è stata osservata una serie di tentativi di accesso insoliti falliti. Ciò indica che l'utente e la password associati al database RDS del tuo account potrebbero essere stati compromessi e che un utente potenzialmente malintenzionato potrebbe aver effettuato l'accesso al database RDS.

Questo accesso di forza bruta riuscito è stato identificato come anomalo dal modello di machine learning (ML) di GuardDuty per il rilevamento delle anomalie. Il modello di ML valuta tutti gli eventi di accesso al database nel tuo Database Amazon Aurora e Amazon supportati RDS e identifica gli eventi anomali associati alle tecniche utilizzate dagli avversari. Il modello di ML tiene traccia di vari fattori dell'attività di accesso RDS, ad esempio l'utente che ha effettuato la richiesta, la posizione da cui è stata effettuata la richiesta e i dettagli specifici di connessione al database utilizzati. Per informazioni sulle attività di accesso RDS potenzialmente insolite, consulta RDSanomalie basate sull'attività di accesso.

Raccomandazioni per la correzione:

Questa attività indica che le credenziali del database potrebbero essere state esposte o compromesse. Ti consigliamo di modificare la password dell'utente del database associato e di esaminare i log di audit disponibili per le attività eseguite dall'utente potenzialmente compromesso. Una serie di tentativi di accesso insoliti falliti indica che la policy di accesso al database è troppo permissiva o che il database potrebbe essere stato esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account da un indirizzo IP dannoso noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che si è verificata un'attività di accesso RDS riuscita a partire da un indirizzo IP associato a un'attività dannosa nota nel tuo ambiente AWS. Ciò indica che l'utente e la password associati al database RDS del tuo account potrebbero essere stati compromessi e che un utente potenzialmente malintenzionato potrebbe aver effettuato l'accesso al database RDS.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che le credenziali dell'utente sono state esposte o compromesse. Ti consigliamo di modificare la password dell'utente del database associato e di esaminare i log di audit disponibili per le attività eseguite dall'utente compromesso. Questa attività può anche indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Un indirizzo IP associato a un'attività dannosa nota ha tentato di accedere a un database RDS del tuo account, senza riuscirci.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che un indirizzo IP associato ad attività dannose note ha tentato di accedere a un database RDS nel tuo ambiente AWS, ma non è riuscito a fornire il nome utente o la password corretti. Ciò indica che un utente potenzialmente malintenzionato potrebbe tentare di compromettere il database RDS del tuo account.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti.

Discovery:RDS/MaliciousIPCaller

Un database RDS del tuo account è stato sottoposto a probing da un indirizzo IP associato a un'attività dannosa nota, ma non è stato effettuato alcun tentativo di autenticazione.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che un database RDS nel tuo ambiente AWS è stato sottoposto a probing da un indirizzo IP associato a un'attività dannosa nota, anche se non è stato effettuato alcun tentativo di accesso. Ciò può indicare che un utente potenzialmente malintenzionato è alla ricerca di un'infrastruttura accessibile pubblicamente.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Un utente ha effettuato correttamente l'accesso a un database RDS del tuo account dall'indirizzo IP di un nodo di uscita Tor.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che un utente ha effettuato correttamente l'accesso a un database RDS nel tuo ambiente AWS dall'indirizzo IP di un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relè tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un

accesso non autorizzato alle risorse RDS del tuo account con l'intento di nascondere la vera identità dell'utente anonimo.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che le credenziali dell'utente sono state esposte o compromesse. Ti consigliamo di modificare la password dell'utente del database associato e di esaminare i log di audit disponibili per le attività eseguite dall'utente compromesso. Questa attività può anche indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Un indirizzo IP Tor ha tentato di accedere a un database RDS del tuo account, senza riuscirci.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che l'indirizzo IP di un nodo di uscita Tor ha tentato di accedere a un database RDS nel tuo ambiente AWS, ma non è riuscito a fornire il nome utente o la password corretti. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relè tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse RDS del tuo account con l'intento di nascondere la vera identità dell'utente anonimo.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti.

Discovery:RDS/TorIPCaller

Un database RDS del tuo account è stato sottoposto a probing dall'indirizzo IP di un nodo di uscita Tor, ma non è stato effettuato alcun tentativo di autenticazione.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di accesso RDS

Questo esito segnala che un database RDS nel tuo ambiente AWS è stato sottoposto a probing dall'indirizzo IP di un nodo di uscita Tor, anche se non è stato effettuato alcun tentativo di accesso. Ciò può indicare che un utente potenzialmente malintenzionato è alla ricerca di infrastrutture accessibili pubblicamente. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relè tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. Ciò può indicare un accesso non autorizzato alle risorse RDS del tuo account con l'intento di nascondere la vera identità dell'utente potenzialmente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il database associato, può indicare che la policy di accesso al database è troppo permissiva o che il database è esposto pubblicamente. Ti consigliamo di collocare il database in un VPC privato e di limitare le regole del gruppo di sicurezza per consentire il traffico solo dalle origini necessarie. Per ulteriori informazioni, consulta Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti.

Tipi di esiti della Protezione Lambda

Questa sezione descrive i tipi di esiti specifici delle tue risorse AWS Lambda e per i quali il `resourceType` è elencato come `Lambda`. Per tutti gli esiti di Lambda, ti consigliamo di esaminare la risorsa in questione e determinare se si comporta nel modo previsto. Se l'attività è autorizzata, puoi utilizzare le Regole di eliminazione o gli Elenchi di indirizzi IP affidabili e gli elenchi minacce per prevenire notifiche false positive per quella risorsa.

Se l'attività non è prevista, la best practice di sicurezza consiste nel presupporre che Lambda sia stata potenzialmente compromessa e seguire le raccomandazioni per la correzione.

Argomenti

- Backdoor:Lambda/C&CActivity.B

- CryptoCurrency:Lambda/BitcoinTool.B
- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient
- UnauthorizedAccess:Lambda/TorRelay

Backdoor:Lambda/C&CActivity.B

Una funzione Lambda esegue una query su un indirizzo IP associato a un server di comando e controllo noto.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che la funzione Lambda elencata all'interno del tuo ambiente AWS esegue una query su un indirizzo IP associato a un server di comando e controllo (C&C) noto. La funzione Lambda associata all'esito generato è potenzialmente compromessa. I server C&C sono computer che inviano comandi ai membri di una botnet.

Una botnet è una raccolta di dispositivi connessi a Internet, come PC, server, dispositivi mobili e dispositivi Internet of Things, infettata e controllata da un tipo comune di malware. Le botnet sono spesso utilizzate per distribuire malware e rubare informazioni sensibili, ad esempio i numeri di carte di credito. A seconda dello scopo e della struttura della botnet, il server C&C potrebbe anche inviare comandi per lanciare un Distributed Denial of Service.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

CryptoCurrency:Lambda/BitcoinTool.B

Una funzione Lambda esegue una query su un indirizzo IP associato a un'attività correlata a una criptovaluta.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che la funzione Lambda elencata nel tuo ambiente AWS esegue una query su un indirizzo IP associato a un'attività correlata a Bitcoin o a un'altra criptovaluta. Gli autori delle minacce potrebbero cercare di assumere il controllo delle funzioni Lambda per riutilizzarle in modo dannoso per il mining non autorizzato di criptovalute.

Raccomandazioni per la correzione:

Se usi questa funzione Lambda per estrarre o gestire criptovaluta o se questa funzione è altrimenti coinvolta in un'attività di blockchain, può trattarsi di un'attività potenzialmente prevista per il tuo ambiente. Se questo è il caso del tuo ambiente AWS, ti consigliamo di impostare una regola di eliminazione per questo esito. La regola di eliminazione deve essere costituita da due criteri di filtro. Il primo criterio deve utilizzare l'attributo tipo di esito con un valore di CryptoCurrency:Lambda/BitcoinTool.B. Il secondo criterio di filtro deve essere il nome della funzione Lambda coinvolta nell'attività di blockchain. Per informazioni sulla creazione di regole di eliminazione, consulta Regole di eliminazione.

Se questa attività non è prevista, la funzione Lambda è potenzialmente compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

Trojan:Lambda/BlackholeTraffic

Una funzione Lambda tenta di comunicare con l'indirizzo IP di un host remoto che è un noto buco nero.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che una funzione Lambda elencata nel tuo ambiente AWS tenta di comunicare con l'indirizzo IP di un buco nero (o sinkhole). I buchi neri sono zone della rete dove il traffico in entrata e in uscita viene eliminato silenziosamente senza che l'origine venga informata del mancato recapito dei dati al destinatario. L'indirizzo IP di un buco nero designa un computer host non in esecuzione o un indirizzo a cui non è stato assegnato alcun host. La funzione Lambda elencata è potenzialmente compromessa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

Trojan:Lambda/DropPoint

Una funzione Lambda tenta di comunicare con l'indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che una funzione Lambda elencata nel tuo ambiente AWS tenta di comunicare con l'indirizzo IP di un host remoto noto per conservare credenziali e altri dati rubati acquisiti tramite malware.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Una funzione Lambda stabilisce connessioni a un indirizzo IP incluso in un elenco minacce personalizzato.

Gravità predefinita: media

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che una funzione Lambda nel tuo ambiente AWS comunica con un indirizzo IP incluso in un elenco minacce che hai caricato. In GuardDuty, un elenco minacce include indirizzi IP dannosi noti. GuardDuty genera esiti in base agli elenchi minacce caricati. Puoi visualizzare i dettagli dell'elenco minacce nei dettagli degli esiti sulla console GuardDuty.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

UnauthorizedAccess:Lambda/TorClient

Una funzione Lambda stabilisce connessioni a un Tor Guard o a un nodo Authority.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che una funzione Lambda nel tuo ambiente AWS stabilisce connessioni a un Tor Guard o a un nodo Authority. Tor è un software che consente la comunicazione anonima. I Tor Guard e i nodi Authority fungono da gateway iniziali per una rete Tor. Questo traffico può indicare che la funzione Lambda è stata potenzialmente compromessa e al momento funge da client su una rete Tor.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

UnauthorizedAccess:Lambda/TorRelay

Una funzione Lambda stabilisce connessioni a una rete Tor come relè Tor.

Gravità predefinita: alta

- Funzionalità: monitoraggio delle attività di rete Lambda

Questo esito segnala che una funzione Lambda nel tuo ambiente AWS stabilisce connessioni a una rete Tor in un modo che suggerisce che funga da relè Tor. Tor è un software che consente la comunicazione anonima. Tor aumenta consente l'anonimato della comunicazione inoltrando il traffico potenzialmente illecito del client da un relè Tor a un altro.

Raccomandazioni per la correzione:

Se questa attività non è prevista, la funzione Lambda potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di una funzione Lambda potenzialmente compromessa.

Tipi di esiti ritirati

Un esito è una notifica che contiene dettagli su un potenziale problema di sicurezza rilevato da GuardDuty. Per informazioni su importanti modifiche apportate ai tipi di risultati di GuardDuty, tra cui tipi di risultati recentemente aggiunti o ritirati, consulta Cronologia dei documenti per Amazon GuardDuty.

I seguenti tipi di esiti sono stati ritirati e non vengono più generati da GuardDuty.

> **Important**
>
> Non puoi riattivare i tipi di esiti ritirati di GuardDuty.

Argomenti

- Backdoor:EC2/XORDDOS
- Behavior:IAMUser/InstanceLaunchUnusual
- CryptoCurrency:EC2/BitcoinTool.A
- UnauthorizedAccess:IAMUser/UnusualASNCaller

Exfiltration:S3/ObjectRead.Unusual

Un'entità IAM ha richiamato un'API S3 in modo sospetto.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

- Origine dati: eventi di dati di CloudTrail per S3

Questo esito segnala che un'entità IAM nel tuo ambiente AWS effettua chiamate API che coinvolgono un bucket S3 e che differiscono dalla linea di base stabilita per tale entità. La chiamata API utilizzata in questa attività è associata alla fase di esfiltrazione di un attacco, in cui un utente malintenzionato tenta di raccogliere dati. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Impact:S3/PermissionsModification.Unusual

Un'entità IAM ha richiamato un'API per modificare le autorizzazioni su una o più risorse S3.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un'entità IAM effettua chiamate API progettate per modificare le autorizzazioni su uno o più bucket o oggetti nel tuo ambiente AWS. Questa operazione può essere eseguita da un utente malintenzionato per consentire la condivisione di informazioni al di fuori dell'account. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Impact:S3/ObjectDelete.Unusual

Un'entità IAM ha richiamato un'API utilizzata per eliminare i dati in un bucket S3.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito indica che un'entità IAM specifica nel tuo ambiente AWS effettua chiamate API progettate per eliminare i dati nel bucket S3 elencato tramite l'eliminazione del bucket stesso. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Discovery:S3/BucketEnumeration.Unusual

Un'entità IAM ha richiamato un'API S3 utilizzata per scoprire i bucket S3 all'interno della rete.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito indica che un'entità IAM ha richiamato un'API S3 per scoprire i bucket S3 nel tuo ambiente, ad esempio `ListBuckets`. Questo tipo di attività è associato alla fase di scoperta di un attacco in cui l'utente malintenzionato raccoglie informazioni per determinare se il tuo ambiente AWS è suscettibile a un attacco più ampio. Questa attività è sospetta perché il modo in cui l'entità IAM ha richiamato l'API è insolito. Ad esempio, l'entità IAM non aveva mai richiamato questo tipo di API in precedenza oppure l'API è stata richiamata da una posizione insolita.

Raccomandazioni per la correzione:

Se questa attività non è prevista per il principale associato, potrebbe indicare che le credenziali sono state esposte o che le autorizzazioni S3 non sono sufficientemente restrittive. Per ulteriori informazioni, consulta Riparazione di un bucket S3 potenzialmente compromesso.

Persistence:IAMUser/NetworkPermissions

Un'entità IAM ha richiamato un'API comunemente utilizzata per modificare le autorizzazioni di accesso alla rete per gruppi di sicurezza, instradamenti e ACL nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un principale specifico (Utente root dell'account AWS, ruolo IAM o utente) nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando le impostazioni di configurazione della rete vengono modificate in circostanze sospette, ad esempio quando un principale richiama l'API `CreateSecurityGroup` senza averlo mai fatto in precedenza. Gli utenti malintenzionati spesso tentano di modificare i gruppi di sicurezza per consentire un determinato traffico in entrata su varie porte e migliorare la capacità di accedere all'istanza EC2.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Persistence:IAMUser/ResourcePermissions

Un principale ha richiamato un'API comunemente utilizzata per modificare le policy di accesso di varie risorse nel tuo Account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un principale specifico (Utente root dell'account AWS, ruolo IAM o utente) nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando viene rilevata una modifica alle policy o alle autorizzazioni collegate alle risorse AWS, ad esempio quando un principale nel tuo ambiente AWS richiama l'API `PutBucketPolicy` senza averlo mai fatto in precedenza. Alcuni servizi, come Amazon S3, supportano le autorizzazioni collegate alle risorse che concedono a uno o più principali di accedere alla risorsa. Con le credenziali rubate, gli utenti malintenzionati possono modificare le policy collegate a una risorsa per potervi accedere.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Persistence:IAMUser/UserPermissions

Un principale ha richiamato un'API comunemente utilizzata per aggiungere, modificare o eliminare utenti, gruppi o policy IAM nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un principale specifico (Utente root dell'account AWS, ruolo IAM o utente) nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato da modifiche sospette apportate alle autorizzazioni collegate agli utenti nel tuo ambiente AWS, ad esempio quando un principale dell'ambiente AWS richiama l'API `AttachUserPolicy` senza averlo mai fatto in precedenza. Gli utenti malintenzionati possono utilizzare le credenziali rubate per creare nuovi utenti, aggiungere policy di accesso agli utenti esistenti o creare chiavi di accesso per massimizzare l'accesso a un account, anche se il punto di accesso originale è chiuso. Ad esempio, il proprietario dell'account potrebbe accorgersi del furto di un determinato utente IAM o di una password ed eliminarli dall'account. Tuttavia, potrebbe non eliminare altri utenti creati da un principale amministratore creato in modo fraudolento, lasciando il loro account AWS accessibile all'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

PrivilegeEscalation:IAMUser/AdministrativePermissions

Un principale ha tentato di assegnare una policy molto permissiva a se stessa.

Gravità predefinita: bassa*

> **Note**
>
> La gravità di questo esito è bassa se il tentativo di escalation dei privilegi non è andato a buon fine e media in caso contrario.

Questo esito indica che un'entità IAM specifica nel tuo ambiente AWS ha un comportamento che può essere indicativo di un attacco di escalation dei privilegi. Questo esito viene attivato quando un utente o un ruolo IAM tentano di autoassegnarsi una policy molto permissiva. Se l'utente o il ruolo in questione non intende godere di privilegi amministrativi, le credenziali dell'utente possono essere state compromesse o le autorizzazioni del ruolo potrebbero non essere configurate correttamente.

Gli utenti malintenzionati utilizzeranno le credenziali rubate per creare nuovi utenti, aggiungere policy di accesso agli utenti esistenti o creare chiavi di accesso per massimizzare l'accesso a un account, anche se il punto di accesso originale è chiuso. Ad esempio, il proprietario dell'account potrebbe notare che una determinata credenziale di un utente IAM è stata rubata ed eliminata dall'account, ma potrebbe non eliminare altri utenti creati da un principale amministratore creato in modo fraudolento, lasciando i loro account AWS ancora accessibili all'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/NetworkPermissions

Un principale ha richiamato un'API comunemente utilizzata per modificare le autorizzazioni di accesso alla rete per gruppi di sicurezza, instradamenti e ACL nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un principale specifico (Utente root dell'account AWS, ruolo IAM o utente) nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando le autorizzazioni di accesso alle risorse nel tuo AWS sono sottoposte a probing in circostanze sospette. Ad esempio, se un principale ha richiamato l'API `DescribeInstances` senza averlo mai fatto in precedenza. Un utente malintenzionato potrebbe utilizzare le credenziali rubate per eseguire questo tipo di ricognizione delle risorse AWS allo scopo di trovare credenziali più utili o determinare le capacità delle credenziali di cui dispone.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/ResourcePermissions

Un principale ha richiamato un'API comunemente utilizzata per modificare le policy di accesso di varie risorse nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito segnala che un principale specifico (Utente root dell'account AWS, ruolo IAM o utente) nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questa entità di sicurezza non ha mai chiamato questa API in precedenza.

Questo esito viene attivato quando le autorizzazioni di accesso alle risorse nel tuo AWS sono sottoposte a probing in circostanze sospette. Ad esempio, se un principale ha richiamato l'API `DescribeInstances` senza averlo mai fatto in precedenza. Un utente malintenzionato potrebbe utilizzare le credenziali rubate per eseguire questo tipo di ricognizione delle risorse AWS allo scopo di trovare credenziali più utili o determinare le capacità delle credenziali di cui dispone.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Recon:IAMUser/UserPermissions

Un principale ha richiamato un'API comunemente utilizzata per aggiungere, modificare o eliminare utenti, gruppi o policy IAM nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito viene attivato quando le autorizzazioni utente nel tuo ambiente AWS sono sottoposte a probing in circostanze sospette. Ad esempio, se un principale (Utente root dell'account AWS, ruolo IAM o utente IAM) ha richiamato l'API `ListInstanceProfilesForRole` senza averlo mai fatto in precedenza. Un utente malintenzionato potrebbe utilizzare le credenziali rubate per eseguire

questo tipo di ricognizione delle risorse AWS allo scopo di trovare credenziali più utili o determinare le capacità delle credenziali di cui dispone.

Questo esito indica che un principale specifico nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questo primcipal non ha mai chiamato questa API in precedenza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

ResourceConsumption:IAMUser/ComputeResources

Un principale ha chiamato un'API comunemente utilizzata per avviare risorse di calcolo come istanze EC2.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito viene generato quando le istanze EC2 nell'account elencato all'interno del tuo ambiente AWS vengono avviate in circostanze sospette. Questo esito indica che un principale specifico nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita, ad esempio se un principale (Utente root dell'account AWS, ruolo IAM o utente IAM) nel tuo ambiente ha richiamato l'API `RunInstances` senza averlo mai fatto in precedenza. Questa attività potrebbe essere un'indicazione che un utente malintenzionato sta utilizzando credenziali rubate per rubare tempo di calcolo (possibilmente per il mining di criptovalute o il password cracking). Può anche essere la prova che un utente malintenzionato sta utilizzando un'istanza EC2 nel tuo ambiente AWS e le relative credenziali per mantenere l'accesso al tuo account.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Stealth:IAMUser/LoggingConfigurationModified

Un principale ha richiamato un'API comunemente utilizzata per interrompere la registrazione CloudTrail, eliminare i log esistenti o eliminare tracce di attività nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo esito viene attivato quando la configurazione della registrazione nell'account AWS elencato all'interno del tuo ambiente viene modificata in circostanze sospette. Questo esito segnala che un principale specifico nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita, ad esempio se un principale (Utente root dell'account AWS, ruolo IAM o utente IAM) nel tuo ambiente ha richiamato l'API `StopLogging` senza averlo mai fatto in precedenza. Ciò può indicare il tentativo di un utente malintenzionato di eliminare le tracce della sua attività.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:IAMUser/ConsoleLogin

È stato osservato un accesso insolito alla console da parte di un principale nel tuo account AWS.

Gravità predefinita: media*

> **Note**
>
> La gravità predefinita di questi esiti è media. Tuttavia, se l'API viene richiamata utilizzando credenziali AWS temporanee create su un'istanza, il livello di gravità dell'esito è alto.

Questo risultato viene generato quando una connessione alla console viene rilevata in circostanze sospette. Ad esempio, se un principale che non ha mai chiamato l'API ConsoleLogin in precedenza, lo fa da un client mai utilizzato o da una posizione inabituale. Ciò potrebbe indicare l'utilizzo di credenziali rubate per accedere al tuo account AWS oppure l'accesso da parte di un utente valido all'account in un modo non valido o meno sicuro (ad esempio, non tramite una VPN approvata).

Questo esito segnala che un principale specifico nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questo principale non ha mai eseguito connessioni con questa applicazione client da questo specifico percorso in precedenza.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

UnauthorizedAccess:EC2/TorIPCaller

Un'istanza EC2 sta ricevendo connessioni in entrata da un nodo di uscita Tor.

Gravità predefinita: media

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS riceve connessioni in entrata da un nodo di uscita Tor. Tor è un software che consente la comunicazione anonima. Crittografa le comunicazioni e le inoltra in modo aleatorio tramite relè tra una serie di nodi di rete. L'ultimo nodo Tor è denominato nodo di uscita. L'esito può indicare un accesso non autorizzato alle risorse AWS con l'intento di nascondere la vera identità dell'utente malintenzionato.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Backdoor:EC2/XORDDOS

Un'istanza EC2 sta tentando di comunicare con un indirizzo IP associato a malware XOR DDoS.

Gravità predefinita: alta

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS sta tentando di comunicare con un indirizzo IP associato a malware XOR DDoS. L'istanza EC2 potrebbe essere compromessa.

XOR DDoS è un trojan che assume il controllo dei sistemi Linux. Per accedere al sistema, lancia un attacco di forza bruta allo scopo di scoprire la password dei servizi SSH (Secure Shell) su Linux. Dopo aver ottenuto le credenziali SSH ed effettuato la connessione, utilizza privilegi utente root per eseguire uno script che scarica e installa XOR DDoS. Questo malware viene in seguito utilizzato in una botnet per lanciare attacchi DDoS (Distributed Denial of Service) contro altri target.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

Behavior:IAMUser/InstanceLaunchUnusual

Un utente ha avviato un tipo insolito di istanza EC2.

Gravità predefinita: alta

Questo esito segnala che un utente specifico nel tuo ambiente AWS ha un comportamento che differisce dalla linea di base stabilita. Questo utente non ha mai avviato un'istanza EC2 di questo tipo in precedenza. Le tue credenziali di accesso potrebbero essere compromesse.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

CryptoCurrency:EC2/BitcoinTool.A

Un'istanza EC2 sta comunicando con pool di mining di bitcoin.

Gravità predefinita: alta

Questo esito segnala che un'istanza EC2 nel tuo ambiente AWS sta comunicando con pool di mining di Bitcoin. Nel settore del mining di criptovalute, un pool di mining designa il raggruppamento delle risorse dei minatori che condividono la loro potenza di elaborazione su una rete per condividere la ricompensa in funzione del loro contributo alla risoluzione di un blocco. Se l'istanza EC2 non è utilizzata per il mining di bitcoin, potrebbe essere compromessa.

Raccomandazioni per la correzione:

Se questa attività non è prevista, l'istanza potrebbe essere compromessa. Per ulteriori informazioni, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

UnauthorizedAccess:IAMUser/UnusualASNCaller

Un'API è stata chiamata da un indirizzo IP di una rete inabituale.

Gravità predefinita: alta

Questo risultato segnala che un'attività è stata chiamata da un indirizzo IP di una rete inabituale. Questa rete non è mai stata osservata nello storico di utilizzo di AWS dell'utente specificato. Questa attività può includere una accesso alla console, un tentativo di avviare un'istanza EC2, di creare un nuovo utente IAM, di modificare i privilegi AWS, ecc. Ciò può indicare un accesso non autorizzato alle risorse AWS.

Raccomandazioni per la correzione:

Se questa attività non è prevista, le credenziali potrebbero essere compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

Esiti per tipo di risorsa

Le pagine seguenti sono suddivise in categorie per tipo di risorsa associata a un GuardDuty risultato:

- Tipi di esiti EC2
- IAMricerca di tipi
- Tipi di esiti S3
- EKStipi di ricerca dei registri di controllo
- Tipi di risultati del monitoraggio del runtime
- Protezione da malware per tipi di ricerca EC2
- Protezione da malware per tipo di ricerca S3
- Tipi di esiti della Protezione RDS
- Tipi di esiti della Protezione Lambda

Tabella degli esiti

La tabella seguente mostra tutti i tipi di esiti attivi ordinati per origine dati o funzionalità fondamentale, a seconda dei casi. Alcuni dei seguenti tipi di esiti possono avere diversi livelli di gravità, indicati da

un asterisco (*). Per informazioni sulla gravità variabile di un tipo di esito, visualizza la descrizione dettagliata corrispondente.

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Discovery:S3/AnomalousBehavior	Amazon S3	CloudTrail eventi di dati per S3	Bassa
Discovery:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Discovery:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Discovery:S3/TorIPCaller	Amazon S3	CloudTrail eventi di dati per S3	Media
Exfiltration:S3/AnomalousBehavior	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Exfiltration:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Impact:S3/AnomalousBehavior.Delete	Amazon S3	CloudTrail eventi di dati per S3	Elevata
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail eventi di dati per S3	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail eventi di dati per S3	Media
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventi di dati per S3	Elevata
PenTest:S3/KaliLinux	Amazon S3	CloudTrail eventi di dati per S3	Media
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail eventi di dati per S3	Media
PenTest:S3/PentooLinux	Amazon S3	CloudTrail eventi di dati per S3	Media
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail eventi di dati per S3	Elevata
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail eventi di dati per S3	Elevata
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Media
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Bassa
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Elevata
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Elevata
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Media
PenTest:IAMUser/KaliLinux	IAM	CloudTrail evento di gestione	Media
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail evento di gestione	Media
PenTest:IAMUser/PentooLinux	IAM	CloudTrail evento di gestione	Media
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail evento di gestione	Basso*
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail evento di gestione	Alta*
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail evento di gestione	Bassa
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail evento di gestione	Elevata
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail evento di gestione	Bassa
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail evento di gestione	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail evento di gestione	Media
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail evento di gestione	Media
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail evento di gestione	Media
Recon:IAMUser/TorIPCaller	IAM	CloudTrail evento di gestione	Media
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail evento di gestione	Bassa
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail evento di gestione	Bassa
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail evento di gestione	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail evento di gestione	Media
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail evento di gestione	Media
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail evento di gestione	Media
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail eventi di gestione o eventi CloudTrail relativi ai dati per S3	Bassa
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail eventi di gestione o eventi CloudTrail relativi ai dati per S3	Elevata
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	DNStronchi	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	DNStronchi	Elevata
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	DNStronchi	Media
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	DNStronchi	Elevata
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	DNStronchi	Elevata
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	DNStronchi	Bassa
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	DNStronchi	Media
Trojan:EC2/DGADomainRequest.B	Amazon EC2	DNStronchi	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	DNStronchi	Elevata
Trojan:EC2/DNSDataExfiltration	Amazon EC2	DNStronchi	Elevata
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	DNStronchi	Elevata
Trojan:EC2/DropPoint!DNS	Amazon EC2	DNStronchi	Media
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	DNStronchi	Elevata
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	DNStronchi	Elevata
Execution:Container/MaliciousFile	Container	EBSProtezione da malware	Varia a seconda della minaccia rilevata
Execution:Container/SuspiciousFile	Container	EBSProtezione da malware	Varia a seconda della minaccia rilevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Execution:EC2/MaliciousFile	EC2	EBSProtezione da malware	Varia a seconda della minaccia rilevata
Execution:EC2/SuspiciousFile	EC2	EBSProtezione da malware	Varia a seconda della minaccia rilevata
Execution:ECS/MaliciousFile	ECS	EBSProtezione da malware	Varia a seconda della minaccia rilevata
Execution:ECS/SuspiciousFile	ECS	EBSProtezione da malware	Varia a seconda della minaccia rilevata
Execution:Kubernetes/MaliciousFile	Kubernetes	EBSProtezione da malware	Varia a seconda della minaccia rilevata
Execution:Kubernetes/SuspiciousFile	Kubernetes	EBSProtezione da malware	Varia a seconda della minaccia rilevata
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	EKSregistri di controllo	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	EKSregistri di controllo	Elevata
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSregistri di controllo	Elevata
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSregistri di controllo	Elevata
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	EKSregistri di controllo	Elevata
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	EKSregistri di controllo	Elevata
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSregistri di controllo	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSregistri di controllo	Elevata
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	EKSregistri di controllo	Elevata
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	EKSregistri di controllo	Bassa
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	EKSregistri di controllo	Media
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSregistri di controllo	Media
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSregistri di controllo	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Discovery:Kubernetes/TorIPCaller	Kubernetes	EKSregistri di controllo	Media
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	EKSregistri di controllo	Media
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	EKSregistri di controllo	Media
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	EKSregistri di controllo	Bassa
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	EKSregistri di controllo	Elevata
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSregistri di controllo	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSregistri di controllo	Elevata
Impact:Kubernetes/TorIPCaller	Kubernetes	EKSregistri di controllo	Elevata
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	EKSregistri di controllo	Media
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	EKSregistri di controllo	Media
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	EKSregistri di controllo	Media
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	EKSregistri di controllo	Elevata
Persistence:Kubernetes/TorIPCaller	Kubernetes	EKSregistri di controllo	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	EKSregistri di controllo	Elevata
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	EKSregistri di controllo	Elevata
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	EKSregistri di controllo	Media
Policy:Kubernetes/ExposedDashboard	Kubernetes	EKSregistri di controllo	Media
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	EKSregistri di controllo	Medio*

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	EKSregistri di controllo	Bassa
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	EKSregistri di controllo	Elevata
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	EKSregistri di controllo	Elevata
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	EKSregistri di controllo	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Backdoor:Lambda/C&CActivity.B	Lambda	Monitoraggio delle attività di rete Lambda	Elevata
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Monitoraggio delle attività di rete Lambda	Elevata
Trojan:Lambda/BlackholeTraffic	Lambda	Monitoraggio delle attività di rete Lambda	Media
Trojan:Lambda/DropPoint	Lambda	Monitoraggio delle attività di rete Lambda	Media
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Monitoraggio delle attività di rete Lambda	Media
UnauthorizedAccess:Lambda/TorClient	Lambda	Monitoraggio delle attività di rete Lambda	Elevata
UnauthorizedAccess:Lambda/TorRelay	Lambda	Monitoraggio delle attività di rete Lambda	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Database Amazon Aurora e Amazon RDS supportati	Monitoraggio delle attività di accesso	Bassa
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Database Amazon Aurora e Amazon RDS supportati	Monitoraggio delle attività di accesso	Elevata
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Database Amazon Aurora e Amazon RDS supportati	Monitoraggio delle attività di accesso	Variabile*
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Database Amazon Aurora e Amazon RDS supportati	Monitoraggio delle attività di accesso	Media
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Database Amazon Aurora e Amazon RDS supportati	Monitoraggio delle attività di accesso	Elevata
CredentialAccess:RDS/TorIPCaller.FailedLogin	Database Amazon Aurora e Amazon RDS supportati	Monitoraggio delle attività di accesso	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Database Amazon Aurora e Amazon supportati RDS	RDSMonitoraggio delle attività di accesso	Elevata
Discovery:RDS/MaliciousIPCaller	Database Amazon Aurora e Amazon supportati RDS	RDSMonitoraggio delle attività di accesso	Media
Discovery:RDS/TorIPCaller	Database Amazon Aurora e Amazon supportati RDS	RDSMonitoraggio delle attività di accesso	Media
Backdoor:Runtime/C&CActivity.B	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
Backdoor:Runtime/C&CActivity.B!DNS	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
CryptoCurrency:Runtime/BitcoinTool.B	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
DefenseEvasion:Runtime/FilelessExecution	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media
DefenseEvasion:Runtime/ProcessInjection.Proc	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
DefenseEvasion:Runtime/PtraceAntiDebugging	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Bassa
DefenseEvasion:Runtime/SuspiciousCommand	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
Execution:Runtime/MaliciousFileExecuted	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Execution:Runtime/NewBinaryExecuted	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media
Execution:Runtime/NewLibraryLoaded	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media
Execution:Runtime/SuspiciousCommand	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Variabile
Execution:Runtime/SuspiciousShellCreated	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Bassa
Execution:Runtime/SuspiciousTool	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Variabile
Execution:Runtime/ReverseShell	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
Impact:Runtime/AbusedDomainRequest.Reputation	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Impact:Runtime/BitcoinDomainRequest.Reputation	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
Impact:Runtime/CryptoMinerExecuted	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
Impact:Runtime/MaliciousDomainRequest.Reputation	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media
Impact:Runtime/SuspiciousDomainRequest.Reputation	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Bassa
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
PrivilegeEscalation:Runtime/DockerSocketAccessed	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media
PrivilegeEscalation:Runtime/ElevationToRoot	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media
PrivilegeEscalation:Runtime/RuncContainerEscape	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
PrivilegeEscalation:Runtime/UserfaultfdUsage	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media
Object:S3/MaliciousFile	S3Object	Protezione da malware per S3	Elevata
Trojan:Runtime/BlackholeTraffic	Istanza, EKS cluster, ECS cluster o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/BlackholeTraffic!DNS	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Trojan:Runtime/DropPoint	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/DGADomainRequest.C!DNS	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
Trojan:Runtime/DriveBySourceTraffic!DNS	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
Trojan:Runtime/DropPoint!DNS	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Media
Trojan:Runtime/PhishingDomainRequest!DNS	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
UnauthorizedAccess:Runtime/MetadataDNSRebind	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
UnauthorizedAccess:Runtime/TorClient	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
UnauthorizedAccess:Runtime/TorRelay	Istanza, EKS ECS cluster, cluster o contenitore	Monitoraggio del runtime	Elevata
Backdoor:EC2/C&CActivity.B	EC2	VPC log di flusso	Elevata
Backdoor:EC2/DenialOfService.Dns	EC2	VPC log di flusso	Elevata
Backdoor:EC2/DenialOfService.Tcp	EC2	VPC log di flusso	Elevata
Backdoor:EC2/DenialOfService.Udp	EC2	VPC log di flusso	Elevata
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	VPC log di flusso	Elevata
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	VPC log di flusso	Elevata
Backdoor:EC2/Spambot	EC2	VPC log di flusso	Media
Behavior:EC2/NetworkPortUnusual	EC2	VPC log di flusso	Media

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Behavior:EC2/TrafficVolumeUnusual	EC2	VPC log di flusso	Media
CryptoCurrency:EC2/BitcoinTool.B	EC2	VPC log di flusso	Elevata
DefenseEvasion:EC2/UnusualDNSResolver	EC2	VPC log di flusso	Media
DefenseEvasion:EC2/UnusualDoHActivity	EC2	VPC log di flusso	Media
DefenseEvasion:EC2/UnusualDoTActivity	EC2	VPC log di flusso	Media
Impact:EC2/PortSweep	EC2	VPC log di flusso	Elevata
Impact:EC2/WinRMBruteForce	EC2	VPC log di flusso	Basso*
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	VPC log di flusso	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
Recon:EC2/PortProbeUnprotectedPort	EC2	VPC log di flusso	Basso*
Recon:EC2/Portscan	EC2	VPC log di flusso	Media
Trojan:EC2/BlackholeTraffic	EC2	VPC log di flusso	Media
Trojan:EC2/DropPoint	EC2	VPC log di flusso	Media
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	VPC log di flusso	Media
UnauthorizedAccess:EC2/RDPBruteForce	EC2	VPC log di flusso	Basso*
UnauthorizedAccess:EC2/SSHBruteForce	EC2	VPC log di flusso	Basso*
UnauthorizedAccess:EC2/TorClient	EC2	VPC log di flusso	Elevata

Tipo di risultato	Tipo di risorsa	Origine dati/funzionalità fondamentale	Gravità dell'esito
UnauthorizedAccess:EC2/TorRelay	EC2	VPC log di flusso	Elevata

Gestione dei GuardDuty risultati di Amazon

GuardDuty offre diverse funzioni importanti per aiutarti a ordinare, archiviare e gestire i risultati. Queste funzionalità ti consentono di personalizzare gli esiti in base al tuo ambiente. In questo modo ridurrai il rumore derivante da risultati di basso valore e potrai concentrarti sulle minacce al tuo ambiente AWS . Consulta gli argomenti di questa pagina per capire come utilizzare queste funzionalità per aumentare il valore GuardDuty dei risultati.

Argomenti:

Pannello di riepilogo

Scopri i componenti della dashboard di riepilogo disponibile nella GuardDuty console.

Filtro dei risultati

Scopri come filtrare GuardDuty i risultati in base ai criteri che hai specificato.

Regole di eliminazione

Scopri come filtrare automaticamente GuardDuty gli avvisi sui risultati tramite regole di soppressione. Le regole di eliminazione archiviano automaticamente gli esiti a seconda dei filtri impostati.

Utilizzo di elenchi di indirizzi IP affidabili ed elenchi minacce

Personalizza l'ambito del GuardDuty monitoraggio utilizzando elenchi di IP ed elenchi di minacce basati su indirizzi IP instradabili pubblicamente. Gli elenchi di IP affidabili impediscono la generazione di DNS risultati non rilevati a partire da indirizzi IP considerati attendibili, mentre Threat Intel Lists provvede GuardDuty ad avvisare l'utente in caso di attività definite dall'utente. IPs

Esportazione degli esiti

Esporta i risultati generati in un bucket Amazon S3 in modo da poter conservare i record oltre il periodo di conservazione dei risultati di 90 giorni. GuardDuty Utilizza questi dati storici per tenere traccia delle potenziali attività sospette nel tuo account e valutare se le misure correttive consigliate hanno avuto successo.

Creazione di risposte personalizzate ai GuardDuty risultati con Amazon CloudWatch Events

Imposta notifiche automatiche per GuardDuty i risultati tramite Amazon CloudWatch Events. Puoi anche automatizzare altre attività tramite CloudWatch Events per aiutarti a rispondere ai risultati.

Comprensione CloudWatch dei log e dei motivi per cui le risorse vengono ignorate durante la scansione Malware Protection for EC2

Scopri come controllare CloudWatch Logs for GuardDuty Malware Protection EC2 e quali sono i motivi per cui l'EC2istanza Amazon interessata o i EBS volumi Amazon interessati potrebbero essere stati ignorati durante il processo di scansione.

Segnalazione di falsi positivi in GuardDuty Malware Protection for EC2

Scopri come segnalare potenziali rilevamenti di minacce false positive in Malware Protection for S3.

Pannello di riepilogo

La dashboard di riepilogo fornisce una visualizzazione aggregata dei GuardDuty risultati generati Account AWS nella regione corrente. Attualmente, il pannello supporta un volume fino a 5.000 esiti. Tuttavia, puoi visualizzare i dettagli di tutti i risultati utilizzando la pagina Findings sulla GuardDuty console GetFindingsoppure ListFindings.

> **Note**
>
> Il riepilogo dei risultati è disponibile solo tramite la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

Le sezioni seguenti consentono di accedere al pannello e di comprenderne i componenti.

Indice

Accesso al pannello di Riepilogo

Sulla GuardDuty console, la dashboard di riepilogo mostra una visualizzazione consolidata degli ultimi 5.000 GuardDuty risultati generati nella regione corrente.

Per accedere al pannello di Riepilogo

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Riepilogo. Quando apri la console, GuardDuty mostra la dashboard di riepilogo.
3. Per impostazione predefinita, il riepilogo viene visualizzato per lo stesso giorno, ossia Oggi. La GuardDuty console offre un'opzione per visualizzare il riepilogo degli ultimi 2 giorni, degli ultimi 7 giorni e degli ultimi 30 giorni. Per modificare l'intervallo di tempo predefinito, scegli una delle opzioni dal menu a discesa sopra il riquadro Panoramica.
4. Filtro dei dati

   - I widget Account con il maggior numero di esiti, Risorse con il maggior numero di esiti ed Esiti meno ricorrenti consentono di filtrare i dati in base al livello di gravità degli esiti.
   - Il widget Risorse con il maggior numero di esiti consente inoltre di filtrare i dati in base al tipo di risorsa potenzialmente interessata.

     Un account membro può visualizzare i dettagli della risorsa potenzialmente interessata che appartiene al proprio account. Se sei un account GuardDuty amministratore e desideri visualizzare i dettagli della risorsa potenzialmente interessata, apri la GuardDuty console utilizzando le credenziali dell'account membro associato.
5. Copertura dei piani di protezione

   La copertura dei piani di protezione fornisce il numero di account membri attivati GuardDuty nell'organizzazione. Le statistiche sono visibili solo all' GuardDuty amministratore delegato.

Comprensione del pannello di Riepilogo

Il pannello di Riepilogo mostra i dati aggregati nelle sezioni seguenti. Prima di procedere alla visualizzazione e alla lettura del riepilogo, assicurati di scegliere la Regione AWS desiderata dal selettore della regione nella parte superiore della console. Inoltre, assicurati di scegliere l'intervallo di tempo desiderato dal menu a discesa fornito sopra il riquadro Panoramica. Se non sono stati generati esiti per i parametri scelti, nessun dato sarà disponibile in alcun widget.

Su un volume fino agli ultimi 5.000 GuardDuty risultati, la dashboard di riepilogo con Account con il maggior numero di risultati, Risorse con il maggior numero di risultati e Risultati meno ricorrenti mostra i dati basati sui primi 5 risultati. Per un'analisi più approfondita, consulta la pagina Findings nella GuardDuty console.

Panoramica

Questa sezione fornisce i dati seguenti:

- Esiti totali: indica il numero totale di esiti generati nel tuo account nella regione attuale.
- Risultati di elevata gravità: indica il numero di GuardDuty risultati con un livello di gravità elevato nella regione corrente.
- Risorse con esiti: indica il numero di risorse che sono associate a un esito e che sono state potenzialmente compromesse.
- Account con esiti: indica il numero di account in cui è stato generato almeno un esito. Se sei un account indipendente, il valore di questo campo è 1.

Per gli intervalli di tempo Ultimi 7 giorni e Ultimi 30 giorni, il riquadro Panoramica può mostrare la differenza percentuale rispettivamente degli esiti generati settimanalmente (WoW) o mensilmente (MoM). Se non sono stati generati esiti nella settimana o nel mese precedente, in assenza quindi di dati da confrontare, la differenza percentuale potrebbe non essere disponibile.

Se sei un account GuardDuty amministratore, tutti questi campi forniscono i dati riepilogati di tutti gli account dei membri della tua organizzazione.

Esiti per gravità

Questa sezione mostra un grafico a barre con il numero totale di esiti rispetto all'intervallo di tempo scelto. Puoi visualizzare il numero di esiti con gravità bassa, media o alta generati in una data specifica all'interno dell'intervallo di tempo scelto.

Tipi di esiti più comuni

Questa sezione fornisce un grafico a torta dei cinque principali tipi di risultati più comuni osservati su un volume di fino agli ultimi 5.000 GuardDuty risultati generati nella regione corrente. Questo grafico a torta mostra i seguenti dati quando il puntatore del mouse viene posizionato su ciascun settore:

- Conteggio degli esiti: indica il numero di volte in cui questo esito è stato generato nell'intervallo di tempo selezionato.

- Gravità: indica il livello di gravità dell'esito, ad esempio medio e alto.
- Percentuale: indica la quota di questo tipo di esito nel grafico a torta.
- Ultima generazione: indica quanto tempo è trascorso dall'ultima generazione di questo tipo di esito.

Account con il maggior numero di esiti

Questa sezione fornisce i dati seguenti:

- Account: indica l' Account AWS ID in cui è stato generato il risultato.
- Conteggio dell'esito: indica il numero di volte in cui è stato generato un esito per questo ID account.
- Ultima generazione: indica quanto tempo è trascorso dall'ultima generazione di un tipo di esito per questo ID account.
- Gravità alta: per impostazione predefinita, vengono visualizzati i dati per i tipi di esiti con gravità alta. Le opzioni possibili per questo campo sono Gravità alta, Gravità media e Tutte le gravità.

Risorse con esiti

Questa sezione fornisce i dati seguenti:

- Risorsa: indica il tipo di risorsa potenzialmente interessata e se questa risorsa appartiene al tuo account puoi accedere al collegamento rapido per visualizzarne i dettagli. Se sei un account GuardDuty amministratore, puoi visualizzare i dettagli della risorsa potenzialmente interessata accedendo alla GuardDuty console con le credenziali dell'account membro a cui appartiene questa risorsa.
- Account: indica l' Account AWS ID a cui appartiene questa risorsa.
- Conteggio dell'esito: indica il numero di volte in cui questa risorsa è stata associata a un esito.
- Ultima generazione: indica quanto tempo è trascorso dall'ultima generazione di un tipo di esito associato a questa risorsa.
- Tutti i tipi di risorsa: per impostazione predefinita, i dati vengono visualizzati per tutti i tipi di risorse. Utilizzando il menu a discesa, puoi visualizzare i dati per un tipo di risorsa specifico, come Instance AccessKey, Lambda e altri.
- Gravità alta: per impostazione predefinita, vengono visualizzati i dati per i tipi di esiti con gravità alta. Utilizzando il menu a discesa, puoi visualizzare i dati per altri livelli di gravità. Le opzioni possibili sono Gravità alta, Gravità media e Tutte le gravità.

Esiti meno ricorrenti

Questa sezione fornisce i dettagli dei tipi di risultati che non vengono generati spesso nell'ambiente in uso. AWS Queste informazioni possono essere utili per indagare e agire su un modello di minaccia emergente nel tuo ambiente. La tabella mostra i dati seguenti:

- Tipo di risultato: indica il nome del tipo di esito.
- Conteggio dell'esito: indica il numero di volte in cui questo esito è stato generato nell'intervallo di tempo selezionato.
- Ultima generazione: indica quanto tempo è trascorso dall'ultima generazione di questo tipo di esito.
- Gravità alta: per impostazione predefinita, vengono visualizzati i dati per i tipi di esiti con gravità alta. Le opzioni possibili per questo campo sono Gravità alta, Gravità media e Tutte le gravità.

Copertura dei piani di protezione

Questa sezione fornisce il numero di account membri attivi che appartengono all'organizzazione e che hanno abilitato una o più funzionalità e funzionalità aggiuntive (a seconda dei casi) nella configurazione corrente Regione AWS.

Solo un GuardDuty amministratore delegato può visualizzare le statistiche relative agli account dei membri all'interno della propria organizzazione. Se una funzionalità non è configurata, scegli Configura nella colonna Azioni.

Quando crei una nuova AWS organizzazione, potrebbero essere necessarie fino a 24 ore per generare le statistiche per l'intera organizzazione.

Feedback sul pannello di Riepilogo

GuardDuty ti incoraggia a fornire feedback sull'usabilità, le funzionalità e le prestazioni della dashboard di riepilogo. per sapere come migliorarlo.

Per fornire feedback sul pannello di Riepilogo

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Riepilogo. Quando apri la GuardDuty console, viene visualizzata la dashboard di riepilogo.
3. Scegli Feedback nell'angolo in alto a destra del pannello. Si aprirà un modulo. Dopo aver fornito il feedback, scegli Invia.

Filtro dei risultati

Un filtro per gli esiti ti consente di visualizzare gli esiti che corrispondono ai criteri specificati e di escludere gli esiti non corrispondenti. Puoi creare facilmente filtri di ricerca utilizzando la GuardDuty console Amazon oppure puoi crearli CreateFilterAPIutilizzandoJSON. Consulta le sezioni seguenti per capire come creare un filtro nella console. Per utilizzare questi filtri in modo da archiviare automaticamente gli esiti in arrivo, consulta Regole di eliminazione.

Creazione di filtri nella GuardDuty console

I filtri di ricerca possono essere creati e testati tramite la GuardDuty console. Puoi salvare i filtri che hai creato tramite la console per utilizzarli nelle regole di eliminazione o nelle operazioni di filtro future. Un filtro è composto da almeno un criterio di filtro, che consiste in un attributo del filtro abbinato ad almeno un valore.

Quando crei un nuovo utente, tieni in considerazione quanto segue:

- I filtri non accettano caratteri jolly.
- Puoi specificare da uno a 50 attributi come criteri per un determinato filtro.
- Quando utilizzi la condizione uguale a o non uguale a per filtrare in base a un valore di attributo, ad esempio ID account, puoi specificare un massimo di 50 valori.
- Ogni attributo dei criteri di filtro viene valutato come operatore `AND`. Più valori per lo stesso attributo vengono valutati come `AND/OR`.

Per filtrare i risultati (console)

1. In Filtra per attributo, scegli Aggiungi criteri di filtro. Verrà visualizzato un elenco esteso di attributi del filtro.
2. Dall'elenco esteso di attributi, seleziona l'attributo che desideri specificare come criterio per il filtro, ad esempio ID account o Tipo di azione.

   Per un elenco completo degli attributi, consultaAttributi del filtro.
3. Nel campo di testo visualizzato, specificate un valore per l'attributo selezionato, quindi scegliete Applica.
4. Per aggiungere più di un criterio di filtro, ripeti i passaggi 1-3.

5. Per impostazione predefinita, l'elenco mostra i risultati che corrispondono al filtro applicato. Se desideri visualizzare i risultati che non corrispondono all'attributo del filtro, scegli Escludi accanto al filtro.

6. Salva gli attributi e i valori specificati come filtri

   a. Per salvare gli attributi specificati e i relativi valori (criteri di filtro) come filtro, selezionare Salva/Modifica.

   b. Inserite il nome e la descrizione della regola di filtro.

   c. Seleziona Salva.

Attributi del filtro

Quando si creano filtri o si ordinano i risultati utilizzando le API operazioni, è necessario specificare i criteri di filtro inJSON. Questi criteri di filtro sono correlati ai dettagli di un risultatoJSON. La tabella seguente contiene un elenco dei nomi visualizzati sulla console per gli attributi dei filtri e i nomi di JSON campo equivalenti.

Nome campo console	Nome campo JSON
ID account	accountId
ID risultato	id
Regione	Regione
Gravità	severity È possibile filtrare i tipi di risultati in base al livello di gravità dei tipi di risultati. Per ulteriori informazioni sui valori di gravità, vedereLivelli di gravità dei GuardDuty risultati

Nome campo console	Nome campo JSON
	. Se si utilizza `severity` with API AWS CLI, o AWS CloudFormation, viene assegnato un valore numerico. Per ulteriori informazioni, findingCriteriaconsulta Amazon GuardDuty API Reference.
Tipo di risultato	tipo
Ora aggiornamento	updatedAt
ID chiave di accesso	risorsa. accessKeyDetails. accessKeyId
ID principale	risorsa. accessKeyDetails. principalId
Username	risorsa. accessKeyDetails. userName
Tipo di utente	risorsa. accessKeyDetails. userType
IAMID del profilo di istanza	risorsa. instanceDetails. iamInstanceProfile.id
ID istanza	risorsa. instanceDetails. instanceId
ID immagine istanza	risorsa. instanceDetails. imageId
Chiave di tag dell'istanza	risorsa. instanceDetails.tags.key
Valore del tag dell'istanza	risorsa. instanceDetails.tags.value
IPv6indirizzo	risorsa. instanceDetails. networkInterfaces. Indirizzi IPv6
Indirizzo privato IPv4	risorsa. instanceDetails. networkInterfaces. privateIpAddresses. privateIpAddress
DNSNome pubblico	risorsa. instanceDetails. networkInterfaces. publicDnsName
IP pubblico	risorsa. instanceDetails. networkInterfaces. publicIp

Nome campo console	Nome campo JSON
ID gruppo di sicurezza	risorsa. instanceDetails. networkInterfaces. securityGroups. groupId
Nome del gruppo di sicurezza	risorsa. instanceDetails. networkInterfaces. securityGroups. groupName
ID sottorete	risorsa. instanceDetails. networkInterfaces. subnetId
VPCID	risorsa. instanceDetails. networkInterfaces. vpcId
Avamposto ARN	risorsa. instanceDetails.avamposto ARN
Tipo di risorsa	risorsa. resourceType
Autorizzazioni del bucket	risorse.3BucketDetails. publicAccess. effective Permission
Nome bucket	resource.s3 .name BucketDetails
Chiave tag bucket	risorse.s3 .tags.key BucketDetails
Valore tag bucket	risorse.s3 .tags.value BucketDetails
Tipo bucket	risorse.s3 .type BucketDetails
Tipo di operazione	servizio.azione. actionType
APIchiamato	servizio.azione. awsApiCallAzione.api
APItipo di chiamante	servizio.azione. awsApiCallAzione. callerType
APICodice di errore	service.action. awsApiCallAzione. errorCode
APIcittà chiamante	servizio. azione. awsApiCallAzione. remoteIpDetails.città. cityName

Nome campo console	Nome campo JSON
APIpaese chiamante	servizio.azione. awsApiCallAzione. remoteIpDetails.paese. countryName
APIindirizzo del chiamante IPv4	servizio.azione. awsApiCallAzione. remoteIpDetails. ipAddressV4
APIindirizzo del chiamante IPv6	servizio.azione. awsApiCallAzione. remoteIpDetails. ipAddressV6
APIID chiamante ASN	servizio.azione. awsApiCallAzione. remoteIpDetails.organizzazione.asn
APInome del ASN chiamante	servizio.azione. awsApiCallAzione. remoteIpDetails.organizzazione. asnOrg
APInome del servizio chiamante	service.action. awsApiCallAzione. serviceName
DNSrichiedi dominio	service.action. dnsRequestAction.dominio
DNSrichiedi il suffisso del dominio	service.action. dnsRequestAction. domainWithSuffix
Connessione di rete bloccata	servizio.azione. networkConnectionAction.bloccato
Direzione connessione rete	servizio.azione. networkConnectionAction. connectionDirection
Porta locale connessione rete	servizio.azione. networkConnectionAction. localPortDetails.porta
Protocollo connessione rete	servizio.azione. networkConnectionAction.protocollo
Città connessione di rete	servizio.azione. networkConnectionAction. remoteIpDetails.città. cityName

Nome campo console	Nome campo JSON
Paese connessione di rete	servizio.azione. networkConnectionAction. remoteIpDetails.paese. countryName
IPv4Indirizzo remoto della connessione di rete	servizio.azione. networkConnectionAction. remoteIpDetails. ipAddressV4
Indirizzo remoto IPv6 della connessione di rete	servizio.azione. networkConnectionAction. remoteIpDetails. ipAddressV6
ID IP ASN remoto della connessione di rete	servizio.azione. networkConnectionAction. remoteIpDetails.organizzazione.asn
Nome IP remoto della connessione di rete ASN	servizio.azione. networkConnectionAction. remoteIpDetails.organizzazione. asnOrg
Porta remota connessione rete	servizio.azione. networkConnectionAction. remotePortDetails.porta
Account remoto affiliato	servizio.azione. awsApiCallAzione. remoteAcc ountDetails.affiliato
Indirizzo del chiamante Kubernetes API IPv4	servizio.azione. kubernetesApiCallAzione. remoteIpDetails. ipAddressV4
Indirizzo del chiamante Kubernetes API IPv6	servizio.azione. kubernetesApiCallAzione. remoteIpDetails. ipAddressV6
Spazio dei nomi Kubernetes	servizio. azione. kubernetesApiCallAction.nam espace
ID chiamante Kubernetes API ASN	servizio.azione. kubernetesApiCallAzione. remoteIpDetails.organizzazione.asn
Richiesta di chiamata Kubernetes API URI	servizio.azione. kubernetesApiCallAzione. requestUri
Codice di stato Kubernetes API	servizio.azione. kubernetesApiCallAzione. statusCode

Nome campo console	Nome campo JSON
IPv4Indirizzo locale della connessione di rete	service.action. networkConnectionAction. localIpDetails. ipAddressV4
Indirizzo locale IPv6 della connessione di rete	service.action. networkConnectionAction. localIpDetails. ipAddressV6
Protocollo	servizio. azione. networkConnectionAction.protocollo
APInome del servizio di chiamata	service.action. awsApiCallAzione. serviceName
APIID dell'account chiamante	servizio.azione. awsApiCallAzione. remoteAccountDetails. accountId
Nome elenco minacce	servizio. additionalInfo. threatListName
Ruolo risorsa	servizio. resourceRole
EKSnome del cluster	risorsa. eksClusterDetails.nome
Nome del carico di lavoro Kubernetes	risorsa. kubernetesDetails. kubernetesWorkloadDetails.nome
Spazio dei nomi del carico di lavoro Kubernetes	risorsa. kubernetesDetails. kubernetesWorkloadDetails.namespace
Nome utente Kubernetes	risorsa. kubernetesDetails. kubernetesUserDetails.nome utente
Immagine del container di Kubernetes	risorsa. kubernetesDetails. kubernetesWorkloadDetails.contenitori.immagine
Prefisso dell'immagine del container di Kubernetes	risorsa. kubernetesDetails. kubernetesWorkloadDetails.contenitori. imagePrefix
ID scansione	servizio. ebsVolumeScanDettagli. scanId

Nome campo console	Nome campo JSON
EBSnome della minaccia di scansione del volume	servizio. ebsVolumeScanDettagli. scanDetections. threatDetectedByNome. threatNames.nome
nome della minaccia di scansione degli oggetti S3	servizio. malwareScanDetails.threats.name
Gravità delle minacce	servizio. ebsVolumeScanDettagli. scanDetections. threatDetectedByNome. threatNames.severità
File SHA	servizio. ebsVolumeScanDettagli. scanDetections. threatDetectedByNome. threatNames. filePaths.hash
ECSnome del cluster	risorsa. ecsClusterDetails.nome
ECSimmagine del contenitore	risorsa. ecsClusterDetails. taskDetails.contenitori.immagine
ECSdefinizione dell'attività ARN	risorsa. ecsClusterDetails. taskDetails. definitionArn
Immagine del container autonomo	risorsa. containerDetails.immagine
ID istanza di database	risorsa. rdsDbInstanceDettagli. dbInstanceIdentifier
ID del cluster di database	risorsa. rdsDbInstanceDettagli. dbCluster Identifier
Motore di database	risorsa. rdsDbInstanceDettagli.Motore
Utente del database	risorsa. rdsDbUserDettagli. Utente
Chiave di tag dell'istanza database	risorsa. rdsDbInstancedetails.tags.key
Valore del tag dell'istanza database	risorsa. rdsDbInstancedetails.tags.value

Nome campo console	Nome campo JSON
Eseguibile -256 SHA	servizio. runtimeDetails.processo. executabl eSha256
Process name (Nome del processo)	servizio. runtimeDetails.nome.processo
Percorso eseguibile	servizio. runtimeDetails.processo. executabl ePath
Nome della funzione Lambda	risorsa. lambdaDetails. functionName
Funzione Lambda ARN	risorsa. lambdaDetails. functionArn
Chiave di tag con funzione Lambda	risorsa. lambdaDetails.tags.key
Valore del tag della funzione lambda	risorsa. lambdaDetails.tags.value
DNSrichiedi dominio	service.action. dnsRequestAction. domainWit hSuffix

Regole di eliminazione

Una regola di eliminazione è un insieme di criteri in cui ogni attributo di filtro è abbinato a un valore. Questi criteri vengono utilizzati per filtrare gli esiti, archiviando automaticamente i nuovi esiti che corrispondono ai criteri specificati. Le regole di soppressione possono essere utilizzate per filtrare risultati di basso valore, risultati falsi positivi o minacce su cui non si intende agire, per facilitare il riconoscimento delle minacce alla sicurezza con l'impatto maggiore sull'ambiente.

Dopo aver creato una regola di soppressione, i nuovi risultati che corrispondono ai criteri definiti nella regola vengono archiviati automaticamente finché la regola di soppressione è in vigore. Puoi utilizzare un filtro esistente per creare una regola di eliminazione oppure puoi crearne una a partire da un nuovo filtro definito. È possibile configurare le regole di eliminazione in modo da eliminare interi tipi di risultati oppure definire criteri di filtro più granulari per sopprimere solo istanze specifiche di un particolare tipo di risultato. È possibile modificare le regole di soppressione in qualsiasi momento.

I risultati soppressi non vengono inviati ad AWS Security Hub Amazon Simple Storage Service, Amazon Detective o Amazon EventBridge, riducendo il livello di rumore delle ricerche se si utilizzano GuardDuty i risultati tramite Security Hub, una terza parte SIEM o altre applicazioni di avviso e

emissione di ticket. Se l'hai abilitatoProtezione da malware per EC2, i GuardDuty risultati soppressi non avvieranno una scansione antimalware.

GuardDuty continua a generare risultati anche quando corrispondono alle regole di soppressione impostate, tuttavia tali risultati vengono automaticamente contrassegnati come archiviati. I risultati archiviati vengono archiviati GuardDuty per 90 giorni e possono essere visualizzati in qualsiasi momento durante tale periodo. È possibile visualizzare i risultati soppressi nella GuardDuty console selezionando Archiviato dalla tabella dei risultati o GuardDuty API utilizzando il criterio ListFindingsAPIcon un `findingCriteria` criterio uguale a vero. `service.archived`

> **Note**
>
> In un ambiente con più account solo l' GuardDuty amministratore può creare regole di soppressione.

Casi d'uso comuni per le regole di eliminazione ed esempi

I seguenti tipi di risultati presentano casi d'uso comuni per l'applicazione delle regole di soppressione. Seleziona il nome del risultato per saperne di più su tale risultato. Esamina la descrizione del caso d'uso per decidere se creare una regola di soppressione per quel tipo di risultato.

> **Important**
>
> GuardDuty consiglia di creare regole di soppressione in modo reattivo e solo per i risultati per i quali sono stati ripetutamente identificati falsi positivi nel proprio ambiente.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS— Utilizzare una regola di soppressione per archiviare automaticamente i risultati generati quando la VPC rete è configurata per instradare il traffico Internet in modo che esca da un gateway locale anziché da un Internet VPC Gateway.

  Questo risultato viene generato quando la rete è configurata per instradare il traffico Internet in modo che esca da un gateway locale anziché da un VPC Internet Gateway ()IGW. Le configurazioni comuni, ad esempio l'utilizzo o le VPC VPN connessioni AWS Outposts, possono far sì che il traffico venga instradato in questo modo. Se si tratta di un comportamento previsto, si consiglia di utilizzare le regole di soppressione e di creare una regola composta da due criteri di filtro. Il primo criterio è trovare il tipo, che dovrebbe essere `UnauthorizedAccess:IAMUser/`

`InstanceCredentialExfiltration.OutsideAWS`. Il secondo criterio di filtro è l'IPv4indirizzo del API chiamante con l'indirizzo IP o l'CIDRintervallo del gateway Internet locale. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di risultato in base all'indirizzo IP del API chiamante.

```
Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
 API caller IPv4 address: 198.51.100.6
```

> **Note**
>
> Per includere più API chiamanti, IPs puoi aggiungere un nuovo filtro per l'IPv4indirizzo del API chiamante per ciascuno.

- Recon:EC2/Portscan: utilizza una regola di eliminazione per archiviare automaticamente gli esiti quando utilizzi un'applicazione di valutazione della vulnerabilità.

  La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `Recon:EC2/Portscan`. Il secondo criterio di filtro dovrebbe corrispondere all'istanza o alle istanze che ospitano questi strumenti di valutazione della vulnerabilità. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda dei criteri identificabili con le istanze che ospitano questi strumenti. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di ricerca in base a istanze con un determinato valore. AMI

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce: utilizza una regola di eliminazione per archiviare automaticamente gli esiti quando è destinata a istanze di host bastione.

  Se l'obiettivo del tentativo di forza bruta è un bastion host, ciò può rappresentare il comportamento previsto per l'ambiente in uso. AWS In questo caso, si consiglia di impostare una regola di eliminazione per questa individuazione. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `UnauthorizedAccess:EC2/SSHBruteForce`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da bastion host. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di esito in base a istanze con un determinato valore del tag dell'istanza.

```
Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
```

- Recon:EC2/PortProbeUnprotectedPort: utilizza una regola di eliminazione per archiviare automaticamente gli esiti quando è destinata a istanze esposte intenzionalmente.

  Tuttavia, ci possono essere casi in cui le istanze sono intenzionalmente esposte, ad esempio se ospitano server web. Se questo è il caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo risultato. La regola di soppressione deve essere costituita da due criteri di filtro. Il primo criterio dovrebbe utilizzare l'attributo Tipo di risultato con un valore di `Recon:EC2/PortProbeUnprotectedPort`. Il secondo criterio di filtro deve corrispondere all'istanza o alle istanze che fungono da bastion host. Puoi utilizzare l'attributo ID immagine istanza o l'attributo di valore Tag a seconda del criterio identificabile con le istanze che ospitano questi strumenti. L'esempio seguente rappresenta il filtro da utilizzare per eliminare questo tipo di esito in base a istanze con una determinata chiave di tag dell'istanza nella console.

  ```
  Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
  ```

Regole di soppressione consigliate per i risultati del Runtime Monitoring

- PrivilegeEscalation:Runtime/DockerSocketAccessed viene generato quando un processo all'interno di un container comunica con il socket Docker. Nel tuo ambiente potrebbero esserci container che devono accedere al socket Docker per motivi legittimi. L'accesso da parte di tali container genererà esiti PrivilegeEscalation:Runtime/DockerSocketAccessed. Se questo è un caso nel tuo AWS ambiente, ti consigliamo di impostare una regola di soppressione per questo tipo di risultati. Il primo criterio dovrebbe utilizzare il campo Tipo di risultato con valore uguale a `PrivilegeEscalation:Runtime/DockerSocketAccessed`. Il secondo criterio di filtro è il campo Percorso eseguibile con valore uguale al `executablePath` del processo nell'esito generato. In alternativa, il secondo criterio di filtro può utilizzare il campo Executable SHA -256 con un valore uguale a quello del processo `executableSha256` nel risultato generato.
- I cluster Kubernetes gestiscono i propri DNS server come pod, ad esempio. `coredns` Pertanto, per ogni DNS ricerca da un pod, GuardDuty acquisisce due DNS eventi, uno dal pod e l'altro dal pod del server. Ciò può generare duplicati per i seguenti risultati: DNS
  - 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

I risultati duplicati includeranno i dettagli del pod, del contenitore e del processo che corrispondono al pod DNS del server. Puoi impostare una regola di eliminazione per eliminare gli esiti duplicati utilizzando questi campi. Il primo criterio di filtro deve utilizzare il campo Tipo di ricerca con un valore uguale a un tipo di DNS risultato dall'elenco dei risultati fornito in precedenza in questa sezione. Il secondo criterio di filtro potrebbe essere il percorso eseguibile con valore uguale a quello del DNS server `executablePath` o l'eseguibile SHA -256 con valore uguale a quello del DNS server `executableSHA256` nel risultato generato. Come terzo criterio di filtro opzionale, puoi utilizzare il campo di immagine del contenitore Kubernetes con un valore uguale all'immagine del contenitore del pod del tuo DNS server nel risultato generato.

Creazione di regole di soppressione

Scegliete il metodo di accesso preferito per creare una regola di soppressione per la GuardDuty ricerca dei tipi.

Console

È possibile visualizzare, creare e gestire le regole di soppressione utilizzando la console. GuardDuty Le regole di eliminazione vengono generate nello stesso modo dei filtri e i filtri esistenti salvati possono essere utilizzati come regole di eliminazione. Per ulteriori informazioni sulla creazione dei filtri, consulta Filtro dei risultati.

Per creare una regola di eliminazione utilizzando la console:

1. Apri la GuardDuty console all'indirizzo. https://console.aws.amazon.com/guardduty/
2. Nella pagina Risultati, scegli Elimina risultati per aprire il pannello delle regole di eliminazione.

3. Per aprire il menu dei criteri di filtro, inserisci i **`filter criteria`** in Aggiungi criteri filtro. Puoi scegliere un criterio dall'elenco. Inserisci un valore valido per il criterio scelto.

   > **Note**
   >
   > Per determinare quale sia il valore valido, visualizza la tabella degli esiti e scegli un esito da eliminare. Consulta i dettagli nel pannello dei risultati.

   Puoi aggiungere più criteri di filtro e assicurarti che nella tabella compaiano solo gli esiti che desideri eliminare.

4. Inserisci un Nome e una Descrizione per la regola di eliminazione. I caratteri validi includono i caratteri alfanumerici, il punto (.), il trattino (-), il carattere di sottolineatura (_) e gli spazi bianchi.
5. Selezionare Salva.

Puoi anche creare una regola di eliminazione da un filtro esistente salvato. Per ulteriori informazioni sulla creazione dei filtri, consulta Filtro dei risultati.

Per creare una regola di eliminazione da un filtro salvato:

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nella pagina Risultati, scegli Elimina risultati per aprire il pannello delle regole di eliminazione.
3. Dal menu a discesa Regole salvate, scegli un filtro salvato.
4. Puoi anche aggiungere nuovi criteri di filtro. Salta questo passaggio se non sono necessari criteri di filtro aggiuntivi.

   Per aprire il menu dei criteri di filtro, inserisci i **`filter criteria`** in Aggiungi criteri filtro. Puoi scegliere un criterio dall'elenco. Inserisci un valore valido per il criterio scelto.

   > **Note**
   >
   > Per determinare quale sia il valore valido, visualizza la tabella degli esiti e scegli un esito da eliminare. Consulta i dettagli nel pannello dei risultati.

5. Inserisci un Nome e una Descrizione per la regola di eliminazione. I caratteri validi includono i caratteri alfanumerici, il punto (.), il trattino (-), il carattere di sottolineatura (_) e gli spazi bianchi.
6. Selezionare Salva.

API/CLI

Per creare una regola di soppressione utilizzandoAPI:

1. È possibile creare regole di soppressione tramite. CreateFilterAPI A tale scopo, specificate i criteri di filtro in un JSON file seguendo il formato dell'esempio riportato di seguito. L'esempio seguente sopprimerà tutti i risultati non archiviati a bassa gravità che contengono una DNS richiesta al dominio test.example.com. Per gli esiti di gravità media, l'elenco di input sarà `["4", "5", "7"]`, mentre per quelli di gravità alta, l'elenco di input sarà `["6", "7", "8"]`. Puoi anche applicare filtri in base a qualsiasi valore dell'elenco.

```
{
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
                "test.example.com"
            ]
        },
        "severity": {
            "Eq": [
                "1",
                "2",
                "3"
            ]
        }
    }
}
```

Per un elenco dei nomi di campo e dei relativi equivalenti per console, consulta. JSON Attributi del filtro

Per testare i criteri di filtro, utilizza lo stesso JSON criterio in e conferma che siano stati selezionati i risultati corretti. ListFindingsAPI Per testare i criteri di filtro utilizzati, AWS CLI segui l'esempio utilizzando il tuo file detectorId e quello in formato.json.

Per trovare i dati `detectorId` relativi al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. Carica il filtro da utilizzare come regola di soppressione con CreateFilterAPIo utilizzando l'esempio AWS CLI seguente, con il tuo ID del rilevatore, un nome per la regola di soppressione e un file.json.

   Per trovare il file relativo `detectorId` al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il. ListDetectorsAPI

   ```
   aws guardduty create-filter --action ARCHIVE --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
    file://criteria.json
   ```

Puoi visualizzare un elenco dei tuoi filtri a livello di codice con. ListFilterAPI È possibile visualizzare i dettagli di un singolo filtro fornendo il nome del filtro a. GetFilterAPI Aggiorna i filtri utilizzando UpdateFiltero eliminali con. DeleteFilterAPI

Eliminazione delle regole di soppressione

Scegliete il metodo di accesso preferito per eliminare una regola di soppressione per GuardDuty la ricerca dei tipi.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nella pagina Risultati, scegli Elimina risultati per aprire il pannello delle regole di eliminazione.

3. Dal menu a discesa Regole salvate, scegli un filtro salvato.
4. Scegliere Delete rule (Elimina regola).

API/CLI

Esegui il DeleteFilterAPI. Specificare il nome del filtro e l'ID del rilevatore associato per la regione specifica.

In alternativa, è possibile utilizzare il seguente AWS CLI esempio sostituendo i valori formattati in *red*:

```
aws guardduty delete-filter --region us-east-1 --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --filter-name filterName
```

Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

Utilizzo di elenchi di indirizzi IP affidabili ed elenchi minacce

Amazon GuardDuty monitora la sicurezza del tuo AWS ambiente analizzando ed elaborando i log di VPC flusso, i log degli AWS CloudTrail eventi e i log. DNS Puoi personalizzare questo ambito di monitoraggio GuardDuty configurando l'opzione di bloccare gli avvisi di persone attendibili presenti nei tuoi elenchi di IP attendibili IPs e di segnalare eventuali minacce note presenti nei tuoi elenchi di minacce. IPs

Gli elenchi di indirizzi IP affidabili e gli elenchi minacce si applicano solo al traffico destinato a indirizzi IP instradabili pubblicamente. Gli effetti di un elenco si applicano a tutti i VPC Flow Log e ai CloudTrail risultati, ma non ai DNS risultati.

GuardDuty può essere configurato per utilizzare i seguenti tipi di elenchi.

Elenco di indirizzi IP affidabili

Gli elenchi di IP affidabili sono costituiti da indirizzi IP attendibili per comunicazioni sicure con AWS l'infrastruttura e le applicazioni. GuardDuty non genera log di VPC flusso o CloudTrail

risultati per gli indirizzi IP negli elenchi IP affidabili. È possibile includere un massimo di 2000 indirizzi IP e CIDR intervalli in un unico elenco di IP affidabili. In qualsiasi momento, puoi avere soltanto un elenco di indirizzi IP affidabili caricato per account AWS per regione.

Elenco di IP delle minacce

Un elenco minacce è costituito dagli indirizzi IP dannosi noti. Questo elenco può essere fornito dall'intelligence sulle minacce di terze parti o creato appositamente per l'organizzazione. Oltre a generare risultati a causa di un'attività potenzialmente sospetta, genera GuardDuty anche risultati basati su questi elenchi di minacce. È possibile includere un massimo di 250.000 indirizzi IP e CIDR intervalli in un unico elenco di minacce. GuardDuty genera risultati solo sulla base di un'attività che coinvolge indirizzi IP e CIDR intervalli negli elenchi di minacce; i risultati non vengono generati in base ai nomi di dominio. In qualsiasi momento, puoi caricare fino a sei elenchi di minacce Account AWS per ogni regione.

> **Note**
>
> Se includi lo stesso IP sia in un elenco di IP affidabili che in un elenco minacce, l'IP verrà elaborato prima dall'elenco di indirizzi IP affidabili e non verrà generato alcun esito.

In ambienti con più account, solo gli utenti con account di GuardDuty amministratore possono aggiungere e gestire elenchi di IP affidabili ed elenchi di minacce. Gli elenchi di IP affidabili e gli elenchi di minacce caricati dall'account amministratore non possono funzionare GuardDuty correttamente negli account dei membri. In altre parole, negli account dei membri GuardDuty genera risultati basati su attività che coinvolgono indirizzi IP dannosi noti presenti negli elenchi di minacce dell'account amministratore e non genera risultati basati su attività che coinvolgono gli indirizzi IP degli elenchi di IP affidabili dell'account amministratore. Per ulteriori informazioni, consulta Gestione di più account in Amazon GuardDuty.

Formati di elenco

GuardDuty accetta elenchi nei seguenti formati.

La dimensione massima di ogni file che ospita l'elenco di indirizzi IP affidabili o di IP delle minacce è 35 MB. Negli elenchi di IP affidabili e negli elenchi di indirizzi IP delle minacce, gli indirizzi IP e gli CIDR intervalli devono apparire uno per riga. Sono accettati solo IPv4 gli indirizzi.

- Testo semplice () TXT

Questo formato supporta sia indirizzi IP a CIDR blocchi che singoli. Il seguente elenco di esempio utilizza il formato Plaintext (TXT).

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

- Espressione di informazioni strutturate sulle minacce () STIX

  Questo formato supporta sia indirizzi IP a CIDR blocchi che singoli. Il seguente elenco di esempio utilizza il STIX formato.

```
<?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>
```

- Open Threat Exchange (OTX) ™ CSV

  Questo formato supporta sia indirizzi IP a CIDR blocchi che singoli. Il seguente elenco di esempio utilizza il 0TX™ CSV formato.

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEye™ è SIGHT Threat Intelligence CSV

Questo formato supporta sia indirizzi IP a CIDR blocchi che singoli. Il seguente elenco di esempio utilizza un `FireEye`™ CSV formato.

```
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 ™ ET Intelligence Feed CSV

  Questo formato supporta solo indirizzi IP individuali. Il seguente elenco di esempio utilizza il `Proofpoint` CSV formato. Il parametro `ports` è facoltativo. Se non inserisci il parametro porta, assicurati di lasciare una virgola finale (,).

  ```
  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™ Reputation Feed

Questo formato supporta solo indirizzi IP individuali. Il seguente elenco di esempio utilizza il formato `AlienVault`.

```
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
```

Autorizzazioni necessarie per caricare elenchi di indirizzi IP affidabili ed elenchi minacce

Diverse IAM identità richiedono autorizzazioni speciali per utilizzare elenchi di IP affidabili e elenchi di minacce. GuardDuty Un'identità con la policy gestita AmazonGuardDutyFullAccess collegata può rinominare e disattivare soltanto gli elenchi di indirizzi IP affidabili e gli elenchi minacce caricati.

Per concedere a varie identità l'accesso completo alla gestione degli elenchi di indirizzi IP affidabili e gli elenchi minacce (in aggiunta alla ridenominazione e alla disattivazione, sono inclusi anche l'aggiunta, l'attivazione, l'eliminazione e l'aggiornamento della posizione o del nome degli elenchi), assicurati che le operazioni seguenti siano presenti nella policy di autorizzazioni collegata a un utente, gruppo o ruolo:

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> Queste operazioni non sono incluse nella policy gestita `AmazonGuardDutyFullAccess`.

Utilizzo della crittografia lato server per elenchi di indirizzi IP affidabili ed elenchi minacce

GuardDuty supporta i seguenti tipi di crittografia per gli elenchi: SSE - AES256 e SSE -. KMS SSE-C non è supportato. Per ulteriori informazioni sui tipi di crittografia per S3, consulta Protezione dei dati con la crittografia lato server.

Se l'elenco è crittografato utilizzando la crittografia SSE lato server, è KMS necessario concedere al ruolo GuardDuty collegato al servizio l'AWSServiceRoleForAmazonGuardDutyautorizzazione a decrittografare il file per attivare l'elenco. Aggiungi la seguente dichiarazione alla politica KMS chiave e sostituisci l'ID dell'account con il tuo:

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

Aggiunta e attivazione di un elenco di indirizzi IP affidabili o di IP delle minacce

Scegli uno dei seguenti metodi di accesso per aggiungere e attivare un elenco di indirizzi IP affidabili o di IP delle minacce.

Console

Fase 1 (Facoltativa): Recupero URL della posizione dell'elenco

1. Apri la console Amazon S3 all'indirizzo. https://console.aws.amazon.com/s3/
2. Nel pannello di navigazione, scegli Bucket.
3. Scegli il nome del bucket Amazon S3 che contiene l'elenco specifico che vuoi aggiungere.
4. Scegli il nome dell'oggetto (elenco) per visualizzarne i dettagli.
5. Nella scheda Proprietà, copia l'S3 URI per questo oggetto.

Fase 2: aggiunta di un elenco di indirizzi IP affidabili o un elenco minacce

> **Important**
>
> Per impostazione predefinita, in qualsiasi momento, puoi avere un solo elenco di indirizzi IP affidabili e fino a sei elenchi minacce.

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina List management (Gestione dell'elenco), scegliere Add a trusted IP list (Aggiungi un elenco di IP affidabili) o Add a threat list (Aggiungi un elenco minacce).
4. In base alla selezione effettuata, verrà visualizzata una finestra di dialogo. Procedi come segue:

   a. Per Nome elenco, inserisci un nome per l'elenco.

      Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

   b. Per Posizione, fornisci la posizione in cui hai caricato l'elenco. Se non hai ancora una posizione, consulta Step 1: Fetching location URL of your list.

      Formato della posizione 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. Selezionare la casella di controllo I agree (Accetto).

   d. Scegliere Add list (Aggiungi elenco). Per impostazione predefinita, lo Stato dell'elenco aggiunto è Inattivo. Affinché l'elenco sia efficace, è necessario attivarlo.

Fase 3: attivazione di un elenco di indirizzi IP affidabili o di un elenco minacce

1. Aprire la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina Gestione dell'elenco, seleziona l'elenco che desideri attivare.
4. Scegli Operazioni, quindi Attiva. Potrebbero essere necessari fino a 15 minuti prima che l'elenco sia efficace.

API/CLI

Per elenchi di indirizzi IP affidabili

- Esegui reateIPSetC. Assicurati di fornire il `detectorId` dell'account membro per il quale desideri creare questo elenco di indirizzi IP affidabili.

  Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).

  - In alternativa, puoi farlo eseguendo il comando AWS Command Line Interface seguente. Assicurati di sostituire il `detector-id` con l'ID rilevatore dell'account membro per il quale aggiornerai l'elenco degli indirizzi IP affidabili.

    ```
    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
    ```

Per gli elenchi minacce

- Esegui. CreateThreatIntelSet Assicurati di fornire il `detectorId` dell'account membro per il quale desideri creare questo elenco minacce.
  - In alternativa, è possibile eseguire questa operazione eseguendo il AWS Command Line Interface comando seguente. Assicurati di fornire il `detectorId` dell'account membro per il quale desideri creare un elenco minacce.

    ```
    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**
>
> Dopo aver attivato o aggiornato un elenco di IP, la sincronizzazione dell'elenco GuardDuty potrebbe richiedere fino a 15 minuti.

Aggiornamento di elenchi di indirizzi IP affidabili e di elenchi minacce

È possibile aggiornare il nome di un elenco o gli indirizzi IP aggiunti a un elenco che è già stato aggiunto e attivato. Se si aggiorna un elenco, è necessario riattivarlo GuardDuty per utilizzare la versione più recente dell'elenco.

Scegli uno dei metodi di accesso per aggiornare un elenco di IP affidabili o un elenco minacce.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina Gestione dell'elenco, seleziona il set di IP affidabili o un elenco minacce che desideri aggiornare.
4. Seleziona Azioni, quindi scegli Modifica.
5. Nella finestra di dialogo Aggiorna elenco, aggiorna le informazioni in base alle esigenze.

   Vincoli di denominazione degli elenchi: il nome dell'elenco può includere lettere minuscole, lettere maiuscole, numeri, trattino (-) e trattino basso (_).
6. Scegli la casella Accetto, quindi Aggiorna elenco. Il valore nella colonna Stato diventerà Inattivo.
7. Riattivazione dell'elenco aggiornato

   a. Nella pagina Gestione dell'elenco, seleziona l'elenco che desideri riattivare.

   b. Scegli Operazioni, quindi Attiva.

API/CLI

1. Esegui UpdateIPSet per aggiornare un elenco di indirizzi IP affidabili.

- In alternativa, puoi eseguire il comando AWS CLI seguente per aggiornare un elenco di indirizzi IP affidabili. Assicurati di sostituire il `detector-id` con l'ID rilevatore dell'account membro per il quale aggiornerai l'elenco degli indirizzi IP affidabili.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
activate
```

2. Eseguire UpdateThreatIntelSet per aggiornare un elenco minacce
   - In alternativa, puoi eseguire il comando AWS CLI seguente per aggiornare un elenco minacce. Assicurati di sostituire il `detector-id` con l'ID rilevatore dell'account membro per il quale aggiornerai l'elenco minacce.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --activate
```

Disattivazione o eliminazione di un elenco di indirizzi IP affidabili o un elenco minacce

Scegli uno dei metodi di accesso per eliminare (utilizzando la console) o disattivare (utilizzandoAPI/CLI) un elenco di IP affidabili o un elenco di minacce.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel riquadro di navigazione, scegli Elenchi.
3. Nella pagina Gestione dell'elenco, seleziona l'elenco che desideri eliminare.
4. Scegli Azioni, quindi Elimina.
5. Conferma l'operazione e scegli Elimina. L'elenco specifico non sarà più disponibile nella tabella.

API/CLI

1. Per un elenco di indirizzi IP affidabili

   Esegui UpdateIPSet per aggiornare un elenco di indirizzi IP affidabili.

- In alternativa, puoi eseguire il comando AWS CLI seguente per aggiornare un elenco di indirizzi IP affidabili. Assicurati di sostituire il `detector-id` con l'ID rilevatore dell'account membro per il quale aggiornerai l'elenco degli indirizzi IP affidabili.

  Per trovare le `detectorId` impostazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

```
aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
no-activate
```

2. Per un elenco minacce

   Eseguire UpdateThreatIntelSet per aggiornare un elenco minacce

   - In alternativa, puoi eseguire il comando AWS CLI seguente per aggiornare un elenco di indirizzi IP affidabili. Assicurati di sostituire il `detector-id` con l'ID rilevatore dell'account membro per il quale aggiornerai l'elenco minacce.

```
aws guardduty update-threatintel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
intel-set-id d4b94fc952d6912b8f3060768example --no-activate
```

Esportazione degli esiti

GuardDuty conserva i risultati generati per un periodo di 90 giorni. GuardDuty esporta i risultati attivi su Amazon EventBridge (EventBridge). Facoltativamente, puoi esportare i risultati generati in un bucket Amazon Simple Storage Service (Amazon S3). Questo ti aiuterà a tenere traccia dei dati storici delle attività potenzialmente sospette nel tuo account e a valutare se le misure correttive consigliate hanno avuto successo.

Tutti i nuovi risultati attivi GuardDuty generati vengono esportati automaticamente entro circa 5 minuti dalla generazione del risultato. È possibile impostare la frequenza con cui vengono esportati gli aggiornamenti dei risultati attivi. EventBridge La frequenza selezionata si applica all'esportazione di nuove occorrenze di risultati esistenti nel bucket S3 (se configurato) e in Detective (se integrato). EventBridge Per informazioni su come GuardDuty aggrega più occorrenze di risultati esistenti, vedere. GuardDuty trovare l'aggregazione

Quando configuri le impostazioni per esportare i risultati in un bucket Amazon S3, GuardDuty utilizza AWS Key Management Service (AWS KMS) per crittografare i dati dei risultati nel bucket S3. Ciò richiede l'aggiunta di autorizzazioni al bucket S3 e alla AWS KMS chiave in modo che GuardDuty possa utilizzarle per esportare i risultati nel tuo account.

Indice

Considerazioni

Prima di procedere con i prerequisiti e i passaggi per esportare i risultati, considera i seguenti concetti chiave:

- Le impostazioni di esportazione sono regionali: è necessario configurare le opzioni di esportazione in ogni regione in cui si utilizza. GuardDuty
- Esportazione dei risultati in bucket Amazon S3 in Regioni AWS diverse aree geografiche GuardDuty : supporta le seguenti impostazioni di esportazione:
  - Il bucket o l'oggetto Amazon S3 e la AWS KMS chiave devono appartenere allo stesso. Regione AWS
  - Per i risultati generati in una regione commerciale, puoi scegliere di esportarli in un bucket S3 in qualsiasi regione commerciale. Tuttavia, non puoi esportare questi risultati in un bucket S3 in una regione opt-in.
  - Per i risultati generati in una regione opt-in, puoi scegliere di esportarli nella stessa regione opt-in in cui vengono generati o in qualsiasi regione commerciale. Tuttavia, non puoi esportare i risultati da una regione opt-in a un'altra regione opt-in.
- Autorizzazioni per esportare i risultati: per configurare le impostazioni per l'esportazione dei risultati attivi, il bucket S3 deve disporre delle autorizzazioni che consentano di caricare oggetti. GuardDuty È inoltre necessario disporre di una AWS KMS chiave che GuardDuty possa essere utilizzata per crittografare i risultati.

- I risultati archiviati non vengono esportati: il comportamento predefinito prevede che i risultati archiviati, incluse le nuove istanze di risultati soppressi, non vengano esportati.

  Quando un GuardDuty risultato viene generato come archiviato, è necessario estrarlo dall'archivio. Ciò modifica lo stato di ricerca del filtro su Attivo. GuardDuty esporta gli aggiornamenti ai risultati non archiviati esistenti in base alla configurazione. Fase 5 — Frequenza di esportazione dei risultati
- GuardDuty l'account amministratore può esportare i risultati generati negli account membro associati: quando si configurano i risultati di esportazione in un account amministratore, tutti i risultati degli account membro associati generati nella stessa regione vengono esportati nella stessa posizione configurata per l'account amministratore. Per ulteriori informazioni, consulta Comprensione della relazione tra account GuardDuty amministratore e account membro.

Fase 1 — Autorizzazioni necessarie per esportare i risultati

Quando configuri le impostazioni per l'esportazione dei risultati, selezioni un bucket Amazon S3 in cui archiviare i risultati e AWS KMS una chiave da utilizzare per la crittografia dei dati. Oltre alle GuardDuty autorizzazioni per le azioni, devi disporre anche delle autorizzazioni per le seguenti azioni per configurare correttamente le impostazioni per esportare i risultati:

- `s3:GetBucketLocation`
- `s3:PutObject`
- `s3:ListBucket`

Passaggio 2: allegare la politica alla chiave KMS

GuardDuty crittografa i dati dei risultati nel bucket utilizzando. AWS Key Management Service Per configurare correttamente le impostazioni, devi prima GuardDuty autorizzare l'uso di una KMS chiave. Puoi concedere le autorizzazioni allegando la policy alla tua KMS chiave.

Quando utilizzi una KMS chiave di un altro account, devi applicare la politica delle chiavi accedendo al proprietario della Account AWS chiave. Quando configuri le impostazioni per esportare i risultati, avrai anche bisogno della chiave ARN dell'account che possiede la chiave.

Per modificare la politica delle KMS chiavi per GuardDuty crittografare i risultati esportati

1. Apri la AWS KMS console in /kms. https://console.aws.amazon.com

2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.
3. Seleziona una KMS chiave esistente o esegui i passaggi per creare una nuova chiave nella Guida per gli AWS Key Management Service sviluppatori, che utilizzerai per crittografare i risultati esportati.

   > **Note**
   >
   > La Regione AWS KMS chiave e il bucket Amazon S3 devono coincidere.

   Puoi utilizzare lo stesso bucket S3 e la stessa KMS key pair per esportare i risultati da qualsiasi regione applicabile. Per ulteriori informazioni, consulta Esportazione Considerazioni dei risultati tra le regioni.
4. Nella sezione Key policy (Policy chiave), scegli Edit (Modifica).

   Se è visualizzata la visualizzazione Passa alla politica, selezionala per visualizzare la Politica chiave, quindi scegli Modifica.
5. Copia il seguente blocco di policy nella tua policy KMS chiave, per concedere l' GuardDuty autorizzazione all'uso della tua chiave.

```
{
    "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. Modifica la politica sostituendo i seguenti valori formattati in *red*nell'esempio di politica:

1. Replace (Sostituisci) *KMS key ARN* con l'Amazon Resource Name (ARN) della KMS chiave. Per individuare la chiaveARN, consulta Finding the key ID e ARN nella AWS Key Management Service Developer Guide.
2. Replace (Sostituisci) *123456789012* con l' Account AWS ID proprietario dell' GuardDuty account che esporta i risultati.
3. Replace (Sostituisci) *Region2* con il Regione AWS luogo in cui vengono generati i GuardDuty risultati.
4. Replace (Sostituisci) *SourceDetectorID* con il GuardDuty conto `detectorID` della regione specifica in cui sono stati generati i risultati.

   Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

> **Note**
>
> Se lo utilizzi GuardDuty in una regione che richiede l'attivazione, sostituisci il valore per «Servizio» con l'endpoint regionale per quella regione. Ad esempio, se utilizzi GuardDuty nella regione Medio Oriente (Bahrain) (me-south-1), sostituisci con. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Per informazioni sugli endpoint per ogni regione opt-in, consulta endpoint e quote. GuardDuty

7. Se hai aggiunto l'informativa prima dell'informativa finale, aggiungi una virgola prima di aggiungere questa dichiarazione. Assicurati che la JSON sintassi della tua politica KMS chiave sia valida.

   Seleziona Salva.
8. (Facoltativo) Copia la chiave ARN su un blocco note per utilizzarla nei passaggi successivi.

Fase 3: Allegare la policy al bucket Amazon S3

Aggiungi le autorizzazioni al bucket Amazon S3 in cui esporterai i risultati in modo da poter caricare oggetti in GuardDuty questo bucket S3. Indipendentemente dall'utilizzo di un bucket Amazon S3 che appartiene al tuo account o a un altro Account AWS, devi aggiungere queste autorizzazioni.

Se in qualsiasi momento decidi di esportare i risultati in un altro bucket S3, per continuare a esportare i risultati, devi aggiungere le autorizzazioni a quel bucket S3 e configurare nuovamente le impostazioni dei risultati di esportazione.

Se non disponi già di un bucket Amazon S3 in cui esportare questi risultati, consulta Creating a bucket nella Amazon S3 User Guide.

Per allegare le autorizzazioni alla tua policy sui bucket S3

1. Esegui i passaggi indicati in Per creare o modificare una policy sui bucket nella Guida per l'utente di Amazon S3, finché non viene visualizzata la pagina Modifica policy del bucket.
2. La policy di esempio mostra come concedere GuardDuty l'autorizzazione all'esportazione dei risultati nel bucket Amazon S3. Se modifichi il percorso dopo aver configurato i risultati di esportazione, devi modificare la politica per concedere l'autorizzazione alla nuova posizione.

   Copia la seguente politica di esempio e incollala nell'editor delle politiche Bucket.

   Se hai aggiunto l'informativa prima dell'informativa finale, aggiungi una virgola prima di aggiungere questa dichiarazione. Assicurati che la JSON sintassi della tua politica KMS chiave sia valida.

   Esempio di politica del bucket S3

```
{
    "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. Modifica la politica sostituendo i seguenti valori formattati in *red*nell'esempio di politica:

   1. Replace (Sostituisci) *Amazon S3 bucket ARN* con l'Amazon Resource Name (ARN) del bucket Amazon S3. Puoi trovare il Bucket ARN nella pagina Modifica policy del bucket nella console. https://console.aws.amazon.com/s3/
   2. Replace (Sostituisci) *123456789012* con l' Account AWS ID proprietario dell' GuardDuty account che esporta i risultati.
   3. Replace (Sostituisci) *Region2* con il Regione AWS luogo in cui vengono generati i GuardDuty risultati.
   4. Replace (Sostituisci) *SourceDetectorID* con il GuardDuty conto `detectorID` della regione specifica in cui sono stati generati i risultati.

      Per trovare le `detectorId` informazioni relative al tuo account e alla regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.
   5. Replace (Sostituisci) *[optional prefix]* parte del *S3 bucket ARN/[optional prefix]* valore segnaposto con una posizione opzionale nella cartella in cui si desidera esportare i risultati. Per ulteriori informazioni sull'uso dei prefissi, consulta Organizing objects using prefixes nella Amazon S3 User Guide.

Se fornisci una posizione opzionale per la cartella che non esiste già, la GuardDuty creerà solo se l'account associato al bucket S3 è lo stesso dell'account che esporta i risultati. Quando esporti i risultati in un bucket S3 che appartiene a un altro account, la posizione della cartella deve già esistere.

6. Replace (Sostituisci) *KMS key ARN* con l'Amazon Resource Name (ARN) della KMS chiave associata alla crittografia dei risultati esportati nel bucket S3. Per individuare la chiaveARN, consulta Finding the key ID e ARN nella Developer Guide.AWS Key Management Service

> **Note**
>
> Se lo utilizzi GuardDuty in una regione che richiede l'attivazione, sostituisci il valore per «Servizio» con l'endpoint regionale per quella regione. Ad esempio, se utilizzi GuardDuty nella regione Medio Oriente (Bahrain) (me-south-1), sostituisci con. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Per informazioni sugli endpoint per ogni regione opt-in, consulta endpoint e quote. GuardDuty

4. Seleziona Salva.

Fase 4 - Esportazione dei risultati in un bucket S3 (console)

GuardDuty consente di esportare i risultati in un bucket esistente in un altro. Account AWS

Quando crei un nuovo bucket S3 o scegli un bucket esistente nel tuo account, puoi aggiungere un prefisso opzionale. Quando configuri i risultati dell'esportazione, GuardDuty crea una nuova cartella nel bucket S3 per i risultati. Il prefisso verrà aggiunto alla struttura di cartelle predefinita creata. GuardDuty Ad esempio, il formato del prefisso opzionale. `/AWSLogs/123456789012/GuardDuty/Region`

L'intero percorso dell'oggetto S3 sarà. *amzn-s3-demo-bucket*`/`*prefix-name*`/UUID.jsonl.gz` `UUID`Viene generato casualmente e non rappresenta l'ID del rilevatore o l'ID del ritrovamento.

> **Important**
>
> La KMS chiave e il bucket S3 devono trovarsi nella stessa regione.

Prima di completare questi passaggi, assicurati di aver collegato le rispettive politiche alla tua KMS chiave e al bucket S3 esistente.

Per configurare i risultati delle esportazioni

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella pagina Impostazioni, in Opzioni di esportazione di Findings, per il bucket S3, scegli Configura ora (o Modifica, se necessario).
4. Per il bucket ARN S3, inserisci il. **`bucket ARN`** Per trovare il bucketARN, consulta Visualizzazione delle proprietà di un bucket S3 nella Amazon S3 User Guide. Nella scheda Autorizzazioni della pagina delle proprietà del bucket associato nella console. https://console.aws.amazon.com/guardduty/
5. Come KMSchiave ARN, inserisci il. **`key ARN`** Per individuare la chiaveARN, consulta Finding the key ID e ARN nella AWS Key Management Service Developer Guide.
6. Allega politiche
   - Esegui i passaggi per allegare la policy del bucket S3. Per ulteriori informazioni, consulta Fase 3: Allegare la policy al bucket Amazon S3.
   - Esegui i passaggi per allegare la policy KMS chiave. Per ulteriori informazioni, consulta Passaggio 2: allegare la politica alla chiave KMS.
7. Seleziona Save (Salva.

Fase 5 — Impostazione della frequenza per esportare i risultati attivi aggiornati

Configura la frequenza di esportazione dei risultati attivi aggiornati in base al tuo ambiente. Per impostazione predefinita, i risultati aggiornati vengono esportati ogni 6 ore. Ciò significa che tutti i risultati aggiornati dopo l'esportazione più recente sono inclusi nella successiva esportazione. Se i risultati aggiornati vengono esportati ogni 6 ore e l'esportazione avviene alle 12:00, qualsiasi scoperta che si aggiorna dopo le 12:00 viene esportata alle 18:00.

Per impostare la frequenza

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

2. Seleziona Impostazioni.
3. Nella sezione Opzioni di esportazione dei risultati, scegli Frequenza dei risultati aggiornati. Questo imposta la frequenza per l'esportazione dei risultati Active aggiornati sia EventBridge su Amazon S3 che su Amazon S3. Puoi scegliere tra le seguenti opzioni:
   - Update EventBridge e S3 ogni 15 minuti
   - Update EventBridge e S3 ogni 1 ora
   - Aggiornamento CWE e S3 ogni 6 ore (impostazione predefinita)
4. Scegli Save changes (Salva modifiche).

Creazione di risposte personalizzate ai GuardDuty risultati con Amazon CloudWatch Events

GuardDuty crea un evento per Amazon CloudWatch Events quando si verifica una modifica dei risultati. La ricerca di modifiche che creerà un CloudWatch evento include risultati appena generati o risultati appena aggregati. Gli eventi vengono emessi secondo il principio del massimo sforzo.

A ogni GuardDuty risultato viene assegnato un ID di ricerca. GuardDuty crea un CloudWatch evento per ogni risultato con un ID di ricerca univoco. Tutte le occorrenze successive di un esito esistente vengono aggregate all'esito originale. Per ulteriori informazioni, consulta GuardDuty trovare l'aggregazione.

> **Note**
>
> Se il tuo account è un amministratore GuardDuty delegato, gli CloudWatch eventi vengono pubblicati sul tuo account e sull'account membro in cui è stato generato il risultato.

Utilizzando CloudWatch events with GuardDuty, puoi automatizzare le attività per aiutarti a rispondere ai problemi di sicurezza rivelati dai GuardDuty risultati.

Per ricevere notifiche sui GuardDuty risultati basati sugli CloudWatch Eventi, devi creare una regola CloudWatch Events e un obiettivo per GuardDuty. Questa regola consente CloudWatch di inviare notifiche relative ai risultati GuardDuty generati alla destinazione specificata nella regola. Per ulteriori informazioni, consulta Creazione di una regola CloudWatch Events e di un target per GuardDuty (CLI).

Argomenti

CloudWatch Frequenza di notifica degli eventi per GuardDuty

Notifiche per gli esiti appena generati con un ID esito univoco

GuardDuty invia una notifica in base all' CloudWatch evento entro 5 minuti dal riscontro. Questo evento (e questa notifica) include inoltre tutte le occorrenze successive di tale risultato che avvengono nei 5 minuti successivi alla generazione del risultato con un ID univoco.

> **Note**
>
> Per impostazione predefinita, le notifiche per gli esiti appena generati vengono inviate ogni 5 minuti. Questa frequenza non può essere aggiornata.

Notifiche per occorrenze di esiti successive

Per impostazione predefinita, per ogni risultato con un ID di risultato univoco, GuardDuty aggrega tutte le occorrenze successive di un particolare tipo di risultato che si verificano entro intervalli di 6 ore in un unico evento. GuardDuty invia quindi una notifica su queste occorrenze successive in base a questo evento. Per impostazione predefinita, per le ricorrenze successive dei risultati esistenti, GuardDuty invia notifiche basate sugli CloudWatch eventi ogni 6 ore.

Solo un account amministratore può personalizzare la frequenza predefinita delle notifiche inviate relative alle CloudWatch successive rilevazioni di eventi. Gli utenti di account membri non possono personalizzare la frequenza. Il valore di frequenza impostato dall'account amministratore nel proprio account è imposto alla GuardDuty funzionalità di tutti gli account membri. Se un utente di un account amministratore imposta questo valore di frequenza su 1 ora, tutti gli account membro avranno anche la frequenza di 1 ora di ricezione delle notifiche relative ai successivi ritrovamenti. Per ulteriori informazioni, consulta Gestione di più account in Amazon GuardDuty.

> **Note**
>
> In qualità di account amministratore, puoi personalizzare la frequenza predefinita delle notifiche relative ai successivi ritrovamenti. I valori possibili sono 15 minuti, 1 ora o 6 ore (impostazione predefinita). Per ulteriori informazioni sull'impostazione della frequenza di queste notifiche, consulta Fase 5 — Impostazione della frequenza per esportare i risultati attivi aggiornati.

Monitoraggio dei GuardDuty risultati archiviati con Events CloudWatch

Per i risultati archiviati manualmente, le occorrenze iniziali e tutte le successive di questi risultati (generate dopo il completamento dell'archiviazione) vengono inviate a CloudWatch Events secondo la frequenza sopra descritta.

Per i risultati archiviati automaticamente, le occorrenze iniziali e tutte le successive di questi risultati (generate dopo il completamento dell'archiviazione) non vengono inviate agli Eventi. CloudWatch

CloudWatch formato di evento per GuardDuty

Il formato dell' CloudWatch evento per GuardDuty .

```
{
 "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**
>
> Il valore di dettaglio restituisce i dettagli JSON di un singolo esito come oggetto, invece di restituire il valore "esiti", che può supportare più esiti all'interno di un array.

Per un elenco completo di tutti i parametri inclusi in `GUARDDUTY_FINDING_JSON_OBJECT`, consulta GetFindings. Il parametro `id` visualizzato in `GUARDDUTY_FINDING_JSON_OBJECT` è l'ID risultato descritto precedentemente.

Creazione di una regola CloudWatch Events per notificare GuardDuty i risultati (console)

Puoi utilizzare CloudWatch Events with GuardDuty per impostare avvisi di ricerca automatici inviando eventi di GuardDuty ricerca a un hub di messaggistica per aumentare la visibilità dei GuardDuty risultati. Questo argomento mostra come inviare avvisi di risultati via e-mail, Slack o Amazon Chime configurando un argomento SNS e collegando tale argomento a CloudWatch una regola di evento Events.

Impostare un argomento Amazon SNS e un endpoint

Per iniziare, devi impostare innanzitutto un argomento in Amazon Simple Notification Service e aggiungere un endpoint. Per ulteriori informazioni, consulta Nozioni di base nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Questa procedura stabilisce dove inviare i dati di ricerca. GuardDuty L'argomento SNS può essere aggiunto a una regola CloudWatch Events Event durante o dopo la creazione della Regola di evento.

Email setup

Creazione di un argomento SNS

1. Accedi alla console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Selezionare Argomenti dal riquadro di navigazione e quindi Crea argomento.
3. Nella sezione Crea argomento, seleziona Standard. Inserisci quindi un Nome argomento, ad esempio **`GuardDuty_to_Email`**. Altri dettagli sono facoltativi.
4. Seleziona Create Topic (Crea argomento). Verranno aperti i dettagli dell'argomento per il nuovo argomento.

5. Nella sezione Sottoscrizioni, scegliere Crea sottoscrizione.
6. a. Dal menu Protocollo selezionare E-mail.
   b. Nel campo Endpoint, aggiungere l'indirizzo e-mail a cui si desidera ricevere le notifiche.

   > **Note**
   >
   > Dopo averlo creato, ti verrà richiesto di confermare l'abbonamento tramite il tuo client e-mail.

   c. Scegli Crea sottoscrizione
7. Controlla la presenza di un messaggio di abbonamento nella Posta in arrivo e scegli Conferma sottoscrizione

Slack setup

Creazione di un argomento SNS

1. Accedi alla console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Selezionare Argomenti dal riquadro di navigazione e quindi Crea argomento.
3. Nella sezione Crea argomento, seleziona Standard. Inserisci quindi un Nome argomento, ad esempio **`GuardDuty_to_Slack`**. Altri dettagli sono facoltativi. Scegli Crea argomento per finalizzare.

Configurazione di un client AWS Chatbot

1. Passa alla console AWS Chatbot
2. Dal pannello Client configurati, seleziona Configura nuovo client.
3. Scegli Slack e conferma con "Configura".

   > **Note**
   >
   > Quando scegli Slack devi confermare le autorizzazioni per permettere a AWS Chatbot di accedere al tuo canale selezionando "consenti".

4. Seleziona Configura un nuovo canale per aprire il riquadro dei dettagli di configurazione.
   a. Inserisci un nome per il canale.

b. Per il canale Slack, scegli il canale che desideri utilizzare. Per utilizzare il canale Slack privato con AWS Chatbot, scegli Canale privato.

c. In Slack, copia l'ID del canale privato facendo clic con il pulsante destro del mouse sul nome del canale e selezionando Copia collegamento.

d. Sulla Console di gestione AWS, nella finestra AWS Chatbot, incolla l'ID che hai copiato da Slack nel campo ID canale privato.

e. In Autorizzazioni, scegli di creare un ruolo IAM utilizzando un modello, se non disponi già di un ruolo.

f. Per i Modelli di policy, scegli Autorizzazioni di notifica. Questo è il modello di policy IAM per AWS Chatbot. Fornisce le autorizzazioni di lettura ed elenco necessarie per CloudWatch allarmi, eventi e registri e per argomenti di Amazon SNS.

g. Scegli la regione in cui hai creato in precedenza l'argomento SNS, quindi seleziona l'argomento Amazon SNS che hai creato per inviare notifiche al canale Slack.

5. Selezionare Configura.

Chime setup

Creazione di un argomento SNS

1. Accedi alla console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Selezionare Argomenti dal riquadro di navigazione e quindi Crea argomento.
3. Nella sezione Crea argomento, seleziona Standard. Inserisci quindi un Nome argomento, ad esempio **`GuardDuty_to_Chime`**. Altri dettagli sono facoltativi. Scegli Crea argomento per finalizzare.

Configurazione di un client AWS Chatbot

1. Passa alla console AWS Chatbot
2. Dal pannello Client configurati, seleziona Configura nuovo client.
3. Scegli Chime e conferma con "Configura".
4. Dal riquadro Dettagli di configurazione, inserisci un nome per il canale.
5. In Chime, apri la chat room desiderata

   a. Seleziona l'icona a forma di ingranaggio nell'angolo in alto a destra e scegli Manage webhooks and bots (Gestisci webhook e bot).

b. Seleziona Copia URL per copiare l'URL del webhook negli appunti.

6. Nella Console di gestione AWS, nella finestra AWS Chatbot, incolla l'URL che hai copiato nel campo URL webhook.
7. In Autorizzazioni, scegli di creare un ruolo IAM utilizzando un modello, se non disponi già di un ruolo.
8. Per i Modelli di policy, scegli Autorizzazioni di notifica. Questo è il modello di policy IAM per AWS Chatbot. Fornisce le autorizzazioni di lettura ed elenco necessarie per CloudWatch allarmi, eventi e registri e per argomenti di Amazon SNS.
9. Scegli la regione in cui hai creato in precedenza l'argomento SNS, quindi seleziona l'argomento Amazon SNS che hai creato per inviare notifiche alla room Chime.
10. Selezionare Configura.

Imposta un evento per i risultati CloudWatch GuardDuty

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Selezionare Regole nel riquadro di navigazione e quindi Crea regola.
3. Dal menu Service Name, scegli GuardDuty.
4. Dal menu Tipo di evento, scegli GuardDutyRicerca.
5. Accanto a Anteprima modello di eventi, selezionare Modifica.
6. Incollare il codice JSON riportato di seguito in Anteprima modello di eventi e scegliere Salva

```
{
  "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**
>
> Il codice di cui sopra avviserà per qualsiasi ricerca media o alta.

7. Nella sezione Destinazioni fare clic su Aggiungi destinazione.
8. Dal menu Seleziona destinazioni, scegliere Argomento SNS.
9. Per Seleziona argomento, selezionare il nome dell'argomento SNS creato nel passaggio 1.
10. Configura l'input per l'evento.

    - Se stai configurando le notifiche per Chime o Slack, vai alla fase 11, il tipo di input predefinito è Evento con corrispondenza.
    - Se stai configurando le notifiche per e-mail tramite SNS, segui i passaggi seguenti per personalizzare il messaggio inviato alla tua casella di posta:

    a. Espandere Configura input, quindi selezionare Trasformatore di input.

    b. Copiare il codice seguente e incollarlo nel campo Percorso di input.

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

    c. Copiare il codice seguente e incollarlo nel campo Modello di input per formattare l'e-mail.

```
"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. Fare clic su Configura dettagli.
12. Nella pagina Configura dettagli della regola, immettere Nome e Descrizione per la regola, quindi scegliere Crea regola.

Creazione di una regola CloudWatch Events e di un target per GuardDuty (CLI)

La procedura seguente mostra come utilizzare AWS CLI i comandi per creare una regola CloudWatch Events e un target per GuardDuty. In particolare, la procedura mostra come creare una regola che CloudWatch consenta di inviare eventi per tutti i risultati che GuardDuty generano e aggiungono una AWS Lambda funzione come destinazione per la regola.

> **Note**
>
> Oltre alle funzioni Lambda, CloudWatch supporta GuardDuty i seguenti tipi di destinazione: istanze Amazon EC2, flussi Amazon Kinesis, AWS Step Functions attività Amazon ECS, macchine a stati, comandi e destinazioni integrate. `run`

Puoi anche creare una regola e un target per CloudWatch gli eventi tramite la console Events. GuardDuty CloudWatch Per ulteriori informazioni e passaggi dettagliati, consulta Creazione di una regola CloudWatch Events che si attiva in base a un evento. Nella sezione Event Source (Origine eventi), selezionare **`GuardDuty`** per Service name (Nome servizio) e **`GuardDuty Finding`** per Event Type (Tipo di evento).

Per creare una regola e un target

1. Per creare una regola che CloudWatch consenta di inviare eventi per tutti i risultati GuardDuty generati, esegui il seguente comando CloudWatch CLI.

```
AWS events put-rule --name Test --event-pattern "{\"source\":
[\"aws.guardduty\"]}"
```

> **Important**
>
> Puoi personalizzare ulteriormente la regola in modo che indichi di CloudWatch inviare eventi solo per un sottoinsieme dei risultati generati GuardDuty. Questo sottoinsieme è basato sull'attributo o sugli attributi di risultato specificati nella regola. Ad esempio, utilizzate il seguente comando CLI per creare una regola che CloudWatch consenta di inviare solo eventi per i GuardDuty risultati con la gravità di 5 o 8:
> `AWS events put-rule --name Test --event-pattern "{\"source\": [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"], \"detail\":{\"severity\":[5,8]}}"`
> A tale scopo, è possibile utilizzare uno qualsiasi dei valori di proprietà disponibili in JSON per GuardDuty i risultati.

2. Per collegare una funzione Lambda come destinazione per la regola creata nel passaggio 1, esegui il seguente comando CLI CloudWatch .

   ```
   AWS events put-targets --rule Test --targets
   Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
   ```

   > **Note**
   >
   > Assicurati di sostituire <your_function>nel comando precedente con la tua effettiva funzione Lambda per gli GuardDuty eventi.

3. Per aggiungere le autorizzazioni necessarie per richiamare la destinazione, esegui il comando CLI di Lambda seguente.

   ```
   AWS lambda add-permission --function-name <your_function> --statement-
   id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
   ```

   > **Note**
   >
   > Assicurati di sostituire <your_function>nel comando precedente con la tua effettiva funzione Lambda per gli GuardDuty eventi.

> **Note**
>
> Nella procedura precedente, utilizziamo una funzione Lambda come obiettivo per la regola che attiva CloudWatch gli eventi. Puoi anche configurare altre AWS risorse come obiettivi per attivare CloudWatch gli eventi. Per ulteriori informazioni, consulta PutTargets.

CloudWatch Eventi per ambienti GuardDuty con più account

In qualità di GuardDuty amministratore, le regole relative agli CloudWatch eventi nel tuo account verranno attivate in base ai risultati applicabili degli account dei tuoi membri. Ciò significa che se imposti una notifica di ricerca tramite CloudWatch Eventi nel tuo account amministratore, come descritto nella sezione precedente, riceverai una notifica in merito ai risultati di alta e media gravità generati dai tuoi account membro oltre che dai tuoi.

Puoi identificare l'account membro da cui ha avuto origine la GuardDuty scoperta utilizzando il `accountId` campo dei dettagli JSON del risultato.

Per iniziare a scrivere una regola di evento personalizzata per un account membro specifico nel tuo ambiente nella console, crea una nuova regola e incolla il seguente modello nell'Anteprima modello di eventi, aggiungendo l'ID dell'account membro per cui desideri attivare l'evento.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> Questo esempio si attiverà con il rilevamento di qualsiasi esito relativo all'ID account elencato. È possibile aggiungere più ID separati da una virgola seguendo la sintassi JSON.

Comprensione CloudWatch dei log e dei motivi per cui le risorse vengono ignorate durante la scansione Malware Protection for EC2

GuardDuty Malware Protection for EC2 pubblica gli eventi nel CloudWatch tuo gruppo di log Amazon /aws/guardduty/. malware-scan-events Puoi monitorare lo stato e il risultato della scansione delle risorse interessate per ciascuno degli eventi relativi alla scansione malware. Alcune risorse Amazon EC2 e volumi Amazon EBS potrebbero essere stati ignorati durante la scansione Malware Protection for EC2.

Controllo dei CloudWatch log in Malware Protection for EC2 GuardDuty

Esistono tre tipi di eventi di scansione supportati nel gruppo di log malware-scan-events CloudWatch /aws/guardduty/.

Nome dell'evento di scansione Malware Protection for EC2	Spiegazione
`EC2_SCAN_STARTED`	Creato quando un GuardDuty Malware Protection for EC2 avvia il processo di scansione antimalware, ad esempio quando si prepara a scattare un'istantanea di un volume EBS.
`EC2_SCAN_COMPLETED`	Creato al termine della scansione di GuardDuty Malware Protection for EC2 per almeno uno dei volumi EBS della risorsa interessata. Questo evento include anche lo `snapshotId` appartenente al volume EBS scansionato. Al termine della scansione, il risultato sarà `CLEAN`, `THREATS_FOUND` o `NOT_SCANNED` .

Nome dell'evento di scansione Malware Protection for EC2	Spiegazione
`EC2_SCAN_SKIPPED`	Creato quando la scansione di GuardDuty Malware Protection for EC2 ignora tutti i volumi EBS della risorsa interessata. Per identificare il motivo per cui vengono ignorati, seleziona l'evento corrispondente e visualizza i dettagli. Per ulteriori informazioni sui motivi per cui le risorse vengono ignorate, consulta Motivi per cui una risorsa viene ignorata durante la scansione malware di seguito.

> **Note**
>
> Se utilizzi un AWS Organizations, gli eventi di CloudWatch registro degli account dei membri in Organizations vengono pubblicati sia nell'account amministratore che nel gruppo di registro dell'account membro.

Scegli il metodo di accesso preferito per visualizzare e interrogare CloudWatch gli eventi.

Console

1. Accedi AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, in Log, scegli Gruppi di log. Scegli il gruppo di malware-scan-events log /aws/guardduty/ per visualizzare gli eventi di scansione per Malware Protection for EC2. GuardDuty

   Per eseguire una query, scegli Log Insights.

   Per informazioni sull'esecuzione di una query, consulta Analyzing log data with CloudWatch Logs Insights nella Amazon CloudWatch User Guide.
3. Scegli ID scansione per monitorare i dettagli della risorsa interessata e gli esiti relativi al malware. Ad esempio, puoi eseguire la seguente query per filtrare gli eventi di CloudWatch registro utilizzando. `scanId` Assicurati di utilizzare il tuo *`scan-id`* valido.

```
fields @timestamp, @message, scanRequestDetails.scanId as scanId
| filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
| sort @timestamp asc
```

API/CLI

- Per lavorare con i gruppi di log, consulta la sezione Ricerca AWS CLI nelle voci di log utilizzando l'Amazon CloudWatch User Guide.

  Scegli il gruppo di malware-scan-events log /aws/guardduty/ per visualizzare gli eventi di scansione per Malware Protection for EC2. GuardDuty
- Per visualizzare e filtrare gli eventi di log, consulta GetLogEventse FilterLogEvents, rispettivamente, nell'Amazon CloudWatch API Reference.

GuardDuty Protezione da malware per la conservazione dei log EC2

Il periodo di conservazione dei log predefinito per il gruppo /aws/guardduty/ è di 90 giorni, dopodiché gli eventi di malware-scan-events registro vengono eliminati automaticamente. Per modificare la politica di conservazione dei log per il tuo gruppo di CloudWatch log, consulta Change log data retention in CloudWatch Logs nella Amazon CloudWatch User Guide o PutRetentionPolicynell'Amazon CloudWatch API Reference.

Motivi per cui una risorsa viene ignorata durante la scansione malware

Negli eventi relativi alla scansione malware, alcune risorse EC2 e alcuni volumi EBS potrebbero essere stati ignorati durante il processo di scansione. La tabella seguente elenca i motivi per cui GuardDuty Malware Protection for EC2 potrebbe non scansionare le risorse. Se applicabile, utilizza i passaggi proposti per risolvere questi problemi ed esegui la scansione di queste risorse la prossima volta che GuardDuty Malware Protection for EC2 avvia una scansione antimalware. Gli altri problemi vengono utilizzati per informarti sul corso degli eventi e non possono essere risolti.

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
`RESOURCE_NOT_FOUND`	La scansione antimalware `resourceArn` fornita per avviare la scansione antimalware su richiesta non è stata trovata nel tuo ambiente. AWS	Convalida il `resourceArn` dell'istanza Amazon EC2 o del carico di lavoro di un container e riprova.	
`ACCOUNT_INELIGIBLE`	L'ID AWS dell'account da cui hai provato ad avviare una scansione antimalware su richiesta non è abilitato. GuardDuty	Verifica che GuardDuty sia abilitato per questo AWS account. Quando ne GuardDuty abiliti uno nuovo Regione AWS , la sincronizzazione potrebbe richiedere fino a 20 minuti.	
`UNSUPPORTED_KEY_ENCRYPTION`	GuardDuty Malware Protection for EC2 supporta volumi non crittografati e crittografati con chiave gestita dal cliente. Non supporta la scansione di volumi EBS crittografati utilizzando la Crittografia di Amazon EBS.	Sostituisci la chiave di crittografia con una chiave gestita dal cliente. Per ulteriori informazioni sui tipi di crittografia GuardDuty supportati, vedereEBSVolumi Amazon supportati per la scansione di malware.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
	Attualmente, esiste una differenza regionale per cui questo motivo di salto non è applicabile. Per ulteriori informazioni su questi aspetti Regioni AWS, vedere. Disponibilità di funzionalità specifiche per ogni regione		
`EXCLUDED_BY_SCAN_SETTINGS`	L'istanza EC2 o il volume EBS sono stati esclusi durante la scansione malware. Esistono due motivazioni possibili: il tag è stato aggiunto all'elenco di inclusione, ma la risorsa non è associata a questo tag, il tag è stato aggiunto all'elenco di esclusione e la risorsa è associata a questo tag oppure il tag `GuardDutyExcluded` è impostato su `true` per questa risorsa.	Aggiorna le opzioni di scansione o i tag associati alla tua risorsa Amazon EC2. Per ulteriori informazioni, consulta Opzioni di scansione con tag definiti dall'utente.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
UNSUPPORTED_VOLUME_SIZE	Il volume è superiore a 2048 GB.	Non utilizzabile.	
NO_VOLUMES_ATTACHED	GuardDuty Malware Protection for EC2 ha rilevato l'istanza nel tuo account, ma nessun volume EBS è stato collegato a questa istanza per procedere con la scansione.	Non utilizzabile.	
UNABLE_TO_SCAN	Si tratta di un errore interno del servizio.	Non utilizzabile.	
SNAPSHOT_NOT_FOUND	Le istantanee create dai volumi EBS e condivise con l'account del servizio non sono state trovate e GuardDuty Malware Protection for EC2 non è riuscito a procedere con la scansione.	Verifica che CloudTrail le istantanee non siano state rimosse intenzionalmente.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
SNAPSHOT_QUOTA_REACHED	Hai raggiunto il volume massimo consentito per gli snapshot per ogni regione. Per questo motivo non è possibile né conservare né creare nuovi snapshot.	Puoi rimuovere gli snapshot meno recenti o richieder e un aumento della quota. Puoi visualizz are il limite predefini to per gli snapshot per ogni regione e scoprire come richiedere l'aumento della quota in Service Quotas nella Guida di riferimento generale di AWS .	
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	Più di 11 volumi EBS sono stati collegati a un'istanza EC2. GuardDuty Malware Protection for EC2 ha analizzato i primi 11 volumi EBS, ottenuti ordinandoli alfabetic amente. deviceName	Non utilizzabile.	

Motivi per cui una risorsa potrebbe essere ignorata	Spiegazione	Fasi proposte	
`UNSUPPORTED_PRODUCT_CODE_TYPE`	GuardDuty non supporta la scansione delle istanze con as. `productCode` `marketplace` Per ulteriori informazioni, consulta AMI a pagamento nella Guida per l'utente di Amazon EC2. Per informazioni su `productCode` , consulta ProductCode, nella Documentazione di riferimento delle API di Amazon EC2.	Non utilizzabile.	

Segnalazione di falsi positivi in GuardDuty Malware Protection for EC2

GuardDuty Le scansioni di Malware Protection for EC2 possono identificare un file innocuo nell'istanza di Amazon EC2 o nel carico di lavoro del container come malevolo o dannoso. Per migliorare la tua esperienza con Malware Protection for EC2 e il GuardDuty servizio, puoi segnalare risultati falsi positivi se ritieni che un file identificato come dannoso o dannoso durante una scansione non contenga effettivamente malware.

Invio di un file falso positivo

1. Accedi alla console https://console.aws.amazon.com/guardduty/.

2. Quando identifichi quello che sembra essere un risultato falso positivo, contatta AWS Support per avviare il processo di invio del file falso positivo.
3. Scegli Scansioni malware.
4. Scegli una scansione per visualizzare l'ID risultato.
5. Fornisci l'ID risultato. Devi fornire anche l'hash SHA-256 del file Ciò è necessario per garantire che GuardDuty Malware Protection for EC2 abbia ricevuto il file corretto.
6. Il AWS Support team ti fornirà un URL di Amazon Simple Storage Service (S3) che potrai utilizzare per caricare il file e l'hash SHA-256. Informa il AWS Support team dopo aver caricato correttamente il file.

> **Warning**
>
> Non fornire direttamente il file o l'hash SHA-256 a AWS Support. Carica il file e l'hash su Amazon S3 solo tramite l'URL fornito. Se non carichi il file e l'hash entro sette giorni dalla ricezione dell'URL, quest'ultimo non sarà più valido. Se l'URL non è valido, dovrai contattarci per AWS Support ricevere un nuovo URL.

GuardDuty conserva il file per non più di 30 giorni. GuardDuty i membri del team analizzeranno la tua richiesta e prenderanno le misure appropriate per migliorare la tua esperienza con Malware Protection for EC2 e il GuardDuty servizio.

Risolvere i problemi di sicurezza scoperti da GuardDuty

Amazon GuardDuty genera risultati che indicano potenziali problemi di sicurezza. In questa versione di GuardDuty, i potenziali problemi di sicurezza indicano una compromissione del carico di lavoro dell'EC2istanza o del container oppure un insieme di credenziali compromesse nell'ambiente in uso. AWS Le sezioni seguenti descrivono le operazioni di correzione consigliate per questi scenari. Eventuali scenari di correzione alternativi verranno descritti nella voce del tipo di esito specifico. Puoi accedere alle informazioni complete su un tipo di esito selezionandolo dalla tabella relativa ai tipi di esiti attivi.

Indice

Correzione di un'istanza Amazon potenzialmente compromessa EC2

Segui questi passaggi consigliati per correggere un'EC2istanza potenzialmente compromessa nel tuo ambiente: AWS

1. Identifica l'istanza Amazon EC2 potenzialmente compromessa

   Ricerca malware nell'istanza potenzialmente compromessa e rimuovi quello rilevato. Puoi utilizzarla Scansione antimalware on demand per identificare il malware nell'EC2istanza potenzialmente compromessa o Marketplace AWSverificare se esistono prodotti partner utili per identificare e rimuovere il malware.

2. Isolare l'istanza Amazon potenzialmente compromessa EC2

   Se possibile, utilizza i seguenti passaggi per isolare l'istanza potenzialmente compromessa:

   1. Crea un gruppo di sicurezza Isolation dedicato. Un gruppo di sicurezza di isolamento deve avere accesso in entrata e in uscita solo da indirizzi IP specifici. Assicurati che non esista alcuna regola in entrata o in uscita che consenta il traffico di. `0.0.0.0/0 (0-65535)`
   2. Associate il gruppo di sicurezza Isolation a questa istanza.
   3. Rimuovi tutte le associazioni dei gruppi di sicurezza diverse dal gruppo di sicurezza Isolation appena creato dall'istanza potenzialmente compromessa.

   > **Note**
   >
   > Le connessioni tracciate esistenti non verranno interrotte a seguito della modifica dei gruppi di sicurezza: solo il traffico futuro verrà effettivamente bloccato dal nuovo gruppo di sicurezza.
   > Per informazioni sulle connessioni tracciate e non tracciate, consulta il monitoraggio delle connessioni dei gruppi EC2 di sicurezza Amazon nella Amazon EC2 User Guide.
   > Per informazioni su come bloccare ulteriore traffico proveniente da connessioni sospette esistenti, consulta Implementare in NACLs base IoCs alla rete per prevenire ulteriore traffico nell'Incident Response Playbook.

3. Identifica l'origine dell'attività sospetta

   Se viene rilevato un malware, individua e interrompi le attività potenzialmente non autorizzate sulla tua istanza in base al tipo di risultato trovato nel tuo account. EC2 Ciò potrebbe richiedere operazioni come la chiusura di tutte le porte aperte, la modifica delle policy di accesso e l'aggiornamento delle applicazioni per correggere le vulnerabilità.

   Se non sei in grado di identificare e fermare attività non autorizzate sulla tua istanza potenzialmente compromessa, ti consigliamo di chiudere l'EC2istanza compromessa e sostituirla con una EC2 nuova istanza, se necessario. Di seguito sono riportate risorse aggiuntive per proteggere le istanze: EC2

   - Sezioni su sicurezza e rete nelle migliori pratiche per Amazon EC2
   - Gruppi EC2 di sicurezza Amazon per istanze Linux e gruppi EC2 di sicurezza Amazon per istanze Windows
   - Sicurezza in Amazon EC2

- Suggerimenti per proteggere le tue EC2 istanze (Linux).
- AWS best practice in materia di sicurezza
- Incidenti relativi al dominio dell'infrastruttura su AWS

4. Sfoglia AWS re:Post

   Naviga AWS re:Postper ricevere ulteriore assistenza.

5. Invia una richiesta di supporto tecnico

   Se sei abbonato a un pacchetto Premium Support, puoi inviare una richiesta di supporto tecnico.

Riparazione di un bucket S3 potenzialmente compromesso

Segui questi passaggi consigliati per correggere un bucket Amazon S3 potenzialmente compromesso nel tuo ambiente: AWS

1. Identifica la risorsa S3 potenzialmente compromessa.

   Un GuardDuty risultato per S3 elencherà il bucket S3 associato, il relativo Amazon Resource Name (ARN) e il suo proprietario nei dettagli del risultato.

2. Identifica l'origine dell'attività sospetta e la chiamata utilizzata. API

   La API chiamata utilizzata verrà elencata come indicato `API` nei dettagli del ritrovamento. La fonte sarà un IAM principale (un IAM ruolo, un utente o un account) e i dettagli identificativi verranno elencati nel risultato. A seconda del tipo di origine, saranno disponibili informazioni sull'indirizzo IP remoto o sul dominio di origine che servono per valutare se l'origine era autorizzata o meno. Se il risultato riguardava credenziali di un'EC2istanza Amazon, verranno inclusi anche i dettagli per quella risorsa.

3. Determina se l'origine della chiamata era autorizzata ad accedere alla risorsa identificata.

   Ad esempio, considera i quesiti seguenti:

   - Se è stato coinvolto un IAM utente, è possibile che le sue credenziali siano state potenzialmente compromesse? Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.
   - Se un API è stato richiamato da un principale che non ha precedenti di invocazioni di questo tipoAPI, questa fonte necessita delle autorizzazioni di accesso per questa operazione? Le autorizzazioni del bucket possono essere ulteriormente limitate?

- Se l'accesso è stato visualizzato dal nome utente `ANONYMOUS_PRINCIPAL` con tipo di utente di `AWSAccount`, significa che il bucket è pubblico e vi è stato effettuato l'accesso. Questo bucket dovrebbe essere pubblico? In caso negativo, consulta i consigli di sicurezza riportati di seguito per trovare soluzioni alternative alla condivisione delle risorse S3.
- Se l'accesso è avvenuto tramite una `PreflightRequest` chiamata riuscita visualizzata dal nome utente **`ANONYMOUS_PRINCIPAL`** con tipo di utente, `AWSAccount` ciò indica che il bucket ha un set di criteri di condivisione delle risorse () tra origini diverse. CORS Questo bucket dovrebbe avere una politica? CORS In caso negativo, assicurati che il bucket non sia stato involontariamente reso pubblico e consulta i consigli di sicurezza riportati di seguito per trovare soluzioni alternative alla condivisione delle risorse S3. Per ulteriori informazioni, CORS consulta Using cross-origin resource sharing (CORS) nella guida per l'utente di S3.

4. Determina se il bucket S3 contiene dati sensibili.

   Usa Amazon Macie per determinare se il bucket S3 contiene dati sensibili, come informazioni di identificazione personale (PII), dati finanziari o credenziali. Se il rilevamento automatico dei dati sensibili è abilitato per il tuo account Macie, esamina i dettagli del bucket S3 per comprendere meglio il contenuto del bucket S3. Se questa funzionalità è disabilitata per il tuo account Macie, ti consigliamo di attivarla per accelerare la valutazione. In alternativa, puoi creare ed eseguire un processo di rilevamento dei dati sensibili per ispezionare gli oggetti del bucket S3 alla ricerca di dati sensibili. Per ulteriori informazioni, consulta Rilevamento dei dati sensibili con Macie.

Se l'accesso era autorizzato, puoi ignorare l'esito. La https://console.aws.amazon.com/guardduty/console ti consente di configurare regole per eliminare completamente i singoli risultati in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta Regole di eliminazione.

Se ritieni che i tuoi dati S3 siano stati esposti o consultati da soggetti non autorizzati, consulta i seguenti consigli sulla sicurezza di S3 per rafforzare le autorizzazioni e limitare l'accesso. Le soluzioni di correzione appropriate dipenderanno dalle esigenze dell'ambiente specifico.

Consigli basati su esigenze specifiche di accesso ai bucket S3

L'elenco seguente fornisce consigli basati su esigenze specifiche di accesso ai bucket Amazon S3:

- Per limitare l'accesso pubblico all'uso dei dati S3 in modo centralizzato, S3 blocca l'accesso pubblico. Le impostazioni di blocco dell'accesso pubblico possono essere abilitate per punti di accesso, bucket e AWS account tramite quattro diverse impostazioni per controllare la granularità dell'accesso. Per ulteriori informazioni, consulta Impostazioni del blocco dell'accesso pubblico S3.

- AWS Le policy di accesso possono essere utilizzate per controllare in che modo IAM gli utenti possono accedere alle tue risorse o come accedere ai tuoi bucket. Per ulteriori informazioni, consulta Utilizzo delle policy di bucket e delle policy utente.

  Inoltre, puoi utilizzare gli endpoint Virtual Private Cloud (VPC) con policy S3 bucket per limitare l'accesso a endpoint specifici. VPC Per ulteriori informazioni, consulta Example Bucket Policies for VPC Endpoints for Amazon S3
- Per consentire temporaneamente l'accesso ai tuoi oggetti S3 a entità attendibili esterne al tuo account, puoi creare un Presigned tramite S3. URL Questo accesso viene creato utilizzando le credenziali dell'account e, a seconda delle credenziali utilizzate, può durare da 6 ore a 7 giorni. Per maggiori informazioni, consulta Generazione di dati URLs prefirmati con S3.
- Per i casi d'uso che richiedono la condivisione di oggetti S3 tra diverse origini, puoi utilizzare i punti di accesso S3 per creare set di autorizzazioni che limitano l'accesso solo a quelli che si trovano all'interno della tua rete privata. Per ulteriori informazioni, consulta Gestione dell'accesso ai dati con i punti di accesso Amazon S3.
- Per concedere l'accesso sicuro alle tue risorse S3 ad altri AWS account puoi utilizzare una lista di controllo degli accessi (ACL), per maggiori informazioni consulta Gestire S3 Access con. ACLs

Per ulteriori informazioni sulle opzioni di sicurezza di S3, consulta le migliori pratiche di sicurezza di S3.

Correzione di un oggetto S3 potenzialmente dannoso

Quando un Protezione da malware per tipo di ricerca S3 viene generato nel tuo Account AWS, il tipo di risorsa potenzialmente dannoso è un S3Object.

Utilizza i seguenti passaggi consigliati per correggere potenzialmente il risultato generato:

1. Identifica l'oggetto S3 potenzialmente dannoso controllando l'S3 ObjectDetails associato al risultato.
2. Isola l'oggetto S3 interessato. Se avevi abilitato il tagging al momento dell'attivazione di Malware Protection for S3 per il bucket Amazon S3 associato GuardDuty , devi aver assegnato un tag Malicious a questo oggetto. Usa il controllo di accesso basato su tag (TBAC) per limitare l'accesso a questo oggetto S3. Per ulteriori informazioni, consulta Utilizzo del controllo degli accessi basato su tag () TBAC.

In alternativa, se non hai più bisogno di questo oggetto, puoi anche scegliere di eliminarlo o spostarlo in un bucket S3 isolato. Per informazioni sulle considerazioni relative all'eliminazione di un oggetto S3, consulta Eliminazione di oggetti nella Amazon S3 User Guide.

Riparazione di un cluster potenzialmente compromesso ECS

Segui questi passaggi consigliati per correggere un ECS cluster Amazon potenzialmente compromesso nel tuo AWS ambiente:

1. Identifica il cluster potenzialmente compromessoECS.

   La protezione GuardDuty da malware per la EC2 ricerca ECS fornisce i dettagli del ECS cluster nel pannello dei dettagli del risultato.
2. Valuta l'origine del malware

   Valuta se il malware rilevato era presente nell'immagine del container. Se nell'immagine era presente un malware, identifica tutte le altre attività in esecuzione che utilizzano questa immagine. Per informazioni sull'esecuzione delle attività, vedere ListTasks.
3. Isolare le attività potenzialmente interessate

   Isola le attività interessate negando tutto il traffico in entrata e in uscita dall'attività. Una regola di negazione totale del traffico può aiutarti a fermare un attacco già in corso, interrompendo tutte le connessioni all'attività.

Se l'accesso era autorizzato, puoi ignorare l'esito. La https://console.aws.amazon.com/guardduty/console consente di configurare regole per eliminare completamente i singoli risultati in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta Regole di eliminazione.

Riparazione delle credenziali potenzialmente compromesse AWS

Segui questi passaggi consigliati per correggere le credenziali potenzialmente compromesse nel tuo ambiente: AWS

1. Identifica l'IAMentità potenzialmente compromessa e la chiamata utilizzata. API

   La API chiamata utilizzata verrà elencata come indicato `API` nei dettagli del ritrovamento. L'IAMentità (IAMruolo o utente) e le relative informazioni identificative verranno elencate nella

sezione Risorse dei dettagli del risultato. Il tipo di IAM entità coinvolta può essere determinato dal campo Tipo utente, il nome dell'IAMentità sarà nel campo Nome utente. Il tipo di IAM entità coinvolta nella scoperta può essere determinato anche dall'ID della chiave di accesso utilizzato.

Per le chiavi che iniziano con `AKIA`:

Questo tipo di chiave è una credenziale gestita dal cliente a lungo termine associata a un IAM utente o. Utente root dell'account AWS Per informazioni sulla gestione delle chiavi di accesso per IAM gli utenti, vedere Gestione delle chiavi di accesso per gli utenti. IAM

Per le chiavi che iniziano con `ASIA`:

Questo tipo di chiave è una credenziale temporanea a breve termine generata da AWS Security Token Service. Queste chiavi esistono solo per un breve periodo e non possono essere visualizzate o gestite nella console di AWS gestione. IAMi ruoli utilizzeranno sempre AWS STS le credenziali, ma possono anche essere generati per IAM gli utenti, per ulteriori informazioni, AWS STS consulta IAM: Credenziali di sicurezza temporanee.

Se è stato utilizzato un ruolo, il campo Nome utente indicherà il nome del ruolo utilizzato. È possibile determinare in che modo è stata richiesta la chiave AWS CloudTrail esaminando l'`sessionIssuer`elemento della voce di CloudTrail registro, per ulteriori informazioni vedi IAMe AWS STS informazioni in. CloudTrail

2. Rivedi le autorizzazioni per l'entità. IAM

   Apri la IAM console. A seconda del tipo di entità utilizzata, scegli la scheda Utenti o Ruoli e individua l'entità interessata digitando il nome identificato nel campo di ricerca. Utilizzare le schede Autorizzazione e Access Advisor per esaminare le autorizzazioni effettive per tale entità.

3. Determina se le credenziali IAM dell'entità sono state utilizzate legittimamente.

   Contattare l'utente delle credenziali per stabilire se l'attività era intenzionale.

   Ad esempio, determina se l'utente ha:

   - Ha richiamato l'APIoperazione elencata nel risultato GuardDuty
   - Ha richiamato l'APIoperazione nel momento indicato nel risultato GuardDuty
   - Ha richiamato l'APIoperazione dall'indirizzo IP elencato nel risultato GuardDuty

Se questa attività è un uso legittimo delle AWS credenziali, puoi ignorare il GuardDuty risultato. La https://console.aws.amazon.com/guardduty/console consente di impostare regole per eliminare

completamente i singoli risultati in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta Regole di eliminazione.

Se non riesci a confermare se questa attività è un uso legittimo, potrebbe essere il risultato di una compromissione di una particolare chiave di accesso, ovvero delle credenziali di accesso IAM dell'utente o forse dell'intera. Account AWS Se sospetti che le tue credenziali siano state compromesse, consulta le informazioni contenute nell'articolo Le mie credenziali Account AWS potrebbero essere compromesse per risolvere il problema.

Riparazione di un contenitore autonomo potenzialmente compromesso

1. Isolare il contenitore potenzialmente compromesso

   I seguenti passaggi ti aiuteranno a identificare il carico di lavoro dei container potenzialmente dannoso:

   - Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
   - Nella pagina Risultati, scegli il risultato corrispondente per visualizzare il pannello dei risultati.
   - Nel pannello degli esiti, nella sezione Risorsa interessata, puoi visualizzare l'ID e il nome del container.

   Isola questo container dagli altri carichi di lavoro del container.
2. Metti in pausa il container

   Sospendi tutti i processi nel container.

   Per informazioni sul congelamento del contenitore, consulta Mettere in pausa un contenitore.

   Arresta il container

   Se la fase precedente ha esito negativo e il container non si ferma, arrestane il funzionamento. Se hai abilitato la Conservazione degli snapshot funzione, GuardDuty conserverà le istantanee dei tuoi EBS volumi che contengono malware.

   Per informazioni sull'arresto del contenitore, consulta Arrestare un contenitore.
3. Valuta la presenza di malware

   Valuta se nell'immagine del container è presente un malware.

Se l'accesso era autorizzato, puoi ignorare l'esito. La https://console.aws.amazon.com/guardduty/console consente di impostare regole per eliminare completamente i singoli risultati in modo che non vengano più visualizzati. La GuardDuty console consente di impostare regole per eliminare completamente i singoli risultati in modo che non vengano più visualizzati. Per ulteriori informazioni, consulta Regole di eliminazione.

Correzione degli esiti del monitoraggio dei log di audit EKS

Amazon GuardDuty genera risultati che indicano potenziali problemi di sicurezza di Kubernetes quando EKS Audit Log Monitoring è abilitato per il tuo account. Per ulteriori informazioni, consulta EKSMonitoraggio dei registri di controllo. Le sezioni seguenti descrivono le operazioni di correzione consigliate per questi scenari. Le operazioni correttive sono descritte nella voce relativa al tipo di esito specifico. Puoi accedere alle informazioni complete su un tipo di esito selezionandolo dalla tabella relativa ai tipi di esiti attivi.

Se uno qualsiasi dei tipi di esiti del monitoraggio dei log di audit EKS è stato generato per un'attività prevista, puoi prendere in considerazione l'aggiunta di Regole di eliminazione per evitare di ricevere avvisi in futuro.

Diversi tipi di attacchi e problemi di configurazione possono innescare GuardDuty i risultati di Kubernetes. Questa guida ti aiuta a identificare le cause principali delle GuardDuty rilevazioni relative al cluster e delinea le linee guida appropriate per la correzione. Le seguenti sono le cause principali che hanno portato ai risultati di GuardDuty Kubernetes:

- Potenziali problemi di configurazione
- Riparare gli utenti Kubernetes potenzialmente compromessi
- Riparazione dei pod Kubernetes potenzialmente compromessi
- Riparazione dei nodi Kubernetes potenzialmente compromessi
- Riparazione delle immagini dei container potenzialmente compromesse

> **Note**
>
> Prima della versione 1.14 di Kubernetes, il `system:unauthenticated` gruppo era associato a e per impostazione predefinita. `system:discovery` `system:basic-user` ClusterRoles Ciò potrebbe consentire l'accesso non intenzionale a utenti anonimi. Gli aggiornamenti del cluster non revocano le autorizzazioni, quindi potrebbero essere ancora

valide anche se hai aggiornato il cluster alla versione 1.14 o successiva. Ti consigliamo di disassociare queste autorizzazioni dal gruppo `system:unauthenticated`.
Per ulteriori informazioni sulla rimozione di queste autorizzazioni, consulta le best practice di sicurezza per Amazon EKS nella Amazon EKS User Guide.

Potenziali problemi di configurazione

Se un esito indica un problema di configurazione, consulta la sezione sulla correzione di tale esito per indicazioni su come risolvere il problema. Per ulteriori informazioni, consulta i seguenti tipi di esiti che indicano problemi di configurazione:

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- Qualsiasi scoperta che finisce con SuccessfulAnonymousAccess

Riparare gli utenti Kubernetes potenzialmente compromessi

Un GuardDuty risultato può indicare un utente Kubernetes compromesso quando un utente identificato nel risultato ha eseguito un'azione API inaspettata. Puoi identificare l'utente nella sezione Dettagli utente Kubernetes dei dettagli di un esito nella console o nei `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` del file JSON degli esiti. Questi dettagli utente includono `user name`, `uid` e i gruppi Kubernetes a cui appartiene l'utente.

Se l'utente accedeva al carico di lavoro utilizzando un'entità IAM, puoi utilizzare la sezione `Access Key details` per identificare i dettagli di un ruolo o di un utente IAM. Consulta i seguenti tipi di utente e le linee guida per la correzione.

> **Note**
>
> Puoi utilizzare Amazon Detective per esaminare ulteriormente il ruolo o l'utente IAM identificato nell'esito. Mentre visualizzi i dettagli del ritrovamento GuardDuty sulla console,

scegli Investiga in Detective. Quindi seleziona AWS l'utente o il ruolo dagli elementi elencati per esaminarlo in Detective.

Amministratore Kubernetes integrato: l'utente predefinito assegnato da Amazon EKS all'identità IAM che ha creato il cluster. Questo tipo di utente è identificato dal nome utente `kubernetes-admin`.

Per revocare l'accesso a un amministratore Kubernetes integrato:

- Identifica il `userType` nella sezione `Access Key details`.
  - Se il `userType` è un Ruolo e il ruolo appartiene a un ruolo dell'istanza EC2:
    - Identifica l'istanza e segui le istruzioni riportate in Correzione di un'istanza Amazon potenzialmente compromessa EC2.
  - Se il `userType` è un Utente o un Ruolo assunto da un utente:
    1. Ruota la chiave di accesso dell'utente.
    2. Ruota tutti i segreti a cui l'utente ha avuto accesso.
    3. Controlla le informazioni in Il mio AWS account potrebbe essere compromesso per ulteriori dettagli.

Utente autenticato OIDC: un utente a cui è stato concesso l'accesso tramite un provider OIDC. In genere un utente OIDC ha un indirizzo e-mail come nome utente. Puoi verificare se il cluster utilizza OIDC con il comando seguente: `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`*

Per revocare l'accesso a un utente autenticato OIDC:

1. Ruota le credenziali dell'utente nel provider OIDC.
2. Ruota tutti i segreti a cui l'utente ha avuto accesso.

AWS-Auth ConfigMap defined user: un utente IAM a cui è stato concesso l'accesso tramite un -auth. AWSConfigMap Per maggiori informazioni, consulta Gestione di utenti o ruoli IAM per il cluster nella guida per l'utente &EKS. Puoi esaminarne le autorizzazioni utilizzando il comando seguente: `kubectl edit configmaps aws-auth --namespace kube-system`

Per revocare l'accesso di un utente: AWS ConfigMap

1. Utilizzate il seguente comando per aprire. ConfigMap

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifica il ruolo o la voce utente nella sezione MapRoles o MapUsers con lo stesso nome utente riportato nella sezione dei dettagli utente di Kubernetes del tuo risultato. GuardDuty Consulta l'esempio seguente, in cui l'utente amministratore è stato identificato in un esito.

```
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. Rimuovi quell'utente da. ConfigMap Consulta l'esempio seguente, in cui l'utente amministratore è stato rimosso.

```
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. Se il `userType` è un Utente o un Ruolo assunto da un utente:
   a. Ruota la chiave di accesso dell'utente.
   b. Ruota tutti i segreti a cui l'utente ha avuto accesso.
   c. Controlla le informazioni in Il mio AWS account potrebbe essere compromesso per ulteriori dettagli.

Se l'esito non ha una sezione `resource.accessKeyDetails`, l'utente è un account di servizio Kubernetes.

Account di servizio: l'account di servizio fornisce un'identità per i pod e può essere identificato da un nome utente con il formato seguente: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Per revocare l'accesso a un account di servizio:

1. Ruota le credenziali dell'account di servizio.
2. Consulta le linee guida sulla compromissione dei pod nella sezione seguente.

Riparazione dei pod Kubernetes potenzialmente compromessi

Quando si GuardDuty specificano i dettagli di un pod o di una risorsa di carico di lavoro all'interno della `resource.kubernetesDetails.kubernetesWorkloadDetails` sezione, quel pod o risorsa del carico di lavoro è stato potenzialmente compromesso. Un GuardDuty risultato può indicare che un singolo pod è stato compromesso o che più pod sono stati compromessi a causa di una risorsa di livello superiore. Consulta i seguenti scenari di compromissione per indicazioni su come identificare il pod o i pod che sono stati compromessi.

Compromissione di pod singoli

Se il campo `type` all'interno della sezione `resource.kubernetesDetails.kubernetesWorkloadDetails` è pod, l'esito identifica un singolo pod. Il campo nome è il `name` del pod e il campo `namespace` è il relativo spazio del nome.

Per informazioni sull'identificazione del nodo di lavoro che esegue i pod, consulta Identificare i pod e il nodo di lavoro in questione.

Pod compromessi tramite una risorsa del carico di lavoro

Se il campo `type` all'interno della sezione `resource.kubernetesDetails.kubernetesWorkloadDetails` identifica una Risorsa del carico di lavoro, ad esempio un'`Deployment`, è probabile che tutti i pod all'interno della risorsa del carico di lavoro siano stati compromessi.

Per informazioni sull'identificazione di tutti i pod della risorsa del carico di lavoro e dei nodi su cui sono in esecuzione, consulta Identificare i pod e i nodi di lavoro pericolosi utilizzando il nome del carico di lavoro.

I pod sono stati compromessi tramite un account di servizio

Se un GuardDuty risultato identifica un account di servizio nella `resource.kubernetesDetails.kubernetesUserDetails` sezione, è probabile che i pod che utilizzano l'account di servizio identificato siano compromessi. Il nome utente riportato da un esito è un account di servizio se ha il formato seguente: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Per informazioni sull'identificazione di tutti i pod e i nodi di lavoro che utilizzano l'account di servizio e i nodi su cui sono in esecuzione, consulta Identificare i pod e i nodi di lavoro pericolosi utilizzando il nome dell'account di servizio.

Dopo aver identificato tutti i pod compromessi e i nodi su cui sono in esecuzione, consulta la guida alle best practice di Amazon EKS per isolare il pod, ruotarne le credenziali e raccogliere dati per l'analisi forense.

Per riparare un pod potenzialmente compromesso:

1. Identifica la vulnerabilità che ha compromesso i pod.
2. Implementa la correzione di tale vulnerabilità e avvia nuovi pod sostitutivi.
3. Eliminare i pod vulnerabili.

   Per ulteriori informazioni, consulta Ridistribuire il pod o la risorsa del carico di lavoro compromessa.

Se al nodo di lavoro è stato assegnato un ruolo IAM che consente ai Pods di accedere ad altre AWS risorse, rimuovi tali ruoli dall'istanza per evitare ulteriori danni causati dall'attacco. Allo stesso modo,

se al pod è stato assegnato un ruolo IAM, valuta se puoi rimuovere in sicurezza le policy IAM dal ruolo senza influire sugli altri carichi di lavoro.

Riparazione delle immagini dei container potenzialmente compromesse

Quando un GuardDuty risultato indica una compromissione del pod, l'immagine utilizzata per avviare il pod potrebbe essere potenzialmente dannosa o compromessa. GuardDuty i risultati identificano l'immagine del contenitore all'interno del `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` campo. Puoi determinare se l'immagine è dannosa scansionandola alla ricerca di malware.

Per correggere un'immagine del contenitore potenzialmente compromessa:

1. Interrompi immediatamente l'utilizzo dell'immagine e rimuovila dal tuo repository di immagini.
2. Identifica tutti i pod utilizzando l'immagine potenzialmente compromessa.

   Per ulteriori informazioni, consulta Identificare i pod con immagini di container e nodi di lavoro potenzialmente vulnerabili o compromessi.
3. Isola i pod potenzialmente compromessi, ruota le credenziali e raccogli dati per l'analisi. Per ulteriori informazioni, consulta la guida alle best practice di Amazon EKS.
4. Elimina tutti i pod utilizzando l'immagine potenzialmente compromessa.

Riparazione dei nodi Kubernetes potenzialmente compromessi

Un GuardDuty risultato può indicare una compromissione del nodo se l'utente identificato nel risultato rappresenta l'identità di un nodo o se il risultato indica l'uso di un contenitore privilegiato.

L'identità utente è un nodo worker se il campo nome utente ha il seguente formato: `system:node:node name`. Ad esempio, `system:node:ip-192-168-3-201.ec2.internal`. Ciò indica che l'avversario ha ottenuto l'accesso al nodo e ne utilizza le credenziali per comunicare con l'endpoint dell'API Kubernetes.

Un esito indica l'uso di un container privilegiato se il campo `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` dell'esito di uno o più container elencati nell'esito è impostato su `True`.

Per riparare un nodo potenzialmente compromesso:

1. Isola il pod, ruota le sue credenziali e raccogli dati per l'analisi forense.

Per ulteriori informazioni, consulta la guida alle best practice di Amazon EKS.

2. Identifica gli account di servizio utilizzati da tutti i pod in esecuzione sul nodo potenzialmente compromesso. Controlla le relative autorizzazioni e, se necessario, ruota gli account di servizio.
3. Termina il nodo potenzialmente compromesso.

Correzione dei risultati del Runtime Monitoring

Quando abiliti il Runtime Monitoring per il tuo account, Amazon GuardDuty potrebbe generare dati Tipi di risultati del monitoraggio del runtime che indicano potenziali problemi di sicurezza nel tuo AWS ambiente. I potenziali problemi di sicurezza indicano un'istanza Amazon EC2 compromessa, un carico di lavoro del container, un cluster Amazon EKS o un set di credenziali compromesse nel tuo ambiente. AWS L'agente di sicurezza monitora gli eventi di runtime da più tipi di risorse. Per identificare la risorsa potenzialmente compromessa, visualizza il tipo di risorsa nei dettagli di ricerca generati nella GuardDuty console. La sezione seguente descrive le procedure di correzione consigliate per ogni tipo di risorsa.

Instance

Se il Tipo di risorsa nei dettagli dell'esito è Istanza, significa che un'istanza EC2 o un nodo EKS sono potenzialmente compromessi.

- Per correggere un nodo EKS compromesso, consulta Riparazione dei nodi Kubernetes potenzialmente compromessi.
- Per correggere un'istanza EC2 compromessa, consulta Correzione di un'istanza Amazon potenzialmente compromessa EC2.

EKSCluster

Se il Tipo di risorsa nei dettagli dell'esito è EKSCluster, significa che un pod o un container in un cluster EKS sono potenzialmente compromessi.

- Per correggere un pod compromesso, consulta Riparazione dei pod Kubernetes potenzialmente compromessi.
- Per correggere l'immagine di un container compromessa, consulta Riparazione delle immagini dei container potenzialmente compromesse.

ECSCluster

Se il tipo di risorsa nei dettagli del risultato è ECSCluster, indica che un'attività ECS o un contenitore all'interno di un'attività ECS è potenzialmente compromessa.

1. Identifica il cluster ECS interessato

   Il risultato del GuardDuty Runtime Monitoring fornisce i dettagli del cluster ECS nel pannello dei dettagli del risultato o nella `resource.ecsClusterDetails` sezione del JSON di ricerca.

2. Identifica l'attività ECS interessata

   Il risultato GuardDuty di Runtime Monitoring fornisce i dettagli dell'attività ECS nel pannello dei dettagli del risultato o nella `resource.ecsClusterDetails.taskDetails` sezione del file JSON di ricerca.

3. Isola l'attività interessata

   Isola l'attività interessata bloccando tutto il traffico in entrata e in uscita verso l'attività. Una regola di blocco totale del traffico può contribuire a fermare un attacco già in corso, interrompendo tutte le connessioni all'attività.

4. Risolvi l'attività compromessa

   a. Identifica la vulnerabilità che ha compromesso l'attività.

   b. Implementa la correzione di tale vulnerabilità e avvia una nuova attività sostitutiva.

   c. Interrompi l'attività vulnerabile.

Container

Se il Tipo di risorsa nei dettagli dell'esito è Container, significa che un container autonomo è potenzialmente compromesso.

- Per procedere alla correzione, consulta Riparazione di un contenitore autonomo potenzialmente compromesso.
- Se l'esito viene generato su più container utilizzando la stessa immagine del container, consulta Riparazione delle immagini dei container potenzialmente compromesse.
- Se il container ha avuto accesso all'host EC2 sottostante, le credenziali dell'istanza associata potrebbero essere state compromesse. Per ulteriori informazioni, consulta Riparazione delle credenziali potenzialmente compromesse AWS.

- Se un utente potenzialmente malintenzionato ha avuto accesso al nodo EKS sottostante o a un'istanza EC2, consulta la correzione consigliata nelle schede EKSCluster e Istanza.

Correzione delle immagini del container compromesse

Quando un GuardDuty risultato indica una compromissione dell'attività, l'immagine utilizzata per avviare l'attività potrebbe essere dannosa o compromessa. GuardDuty i risultati identificano l'immagine del contenitore all'interno del `resource.ecsClusterDetails.taskDetails.containers.image` campo. È possibile determinare se l'immagine è dannosa o meno eseguendo una scansione alla ricerca di malware.

Per correggere l'immagine compromessa di un contenitore

1. Interrompi immediatamente l'utilizzo dell'immagine e rimuovila dal tuo repository di immagini.
2. Identifica tutte le attività che utilizzano questa immagine.
3. Interrompi tutte le attività che utilizzano l'immagine compromessa. Aggiorna le definizioni delle attività in modo che smettano di utilizzare l'immagine compromessa.

Ripristino di un database potenzialmente compromesso

GuardDuty generi Tipi di esiti della Protezione RDS che indicano un comportamento di accesso potenzialmente sospetto e anomalo dopo l'attivazione. Database supportati RDSProtezione Utilizzando l'attività di accesso RDS, GuardDuty analizza e profila le minacce identificando modelli insoliti nei tentativi di accesso.

> **Note**
>
> Puoi accedere alle informazioni complete su un tipo di esito selezionandolo dalla Tabella degli esiti.

Segui questi passaggi consigliati per correggere un database Amazon Aurora potenzialmente compromesso nel tuo ambiente. AWS

Argomenti

- Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti

- Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti
- Correzione di credenziali potenzialmente compromesse
- Limita l'accesso alla rete

Correzione di un database potenzialmente compromesso che presenta eventi di accesso riusciti

I seguenti passaggi consigliati sono utili per correggere un database Aurora potenzialmente compromesso che presenta un comportamento insolito legato a eventi di accesso riusciti.

1. Identifica il database e l'utente interessati.

   Il GuardDuty risultato generato fornisce il nome del database interessato e i dettagli utente corrispondenti. Per ulteriori informazioni, consulta Dettagli degli esiti.

2. Verifica se questo comportamento è previsto o non previsto.

   L'elenco seguente specifica i potenziali scenari che potrebbero aver causato la generazione GuardDuty di un risultato:

   - Un utente che accede al proprio database dopo un lungo periodo di tempo.
   - Un utente che accede occasionalmente al proprio database, ad esempio un analista finanziario che accede ogni tre mesi.
   - Un attore potenzialmente sospetto coinvolto in un tentativo di accesso riuscito può compromettere il database.

3. Inizia questa fase se il comportamento non è previsto.

   1. Limita l'accesso al database

      Limita l'accesso al database per gli account sospetti e per l'origine di questa attività di accesso. Per ulteriori informazioni, consultare Correzione di credenziali potenzialmente compromesse e Limita l'accesso alla rete.

   2. Valuta l'impatto e determina a quali informazioni è stato effettuato l'accesso.

      - Se disponibili, esamina i log di audit per identificare le informazioni a cui potrebbe essere stato effettuato l'accesso. Per ulteriori informazioni, consulta Monitoraggio di eventi, registri e flussi in un cluster di database Amazon Aurora nella Guida per l'utente di Amazon Aurora.
      - Determina se sono stati effettuati accessi o modifiche a informazioni sensibili o protette.

Correzione di un database potenzialmente compromesso che presenta eventi di accesso falliti

I seguenti passaggi consigliati sono utili per correggere un database Aurora potenzialmente compromesso che presenta un comportamento insolito legato a eventi di accesso falliti.

1. Identifica il database e l'utente interessati.

   Il GuardDuty risultato generato fornisce il nome del database interessato e i dettagli utente corrispondenti. Per ulteriori informazioni, consulta Dettagli degli esiti.

2. Identifica l'origine dei tentativi di accesso falliti.

   Il GuardDuty risultato generato fornisce l'indirizzo IP e l'organizzazione ASN (se si trattava di una connessione pubblica) nella sezione Attore del pannello di ricerca.

   Un sistema autonomo (AS) è un gruppo di uno o più prefissi IP (elenchi di indirizzi IP accessibili su una rete) gestiti da uno o più operatori di rete che mantengono un'unica policy di instradamento chiaramente definita. Gli operatori di rete necessitano di numeri di sistema autonomi (ASN) per controllare l'instradamento all'interno delle proprie reti e scambiare informazioni di instradamento con altri provider di servizi Internet (ISP).

3. Verifica che questo comportamento non sia previsto.

   Verifica nel modo seguente se questa attività rappresenta un tentativo di ottenere un ulteriore accesso non autorizzato al database:

   - Se l'origine è interna, verifica se un'applicazione non è configurata correttamente e tenta ripetutamente di stabilire una connessione.
   - Se si tratta di un attore esterno, verificate se il database corrispondente è pubblico o non correttamente configurato, permettendo così ai potenziali utenti malintenzionati di usare la forza bruta con nomi utente comuni.

4. Inizia questa fase se il comportamento non è previsto.

   1. Limita l'accesso al database

      Limita l'accesso al database per gli account sospetti e per l'origine di questa attività di accesso. Per ulteriori informazioni, consultare Correzione di credenziali potenzialmente compromesse e Limita l'accesso alla rete.

2. Esegui l'analisi delle cause principali e determina i passaggi che potenzialmente hanno portato a questa attività.

   Imposta un avviso per ricevere una notifica quando un'attività modifica una policy di rete e crea uno stato di insicurezza. Per ulteriori informazioni, consulta Policy del firewall in AWS Network Firewall nella Guida per gli sviluppatori diAWS Network Firewall .

Correzione di credenziali potenzialmente compromesse

Un GuardDuty risultato può indicare che le credenziali dell'utente per un database interessato sono state compromesse quando l'utente identificato nel risultato ha eseguito un'operazione imprevista sul database. Puoi identificare l'utente nella sezione dei Dettagli utente del database RDS all'interno del pannello dell'esito nella console o all'interno dei `resource.rdsDbUserDetails` del file JSON degli esiti. Questi dettagli utente includono il nome utente, l'applicazione utilizzata, il database a cui si accede, la versione SSL e il metodo di autenticazione.

- Per revocare l'accesso o ruotare le password per utenti specifici coinvolti nell'esito, consulta Sicurezza con Amazon Aurora MySQL o Sicurezza con Amazon Aurora PostgreSQL nella Guida per l'utente di Amazon Aurora.
- Utilizzalo AWS Secrets Manager per archiviare in modo sicuro e ruotare automaticamente i segreti per i database Amazon Relational Database Service (RDS). Per ulteriori informazioni, consulta Tutorial diAWS Secrets Manager nella Guida per l'utente diAWS Secrets Manager .
- Utilizza l'autenticazione del database IAM per gestire l'accesso degli utenti del database senza bisogno di password. Per ulteriori informazioni, consulta Autenticazione database IAM nella Guida per l'utente di Amazon Aurora.

  Per ulteriori informazioni, consulta Best practice di sicurezza per Amazon Relational Database Service nella Guida per l'utente di Amazon RDS.

Limita l'accesso alla rete

Un GuardDuty risultato può indicare che un database è accessibile anche al di fuori delle applicazioni o del Virtual Private Cloud (VPC). Se l'indirizzo IP remoto indicato nell'esito è un'origine di connessione non prevista, controlla i gruppi di sicurezza. Un elenco dei gruppi di sicurezza collegati al database è disponibile in Gruppi di sicurezza nella console https://console.aws.amazon.com/rds/ o nei `resource.rdsDbInstanceDetails.dbSecurityGroups` del file JSON degli esiti. Per

maggiori informazioni sulla configurazione dei gruppi di sicurezza, consulta Controllo dell'accesso con i gruppi di sicurezza nella Guida dell'utente di Amazon RDS.

Se utilizzi un firewall, limita l'accesso alla rete al database riconfigurando le liste di controllo degli accessi di rete (NACL). Per ulteriori informazioni, consulta Firewall in AWS Network Firewall nella Guida per gli sviluppatori diAWS Network Firewall .

Correzione di una funzione Lambda potenzialmente compromessa

Quando GuardDuty genera un risultato di Lambda Protection e l'attività è inaspettata, la funzione Lambda potrebbe essere compromessa. Ti consigliamo di completare la procedura seguente per correggere una funzione Lambda compromessa.

Per correggere gli esiti della Protezione Lambda

1. Identifica la versione della funzione Lambda potenzialmente compromessa.

   Un GuardDuty risultato di Lambda Protection fornisce il nome, Amazon Resource Name (ARN), la versione della funzione e l'ID di revisione associati alla funzione Lambda elencati nei dettagli del risultato.
2. Identifica l'origine dell'attività potenzialmente sospetta.

   a. Esamina il codice associato alla versione della funzione Lambda coinvolta nell'esito.
   b. Esamina le librerie importate e i livelli della versione della funzione Lambda coinvolta nell'esito.
   c. Se hai abilitato AWS Lambda le funzioni di scansione con Amazon Inspector, esamina i risultati di Amazon Inspector associati alla funzione Lambda coinvolta nel risultato.
   d. AWS CloudTrail Esamina i log per identificare la causa principale che ha causato l'aggiornamento della funzione e assicurati che l'attività sia stata autorizzata o prevista.
3. Correggi la funzione Lambda potenzialmente compromessa.

   a. Disabilita i trigger di esecuzione della funzione Lambda coinvolta nell'esito. Per ulteriori informazioni, consulta. DeleteFunctionEventInvokeConfig
   b. Esamina il codice Lambda e aggiorna le importazioni delle librerie e i Livelli della funzione Lambda per rimuovere le librerie e i livelli potenzialmente sospetti.
   c. Contieni gli esiti di Amazon Inspector relativi alla funzione Lambda coinvolta nell'esito.

Stima dei costi GuardDuty

Durante la prova gratuita di 30 giorni, puoi utilizzare la GuardDuty console o API le operazioni per stimare i costi di utilizzo medi giornalieri di. GuardDuty La stima dei costi indica quali saranno i costi stimati dopo il periodo di prova. Tuttavia, per esaminare una stima accurata dei costi durante la prova gratuita, si GuardDuty consiglia di utilizzare AWS Billing at https://console.aws.amazon.com/billing/.

Quando si opera in un ambiente con più account, l'account GuardDuty amministratore può monitorare le metriche dei costi per tutti gli account membri.

> **Nota sui costi di utilizzo di Malware Protection for S3**
>
> Il costo di utilizzo di Malware Protection for S3 non è incluso nella sezione Utilizzo nella GuardDuty console. Per ulteriori informazioni, consulta Visualizzazione dell'utilizzo e dei costi di Malware Protection for S3.

Puoi visualizzare la stima dei costi in base alle seguenti metriche:

- ID account: elenca il costo stimato per il tuo account o per i tuoi account membro se utilizzi un account GuardDuty amministratore.
- Origini dati: elenca il costo stimato per ciascuna fonte di dati fondamentale, ovvero eventi di AWS CloudTrail gestione, registri di VPC flusso e registri delle query di Route53 Resolver. DNS
- Caratteristiche: elenca il costo stimato per le GuardDuty funzionalità: eventi CloudTrail relativi ai dati per S3, EKS Audit Log Monitoring, EBS volume di dati, attività di RDS accesso, Runtime Monitoring, Fargate EKS Runtime Monitoring, Runtime Monitoring EC2 o Lambda Network Activity Monitoring.
- Bucket S3: elenca il costo stimato per gli eventi di dati di S3 su un bucket specifico o sui bucket più costosi per gli account nel tuo ambiente. Questa statistica è disponibile solo quando si abilita un. Protezione S3 Account AWS

Comprendere come GuardDuty calcola i costi di utilizzo

Le stime visualizzate nella GuardDuty console potrebbero differire leggermente da quelle della AWS Billing and Cost Management console. L'elenco seguente spiega come GuardDuty stimare i costi di utilizzo:

- La stima di GuardDuty utilizzo si riferisce solo alla regione corrente.
- Il costo di GuardDuty utilizzo si basa sugli ultimi 30 giorni di utilizzo.
- La stima dei costi di utilizzo della versione di prova include la stima relativa alle origini dati e alle funzionalità fondamentali attualmente nel periodo di prova. Ogni funzionalità e fonte di dati GuardDuty inclusa ha il proprio periodo di prova, ma potrebbe sovrapporsi al periodo di prova di GuardDuty o a un'altra funzionalità abilitata contemporaneamente.
- La stima di GuardDuty utilizzo include sconti sui prezzi per GuardDuty volume per regione, come indicato nella pagina GuardDuty dei prezzi di Amazon, ma solo per i singoli account che soddisfano i livelli di prezzo basati sui volumi. Gli sconti sui prezzi per volume non sono inclusi nelle stime relative all'utilizzo totale combinato tra gli account di un'organizzazione. Per informazioni sui prezzi scontati per volume di utilizzo combinato, consulta Fatturazione AWS : sconti per volume.
- La somma dei costi di utilizzo per ciascun Account AWS utente dell'organizzazione potrebbe non corrispondere sempre al costo stimato degli ultimi 30 giorni per l'origine dati selezionata. Il livello di prezzo può cambiare man mano che GuardDuty elabora più eventi o dati. Per ulteriori informazioni, consulta i livelli di prezzo nella Guida per l'AWS Billing utente.

Questo scenario spiega che per evitare di incorrere in costi di utilizzo per Runtime Monitoring, è necessario disattivare entrambe le funzionalità di Runtime Monitoring e EKS Runtime Monitoring.

GuardDuty ha consolidato l'esperienza della console per EKS Runtime Monitoring in Runtime Monitoring. GuardDuty consiglia Verifica dello stato della configurazione EKS di Runtime Monit e. Migrazione da EKS Runtime Monitoring a Runtime Monitoring

Come parte della migrazione al Runtime Monitoring, assicurati diDisabilita EKS il monitoraggio del runtime. Questo è importante perché se in seguito scegliete di disabilitare il Runtime Monitoring e non disattivate il EKS Runtime Monitoring, continuerete a incorrere in costi di utilizzo per EKS il Runtime Monitoring.

Monitoraggio del runtime: in che modo i log di VPC flusso delle EC2 istanze influiscono sui costi di utilizzo

Se gestisci il security agent (manualmente o tramite GuardDuty) in EKS Runtime Monitoring o Runtime Monitoring per EC2 istanze ed GuardDuty è attualmente distribuito su un'EC2istanza Amazon e riceve Tipi di eventi di runtime raccolti da questa istanza, non GuardDuty ti verrà

addebitato alcun costo Account AWS per l'analisi dei log di VPC flusso di questa istanza Amazon. EC2 Questo aiuta a GuardDuty evitare il doppio dei costi di utilizzo dell'account.

Come GuardDuty stima il costo di utilizzo degli CloudTrail eventi

Quando lo abiliti GuardDuty, inizia automaticamente a consumare i registri degli AWS CloudTrail eventi registrati per il tuo account nell'area selezionata Regione AWS. GuardDuty replica i registri degli eventi del servizio globale e quindi elabora questi eventi in modo indipendente in ogni regione in cui è stata abilitata. GuardDuty Questo aiuta a GuardDuty mantenere i profili utente e di ruolo in ogni regione per identificare le anomalie.

La CloudTrail configurazione non influisce sui costi di GuardDuty utilizzo o sul modo in cui GuardDuty elabora i registri degli eventi. Il costo GuardDuty di utilizzo è influenzato dall'utilizzo da parte dell'utente di AWS APIs quale accesso CloudTrail. Per ulteriori informazioni, consulta AWS CloudTrail eventi di gestione.

Revisione GuardDuty delle statistiche di utilizzo

Scegli il tuo metodo di accesso preferito per rivedere le statistiche di utilizzo del tuo GuardDuty account. Se sei un account GuardDuty amministratore, i seguenti metodi ti aiuteranno a rivedere le statistiche di utilizzo per tutti i membri.

Console

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.

   Assicurati di utilizzare l'account GuardDuty amministratore.
2. Nel riquadro di navigazione, scegli Utilizzo.
3. Nella pagina Utilizzo, un account GuardDuty amministratore con account membro può visualizzare il costo stimato dell'organizzazione per gli ultimi 30 giorni. Si tratta di un costo di utilizzo totale stimato per l'organizzazione.
4. GuardDuty gli account amministratore con membri possono visualizzare la ripartizione dei costi di utilizzo per origine dati o per account. Gli account individuali o autonomi possono visualizzare la suddivisione per fonte di dati.

   Se disponi di account membri, puoi visualizzare le statistiche di un singolo account selezionando tale account nella tabella Conti.

Nella scheda Per origini dati, quando si seleziona un'origine dati a cui è associato un costo di utilizzo, la somma corrispondente della ripartizione dei costi a livello di account potrebbe non essere sempre la stessa.

API/CLI

Esegui l'GetUsageStatisticsAPIoperazione utilizzando le credenziali dell'account GuardDuty amministratore. Fornisci le seguenti informazioni per eseguire il comando:

- (Obbligatorio) Fornisci l'ID del GuardDuty rilevatore regionale dell'account per il quale desideri recuperare le statistiche.
- (Obbligatorio) fornisci uno dei tipi di statistiche da recuperare: `SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE`.

  Attualmente, `TOP_ACCOUNTS_BY_FEATURE` non supporta il recupero delle statistiche di utilizzo per. `RDS_LOGIN_EVENTS`
- (Obbligatorio) Fornisci una o più fonti di dati o funzionalità per interrogare le tue statistiche di utilizzo.
- (Facoltativo) Fornisci un elenco di account IDs per i quali desideri recuperare le statistiche di utilizzo.

Puoi anche utilizzare l' AWS Command Line Interface. Il comando seguente è un esempio di recupero delle statistiche di utilizzo per tutte le fonti di dati e le funzionalità, calcolate dagli account. Assicurati di sostituire il `detector-id` con il tuo ID rilevatore valido. Per gli account autonomi, questo comando restituisce il costo di utilizzo degli ultimi 30 giorni relativi solo al proprio account. Se sei un account GuardDuty amministratore con account membri, vedrai i costi elencati per account per tutti i membri.

Per trovare il `detectorId` codice per il tuo account e la regione corrente, consulta la pagina Impostazioni nella https://console.aws.amazon.com/guardduty/console oppure esegui il ListDetectorsAPI.

Sostituisci `SUM_BY_ACCOUNT` con il tipo con cui desideri calcolare le statistiche di utilizzo.

Per monitorare i costi solo per le fonti di dati

```
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"]}'
```

Per monitorare i costi delle funzionalità

```
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"]}'
```

Sicurezza in Amazon GuardDuty

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il Modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. Gli auditor di terze parti testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei programmi di conformità AWS. Per avere maggiori informazioni sui programmi di conformità applicabili a GuardDuty, consulta Servizi AWS rientranti nell'ambito del programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. Inoltre, sei responsabile anche di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa durante l'utilizzo di GuardDuty. Viene illustrato come configurare GuardDuty per soddisfare gli obiettivi di sicurezza e conformità. Scoprirai anche come utilizzare altri servizi AWS per monitorare e proteggere le risorse GuardDuty.

Indice

Protezione dei dati in Amazon GuardDuty

Il modello di responsabilità AWS condivisa modello di si applica alla protezione dei dati in Amazon GuardDuty. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura

globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i AWS servizi utilizzati. Per ulteriori informazioni sulla privacy dei dati, consulta la sezione Privacy dei dati FAQ. Per informazioni sulla protezione dei dati in Europa, consulta il Modello di responsabilitàAWS condivisa e GDPR il post sul blog sulla AWS sicurezza.

Ai fini della protezione dei dati, ti consigliamo di proteggere Account AWS le credenziali e di configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS servizi.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o unAPI, usa un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere Federal Information Processing Standard () 140-3. FIPS

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori GuardDuty o AWS servizi utilizzi in altro modo la console, API AWS CLI, o. AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Se fornisci un URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

Crittografia a riposo

Tutti i dati GuardDuty dei clienti vengono crittografati quando sono inattivi utilizzando soluzioni di AWS crittografia.

GuardDuty i dati, come i risultati, vengono crittografati quando sono inattivi utilizzando AWS Key Management Service (AWS KMS) utilizzando chiavi gestite dal cliente di AWS proprietà.

Crittografia in transito

GuardDuty analizza i dati di registro di altri servizi. Crittografa tutti i dati in transito da questi servizi con HTTPS e. KMS Una volta GuardDuty estratte le informazioni necessarie dai registri, queste vengono eliminate. Per ulteriori informazioni su come GuardDuty utilizza le informazioni di altri servizi, consulta le fonti di dati. GuardDuty

GuardDuty i dati vengono crittografati durante il transito tra i servizi.

Rifiuto esplicito all'utilizzo dei dati volto al miglioramento del servizio

Puoi scegliere di non utilizzare i tuoi dati per sviluppare GuardDuty e migliorare altri servizi di AWS sicurezza utilizzando la politica di AWS Organizations opt-out. Puoi scegliere di rinunciare anche se al momento GuardDuty non raccoglie tali dati. Per ulteriori informazioni in merito, consulta le Policy di rifiuto dei servizi di IA nella Guida per l'utente di AWS Organizations .

> **Note**
>
> Per poter utilizzare la politica di opt-out, i tuoi AWS account devono essere gestiti centralmente da AWS Organizations. Se non hai ancora creato un'organizzazione per i tuoi AWS account, consulta Creazione e gestione di un'organizzazione nella Guida per l'AWS Organizations utente.

Il rifiuto esplicito ha gli effetti seguenti:

- GuardDuty eliminerà i dati raccolti e archiviati per scopi di miglioramento del servizio prima dell'eventuale rinuncia da parte dell'utente.
- Dopo l'annullamento, non GuardDuty raccoglieremo o memorizzeremo più questi dati per scopi di miglioramento del servizio.

I seguenti argomenti spiegano come ciascuna funzionalità all'interno di ciascuna funzionalità gestisca GuardDuty potenzialmente i dati per il miglioramento del servizio.

Indice

GuardDuty Monitoraggio del runtime

GuardDuty Il monitoraggio del runtime fornisce il rilevamento delle minacce in fase di esecuzione per i cluster Amazon Elastic Kubernetes Service (EKSAmazon) AWS Fargate (Fargate) , solo Amazon Elastic Container Service (ECSAmazon) e le istanze Amazon Elastic Compute Cloud (EC2Amazon) nel tuo ambiente. AWS Dopo aver abilitato il Runtime Monitoring e distribuito l'agente GuardDuty di sicurezza per la tua risorsa, GuardDuty inizia a monitorare e analizzare gli eventi di runtime associati alla tua risorsa. Questi tipi di eventi di runtime includono eventi di processo, eventi di contenitore, DNS eventi e altro ancora. Per ulteriori informazioni, consulta Tipi di eventi di runtime raccolti che utilizza GuardDuty .

Sebbene GuardDuty ora raccolga argomenti della riga di comando che puoi indirizzare ai tuoi carichi di lavoro, attualmente non utilizza questi argomenti per scopi di miglioramento del servizio (potrebbe farlo in futuro). Abbiamo iniziato a raccogliere argomenti da riga di comando in previsione delle nuove regole e dei risultati di rilevamento delle minacce che verranno rilasciati a breve. La tua fiducia, la tua privacy e la sicurezza dei tuoi contenuti sono la nostra massima priorità e garantiamo che il nostro utilizzo rispetta i nostri impegni nei tuoi confronti. Per ulteriori informazioni, consulta la sezione Privacy dei dati. FAQ

GuardDuty Protezione da malware

GuardDuty Malware Protection analizza e rileva il malware contenuto nei EBS volumi allegati ai carichi di lavoro di istanze e container EC2 Amazon potenzialmente compromessi e ai file appena caricati nei bucket Amazon S3 selezionati. Attualmente, GuardDuty non raccoglie né utilizza il malware rilevato per migliorare il servizio. Tuttavia, in futuro, quando GuardDuty Malware Protection identificherà un file di EBS volume o un file S3 come dannoso o dannoso, GuardDuty Malware Protection raccoglierà e archivierà questo file per sviluppare e migliorare i rilevamenti di malware e il servizio. GuardDuty Questo file può essere utilizzato anche per sviluppare e migliorare altri AWS servizi di sicurezza. La tua fiducia, la tua privacy e la sicurezza dei tuoi contenuti sono la nostra massima priorità e garantiamo che il nostro utilizzo rispetta i nostri impegni nei tuoi confronti. Per ulteriori informazioni, consulta la sezione Privacy dei dati FAQ.

Registrazione delle chiamate GuardDuty API Amazon con AWS CloudTrail

Amazon GuardDuty è integrato conAWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in GuardDuty. CloudTrail acquisisce tutte le chiamate API relative GuardDuty agli eventi, incluse le chiamate dalla GuardDuty console e le chiamate in

codice alle GuardDuty API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon Simple Storage Service (Amazon S3), inclusi gli eventi per. GuardDuty Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta a cui è stata effettuata GuardDuty, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, incluse le modalità di configurazione e attivazione, consulta la Guida per l'AWS CloudTrailutente.

GuardDuty informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività di evento supportata in GuardDuty, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di GuardDuty, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le Regioni . Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consultare:

- Panoramica della creazione di un percorso
- Servizi e integrazioni CloudTrail supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali di accesso utente root o utente IAM
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.

- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento userIdentity di CloudTrail .

GuardDuty eventi del piano di controllo in CloudTrail

Per impostazione predefinita, CloudTrail registra tutte le operazioni GuardDuty API fornite in Amazon GuardDuty API Reference come eventi nei CloudTrail file.

GuardDuty eventi relativi ai dati in CloudTrail

GuardDuty Monitoraggio del runtimeutilizza un agente di GuardDuty sicurezza distribuito nei cluster Amazon Elastic Kubernetes Service (Amazon EKS), solo nelle attività Amazon Elastic Compute Cloud (Amazon EC2) e nelle `aws-guardduty-agent` attività (Amazon Elastic Container Service (AWS FargateAmazon ECS)) per raccogliere componenti aggiuntivi () che raccolgono Tipi di eventi di runtime raccolti i carichi di lavoro e inviarli a rilevamento e analisi delle minacce. AWS GuardDuty

Registrazione e monitoraggio degli eventi di dati

Facoltativamente, puoi configurare i log per visualizzare gli eventi relativi ai dati per il tuo agente di sicurezza. AWS CloudTrail GuardDuty

Per creare e configurare CloudTrail, consulta Data events nella Guida per l'AWS CloudTrailutente e segui le istruzioni per Logging data events con selettori di eventi avanzati in. AWS Management Console Durante la registrazione del trail, assicurati di apportare le modifiche seguenti:

- Per il tipo di evento Data, scegli GuardDuty detector.
- Per il Modello di selettore di log, scegli Registra tutti gli eventi.
- Espandi la Visualizzazione JSON per la configurazione, che dovrebbe essere simile al file JSON seguente:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
```

```
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Dopo aver abilitato il selettore per il percorso, accedi alla console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/. Puoi scaricare gli eventi relativi ai dati dal bucket S3 scelto al momento della configurazione dei log. CloudTrail

Esempio: voci dei file di registro GuardDuty

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che mostra l'evento del piano dati.

```
{
        "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"
        }
    }
```


L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`CreateIPThreatIntelSet`azione (evento del piano di controllo).


```
{
    "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"
}
```

Da queste informazioni sull'evento puoi determinare che la richiesta è stata effettuata per creare un elenco di minacce `Example` in GuardDuty. Puoi inoltre vedere che la richiesta è stata effettuata da un utente denominato Alice il 14 giugno 2018.

Identity and Access Management per Amazon GuardDuty

AWS Identity and Access Management (IAM) è un dispositivo AWS servizio che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. IAMgli amministratori controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. GuardDuty IAMè un dispositivo AWS servizio che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi. GuardDuty

Utente del servizio: se utilizzi il GuardDuty servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più GuardDuty funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in GuardDuty, consultaRisoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon.

Amministratore del servizio: se sei responsabile delle GuardDuty risorse della tua azienda, probabilmente hai pieno accesso a GuardDuty. È tuo compito determinare a quali GuardDuty funzionalità e risorse devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAMamministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base diIAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con GuardDuty, consultaCome GuardDuty funziona Amazon con IAM.

IAMamministratore: se sei un IAM amministratore, potresti voler conoscere i dettagli su come scrivere politiche a cui gestire l'accesso GuardDuty. Per visualizzare esempi di policy GuardDuty basate sull'identità che puoi utilizzare inIAM, consulta. Esempi di policy basate sull'identità per Amazon GuardDuty

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAMIdentity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Firmare AWS API le richieste nella Guida per l'IAMutente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione

a più fattori nella Guida per l'AWS IAM Identity Center utente e Utilizzo dell'autenticazione a più fattori (MFA) AWS nella Guida per l'IAMutente.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte AWS servizi le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'IAMutente.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere AWS servizi utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, un provider di identità Web AWS Directory Service, la directory Identity Center o qualsiasi utente che accede AWS servizi utilizzando credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, vedi Cos'è IAM Identity Center? nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un IAMutente è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente. IAM

Un IAMgruppo è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un IAM utente (anziché un ruolo) nella Guida per l'IAMutente.

IAMruoli

Un IAMruolo è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console cambiando ruolo. È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere Utilizzo IAM dei ruoli nella Guida per l'IAMutente.

IAMi ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, vedere Creazione di un ruolo per un provider di identità di terze parti nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni IAM utente temporanee: un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso su più account: puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per

conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse su più account IAM nella Guida per l'utente. IAM

- Accesso tra servizi: alcuni AWS servizi utilizzano funzionalità in altri. AWS servizi Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta di effettuare richieste AWS servizio ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2istanza e che effettuano AWS CLI o richiedono AWS API. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2istanza. Per assegnare un AWS ruolo a un'EC2istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAMutente.

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta Quando creare un IAM ruolo (anziché un utente) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere Panoramica delle JSON politiche nella Guida per l'IAMutente.

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta Scelta tra politiche gestite e politiche in linea nella Guida per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le politiche AWS gestite IAM in una politica basata sulle risorse.

Elenchi di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioniACLs, consulta la panoramica di Access control list (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM
- Politiche di controllo del servizio (SCPs): SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations

AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCPLimita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations andSCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.

- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta le politiche di sessione nella Guida IAM per l'utente.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle politiche nella Guida per l'IAMutente.

Come GuardDuty funziona Amazon con IAM

Prima di IAM utilizzarlo per gestire l'accesso a GuardDuty, scopri con quali IAM funzionalità è disponibile l'uso GuardDuty.

IAMfunzionalità che puoi usare con Amazon GuardDuty

IAMcaratteristica	GuardDuty supporto
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì

IAMcaratteristica	GuardDuty supporto
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC(tag nelle politiche)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una panoramica generale del funzionamento GuardDuty e degli altri AWS servizi con la maggior parte delle IAM funzionalità, consulta AWS i servizi che funzionano con la maggior parte delle funzionalità IAM nella Guida per l'IAMutente.

Politiche basate sull'identità per GuardDuty

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il riferimento agli elementi IAM JSON della politica nella Guida per l'IAMutente.

Esempi di policy basate sull'identità per GuardDuty

Per visualizzare esempi di politiche basate sull' GuardDuty identità, vedere. Esempi di policy basate sull'identità per Amazon GuardDuty

Politiche basate sulle risorse all'interno GuardDuty

Supporta le policy basate su risorse: no

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta la sezione Cross Account Resource Access IAM nella Guida IAM per l'utente.

Azioni politiche per GuardDuty

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'`Action`elemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di GuardDuty azioni, consulta Azioni definite da Amazon GuardDuty nel Service Authorization Reference.

Le azioni politiche in GuardDuty uso utilizzano il seguente prefisso prima dell'azione:

```
guardduty
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

Per visualizzare esempi di politiche GuardDuty basate sull'identità, vedere. Esempi di policy basate sull'identità per Amazon GuardDuty

Risorse politiche per GuardDuty

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Resource` JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il relativo Amazon Resource Name (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di GuardDuty risorse e relativiARNs, consulta Resources defined by Amazon GuardDuty nel Service Authorization Reference. Per sapere con quali azioni puoi specificare le caratteristiche ARN di ogni risorsa, consulta Azioni definite da Amazon GuardDuty.

Per visualizzare esempi di politiche GuardDuty basate sull'identità, consulta. Esempi di policy basate sull'identità per Amazon GuardDuty

Chiavi relative alle condizioni delle politiche per GuardDuty

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare AWS JSON le politiche per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica`OR`. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta gli elementi IAM della politica: variabili e tag nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'IAMutente.

Per visualizzare un elenco di chiavi di GuardDuty condizione, consulta Condition keys for Amazon GuardDuty nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon GuardDuty.

Per visualizzare esempi di politiche GuardDuty basate sull'identità, consulta. Esempi di policy basate sull'identità per Amazon GuardDuty

Liste di controllo degli accessi () in ACLs GuardDuty

SupportiACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLssono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy. JSON

Controllo degli accessi basato sugli attributi () con ABAC GuardDuty

Supporti ABAC (tag nelle politiche): Parziale

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo diABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABACè utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni suABAC, vedere Cos'è? ABAC nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazioneABAC, consulta Utilizzare il controllo di accesso basato sugli attributi (ABAC) nella Guida per l'IAMutente.

Utilizzo di credenziali temporanee con GuardDuty

Supporta le credenziali temporanee: sì

Alcune AWS servizi non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che AWS servizi funzionano con credenziali temporanee, consulta la sezione AWS servizi relativa alla funzionalità IAM nella Guida per l'IAMutente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla

console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta Passare a un ruolo (console) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere Credenziali di sicurezza temporanee in. IAM

Autorizzazioni principali per più servizi per GuardDuty

Supporta sessioni di accesso diretto (FAS): Sì

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FASutilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta AWS servizio per effettuare richieste ai servizi downstream. FASle richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta Forward access sessions.

Ruoli di servizio per GuardDuty

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un IAMruolo che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'internoIAM. Per ulteriori informazioni, vedere Creazione di un ruolo per delegare le autorizzazioni a un utente AWS servizio nella Guida per l'IAMutente.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. GuardDuty Modifica i ruoli di servizio solo quando viene GuardDuty fornita una guida in tal senso.

Ruoli collegati ai servizi per GuardDuty

Supporta ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati GuardDuty ai servizi, consulta. Utilizzo di ruoli collegati ai servizi per Amazon GuardDuty

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con. IAM Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Amazon GuardDuty

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare risorse. GuardDuty Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta Creazione di IAM politiche nella Guida per l'IAMutente.

Per dettagli sulle azioni e sui tipi di risorse definiti da GuardDuty, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon GuardDuty nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della GuardDuty console
- Autorizzazioni necessarie per abilitare GuardDuty
- Consentire agli utenti di visualizzare le loro autorizzazioni
- IAMPolicy personalizzata per concedere l'accesso in sola lettura a GuardDuty
- Negare l'accesso ai risultati GuardDuty
- Utilizzo di una IAM politica personalizzata per limitare l'accesso alle GuardDuty risorse

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare GuardDuty risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative nella Guida per l'IAMutente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta Politiche e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzandoSSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico AWS servizio, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta Elementi IAM JSON della politica: Condizione nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAMAccess Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, vedere Configurazione dell'APIaccesso MFA protetto nella Guida per l'IAMutente.

Per ulteriori informazioni sulle procedure consigliate inIAM, consulta la sezione Procedure consigliate in materia di sicurezza IAM nella Guida per l'IAMutente.

Utilizzo della GuardDuty console

Per accedere alla GuardDuty console Amazon, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle GuardDuty risorse del tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso il AWS CLI o il. AWS API Consenti invece l'accesso solo alle azioni che corrispondono all'APIoperazione che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la GuardDuty console, allega anche la policy GuardDuty `ConsoleAccess` o la policy `ReadOnly` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiungere autorizzazioni a un utente nella Guida per l'IAMutente.

Autorizzazioni necessarie per abilitare GuardDuty

Per concedere le autorizzazioni necessarie a diverse IAM identità (utenti, gruppi e ruoli), allega la AWS politica gestita: AmazonGuardDutyFullAccess politica di attivazione richiesta. GuardDuty

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla propria identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. 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": "*"
        }
    ]
}
```

IAMPolicy personalizzata per concedere l'accesso in sola lettura a GuardDuty

Per concedere l'accesso in sola lettura GuardDuty è possibile utilizzare la policy gestita. `AmazonGuardDutyReadOnlyAccess`

Per creare una politica personalizzata che conceda a un IAM ruolo, un utente o un gruppo l'accesso in sola lettura a GuardDuty, puoi utilizzare la seguente istruzione:

```
{
    "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": "*"
        }
    ]
}
```

Negare l'accesso ai risultati GuardDuty

È possibile utilizzare la seguente politica per negare a un IAM ruolo, un utente o un gruppo l'accesso ai GuardDuty risultati. Gli utenti non possono visualizzare i risultati o i dettagli sui risultati, ma possono accedere a tutte le altre GuardDuty operazioni:

```
{
    "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"
        }
    ]
```

```
}
```

Utilizzo di una IAM politica personalizzata per limitare l'accesso alle GuardDuty risorse

Per definire l'accesso di un utente in GuardDuty base all'ID del rilevatore, puoi utilizzare tutte le GuardDutyAPIazioni nelle tue IAM politiche personalizzate, ad eccezione delle seguenti operazioni:

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`
- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Utilizzate le seguenti operazioni in una IAM politica per definire l'accesso di un utente a in GuardDuty base all'IPSetID e all' ThreatIntelSet ID:

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

I seguenti esempi mostrano come creare delle policy utilizzando alcune delle operazioni precedenti:

- Questa policy consente a un utente di eseguire l'operazione `guardduty:UpdateDetector` utilizzando l'ID rilevatore 1234567 nella regione us-east-1:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateDetector",
```

```
            ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
        }
    ]
}
```

- Questo criterio consente a un utente di eseguire l'`guardduty:UpdateIPSet`operazione, utilizzando l'ID del rilevatore 1234567 e l'IPSetID 000000 nella regione us-east-1:

> **Note**
>
> Assicurati che l'utente disponga delle autorizzazioni necessarie per accedere agli elenchi di IP affidabili e agli elenchi di minacce in. GuardDuty Per ulteriori informazioni, consulta Autorizzazioni necessarie per caricare elenchi di indirizzi IP affidabili ed elenchi minacce.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
            ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
        }
    ]
}
```

- Questo criterio consente a un utente di eseguire l'`guardduty:UpdateIPSet`operazione, utilizzando qualsiasi ID del rilevatore e l'IPSetID 000000 nella regione us-east-1:

> **Note**
>
> Assicurati che l'utente disponga delle autorizzazioni necessarie per accedere agli elenchi di IP affidabili e agli elenchi di minacce in. GuardDuty Per ulteriori informazioni, consulta Autorizzazioni necessarie per caricare elenchi di indirizzi IP affidabili ed elenchi minacce.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- Questa politica consente a un utente di eseguire l'`guardduty:UpdateIPSet`operazione, utilizzando il proprio ID del rilevatore e qualsiasi IPSet ID nella regione us-east-1:

> **Note**
>
> Assicurati che l'utente disponga delle autorizzazioni necessarie per accedere agli elenchi di IP affidabili e agli elenchi di minacce in. GuardDuty Per ulteriori informazioni, consulta Autorizzazioni necessarie per caricare elenchi di indirizzi IP affidabili ed elenchi minacce.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

Utilizzo di ruoli collegati ai servizi per Amazon GuardDuty

Amazon GuardDuty utilizza AWS Identity and Access Management (IAM) ruoli collegati ai servizi. Un ruolo collegato al servizio (SLR) è un tipo di IAM ruolo unico a cui è collegato direttamente. GuardDuty I ruoli collegati ai servizi sono predefiniti GuardDuty e includono tutte le autorizzazioni necessarie per chiamare altri servizi per GuardDuty conto dell'utente. AWS

Con il ruolo collegato al servizio, puoi eseguire la configurazione GuardDuty senza aggiungere manualmente le autorizzazioni necessarie. GuardDuty definisce le autorizzazioni del suo ruolo collegato al servizio e, a meno che le autorizzazioni non siano definite diversamente, solo può assumere il ruolo. GuardDuty Le autorizzazioni definite includono la politica di fiducia e la politica delle autorizzazioni e tale politica di autorizzazione non può essere associata a nessun'altra entità. IAM

GuardDuty supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui è disponibile. GuardDuty Per ulteriori informazioni, consulta Regioni ed endpoint.

È possibile eliminare il ruolo GuardDuty collegato al servizio solo dopo la prima disabilitazione GuardDuty in tutte le regioni in cui è abilitato. In questo modo proteggi GuardDuty le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedervi.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS i servizi con cui funziona IAM nella Guida per l'IAMutente e cerca i servizi con Sì nella colonna Ruolo collegato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per GuardDuty

GuardDuty utilizza il ruolo collegato al servizio () denominato. SLR `AWSServiceRoleForAmazonGuardDuty` SLRConsente di GuardDuty eseguire le seguenti attività. Consente inoltre di GuardDuty includere i metadati recuperati appartenenti all'EC2istanza nei risultati che GuardDuty possono generare sulla potenziale minaccia. Ai fini dell'assunzione del ruolo `AWSServiceRoleForAmazonGuardDuty`, il ruolo collegato ai servizi `guardduty.amazonaws.com`considera attendibile il servizio.

Le politiche di autorizzazione aiutano a GuardDuty svolgere le seguenti attività:

- Usa EC2 le azioni di Amazon per gestire e recuperare informazioni su EC2 istanze, immagini e componenti di rete come sottoreti e VPCs gateway di transito.

- Usa AWS Systems Manager le azioni per gestire SSM le associazioni sulle EC2 istanze Amazon quando abiliti il monitoraggio del GuardDuty runtime con agente automatizzato per AmazonEC2. Quando la configurazione GuardDuty automatica degli agenti è disabilitata, GuardDuty considera solo le EC2 istanze che hanno un tag di inclusione (`GuardDutyManaged:true`).
- Utilizza AWS Organizations le azioni per descrivere gli account e l'ID dell'organizzazione associati.
- Utilizzare le operazioni di Amazon S3 per recuperare informazioni su bucket e oggetti S3.
- Usa AWS Lambda le azioni per recuperare informazioni sulle funzioni e sui tag Lambda.
- Utilizza EKS le azioni Amazon per gestire e recuperare informazioni sui EKS cluster e gestire i EKScomponenti aggiuntivi di Amazon sui cluster. EKS Le EKS azioni recuperano anche le informazioni sui tag associati a. GuardDuty
- Utilizzare IAM per creare il file Autorizzazioni di ruolo collegate al servizio per Malware Protection for EC2 dopo che Malware Protection for EC2 è stato abilitato.
- Utilizza ECS le azioni Amazon per gestire e recuperare informazioni sui ECS cluster Amazon e gestisci le impostazioni ECS dell'account Amazon con. `guarddutyActivate` Le azioni relative ad Amazon recuperano ECS anche le informazioni sui tag associati a. GuardDuty

Il ruolo è configurato con le seguenti policy gestite da AWS, denominate `AmazonGuardDutyServiceRolePolicy`.

```
{
    "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": "*"
        }
    ]
}
```

Di seguito è riportata la policy di attendibilità associata al ruolo collegato ai servizi `AWSServiceRoleForAmazonGuardDuty`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Per dettagli sugli aggiornamenti della `AmazonGuardDutyServiceRolePolicy` politica, consulta. GuardDuty aggiornamenti alle politiche gestite AWS Per ricevere avvisi automatici sulle modifiche a questa politica, iscriviti al RSS feed sulla Cronologia dei documenti pagina.

Creazione di un ruolo collegato al servizio per GuardDuty

Il ruolo `AWSServiceRoleForAmazonGuardDuty` collegato al servizio viene creato automaticamente quando lo si abilita GuardDuty per la prima volta o si abilita GuardDuty in una regione supportata in cui in precedenza non era abilitato. Puoi anche creare il ruolo collegato al servizio manualmente utilizzando la IAM console, il, o il AWS CLI. IAM API

> **Important**
>
> Il ruolo collegato al servizio creato per l'account amministratore GuardDuty delegato non si applica agli account dei membri. GuardDuty

È necessario configurare le autorizzazioni per consentire a un IAM responsabile (ad esempio un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio. `AWSServiceRoleForAmazonGuardDuty`Affinché il ruolo collegato al servizio venga creato correttamente, il IAM principale con cui lo utilizzi deve disporre delle autorizzazioni GuardDuty richieste. Per concedere le autorizzazioni richieste, collega la seguente policy gestita a questo utente, gruppo o ruolo .

> **Note**
>
> Sostituisci il campione *`account ID`* nell'esempio seguente con l'ID effettivo AWS dell'account.

```
{
    "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"
        }
    ]
}
```

Per ulteriori informazioni sulla creazione manuale del ruolo, vedere Creazione di un ruolo collegato al servizio nella Guida per l'IAMutente.

Modifica di un ruolo collegato al servizio per GuardDuty

GuardDuty non consente di modificare il ruolo collegato al `AWSServiceRoleForAmazonGuardDuty` servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Tuttavia, puoi modificare la descrizione del ruolo utilizzando. IAM Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'IAMutente.

Eliminazione di un ruolo collegato al servizio per GuardDuty

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente.

> **Important**
>
> Se hai abilitato Malware Protection perEC2, l'eliminazione `AWSServiceRoleForAmazonGuardDuty` non comporta l'eliminazione automatica.

`AWSServiceRoleForAmazonGuardDutyMalwareProtection` Se desideri eliminare`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, consulta Eliminazione di un ruolo collegato al servizio per Malware Protection per. EC2

È innanzitutto necessario disattivarlo GuardDuty in tutte le regioni in cui è abilitato per eliminare il. `AWSServiceRoleForAmazonGuardDuty` Se il GuardDuty servizio non è disabilitato quando si tenta di eliminare il ruolo collegato al servizio, l'eliminazione non riesce. Per ulteriori informazioni, consulta Sospensione o disabilitazione GuardDuty.

Quando si disattiva GuardDuty, `AWSServiceRoleForAmazonGuardDuty` non viene eliminato automaticamente. Se lo abiliti GuardDuty nuovamente, inizierà a utilizzare l'esistente`AWSServiceRoleForAmazonGuardDuty`.

Per eliminare manualmente il ruolo collegato al servizio utilizzando IAM

Usa la IAM console AWS CLI, o il IAM API per eliminare il ruolo collegato al `AWSServiceRoleForAmazonGuardDuty` servizio. Per ulteriori informazioni, vedere Eliminazione di un ruolo collegato al servizio nella Guida per l'utente. IAM

Supportato Regioni AWS

Amazon GuardDuty supporta l'utilizzo del ruolo `AWSServiceRoleForAmazonGuardDuty` collegato al servizio Regioni AWS ovunque GuardDuty sia disponibile. Per un elenco delle regioni in cui GuardDuty è attualmente disponibile, consulta gli GuardDuty endpoint e le quote di Amazon nel. Riferimenti generali di Amazon Web Services

Autorizzazioni di ruolo collegate al servizio per Malware Protection for EC2

Malware Protection for EC2 utilizza il ruolo collegato al servizio () denominato. SLR `AWSServiceRoleForAmazonGuardDutyMalwareProtection` Ciò SLR consente a Malware Protection for EC2 di eseguire scansioni senza agenti per rilevare malware nel tuo account. GuardDuty Consente di GuardDuty creare un'istantanea di EBS volume nell'account e condividerla con l'account del servizio. GuardDuty Dopo aver GuardDuty valutato l'istantanea, include i metadati del carico di lavoro dell'EC2istanza e del contenitore recuperati in Malware Protection for findings. EC2 Ai fini dell'assunzione del ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, il ruolo collegato ai servizi `malware-protection.guardduty.amazonaws.com`considera attendibile il servizio.

Le politiche di autorizzazione per questo ruolo aiutano Malware Protection for EC2 a svolgere le seguenti attività:

- Usa le azioni di Amazon Elastic Compute Cloud (AmazonEC2) per recuperare informazioni su EC2 istanze, volumi e istantanee Amazon. Malware Protection for fornisce EC2 anche l'autorizzazione per accedere ai metadati Amazon EKS e Amazon ECS cluster.
- Crea istantanee per i EBS volumi il cui `GuardDutyExcluded` tag non è impostato su. `true` Per impostazione predefinita, gli snapshot vengono creati con un tag `GuardDutyScanId`. Non rimuovere questo tag, altrimenti Malware Protection for non EC2 avrà accesso alle istantanee.

  > **Important**
  >
  > Se lo `GuardDutyExcluded` imposti su`true`, il GuardDuty servizio non sarà in grado di accedere a queste istantanee in futuro. Questo perché le altre istruzioni di questo ruolo collegato al servizio GuardDuty impediscono di eseguire qualsiasi azione sulle istantanee impostate su. `GuardDutyExcluded` `true`

- Consenti la condivisione e l'eliminazione degli snapshot solo se il tag `GuardDutyScanId` esiste e se il tag `GuardDutyExcluded` non è impostato su `true`.

  > **Note**
  >
  > Non consente a Malware Protection di EC2 rendere pubbliche le istantanee.

- Accedi alle chiavi gestite dal cliente, ad eccezione di quelle con un `GuardDutyExcluded` tag impostato su`true`, da chiamare `CreateGrant` per creare e accedere a un EBS volume crittografato dall'istantanea crittografata che viene condivisa con l'account del GuardDuty servizio. Per un elenco degli account di GuardDuty servizio per ogni regione, vedereGuardDuty account di servizio di Regione AWS.
- Accedi ai CloudWatch log dei clienti per creare il gruppo di EC2 log Malware Protection for e inserisci i registri degli eventi di scansione antimalware nel `/aws/guardduty/malware-scan-events` gruppo di log.
- Consenti al cliente di decidere se conservare nel proprio account gli snapshot su cui è stato rilevato il malware. Se la scansione rileva malware, il ruolo collegato al servizio consente di aggiungere due tag GuardDuty alle istantanee: e. `GuardDutyFindingDetected` `GuardDutyExcluded`

> **Note**
>
> Il tag `GuardDutyFindingDetected` specifica che gli snapshot contengono malware.

- Determina se un volume è crittografato con una chiave gestita. EBS GuardDuty esegue l'`DescribeKey`azione per determinare `key Id` la chiave EBS gestita nel tuo account.
- Recupera l'istantanea dei EBS volumi crittografati utilizzando Chiave gestita da AWS, dal tuo Account AWS e copiala su. GuardDuty account di servizio A tal fine, utilizziamo le autorizzazioni `GetSnapshotBlock` e. `ListSnapshotBlocks` GuardDuty eseguirà quindi la scansione dell'istantanea nell'account del servizio. Attualmente, la protezione da malware per il EC2 supporto alla scansione di EBS volumi crittografati con Chiave gestita da AWS potrebbe non essere disponibile in tutti i. Regioni AWS Per ulteriori informazioni, consulta Disponibilità di funzionalità specifiche per ogni regione.
- Consenti EC2 ad Amazon di effettuare una chiamata per AWS KMS conto di Malware Protection EC2 per eseguire diverse azioni crittografiche sulle chiavi gestite dal cliente. Operazioni come `kms:ReEncryptTo` e `kms:ReEncryptFrom` sono necessarie per condividere gli snapshot crittografati con le chiavi gestite dal cliente. Sono accessibili solo le chiavi per le quali il tag `GuardDutyExcluded` non è impostato su `true`.

Il ruolo è configurato con le seguenti policy gestite da AWS, denominate `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

```
{
    "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"
                }
            }
        }
    ]
}
```

La policy di attendibilità seguente è associata al ruolo collegato ai servizi `AWSServiceRoleForAmazonGuardDutyMalwareProtection`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Creazione di un ruolo collegato al servizio per Malware Protection for EC2

Il ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection` collegato al servizio viene creato automaticamente quando abiliti Malware Protection EC2 per la prima volta o abiliti Malware Protection per EC2 in una regione supportata in cui in precedenza non era abilitata. Puoi anche creare il ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection` collegato al servizio manualmente utilizzando la IAM console, il, o il IAMCLI. IAM API

> **Note**
>
> Per impostazione predefinita, se sei un nuovo utente di Amazon GuardDuty, Malware Protection for EC2 è abilitato automaticamente.

> **Important**
>
> Il ruolo collegato al servizio creato per l'account GuardDuty amministratore delegato non si applica agli account dei membri. GuardDuty

È necessario configurare le autorizzazioni per consentire a un IAM responsabile (ad esempio un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio. `AWSServiceRoleForAmazonGuardDutyMalwareProtection`Affinché il ruolo collegato al servizio venga creato correttamente, l'IAMidentità con cui viene utilizzato deve disporre delle autorizzazioni GuardDuty richieste. Per concedere le autorizzazioni richieste, collega la seguente policy gestita a questo utente, gruppo o ruolo .

```
{
    "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"
        }
    ]
}
```

Per ulteriori informazioni sulla creazione manuale del ruolo, vedere Creazione di un ruolo collegato al servizio nella Guida per l'utente. IAM

Modifica di un ruolo collegato al servizio per Malware Protection for EC2

Malware Protection for EC2 non consente di modificare il ruolo collegato al `AWSServiceRoleForAmazonGuardDutyMalwareProtection` servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Tuttavia, è possibile modificare la descrizione del ruolo utilizzando. IAM Per ulteriori informazioni, consulta Modifica di un ruolo collegato al servizio nella Guida per l'IAMutente.

Eliminazione di un ruolo collegato al servizio per Malware Protection for EC2

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente.

> **Important**
>
> Per eliminare il`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, devi prima disabilitare Malware Protection for EC2 in tutte le regioni in cui è abilitato.
> Se Malware Protection for EC2 non è disabilitato quando si tenta di eliminare il ruolo collegato al servizio, l'eliminazione avrà esito negativo. Per ulteriori informazioni, consulta Per abilitare o disabilitare la scansione GuardDuty antimalware avviata.

Quando si sceglie Disattiva per interrompere il servizio Malware Protection for, il EC2 servizio non `AWSServiceRoleForAmazonGuardDutyMalwareProtection` viene eliminato automaticamente. Se poi scegli Abilita per avviare nuovamente il EC2 servizio Malware Protection for, GuardDuty inizierà a utilizzare il servizio esistente`AWSServiceRoleForAmazonGuardDutyMalwareProtection`.

Per eliminare manualmente il ruolo collegato al servizio utilizzando IAM

Usa la IAM console AWS CLI, o il IAM API per eliminare il ruolo collegato al `AWSServiceRoleForAmazonGuardDutyMalwareProtection` servizio. Per ulteriori informazioni, vedere Eliminazione di un ruolo collegato al servizio nella Guida per l'utente. IAM

Supportato Regioni AWS

Amazon GuardDuty supporta l'utilizzo del ruolo `AWSServiceRoleForAmazonGuardDutyMalwareProtection` collegato al servizio in tutti i Regioni AWS casi in cui EC2 è disponibile Malware Protection for.

Per un elenco delle regioni in cui GuardDuty è attualmente disponibile, consulta gli GuardDuty endpoint e le quote di Amazon nel. Riferimenti generali di Amazon Web Services

> **Note**
>
> Malware Protection for non EC2 è attualmente disponibile negli AWS GovCloud Stati Uniti orientali e AWS GovCloud negli Stati Uniti occidentali.

AWS politiche gestite per Amazon GuardDuty

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le politiche AWS gestite che scrivere le politiche da soli. Ci vogliono tempo ed esperienza per creare politiche gestite dai IAM clienti che forniscano al team solo le autorizzazioni di cui ha bisogno. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle politiche AWS gestite, consulta le politiche AWS gestite nella Guida IAM per l'utente.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi aggiungono occasionalmente autorizzazioni aggiuntive a una policy AWS gestita per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una politica AWS gestita quando viene lanciata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per un elenco e le descrizioni delle politiche relative alle funzioni lavorative, consulta le politiche AWS gestite per le funzioni lavorative nella Guida per l'utente. IAM

L'elemento della policy `Version` specifica le regole sintattiche di linguaggio che devono essere utilizzate per elaborare una policy. Le seguenti politiche includono la versione corrente che IAM supporta. Per ulteriori informazioni, vedere Elementi IAM JSON della politica: Versione.

AWS politica gestita: AmazonGuardDutyFullAccess

Puoi allegare la `AmazonGuardDutyFullAccess` politica alle tue IAM identità.

Questa politica concede autorizzazioni amministrative che consentono a un utente l'accesso completo a tutte le azioni. GuardDuty

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `GuardDuty`— Consente agli utenti l'accesso completo a tutte le GuardDuty azioni.
- `IAM`:
  - Consente agli utenti di creare il ruolo GuardDuty collegato al servizio.
  - Consente a un account amministratore di abilitare gli account GuardDuty dei membri.
  - Consente agli utenti di passare un ruolo GuardDuty che utilizza questo ruolo per abilitare la funzionalità GuardDuty Malware Protection for S3. Questo indipendentemente dal modo in cui abiliti Malware Protection for S3, all'interno del GuardDuty servizio o in modo indipendente.
- `Organizations`— Consente agli utenti di designare un amministratore delegato e gestire i membri di un'organizzazione. GuardDuty

L'autorizzazione a eseguire un'`iam:GetRole`azione `AWSServiceRoleForAmazonGuardDutyMalwareProtection` stabilisce se il ruolo collegato al servizio (SLR) per Malware Protection for EC2 esiste in un account.

```
{
    "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 politica gestita: AmazonGuardDutyReadOnlyAccess

Puoi allegare la `AmazonGuardDutyReadOnlyAccess` politica alle tue IAM identità.

Questa politica concede autorizzazioni di sola lettura che consentono a un utente di visualizzare i GuardDuty risultati e i dettagli dell'organizzazione. GuardDuty

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `GuardDuty`— Consente agli utenti di visualizzare GuardDuty i risultati ed eseguire API operazioni che iniziano con`Get`, o. `List` `Describe`
- `Organizations`— Consente agli utenti di recuperare informazioni sulla configurazione GuardDuty dell'organizzazione, inclusi i dettagli dell'account amministratore delegato.

```
{
    "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 politica gestita: AmazonGuardDutyServiceRolePolicy

Non puoi collegarti `AmazonGuardDutyServiceRolePolicy` alle tue IAM entità. Questa policy AWS gestita è associata a un ruolo collegato al servizio che consente di eseguire azioni GuardDuty per conto dell'utente. Per ulteriori informazioni, consulta Autorizzazioni di ruolo collegate ai servizi per GuardDuty.

GuardDuty aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite GuardDuty da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al RSS feed nella pagina della cronologia dei GuardDuty documenti.

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy: aggiornamento a una policy esistente	È stata aggiunta l'`ec2:DescribeVpcs` autorizzazione. Ciò consente di GuardDuty tenere traccia VPC degli aggiornamenti, come il recupero di. VPC CIDR	22 agosto 2024
AmazonGuardDutyServiceRolePolicy: aggiornamento a una policy esistente	È stata aggiunta l'autorizzazione che consente di assegnare un IAM ruolo GuardDuty all'attivazione di Malware Protection for S3. `{`	10 giugno 2024

Modifica	Descrizione	Data
	"Sid": "AllowPassRoleToMalwareProtectionPlan", "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam::*:role/*", "Condition": { "StringEquals": { "iam:PassedToService": "guardduty.amazonaws.com" } } }	
AmazonGuardDutyServiceRolePolicy: aggiorna a una policy esistente.	Usa AWS Systems Manager le azioni per gestire SSM le associazioni sulle EC2 istanze Amazon quando abiliti il monitoraggio del GuardDuty runtime con agente automatizzato per AmazonEC2. Quando la configurazione GuardDuty automatica degli agenti è disabilitata, GuardDuty considera solo le EC2 istanze che hanno un tag di inclusione (`GuardDutyManaged :true`).	26 marzo 2024

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy: aggiorna a una policy esistente.	GuardDuty ha aggiunto una nuova autorizzazione: `organization:DescribeOrganization` recuperare l'ID dell'organizzazione dell'VPCaccount Amazon condiviso e impostare la politica degli VPC endpoint di Amazon con l'ID dell'organizzazione.	9 febbraio 2024
AmazonGuardDutyMalwareProtectionServiceRolePolicy: aggiorna a una policy esistente.	Malware Protection for EC2 ha aggiunto due autorizzazioni: `GetSnapshotBlock` quella di `ListSnapshotBlocks` recuperare l'istantanea di un EBS volume (tramite crittografia Chiave gestita da AWS) dall'utente Account AWS e copiarla sull'account del GuardDuty servizio prima di avviare la scansione antimalware.	25 gennaio 2024
AmazonGuardDutyServiceRolePolicy: aggiornamento a una policy esistente	Sono state aggiunte nuove autorizzazioni GuardDuty per consentire di aggiungere impostazioni ECS dell'account `guarddutyActivate` Amazon ed eseguire operazioni di elenco e descrizione sui ECS cluster Amazon.	26 novembre 2023

Modifica	Descrizione	Data
AmazonGuardDutyReadOnlyAccess: aggiornamento a una policy esistente	GuardDuty ha aggiunto una nuova politica `organizations` per. `ListAccounts`	16 novembre 2023
AmazonGuardDutyFullAccess: aggiornamento a una policy esistente	GuardDuty ha aggiunto una nuova politica `organizations` per`ListAccounts` .	16 novembre 2023
AmazonGuardDutyServiceRolePolicy: aggiornamento a una policy esistente	GuardDuty ha aggiunto nuove autorizzazioni per supportare la prossima funzionalità GuardDuty EKS di monitoraggio del runtime.	8 marzo 2023

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy: aggiornamento a una policy esistente	GuardDuty ha aggiunto nuove autorizzazioni per consentire la creazione di un ruolo collegato GuardDuty al servizio per Malware Protection for. EC2 Ciò contribuirà a GuardDuty semplificare il processo di attivazione di Malware Protection for. EC2 GuardDuty ora può eseguire la seguente IAM azione: `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	21 febbraio 2023
AmazonGuardDutyFullAccess: aggiornamento a una policy esistente	GuardDuty aggiornato ARN `iam:GetRole` per`*AWSServiceRoleForAmazonGuardDutyMalwareProtection` .	26 luglio 2022

Modifica	Descrizione	Data
AmazonGuardDutyFullAccess: aggiornamento a una policy esistente	GuardDuty ha aggiunto un nuovo `AWSServiceName` per consentire la creazione di ruoli collegati al servizio utilizzando `iam:CreateServiceLinkedRole` for GuardDuty Malware Protection for EC2 service. GuardDuty ora può eseguire l'`iam:GetRole` azione per ottenere informazioni per. `AWSServiceRole`	26 luglio 2022

Modifica	Descrizione	Data
AmazonGuardDutyServiceRolePolicy: aggiornamento a una policy esistente	GuardDuty ha aggiunto nuove autorizzazioni per consentire di GuardDuty utilizzare le azioni EC2 di rete di Amazon per migliorare i risultati. GuardDuty ora puoi eseguire le seguenti EC2 azioni per ottenere informazioni sul modo in cui le tue EC2 istanze comunicano. Queste informazioni vengono utilizzate per migliorare la precisione degli esiti. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	3 agosto 2021
GuardDuty ha iniziato a tenere traccia delle modifiche	GuardDuty ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	3 agosto 2021

Risoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con GuardDuty eIAM.

Argomenti

Non sono autorizzato a eseguire alcuna azione in GuardDuty

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

L'errore di esempio seguente si verifica quando l'`mateojacksonIAM`utente tenta di utilizzare la console per visualizzare i dettagli su una *`my-example-widget`* risorsa fittizia ma non dispone delle autorizzazioni fittizie`guardduty:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `guardduty:`*`GetWidget`*.

Se hai bisogno di assistenza, contatta l'amministratore. AWS L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam:PassRole.

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di assegnare un ruolo a GuardDuty.

Alcuni AWS servizi consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un IAM utente denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in. GuardDuty Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di assistenza, contatta AWS l'amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne Account AWS a me di accedere alle mie GuardDuty risorse.

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se GuardDuty supporta queste funzionalità, consulta. Come GuardDuty funziona Amazon con IAM
- Per informazioni su Account AWS come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà nella Guida per l'IAMutente.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a persone Account AWS di proprietà di terzi nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso agli utenti autenticati esternamente (federazione delle identità) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle risorse tra account nella Guida per l'utente. IAM IAM

Convalida della conformità per Amazon GuardDuty

Per sapere se un AWS servizio programma rientra nell'ambito di specifici programmi di conformità, consulta AWS servizi la sezione Scope by Compliance Program AWS servizi e scegli il programma

di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo AWS servizi è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee. HIPAA

  > **Note**
  >
  > Non tutte sono idonee. AWS servizi HIPAA Per ulteriori informazioni, consulta la Guida ai servizi HIPAA idonei.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il settore e la località in cui operi.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione AWS servizi e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization ()). ISO
- Evaluating Resources with Rules nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Ciò AWS servizio fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.

- Amazon GuardDuty: AWS servizio rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, ad esempio PCI DSS soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò AWS servizio consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in Amazon GuardDuty

L'infrastruttura globale di AWS è basata su regioni AWS e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le Zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili, rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle Regioni e le Zone di disponibilità AWS, consulta Infrastruttura globale di AWS.

Sicurezza dell'infrastruttura in Amazon GuardDuty

In quanto servizio gestito, Amazon GuardDuty è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Si utilizzano API chiamate AWS pubblicate per accedere tramite GuardDuty la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS) come (Ephemeral Diffie-Hellman) o DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale. IAM In alternativa, è possibile utilizzare AWS Security

Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Integrazione di AWS servizi con GuardDuty

GuardDuty può essere integrato con altri servizi AWS di sicurezza. Questi servizi possono importare dati da cui GuardDuty l'utente può visualizzare i risultati in modi nuovi. Consulta le seguenti opzioni di integrazione per saperne di più su come il servizio è configurato per funzionare. GuardDuty

Integrazione con GuardDuty AWS Security Hub

AWS Security Hub raccoglie dati di sicurezza da tutti AWS gli account, i servizi e i prodotti partner di terze parti supportati per valutare lo stato di sicurezza dell'ambiente in base agli standard e alle migliori pratiche del settore. Oltre a valutare il tuo livello di sicurezza, Security Hub crea una posizione centrale per i risultati di tutti i AWS servizi integrati e i prodotti dei AWS partner. L'attivazione di Security Hub con GuardDuty consentirà automaticamente l' GuardDuty acquisizione dei dati dei risultati da parte di Security Hub.

Per ulteriori informazioni sull'utilizzo di Security Hub, GuardDuty vedereIntegrazione con AWS Security Hub.

Integrazione GuardDuty con Amazon Detective

Amazon Detective utilizza i dati di log provenienti da tutti AWS i tuoi account per creare visualizzazioni di dati per le tue risorse e gli indirizzi IP che interagiscono con il tuo ambiente. Le visualizzazioni di Detective sono utili per indagare in modo rapido e semplice sui problemi di sicurezza. Puoi passare dalla GuardDuty ricerca dei dettagli alle informazioni nella console Detective una volta abilitati entrambi i servizi.

Per ulteriori informazioni sull'utilizzo di Detective, GuardDuty vedereIntegrazione con Amazon Detective.

Integrazione con AWS Security Hub

AWS Security Hub fornisce una visione completa dello stato di sicurezza in AWS e ti aiuta a controllare l'ambiente rispetto agli standard di sicurezza del settore e alle best practice. Security Hub raccoglie dati sulla sicurezza da tutti AWS gli account, i servizi e i prodotti partner di terze parti supportati e ti aiuta ad analizzare le tendenze in materia di sicurezza e identificare i problemi di sicurezza con la massima priorità.

L' GuardDuty integrazione di Amazon con Security Hub ti consente di inviare i risultati GuardDuty da Security Hub. Security Hub può quindi includere tali risultati nella sua analisi della posizione di sicurezza.

Indice

In che modo Amazon GuardDuty invia i risultati a AWS Security Hub

Nel AWS Security Hub, i problemi di sicurezza vengono registrati come risultati. Alcuni risultati derivano da problemi rilevati da altri AWS servizi o da partner terzi. Security Hub dispone inoltre di una serie di regole che utilizza per rilevare problemi di sicurezza e generare risultati.

Security Hub fornisce strumenti per gestire i risultati da tutte queste fonti. È possibile visualizzare e filtrare gli elenchi di risultati e visualizzare i dettagli per un riscontro. Per ulteriori informazioni, consulta Visualizzazione dei riscontri nella Guida per l'utente AWS Security Hub . È inoltre possibile monitorare lo stato di un'indagine in un esito. Per ulteriori informazioni, consulta Azioni sugli esiti nella Guida per l'utente di AWS Security Hub .

Tutti i risultati in Security Hub utilizzano un JSON formato standard chiamato AWS Security Finding Format (ASFF). ASFFInclude dettagli sull'origine del problema, sulle risorse interessate e sullo stato attuale del risultato. Vedi AWS Security Finding Format (ASFF) nella Guida AWS Security Hub per l'utente.

Amazon GuardDuty è uno dei AWS servizi che invia i risultati a Security Hub.

Tipi di risultati che vengono GuardDuty inviati a Security Hub

Una volta abilitato GuardDuty Security Hub nello stesso account all'interno dello stesso Regione AWS, GuardDuty inizia a inviare tutti i risultati generati a Security Hub. Questi risultati vengono inviati a Security Hub utilizzando il AWS Security Finding Format (ASFF). NelASFF, il `Types` campo fornisce il tipo di risultato.

Latenza per l'invio di nuovi risultati

Quando viene GuardDuty creato un nuovo risultato, di solito viene inviato a Security Hub entro cinque minuti.

Nuovo tentativo quando Security Hub non è disponibile

Se Security Hub non è disponibile, GuardDuty riprova a inviare i risultati finché non vengono ricevuti.

Aggiornamento degli esiti esistenti nella Centrale di sicurezza

Dopo aver inviato un risultato a Security Hub, GuardDuty invia aggiornamenti per riflettere ulteriori osservazioni sull'attività di ricerca a Security Hub. Le nuove osservazioni di questi risultati vengono inviate a Security Hub in base alle Fase 5 — Frequenza di esportazione dei risultati impostazioni del tuo Account AWS.

Quando archivi o annulli l'archiviazione di un risultato, GuardDuty non lo invia a Security Hub. Qualsiasi risultato non archiviato manualmente e che successivamente diventerà attivo in non GuardDuty viene inviato a Security Hub.

Visualizzazione dei risultati GuardDuty in AWS Security Hub

Per visualizzare i GuardDuty risultati in Security Hub, seleziona See Findings under Amazon GuardDuty dalla pagina di riepilogo. In alternativa, puoi selezionare Risultati dal pannello di navigazione e filtrare i risultati per visualizzare solo GuardDuty i risultati selezionando il campo Nome prodotto: con un valore di`GuardDuty`.

Interpretazione dei nomi GuardDuty dei risultati in AWS Security Hub

GuardDuty invia i risultati a Security Hub utilizzando il AWS Security Finding Format (ASFF). NelASFF, il `Types` campo fornisce il tipo di risultato. ASFFi tipi utilizzano uno schema di denominazione diverso rispetto ai GuardDuty tipi. La tabella seguente descrive in dettaglio tutti i tipi GuardDuty di risultati con la loro ASFF controparte così come appaiono in Security Hub.

> **Note**
>
> Per alcuni tipi di GuardDuty ricerca, Security Hub assegna nomi di ASFF ricerca diversi a seconda che il ruolo della risorsa del dettaglio del risultato fosse ACTORo TARGET. Per ulteriori informazioni, consulta Dettagli degli esiti.

GuardDuty tipo di ricerca	ASFFtipo di ricerca
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
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual

GuardDuty tipo di ricerca	ASFFtipo di ricerca
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
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin

GuardDuty tipo di ricerca	ASFFtipo di ricerca
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
DefenseEvasion:IAMUser/AnomalousBehavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior

GuardDuty tipo di ricerca	ASFFtipo di ricerca
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
Scoperta:IAMUser/AnomalousBehavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:Kubernetes/MaliciousIPCaller	TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller

GuardDuty tipo di ricerca	ASFFtipo di ricerca
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
Impact:Kubernetes/MaliciousIPCaller	TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller

GuardDuty tipo di ricerca	ASFFtipo di ricerca
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
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile

GuardDuty tipo di ricerca	ASFFtipo di ricerca
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
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual

GuardDuty tipo di ricerca	ASFFtipo di ricerca
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
Impatto: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 tipo di ricerca	ASFFtipo di ricerca
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
Persistenza:/IAMUserAnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions

GuardDuty tipo di ricerca	ASFFtipo di ricerca
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 tipo di ricerca	ASFFtipo di ricerca
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 tipo di ricerca	ASFFtipo di ricerca
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 tipo di ricerca	ASFFtipo di ricerca
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 tipo di ricerca	ASFFtipo di ricerca
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 tipo di ricerca	ASFFtipo di ricerca
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

Esito tipico di GuardDuty

GuardDuty invia i risultati a Security Hub utilizzando il AWS Security Finding Format (ASFF).

Ecco un esempio di un risultato tipico di 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"
}
```


Abilitazione e configurazione dell'integrazione

Per utilizzare l'integrazione con AWS Security Hub, devi abilitare Security Hub. Per informazioni su come abilitare Security Hub, consulta Configurazione di Security Hub nella Guida per l'utente di AWS Security Hub .

Quando abiliti entrambi GuardDuty e Security Hub, l'integrazione viene abilitata automaticamente. GuardDutyinizia immediatamente a inviare i risultati a Security Hub.

Utilizzo GuardDuty dei controlli in Security Hub

AWS Security Hub utilizza i controlli di sicurezza per valutare le AWS risorse e verificare la conformità rispetto agli standard e alle best practice del settore della sicurezza. È possibile utilizzare i controlli relativi alle GuardDuty risorse e ai piani di protezione selezionati. Per ulteriori informazioni, consulta GuardDuty i controlli Amazon nella Guida AWS Security Hub per l'utente.

Per un elenco di tutti i controlli tra AWS servizi e risorse, consulta il riferimento ai controlli di Security Hub nella Guida per l'AWS Security Hub utente.

Interruzione dell'invio degli esiti a Security Hub

Per interrompere l'invio dei risultati a Security Hub, puoi utilizzare la console Security Hub o ilAPI.

Vedi Disabilitazione e abilitazione del flusso di risultati da un'integrazione (console) o Disabilitazione del flusso di risultati da un'integrazione (Security Hub AWS CLI) nella API Guida per l'AWS Security Hub utente.

Integrazione con Amazon Detective

Amazon Detective ti aiuta ad analizzare e indagare rapidamente sugli eventi di sicurezza su uno o più AWS account generando visualizzazioni di dati che rappresentano il modo in cui le tue risorse si comportano e interagiscono nel tempo. Detective crea visualizzazioni dei risultati. GuardDuty

Detective acquisisce i dettagli di tutti ogni tipo di esito e fornisce l'accesso ai profili delle entità per indagare su quelle coinvolte negli esiti. Un'entità può essere una Account AWS AWS risorsa all'interno di un account o un indirizzo IP esterno che ha interagito con le tue risorse. La GuardDuty console supporta il passaggio ad Amazon Detective dalle seguenti entità, a seconda del tipo di ricerca: IAM ruolo Account AWS, utente o sessione di ruolo, agente utente, utente federato, EC2 istanza Amazon o indirizzo IP.

Indice

Abilitazione dell'integrazione

Per utilizzare Amazon Detective con GuardDuty , devi prima abilitare Amazon Detective. Per informazioni su come abilitare Detective, consulta Configurazione di Amazon Detective nella Guida di amministrazione di Amazon Detective.

Quando abiliti entrambi GuardDuty e Detective, l'integrazione viene abilitata automaticamente. Una volta abilitato, Detective acquisirà immediatamente i dati dei GuardDuty risultati.

> **Note**
>
> GuardDuty invia i risultati al Detective in base alla frequenza di esportazione dei GuardDuty risultati. Per impostazione predefinita, la frequenza di esportazione per gli aggiornamenti agli esiti esistenti è di 6 ore. Per garantire che Detective riceva gli aggiornamenti più recenti sulle tue scoperte, ti consigliamo di modificare la frequenza di esportazione a 15 minuti in

ogni regione in cui utilizzi Detective GuardDuty. Per ulteriori informazioni, consulta Fase 5 — Impostazione della frequenza per esportare i risultati attivi aggiornati.

Passare ad Amazon Detective partendo da una scoperta GuardDuty

1. Accedi alla console. https://console.aws.amazon.com/guardduty/
2. Scegli un singolo esito dalla tabella degli esiti.
3. Scegli Esamina con Detective dal riquadro dei dettagli dell'esito.
4. Scegli un aspetto dell'esito su cui indagare con Amazon Detective. Così facendo si apre la console Detective per l'esito o entità in questione.

Se il pivot non si comporta come previsto, consulta Risoluzione dei problemi del pivot nella nella Guida per l'utente di Amazon Detective.

> **Note**
>
> Se archivi un GuardDuty risultato nella console Detective, quel risultato viene archiviato anche nella GuardDuty console.

Utilizzo dell'integrazione con un ambiente GuardDuty multi-account

Se gestisci un ambiente con più account in GuardDuty, devi aggiungere i tuoi account membro ad Amazon Detective per visualizzare le visualizzazioni dei dati di Detective relativi ai risultati e alle entità presenti in tali account.

Si consiglia di utilizzare lo stesso account GuardDuty amministratore dell'account amministratore di Detective. Per ulteriori informazioni sull'aggiunta di account membri in Detective, consulta Invitare account membri.

> **Note**
>
> Detective è un servizio regionale, perciò devi abilitare Detective e aggiungere i tuoi account membri in ogni regione in cui desideri utilizzare l'integrazione.

Sospensione o disabilitazione GuardDuty

Puoi utilizzare la GuardDuty console per sospendere o disabilitare il servizio. GuardDuty Non ti viene addebitato alcun costo per l'utilizzo GuardDuty quando il servizio è sospeso.

- Tutti gli account dei membri devono essere dissociati o eliminati prima di poter sospendere o disabilitare. GuardDuty
- Se si sospende GuardDuty, la sospensione non monitora più la sicurezza dell' AWS ambiente né genera nuovi risultati. I risultati esistenti rimangono intatti e non sono influenzati dalla sospensione. GuardDuty Puoi scegliere di GuardDuty riattivarla in un secondo momento.
- La disattivazione GuardDuty in un account verrà disattivata solo per l'account attualmente selezionato Regione AWS. Se desideri disabilitarlo completamente GuardDuty, devi disabilitarlo in ogni regione in cui è abilitato.
- Se disabiliti GuardDuty, i risultati e la GuardDuty configurazione esistenti vengono persi e non possono essere recuperati. Se desideri salvare i risultati esistenti, devi esportarli prima di confermarne la disabilitazione GuardDuty. Per informazioni su come esportare gli esiti, consulta Esportazione degli esiti.
- Se hai abilitato Malware Protection for S3 per uno o più bucket protetti nel tuo account, la sospensione o la disabilitazione GuardDuty non influiscono sullo stato di un bucket protetto in Malware Protection for S3. Anche dopo la sospensione o la disattivazione GuardDuty, il tuo account continuerà a sostenere i costi di utilizzo associati alla funzionalità Malware Protection for S3. Per informazioni sulla disabilitazione di Malware Protection for S3, consulta. Disattiva la protezione da malware per S3 per un bucket protetto

Per sospendere o disabilitare GuardDuty

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione scegli Impostazioni.
3. Nella GuardDuty sezione Sospendi, scegli Sospendi GuardDuty o Disattiva GuardDuty, quindi Conferma l'azione.

Da riattivare dopo la sospensione GuardDuty

1. Apri la GuardDuty console all'indirizzo https://console.aws.amazon.com/guardduty/.
2. Nel pannello di navigazione scegli Impostazioni.

3. Scegli Riattiva. GuardDuty

Iscrizione agli annunci di Amazon SNS GuardDuty

Questa sezione fornisce informazioni sull'abbonamento ad Amazon SNS (Simple Notification Service) per GuardDuty gli annunci di ricezione di notifiche sui tipi di risultati appena rilasciati, aggiornamenti ai tipi di risultati esistenti e altre modifiche alle funzionalità. Le notifiche sono disponibili in tutti i formati supportati da AmazonSNS.

GuardDuty SNSInvia un annuncio sugli aggiornamenti del GuardDuty servizio AWS a qualsiasi account sottoscritto. Per ricevere notifiche sugli esiti all'interno del tuo account, consulta Creazione di risposte personalizzate ai GuardDuty risultati con Amazon CloudWatch Events.

> **Note**
>
> Il tuo IAM utente deve disporre `sns::subscribe` delle autorizzazioni per iscriversi a un. SNS

Puoi iscrivere una SQS coda Amazon a questo argomento di notifica, ma devi utilizzare un argomento ARN che si trova nella stessa regione. Per ulteriori informazioni, consulta Tutorial: Subscribing an Amazon SQS queue to an Amazon SNS topic nella guida per sviluppatori di Amazon Simple Queue Service.

Puoi anche utilizzare una AWS Lambda funzione per attivare eventi quando vengono ricevute notifiche. Per ulteriori informazioni, consulta Invocare le funzioni Lambda utilizzando le notifiche di SNS Amazon nella guida per sviluppatori di Amazon Simple Queue Service.

Di seguito è riportato ARNs l'SNSargomento Amazon per ciascuna regione.

AWS Regione	SNSArgomento Amazon ARN
`us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`
`us-east-2`	`arn:aws:sns:us-east-2:118283430703:G`

AWS Regione	SNSArgomento Amazon ARN
	uardDutyAnnounceme nts
us-west-1	arn:aws:sns:us-wes t-1:144182107116:G uardDutyAnnounceme nts
us-west-2	arn:aws:sns:us-wes t-2:934957504740:G uardDutyAnnounceme nts
ca-central-1	arn:aws:sns:ca-cen tral-1:10743005193 3:GuardDutyAnnounc ements
ca-west-1	arn:aws:sns:ca-wes t-1:440427180217:G uardDutyAnnounceme nts
eu-north-1	arn:aws:sns:eu-nor th-1:973841112453: GuardDutyAnnouncem ents
eu-west-1	arn:aws:sns:eu-wes t-1:965013871422:G uardDutyAnnounceme nts

AWS Regione	SNSArgomento Amazon 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 Regione	SNSArgomento Amazon 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 Regione	SNSArgomento Amazon 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 Regione	SNSArgomento Amazon 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

Per iscriverti all'e-mail di notifica dell' GuardDuty aggiornamento contenuta nel AWS Management Console

1. Apri la SNS console Amazon su https://console.aws.amazon.com/sns/v3/home.
2. Nell'elenco delle regioni, scegli la stessa regione dell'argomento ARN a cui iscriverti. Questo esempio utilizza la regione `us-west-2`.
3. Nel riquadro di navigazione a sinistra, scegli Subscriptions (Abbonamenti), quindi Create subscription (Crea abbonamento).
4. Nella finestra di dialogo Crea sottoscrizione, per Argomento ARN, incolla l'argomentoARN:`arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. Per Protocollo, scegli E-mail. Per Endpoint, digitare l'indirizzo e-mail a cui deve essere inviata la notifica.
6. Scegli Crea sottoscrizione.
7. Nella tua applicazione di posta elettronica, apri il messaggio da AWS Notifiche e apri il link per confermare l'iscrizione.

   Il tuo browser web visualizza una risposta di conferma da AmazonSNS.

Per iscriverti all'e-mail di notifica dell' GuardDuty aggiornamento con AWS CLI

1. Esegui il comando riportato qui di seguito con la AWS CLI:

```
 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. Nella tua applicazione di posta elettronica, apri il messaggio contenuto in AWS Notifiche e apri il link per confermare l'iscrizione.

   Il tuo browser web visualizza una risposta di conferma da AmazonSNS.

Formato dei SNS messaggi Amazon

Un esempio di messaggio di notifica GuardDuty generale:

```
{
    "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"
}
```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

```
{
        "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"
                ]
             }
        ]
}
```

Di seguito è riportato un esempio di messaggio di notifica di GuardDuty aggiornamento relativo a nuovi risultati:

```
{
    "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"
}
```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

```
{
    "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."
    }]
}
```

Di seguito è riportato un esempio di messaggio di notifica di GuardDuty aggiornamento relativo agli aggiornamenti delle GuardDuty funzionalità:

```
{
    "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"
}
```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

```
{
    "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"
    }]
}
```

Di seguito è riportato un esempio GuardDuty di messaggio di notifica di aggiornamento relativo ai risultati aggiornati:

```
{
    "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"
}
```

Il valore Message analizzato (con la rimozione dei caratteri escape) viene mostrato di seguito:

```
{
    "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 Quote Amazon

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ciascuna di esse. AWS servizio Salvo diversa indicazione, ogni quota si applica a una regione specifica. Puoi richiedere aumenti per alcune quote e altre quote non possono essere aumentate.

Per visualizzare le quote per GuardDuty, apri la console Service Quotas. Nel riquadro di navigazione, scegli AWS servizie seleziona Amazon GuardDuty.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas.

Hai Account AWS le seguenti quote per Amazon GuardDuty per regione.

> **Note**
>
> - Per le quote specifiche di GuardDuty Malware Protection for EC2, consulta. Protezione da malware per le quote EC2
> - Per le quote specifiche di Malware Protection for S3, vedi. Quote nella protezione da malware per S3

GuardDuty quote per regione

Risorsa	Default	Commenti
Rilevatori	1	Il numero massimo di risorse del rilevatore che puoi creare per account AWS per regione. Non puoi richieder e un aumento della quota.
Filtri	100	Il numero massimo di filtri salvati per AWS account per regione.

Risorsa	Default	Commenti
		Non puoi richieder e un aumento della quota.
Ritrovamento del periodo di conservazione	90 giorni	Il numero massimo di giorni di accertamento viene mantenuto. Non puoi richieder e un aumento della quota.
Indirizzi IP e intervalli CIDR per l'elenco degli IP affidabili	2.000	Il numero massimo di indirizzi IP e intervalli CIDR che è possibile includere in un singolo elenco di IP affidabili. Non puoi richieder e un aumento della quota.
Indirizzi IP e intervalli CIDR per l'elenco delle minacce	250.000	Il numero massimo di indirizzi IP e intervalli CIDR che è possibile includere in un elenco di minacce. Non puoi richieder e un aumento della quota.

Risorsa	Default	Commenti
Dimensione massima dei file	35 MB	La dimensione massima del file utilizzato per caricare un elenco di indirizzi IP o intervalli CIDR da includere in un elenco di IP affidabili o in un elenco di minacce. Non puoi richieder e un aumento della quota.
Account membri (su invito)	5000	Il numero massimo di account membro associati a un account amministratore. Non puoi richieder e un aumento della quota.

Risorsa	Default	Commenti
Account membri	50.000	Il numero massimo di account membro associati a un account amministratore tramite AWS Organizations. inclusi gli account membri che vengono aggiunti all'organ izzazione tramite invito. Questo valore predefinito dipende dalla quota attuale di account membri in AWS Organizations. Il numero di account membro GuardDuty che vengono aggiunti non AWS Organizat ions può superare il numero di account membro dell'orga nizzazione. Per informazioni sul numero di membri Account AWS in un'organizzazione, consulta Valori massimi e minimi nella Guida per l'AWS Organizations utente.

Risorsa	Default	Commenti
Set di intelligence delle minacce	6	Il numero massimo di set di intelligence delle minacce che puoi aggiungere per account AWS per regione. Non puoi richiedere un aumento della quota.
Set di IP affidabili	1	Il numero massimo di set IP affidabili che possono essere caricati e attivati per AWS account per regione. Non puoi richiedere un aumento della quota.

Risoluzione dei problemi con Amazon GuardDuty

Se riscontri problemi relativi all'esecuzione di un'azione specifica di GuardDuty, consulta gli argomenti di questa sezione.

Argomenti

Problemi generali in GuardDuty

Ricevo un errore di accesso durante l'esportazione dei GuardDuty risultati. Come posso risolvere questo problema?

Dopo aver configurato le impostazioni per esportare i risultati, se non GuardDuty è possibile esportare i risultati, viene visualizzato un messaggio di errore nella pagina Impostazioni della GuardDuty console. Ciò può accadere potenzialmente quando non è più GuardDuty possibile accedere alla risorsa di destinazione, ad esempio se il bucket Amazon S3 è stato eliminato o l'autorizzazione per accedere al bucket è stata modificata. Ciò può verificarsi anche quando non è più GuardDuty possibile accedere alla AWS KMS chiave utilizzata per crittografare i dati nel bucket Amazon S3. Quando non GuardDuty è in grado di esportare, invia una notifica all'indirizzo e-mail associato all'account per fornire informazioni su questo problema.

Per risolvere il problema, assicurati che le risorse corrispondenti esistano e GuardDuty disponga delle autorizzazioni per accedere alle risorse necessarie. Se non risolvi il problema prima del termine del periodo di conservazione dei risultati di 90 giorni GuardDuty, i risultati non verranno esportati. GuardDuty disabiliterà la ricerca delle impostazioni di esportazione per questo account nella regione specifica. Anche dopo questa data di conservazione, è possibile aggiornare le impostazioni di configurazione per riavviare l'esportazione dei risultati nella regione specifica.

Per ulteriori informazioni, consulta Esportazione degli esiti.

Protezione da malware per problemi relativi a EC2

All'avvio di una scansione antimalware on demand ricevo un messaggio di un errore che segnala la mancanza delle autorizzazioni richieste.

Se ricevi un errore che suggerisce che non disponi delle autorizzazioni necessarie per avviare una scansione antimalware on demand su un'istanza Amazon EC2, verifica di aver collegato la policy AWS politica gestita: AmazonGuardDutyFullAccess al tuo ruolo IAM.

Se sei membro di un' AWS organizzazione e continui a ricevere lo stesso errore, connettiti al tuo account di gestione. Per ulteriori informazioni, consulta AWS Organizations SCP— Accesso negato.

Ricevo un **`iam:GetRole`** errore mentre lavoro con Malware Protection for EC2.

Se ricevi questo erroreUnable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection, significa che non hai l'autorizzazione per abilitare la scansione antimalware GuardDuty avviata o utilizzare la scansione antimalware su richiesta. Verifica di aver collegato la policy AWS politica gestita: AmazonGuardDutyFullAccess al tuo ruolo IAM.

Sono un account GuardDuty amministratore che deve abilitare la scansione antimalware GuardDuty avviata dall'utente, ma non utilizza AWS Managed Policy: to manage. AmazonGuardDutyFullAccess GuardDuty

- Configura il ruolo IAM con cui utilizzi GuardDuty per disporre delle autorizzazioni necessarie per abilitare la scansione GuardDuty antimalware avviata. Per ulteriori informazioni sulle autorizzazioni richieste, consulta Creazione di un ruolo collegato ai servizi per Malware Protection for EC2.
- Collega AWS politica gestita: AmazonGuardDutyFullAccess al tuo ruolo IAM. Questo ti aiuterà ad abilitare la scansione GuardDuty antimalware avviata dagli account dei membri.

Problemi di monitoraggio del runtime

Il mio AWS Step Functions flusso di lavoro non funziona in modo imprevisto

Se il GuardDuty contenitore ha contribuito all'errore del flusso di lavoro, vedi. Risoluzione dei problemi di copertura Se il problema persiste, per evitare che il flusso di lavoro non funzioni a causa del GuardDuty contenitore, esegui una delle seguenti operazioni:

- Aggiungi il `false` tag`GuardDutyManaged`: al cluster Amazon ECS associato.
- Disattiva la configurazione automatica degli agenti per AWS Fargate (solo ECS) a livello di account. Aggiungi il tag di inclusione`GuardDutyManaged`: `true` al cluster Amazon ECS associato che desideri continuare a monitorare con l'agente GuardDuty automatizzato.

Risoluzione degli errori di esaurimento della memoria in Runtime Monitoring (solo supporto Amazon EC2)

Questa sezione fornisce le procedure per la risoluzione dei problemi in caso di esaurimento della memoria in base CPUe limite di memoria alla distribuzione manuale del GuardDuty Security Agent.

Se `systemd` interrompe l' GuardDuty agente a causa del `out-of-memory` problema e si ritiene che fornire più memoria all' GuardDuty agente sia ragionevole, è possibile aggiornare il limite.

1. Con l'autorizzazione root, apri`/lib/systemd/system/amazon-guardduty-agent.service`.
2. Trova `MemoryLimit` e `MemoryMax` aggiorna entrambi i valori.

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. Dopo aver aggiornato i valori, riavviate l' GuardDuty agente utilizzando il seguente comando:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Eseguite il comando seguente per visualizzare lo stato:

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

L'output previsto mostrerà il nuovo limite di memoria:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Gestione dei problemi relativi a più account

Desidero gestire più account ma non dispongo dell'autorizzazione di AWS Organizations gestione richiesta.

Se ricevi questo erroreThe `request failed because you do not have required AWS Organization master permission.`, significa che non hai l'autorizzazione per abilitare la scansione antimalware GuardDuty avviata per più account della tua organizzazione. Per ulteriori informazioni su come concedere l'autorizzazione all'account di gestione, consulta. Stabilire un accesso affidabile per abilitare la scansione GuardDuty antimalware avviata

Altre questioni relative alla risoluzione dei problemi

Se non trovi lo scenario adatto al tuo problema, visualizza le seguenti opzioni di risoluzione dei problemi:

- Per problemi generali relativi a IAM quando accedi a https://console.aws.amazon.com/guardduty/, consulta Risoluzione dei problemi relativi all' GuardDuty identità e all'accesso ad Amazon.
- Per problemi di autenticazione e autorizzazione durante l'accesso AWS AWS Console Home, consulta Risoluzione dei problemi di IAM.

Regioni ed endpoint

Per visualizzare Regioni AWS dove GuardDuty è disponibile Amazon, consulta Amazon GuardDuty endpoints nel Riferimenti generali di Amazon Web Services.

Ti consigliamo di abilitare tutte le GuardDuty funzionalità supportate Regioni AWS. Ciò consente di GuardDuty generare informazioni su attività non autorizzate o insolite anche nelle Regioni che non utilizzi attivamente. Ciò consente inoltre di GuardDuty monitorare AWS CloudTrail gli eventi per il soggetto supportato Regioni AWS, riducendo la sua capacità di rilevare attività che coinvolgono servizi globali.

Disponibilità di funzionalità specifiche per ogni regione

Un elenco di differenze regionali per specificare la disponibilità delle GuardDuty funzionalità.

ListFindings e GetFindingsStatistics API

Le ListFindingsAPI GetFindingsStatisticsand hanno un flag temporaneo`consoleOnly`. Quando utilizzi una o entrambe queste API, il `consoleOnly` flag indica che l'API può recuperare risultati fino a un limite massimo di 1000.

GuardDuty funzionalità con disparità di regione

Protezione da malware per EC2

GuardDuty supporta la funzionalità Malware Protection for EC2 nelle AWS Dedicated Local Zones.

Supporto generale per le API

Le seguenti API in Amazon GuardDuty API Reference possono presentare differenze regionali a causa dell'indisponibilità di alcune fonti di dati o funzionalità specificate in precedenza: Regioni AWS

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector
- GetMemberDetectors

- DescribeOrganizationConfiguration

Tipi di esiti di Amazon EC2: DefenseEvasion:EC2/UnusualDoHActivity e DefenseEvasion:EC2/UnusualDoTActivity

La tabella seguente mostra Regioni AWS dove GuardDuty è disponibile, ma questi due tipi di ricerca di Amazon EC2 non sono ancora supportati.

Regione AWS	Codice regione
Asia Pacifico (Seul)	ap-northeast-2
Asia Pacifico (Osaka-Locale)	ap-northeast-3
Asia Pacifico (Giacarta)	ap-southeast-3

AWS GovCloud (US) Regioni

Per le informazioni più recenti, consulta Amazon GuardDuty nella Guida AWS GovCloud (US) per l'utente.

Regioni della Cina

Per le informazioni più recenti, consulta Differenze nella disponibilità e nell'implementazione delle funzionalità.

GuardDuty azioni e parametri precedenti

Amazon GuardDuty ha reso obsolete alcune azioni e parametri dell'API, ma le supporta ancora. La best practice consiste nell'utilizzare le nuove azioni e parametri API che sostituiscono le opzioni legacy. Nella tabella seguente vengono confrontate le operazioni e i parametri legacy e quelli nuovi.

Operazioni/parametri legacy	Operazioni/parametri nuovi	Confronto
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Con la stessa implementazione in entrambe le azioni, GuardDuty utilizza il termine in. `Administrator` `DisassociateFromAdministratorAccount`
`autoEnable` parametro in DescribeOrganizationConfiguratione UpdateOrganization Configuration	`autoEnableOrganizationMembers`	Con`autoEnableOrganizationMembers`, l'account GuardDuty amministratore può controllare e applicare GuardDuty per tutti gli account membri uno dei valori. Utilizzando le API, l'aggiornamento della configurazione per tutti gli account membri può richiedere fino a 24 ore. Per ulteriori informazioni sui possibili valori del `autoEnableOrganizationMembers` campo, vedi Membri autoEnableOrganization
Parametro `dataSources` nelle API elencate in GuardDuty APImodifiche a marzo 2023.	`features`	A partire da marzo 2023, puoi configurare GuardDuty Protezione da malware per EC2 e utilizzare i nuovi piani di GuardDuty protezion `efeatures`. I piani di protezione lanciati prima di marzo 2023, incluso Malware Protection for EC2, supportano ancora la configura

Operazioni/ parametri legacy	Operazioni/parametri nuovi	Confronto
		zione tramite`dataSources` . Se utilizzi le API per configurare un piano di protezione, ogni richiesta API può includere `dataSources` o `features`, non entrambe.

Cronologia dei documenti per Amazon GuardDuty

La tabella seguente descrive importanti modifiche alla documentazione dall'ultima versione della Amazon GuardDuty User Guide. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi iscriverti a un RSS feed.

Modifica	Descrizione	Data
Ruolo GuardDuty collegato al servizio aggiornato () SLR	GuardDuty ha aggiornato il SLR per includere l'`ec2:Describe:Vpcs` autorizzazione nelle EC2 azioni Amazon. Per ulteriori informazioni, consulta la sezione Autorizzazioni dei ruoli collegati al servizio per. GuardDuty	22 agosto 2024
Significativa aggiunta di contenuti	GuardDuty ha aggiunto importanti aggiornamenti di contenuto alla funzionalità Malware Protection for S3. • Sono stati aggiunti nuovi esempi di schema di notifica di esempio per configurare EventBridge le regole di Amazon per ricevere notifiche relative allo stato delle risorse del piano Malware Protection e ai risultati della scansione degli oggetti S3. Per ulteriori informazioni, consulta Monitoraggio delle scansioni di oggetti S3 con Amazon. EventBridge	20 agosto 2024

	• Sono state aggiunte informazioni sulla risoluzione dei problemi relativi agli errori dei tag post-scansione degli oggetti S3.	
Funzionalità aggiornate in GuardDuty Runtime Monitoring - Amazon EC2	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.3.0 per EC2 le risorse Amazon. Per ulteriori informazioni sulle note di rilascio, consulta GuardDuty Security Agent for Amazon EC2.	19 agosto 2024
Funzionalità aggiornate in GuardDuty Runtime Monitoring - Amazon EKS	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.7.0 per le risorse AmazonEKS. Per ulteriori informazioni sulle note di rilascio, consulta GuardDuty Security Agent for Amazon EKS Clusters.	17 agosto 2024
Significativa aggiunta di contenuti	GuardDuty ha aggiunto nuove informazioni sulla metodologia di rilevamento del malware e sui motori di scansione utilizzati per le funzionalità Malware Protection for S3 e Malware Protection forEC2. Per ulteriori informazioni, consulta il motore di scansione per il rilevamento di GuardDuty malware.	15 agosto 2024

Nuova funzionalità - Protezione dei carichi di lavoro di intelligenza artificiale	GuardDuty il rilevamento delle minacce di base e la protezione Lambda ti aiutano a proteggere e rilevare meglio le minacce ai carichi di lavoro di intelligenza artificiale su cui si basano. AWS Per ulteriori informazioni, consulta Proteggere i carichi di lavoro AI con. GuardDuty	14 agosto 2024
Funzionalità aggiornate in GuardDuty Runtime Monitoring - Fargate (solo AmazonECS)	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.3.0 per le risorse AWS Fargate (ECSsolo Amazon). Per ulteriori informazioni sulle note di rilascio, vedere GuardDuty Security Agent for Fargate-. ECS	9 agosto 2024
Funzionalità aggiornata: protezione da malware per S3	GuardDuty Malware Protection for S3 aumenta la quota del numero massimo di bucket S3 da 10 a 25 bucket. Questa quota si applica a uno per ciascuno. Account AWS Regione AWS Per ulteriori informazioni, consulta Malware Protection for S3.	8 agosto 2024

Aggiornato: nuovi tipi di ricerca in Runtime Monitoring	GuardDuty ha aggiunto due nuovi tipi di ricerca di Runtime Monitoring che consenton o di rilevare le minacce che comportano la creazione di shell sospette sulla risorsa monitorata e l'escalation dei privilegi, quando un processo eleva in modo sospetto i propri privilegi a root. • Execution:Runtime/ SuspiciousShellCreated • PrivilegeEscalation:Runtime/ ElevationToRoot	6 agosto 2024
Aggiornato: integrazione con AWS Security Hub	AWS Security Hub fornisce un elenco di controlli di GuardDuty sicurezza per valutare le risorse e verificar e la conformità rispetto agli standard e alle best practice del settore della sicurezza. Per ulteriori informazioni, vedere Utilizzo GuardDuty dei controlli in Security Hub.	11 luglio 2024

Script GuardDuty tester aggiornato per i risultati	GuardDuty ora supporta oltre 100 risultati con diverse AWS risorse in un account dedicato. Utilizza l'`amazon-guardduty-tester` archivio e segui i passaggi per testare i risultati ed esaminarli per comprenderne i dettagli. Per ulteriori informazioni, consulta GuardDuty Risultati dei test in account dedicati.	28 giugno 2024
Funzionalità aggiornata in Runtime Monitoring	Runtime Monitoring ha rilasciato una nuova versione del security agent 1.2.0 per la EC2 risorsa Amazon. Per informazioni sulle note di rilascio, consulta GuardDuty Security Agent for Amazon EC2 Instance. Per informazioni sull'aggiornamento manuale del security agent a questa versione di rilascio, consulta Managing security agent manual for Amazon EC2 instance.	13 giugno 2024

Nuova funzionalità: protezione da malware per la disponibilità nella regione S3	GuardDuty La protezione da malware per S3 è ora disponibile in tutte le regioni commerciali in cui GuardDuty è disponibile. Questa funzionalità ti aiuta a scansionare gli oggetti appena caricati nei bucket Amazon S3 alla ricerca di potenziali malware e caricamenti sospetti e ad agire per isolarli prima che vengano inseriti nei processi downstream. Per informazioni sull'attivazione di Malware Protection for S3, consulta Malware Protection for S3. GuardDuty	12 giugno 2024

Nuova funzionalità: protezione da malware per S3	GuardDuty annuncia la disponibilità generale di Malware Protection for S3 che ti aiuta a scansionare gli oggetti appena caricati nei bucket Amazon S3 alla ricerca di potenziali malware e caricamenti sospetti e ad agire per isolarli prima che vengano inseriti nei processi downstream. Questa funzionalità è completamente gestita da. AWS GuardDuty pubblica il risultato della scansione degli oggetti S3 sul bus eventi EventBridge predefinito. Puoi consentire di aggiungere tag GuardDuty agli oggetti S3 scansionati. È possibile creare flussi di lavoro a valle, come l'isolamento in un bucket di quarantena, o definire politiche relative ai bucket utilizzando tag che impediscono agli utenti o alle applicazioni di accedere a determinati oggetti. Per ulteriori informazioni, consulta GuardDuty Malware Protection for S3. Attualmente è disponibile nelle seguenti regioni: • Stati Uniti orientali (Virginia settentrionale) • Stati Uniti orientali (Ohio) • US West (Oregon) • Europa (Irlanda)	11 giugno 2024

	• Europa (Francoforte) • Europa (Stoccolma) • Asia Pacifico (Sydney) • Asia Pacifico (Tokyo) • Asia Pacifico (Singapore)	
Politica aggiornata AmazonGuardDutyFullAccess	È stata aggiunta l'autorizzazione che consente di assegnare un IAM ruolo GuardDuty all'attivazione di Malware Protection for S3. Per ulteriori informazioni su questo aggiornamento delle politiche, consulta GuardDuty Aggiornamenti alle politiche AWS gestite.	10 giugno 2024
Funzionalità aggiornate in Protection GuardDuty RDS	RDSLa protezione estende il supporto per monitorare l'attività di accesso sui database RDS di Postgre. SQL Come parte di questa espansione, GuardDuty inizierà automaticamente a monitorare i dati di accesso dai SQL database Postgre RDS per gli account che hanno già abilitato Protection. GuardDuty RDS Per ulteriori informazioni, consulta RDS Protezione.	6 giugno 2024

Funzionalità aggiornate in GuardDuty Runtime Monitoring - Fargate (solo AmazonECS)	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.2.0 per le risorse AWS Fargate (ECSsolo Amazon). Per ulteriori informazioni sulle note di rilascio, vedere GuardDuty Security Agent for Fargate-. ECS	31 maggio 2024
Funzionalità aggiornata in GuardDuty Malware Protection per EC2	Per ogni EBS volume Amazon collegato alle EC2 istanze Amazon e ai carichi di lavoro dei container, GuardDuty Malware Protection for EC2 ha aumentato le dimensioni del EBS volume da scansionare fino a 2048 GB. Per informazioni sulla scansione EBS dei volumi Amazon collegati alle tue istanze, consulta GuardDuty Malware Protection for EC2.	29 maggio 2024
Funzionalità aggiornata in Runtime Monitoring	Le risorse di Runtime Monitoring for Amazon ECS -Fargate ora supportano il rilevamento di potenziali minacce sulle attività avviate da e. AWS Batch AWS CodePipeline Per ulteriori informazioni, consulta Come funziona il monitoraggio del runtime con Fargate (ECSsolo Amazon).	28 maggio 2024

Funzionalità aggiornata in Runtime Monitoring	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.6.1 per le risorse AmazonEKS. Per informazioni sulle note di rilascio, consulta la cronologia dei rilasci dell'agente EKS aggiuntivo.	14 maggio 2024
Supporto regionale esteso per il monitoraggio del runtime	GuardDuty estende il supporto per Runtime Monitoring alla regione Canada occidentale (Calgary). Per informazioni su come iniziare a usare Runtime Monitoring, consulta Enabling Runtime Monitoring.	7 maggio 2024
Supporto regionale esteso per la protezione RDS	GuardDuty estende il supporto di RDS Protection a quanto segue: Regioni AWS • Canada occidentale (Calgary) • Asia Pacific (Hyderabad) • Europa (Spagna) • Europa (Zurigo) • Medio Oriente () UAE • Israele (Tel Aviv) • Asia Pacifico (Melbourne) Per informazioni sull'atti vazione di questa funzionalità, consulta RDSProtezione.	3 maggio 2024

Funzionalità aggiornata in Runtime Monitoring	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.1.0 per le risorse AWS Fargate (ECSsolo Amazon). Per ulteriori informazioni sulle note di rilascio, vedere GuardDuty Security Agent for Fargate-. ECS	1 maggio 2024
Funzionalità aggiornata in Runtime Monitoring	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.6.0 per le risorse AmazonEKS. Per informazioni sulle note di rilascio, consulta la cronologia dei rilasci dell'agente EKS aggiuntivo.	29 aprile 2024
Support per IPAddressv6	GuardDuty ha aggiunto IPAddressv6 il supporto per i dettagli IP locali e remoti. È possibile utilizzare gli attributi Filter associati per filtrare GuardDuty i risultati o creare regole di soppressione.	18 aprile 2024
Esperienza console aggiornata per configurare l'esportazione dei risultati	GuardDuty ha aggiornato l'esperienza della console per esportare i risultati generati nel tuo Account AWS bucket Amazon S3. Per ulteriori informazioni, consulta Esportazione GuardDuty dei risultati.	1 aprile 2024

Funzionalità aggiornata in Runtime Monitoring	Runtime Monitoring ha rilasciato una nuova versione del security agent 1.1.0 per la EC2 risorsa Amazon. Questa versione supporta la configurazione GuardDuty automatica degli agenti in Runtime Monitoring per EC2 le istanze Amazon. Per informazioni sulle note di rilascio, consulta GuardDuty Security Agent for Amazon EC2 Instance.	28 marzo 2024

Disponibilità generale del Runtime Monitoring per le EC2 istanze Amazon	GuardDuty annuncia la disponibilità generale (GA) di Runtime Monitoring per le EC2 istanze Amazon. Ora hai la possibilità di abilitare la configurazione automatica dell'agente che consente GuardDuty di installare e gestire l'agente di sicurezza per le tue EC2 istanze Amazon per tuo conto. Con l'agente GuardDuty automatizzato, puoi anche utilizzare i tag di inclusione o esclusione e GuardDuty per informare sull'installazione e sulla gestione del security agent solo su EC2 istanze Amazon selezionate. Per ulteriori informazioni, consulta Come funziona il monitoraggio del runtime con EC2 le istanze Amazon. Elenco dei nuovi tipi di ricerca rilasciati insieme a questo GA • Esecuzione: Runtime/SuspiciousTool • Esecuzione: Runtime/SuspiciousCommand • DefenseEvasionEsecuzione: Runtime/ ----sep----:runtime/SuspiciousCommand	28 marzo 2024

- DefenseEvasion:Runtime/ ----Sep----:Runtime/PtraceAntiDebugging
- Esecuzione: Runtime/MaliciousFileExecuted

Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi () SLR	Usa AWS Systems Manager le azioni per gestire SSM le associazioni sulle EC2 istanze Amazon quando abiliti il monitoraggio del GuardDuty runtime con agente automatizzato per AmazonEC2. Quando la configurazione GuardDuty automatica degli agenti è disabilitata, GuardDuty considera solo le EC2 istanze che hanno un tag di inclusione (`GuardDuty Managed :true`). • L'elenco seguente mostra le nuove autorizzazioni: `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	26 marzo 2024

Funzionalità aggiornata in Runtime Monitoring	Con l'ultima versione GuardDuty di Security Agent (add-on) v1.5.0 per AmazonEKS, Runtime Monitoring ora supporta la configurazione di parametri specifici del tuo GuardDuty security agent, come impostazi oni di memoria, impostazi oni CPU e impostazioni dei `PriorityClass` criteri. DNS Per ulteriori informazi oni, consulta Configurazione dei parametri del GuardDuty security agent (componente aggiuntivo). EKS	7 marzo 2024
Funzionalità aggiornata in Runtime Monitoring	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.5.0 per EKS le risorse Amazon. Per informazioni sulle note di rilascio, consulta la cronologi a dei rilasci dell'agente EKS aggiuntivo.	7 marzo 2024
Supporto per Canada West (Calgary)	Amazon GuardDuty è ora disponibile nella regione Canada occidentale (Calgary) . Alcuni dei piani di protezion e inclusi GuardDuty potrebber o non essere disponibili in questa regione. Per le informazioni più recenti, consulta Regioni ed endpoint.	6 marzo 2024

Funzionalità aggiornata in Runtime Monitoring	Le versioni del GuardDuty Security Agent 1.0.0 e 1.1.0 per EKS i cluster Amazon non saranno più supportate a partire dal 14 maggio 2024. Per informazioni sui passaggi da eseguire prima della fine del supporto standard, consulta GuardDuty Security Agent for Amazon EKS Clusters.	16 febbraio 2024
Funzionalità aggiornata in Runtime Monitoring	Runtime Monitoring supporta l'ultima versione di Kubernetes 1.29 con la versione 1.4.1 del Security Agent esistente . Il supporto è disponibile dal lancio di questa versione di Kubernetes. Per informazioni sulle versioni di Kubernetes supportate, consulta Versioni di Kubernetes supportate dal security agent. GuardDuty	16 febbraio 2024

Funzionalità aggiornata in Runtime Monitoring - Disponibilità regionale	GuardDuty Il Runtime Monitoring ora supporta Amazon condiviso VPC all'interno dello stesso AWS Organizations. GuardDuty service-linked role (SLR) ha una nuova autorizzazione, `organizations:DescribeOrganization` che aiuta a recuperare l'ID dell'organizzazione per l'VPCaccount Amazon condiviso per impostare la policy degli endpoint. Per informazioni sui prerequisiti per l'utilizzo di un VPC endpoint Amazon condiviso in Runtime Monitoring, consulta Support for shared Amazon. VPC Questa funzionalità è disponibile in tutte le regioni in cui GuardDuty supporta il monitoraggio del runtime.	12 febbraio 2024

Funzionalità aggiornata in Runtime Monitoring - Disponibilità regionale	GuardDuty Il Runtime Monitoring ora supporta Amazon condiviso VPC all'interno dello stesso AWS Organizations. GuardDuty service-linked role (SLR) ha una nuova autorizzazione, `organizations:DescribeOrganization` che aiuta a recuperare l'ID dell'organizzazione per l'VPCaccount Amazon condiviso per impostare la policy degli endpoint. Per informazioni sui prerequisiti per l'utilizzo di un VPC endpoint Amazon condiviso in Runtime Monitoring, consulta Support for shared Amazon. VPC Attualmente, questa funzionalità è disponibile in alcuni dei. Regioni AWS Per ulteriori informazioni, consulta Regioni ed endpoint.	9 febbraio 2024
Funzionalità aggiornata con supporto per la nuova versione Regioni AWS : Malware Protection for EC2	Malware Protection per EC2 ora supporta la scansione EBS dei volumi crittografati con Chiavi gestite da AWS nella regione Stati Uniti occidentali (Oregon).	6 febbraio 2024

Funzionalità aggiornata con supporto per la nuova versione Regioni AWS : Malware Protection for EC2	Malware Protection per EC2 ora supporta la scansione EBS dei volumi crittografati con Chiavi gestite da AWS nei seguenti modi Regioni AWS: • Asia Pacifico (Singapore) (`ap-southeast-1`) • Europa (Francoforte) (`eu-central-1`) • Asia Pacifico (Osaka-Locale) (`ap-northeast-3`) • Stati Uniti orientali (Ohio) (`us-east-2`) • Europa (Milano) (`eu-south-1`) • Asia Pacifico (Tokyo) (`ap-northeast-1`) • Asia Pacifico (Seoul) (`ap-northeast-2`) • Canada (Centrale) (`ca-central-1`) • Europa (Irlanda) (`eu-west-1`) • Stati Uniti orientali (Virginia settentrionale) (`us-east-1`)	5 febbraio 2024

Funzionalità aggiornata in Runtime Monitoring	GuardDuty Runtime Monitoring ha rilasciato una nuova versione del GuardDuty security agent (v1.0.2) per le istanze AmazonEC2. Questa versione per agenti include il supporto per la versione più recente di Amazon ECSAMIs. Per ulteriori informazioni sulla cronologia dei rilasci degli agenti, consulta GuardDuty Security Agent for Amazon EC2 Instances.	2 febbraio 2024

Funzionalità aggiornata con supporto per la nuova versione Regioni AWS : Malware Protection for EC2	Malware Protection per EC2 ora supporta la scansione EBS dei volumi Amazon Chiavi gestite da AWS crittografati con Regioni AWS: • Europa (Londra) (`eu-west-2`) • Europa (Stoccolma) (`eu-north-1`) • Asia Pacifico (Hong Kong) (`ap-east-1`) • Africa (Città del Capo) (`af-south-1`) • Medio Oriente (Bahrein) (`me-south-1`) • Asia Pacifico (Hyderabad) (`ap-south-2`) • Europa (Spagna) (`eu-south-2`) • Asia Pacifico (Melbourne) (`ap-southeast-4`) • Asia Pacifico (Sydney) (`ap-southeast-2`) • Israele (Tel Aviv) (`il-central-1`)	31 gennaio 2024

Aggiornamento: Gestione degli account con AWS Organizations	È stato riorganizzato il contenuto in Gestione degli account con AWS Organizations. , ha aggiunto la procedura per modificare l'account GuardDuty amministratore delegato e aggiornato Comprensione della relazione tra account GuardDuty amministratore e account membro.	30 gennaio 2024
Funzionalità aggiornata con supporto per nuove Regioni AWS	Malware Protection per EC2 ora supporta la scansione EBS dei volumi crittografati con Chiavi gestite da AWS nei seguenti modi Regioni AWS: • Asia Pacifico (Giacarta) (`ap-southeast-3`) • Stati Uniti occidentali (California settentrionale) (`us-west-1`) • Medio Oriente (UAE) (`me-central-1`) • Europa (Zurigo) (`eu-central-2`) • Asia Pacifico (Mumbai) (`ap-south-1`) • Sud America (San Paolo) (`sa-east-1`)	29 gennaio 2024

Funzionalità aggiornata in Malware Protection per EC2	Malware Protection per EC2 ora supporta la scansione EBS dei volumi crittografati utilizzando Chiavi gestite da AWS. Malware Protection for EC2 service-linked role (SLR) dispone di due nuove autorizzazioni: e. `GetSnapshotBlock` `ListSnapshotBlocks` Queste autorizzazioni consentiranno di GuardDuty recuperare l'istantanea di un EBS volume (con crittografia Chiave gestita da AWS) dall'utente Account AWS e copiarla sull'account del GuardDuty servizio prima di avviare la scansione antimalware. Attualmente, questa funzionalità è disponibile solo in Europa (Parigi) (). `eu-west-3` Per ulteriori informazioni, vedere Volumi supportati per la scansione antimalware.	25 gennaio 2024

Funzionalità aggiornata in Runtime Monitoring	GuardDuty Runtime Monitoring ha rilasciato una nuova versione del GuardDuty Security Agent (v1.0.1) con ottimizzazione e miglioramenti generali delle prestazioni. Per ulteriori informazioni sulla cronologia dei rilasci degli agenti, consulta GuardDuty Security Agent for Amazon EC2 Instances.	23 gennaio 2024
Funzionalità aggiornate in Runtime Monitoring	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.4.1 per EKS le risorse Amazon. Per ulteriori informazioni, consulta la cronologia dei rilasci dell'agente EKS aggiuntivo.	16 gennaio 2024
Runtime Monitoring ha rilasciato il nuovo agente v1.4.0 per le risorse Amazon EKS	Runtime Monitoring ha rilasciato una nuova versione dell'agente 1.4.0 per EKS le risorse Amazon. Per ulteriori informazioni, consulta la cronologia dei rilasci dell'agente EKS aggiuntivo.	21 dicembre 2023

Sono stati aggiunti tipi di risultati basati su S3 e AWS CloudTrail machine learning (ML) in Europa (Zurigo), Europa (Spagna), Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne) e Israele (Tel Aviv)	Il seguente S3 e CloudTrail i risultati che identificano il comportamento anomalo utilizzando il modello GuardDuty di machine learning (ML) di rilevamento delle anomalie sono ora disponibili nelle regioni di Europa (Zurigo), Europa (Spagna), Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne) e Israele (Tel Aviv): • 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	21 dicembre 2023

	• Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty supporta 50.000 account membri tramite AWS Organizations	Un GuardDuty amministratore delegato può ora gestire un massimo di 50.000 account membri tramite. AWS Organizations Ciò include anche un massimo di 5000 account membri associati all'account GuardDuty amministratore tramite invito.	20 dicembre 2023
GuardDuty Il supporto per il monitoraggio del runtime è stato esteso a 19 Regioni AWS	Runtime Monitoring è ora disponibile in Asia Pacifico (Giacarta), Europa (Parigi), Asia Pacifico (Osaka), Asia Pacifico (Seoul), Medio Oriente (Bahrain), Europa (Spagna), Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne), Israele (Tel Aviv), Stati Uniti occidentali (California settentrionale), Europa (Londra), Asia Pacifico (Hong Kong), Europa (Milano), Medio Oriente (UAE), Sud America (San Paolo), Asia Pacifico (Mumbai), Canada (Centrale), Africa (Città del Capo), Europa (Zurigo).	6 dicembre 2023

GuardDuty espande la funzionalità di monitoraggio del runtime	Oltre a rilevare le minacce ai tuoi EKS cluster Amazon, GuardDuty annuncia la disponibilità generale di Runtime Monitoring per rilevare le minacce ai tuoi ECS carichi di lavoro Amazon e una versione di anteprima per rilevare le minacce alle tue istanze Amazon. EC2 Per ulteriori informazioni su quali Regioni AWS attualmente supportano il Runtime Monitoring, consulta Regioni ed endpoint.	26 novembre 2023

Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi () SLR	GuardDuty ha aggiunto nuove autorizzazioni per utilizzare ECS le azioni Amazon per gestire e recuperare informazioni sui ECS cluster Amazon e gestire le impostazioni dell'ECSaccount Amazon con. `guarddutyActivate` Le azioni relative ad Amazon recuperano ECS anche le informazioni sui tag associati a. GuardDuty • Le seguenti autorizzazioni sono state aggiunte come parte dell' GuardDuty espansione della funzionalità di Runtime Monitoring: `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	26 novembre 2023
Sono state aggiornate le politiche AWS gestite	GuardDuty ha aggiunto una nuova autorizzazione, `organizations:ListAccounts` alla AmazonGuardDutyFullAccessPolicyfine AmazonGuardDutyReadOnlyAccess.	16 novembre 2023

GuardDuty ha rilasciato nuovi tipi di risultati che utilizzano EKS Audit Log Monitoring.	EKSAudit Log Monitoring ora supporta i seguenti tipi di ricerca in Asia Pacifico (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 novembre 2023

GuardDuty ha rilasciato nuovi tipi di risultati che utilizzano EKS Audit Log Monitoring.	EKSAudit Log Monitoring ora supporta i seguenti tipi di ricerca nelle regioni Asia Pacifico (Hyderabad) (`ap-south-2`), Europa (Zurigo) (`eu-central-2`) ed Europa (Spagna) (`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 novembre 2023

- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

GuardDuty sono stati rilasciati nuovi tipi di risultati che utilizzano EKS Audit Log Monitoring.	EKSAudit Log Monitoring ora supporta i seguenti tipi di risultati. Questi tipi di risultati non sono ancora disponibili nelle regioni Asia Pacifico (Hyderabad`ap-south-2`) (), Europa (Zurigo) (`eu-central-2`), Europa (Spagna) (`eu-south-2`) e Asia Pacifico (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	8 novembre 2023

	• PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
EKSRuntime Monitoring ha rilasciato il nuovo agente v1.3.1	EKSRuntime Monitoring ha rilasciato una nuova versione 1.3.1 dell'agente che include importanti patch e aggiornamenti di sicurezza.	23 ottobre 2023
Nuovo attributo del filtro per gli esiti	GuardDuty ha aggiunto nuovi criteri per filtrare i risultati generati. DNSrequest domain suffix fornisce il dominio di secondo e primo livello coinvolto nell'attività che ha richiesto la generazione del GuardDuty risultato.	17 ottobre 2023
EKSRuntime Monitoring ha rilasciato il nuovo agente v1.3.0 che supporta la versione 1.28 di Kubernetes	EKSRuntime Monitoring ha rilasciato una nuova versione dell'agente 1.3.0 che supporta la versione 1.28 di Kubernetes. È stato aggiunto il supporto per Ubuntu. Per ulteriori informazioni, consulta EKS la cronologia dei rilasci dell'agente aggiuntivo.	5 ottobre 2023

Aggiunti tipi di risultati basati su S3 e AWS CloudTrail machine learning (ML) alle regioni Asia Pacifico (Giacarta) e Medio Oriente () UAE	I seguenti dati S3 e CloudTrail i risultati che identificano il comportamento anomalo utilizzando il modello GuardDuty di machine learning per il rilevamento delle anomalie (ML) sono ora disponibili nelle regioni di Asia Pacifico (Giacarta) e Medio Oriente (): 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	20 settembre 2023

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty EKSRuntime Monitoring introduce la gestione GuardDuty degli agenti di sicurezza a livello di cluster	EKSRuntime Monitoring aggiunge il supporto per la gestione del GuardDuty security agent per i singoli EKS cluster per monitorare gli eventi di runtime solo da questi cluster selettivi. EKSRuntime Monitoring estende questa funzionalità con il supporto dei tag.	13 settembre 2023
GuardDuty Malware Protection for EC2 estende il supporto a più persone Regioni AWS	Malware Protection for EC2 è ora disponibile in Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne), Europa (Zurigo) ed Europa (Spagna).	11 settembre 2023

GuardDuty è ora disponibile nella regione di Israele (Tel Aviv)	È stata aggiunta la regione di Israele (Tel Aviv) all'elenco dei paesi Regioni AWS in cui GuardDuty è ora disponibile. I seguenti piani di protezione sono disponibili anche nella regione Israele (Tel Aviv): • EKSProtezioneinclude sia EKS Audit Log Monitoring che EKS Runtime Monitoring. • Protezione Lambda. • Protezione da malware per EC2. • Protezione S3. Per ulteriori informazioni sulla disponibilità del piano di protezione nella regione Israele (Tel Aviv), consulta Regioni ed endpoint.	24 agosto 2023
GuardDuty aggiunta della configurazione di attivazione automatica per l'organizzazione a livello di piano di protezione	Aggiorna la configurazione dell'organizzazione per i piani di protezione nella tua regione. Le opzioni di configurazione possibili sono: abilitazione per tutti gli account, abilitazione automatica per i nuovi account o abilitazione automatica disattivata per tutti gli account dell'organizzazione.	16 agosto 2023

I tipi di ricerca S3 che identificano comportamenti anomali utilizzando il modello GuardDuty di machine learning (ML) per il rilevamento delle anomalie sono ora disponibili in Asia Pacifico (Osaka)	I seguenti tipi di esiti sono ora disponibili nella regione Asia Pacifico (Osaka-Locale): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	10 agosto 2023
EKSII monitoraggio del runtime è ora disponibile in Asia Pacifico (Melbourne)	EKSII monitoraggio del runtime all'interno di GuardDuty EKS Protection fornisce il rilevamento delle minacce in fase di esecuzione per EKS i cluster Amazon nell' AWS ambiente. Ora è disponibile nella regione Asia Pacifico (Melbourne).	8 agosto 2023
È stato aggiornato l'elenco dei GuardDuty risultati che richiamano la scansione antimalware GuardDuty avviata	Alcuni tipi di risultati EKS di Runtime Monitoring ora possono richiamare la scansione GuardDuty antimalware avviata nel tuo. Account AWS	19 luglio 2023

GuardDuty supporta 10.000 account membri tramite AWS Organizations	Un account GuardDuty amministratore può ora gestire un massimo di 10.000 account membri tramite AWS Organizations. Ciò include anche un massimo di 5000 account membri associati all'account GuardDuty amministratore su invito.	29 giugno 2023
EKSRuntime Monitoring annuncia tre nuovi tipi di risultati.	EKSRuntime Monitorin g supporta tre nuovi tipi di risultati basati sulla tecnica di iniezione del processo. I nuovi tipi di ricerca sono:Runtime/ DefenseEv asion .Proc ,:Runtime/ ProcessInjection .Ptrace e:Runtime/. DefenseEvasion ProcessInjection DefenseEv asion ProcessInjection VirtualMemoryWrite.	22 giugno 2023
EKSRuntime Monitoring ha rilasciato il nuovo agente v1.2.0 che supporta la versione 1.27 di Kubernetes	EKSRuntime Monitoring ha rilasciato una nuova versione dell'agente 1.2.0 che supporta anche le istanze basate. ARM64 È stato aggiunto il supporto per Bottleroc ket. Per ulteriori informazi oni, consulta la cronologia dei rilasci dell'agente EKS aggiuntivo.	16 giugno 2023

GuardDuty la console fornisce una visualizzazione riepilogativa dei risultati.	La dashboard di riepilogo nella GuardDuty console fornisce una visualizzazione aggregata dei GuardDuty risultati. Attualmente, la dashboard mostra i dati tramite vari widget per gli ultimi 10.000 risultati generati per il tuo account (o per gli account membro se sei un account GuardDuty amministratore) per la regione corrente.	12 giugno 2023
EKSAudit Log Monitoring è ora disponibile in Asia Pacifico (Hyderabad), Asia Pacifico (Melbourne), Europa (Zurigo) ed Europa (Spagna)	Abilita EKS Audit Log Monitoring (in EKS Protectio n) per i tuoi account per monitorare i log di EKS controllo dei tuoi EKS cluster Amazon e analizzarli alla ricerca di attività potenzial mente dannose e sospette.	1 giugno 2023
EKSAudit Log Monitoring è ora disponibile in Medio Oriente () UAE	EKSAudit Log Monitoring è ora disponibile in Medio Oriente (UAE). Abilita EKS Audit Log Monitoring per i tuoi account per monitorare i log di EKS controllo dei tuoi EKS cluster Amazon e analizzarli alla ricerca di attività potenzial mente dannose e sospette.	3 maggio 2023

GuardDuty Malware Protection for EC2 annuncia una scansione antimalware su richiesta	Malware Protection for ti EC2 aiuta a rilevare la potenzial e presenza di malware nei EBS volumi Amazon collegati alle EC2 istanze Amazon e ai carichi di lavoro dei container . Ora offre due tipi di scansioni : GuardDuty avviate e su richiesta. GuardDuty-initiated malware scan avvia automatic amente una scansione senza agente nei EBS volumi Amazon solo quando GuardDuty genera uno dei Findings che richiamano la scansione antimalware avviata. GuardDuty Puoi avviare una scansione antimalware On-demand per EC2 le istanze Amazon nel tuo account fornendo l'Amazon Resource Name (ARN) associato a quell'istanza Amazon. EC2 Per ulteriori informazioni sulle differenz e tra i due tipi di scansione, consulta Malware Protection for. EC2 • GuardDuty-scansione antimalware avviata • Scansione antimalware on demand	27 aprile 2023

GuardDuty annuncia Lambda Protection	La Protezione Lambda è utile per identificare potenziali minacce alla sicurezza nelle tue funzioni AWS Lambda . • Tipi di esiti della Protezione Lambda • Correzione di una funzione Lambda potenzialmente compromessa	20 aprile 2023
GuardDuty è ora disponibile nella regione Asia Pacifico (Melbourne)	È stata aggiunta l'area Asia Pacifico (Melbourne) all'elenco delle aree Regioni AWS in cui GuardDuty è disponibile. Per informazioni sulle funzionalità disponibili in questa regione, consulta Regioni ed endpoint.	19 aprile 2023
GuardDuty sono stati aggiunti 3 nuovi tipi di EC2 risultati	GuardDuty introduce nuovi tipi di ricerca per rilevare l'uso di DNS resolver esterni e tecnologie crittografate. DNS Per informazioni su Regioni AWS dove sono supportati questi tipi di ricerca, consulta Regioni ed endpoint. • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	5 aprile 2023

GuardDuty annuncia EKS Runtime Monitoring in Protection EKS	EKSIl monitoraggio del runtime all'interno di EKS Protection fornisce il rilevamento delle minacce in fase di esecuzione per EKS i cluster Amazon nell' AWS ambiente. Utilizza un agente EKS aggiuntivo Amazon (`aws-guardduty-agent`) che raccoglie gli eventi Runtime dai tuoi EKS carichi di lavoro. Dopo aver GuardDuty ricevuto questi eventi di runtime, li monitora e li analizza per identificare potenziali minacce sospette alla sicurezza. Per ulteriori informazioni, consulta Finding details e EKSRuntime Monitoring: tipi di risultati.	30 marzo 2023

GuardDuty aggiunge una nuova funzionalità: `autoEnableOrganizationMembers`	Amazon GuardDuty aggiunge una nuova opzione di configurazione dell'organizzazione che aiuta a controllare e applicare gli account degli GuardDuty amministratori (se necessario) GuardDuty abilitata per `ALL` i membri dell'organizzazione. La best practice consiste ora nell'utilizzare `autoEnableOrganizationMembers` invece di `autoEnable` . L'opzione `autoEnable` è obsoleta, ma è ancora supportata. Quanto segue è APIs interessato da questa nuova funzionalità: • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	23 marzo 2023

La funzionalità di RDS protezione in Amazon GuardDuty è ora disponibile a livello generale	GuardDuty RDSLa protezione monitora e profila l'attività di RDS accesso per identificare comportamenti di accesso sospetti sulle istanze di database Amazon Aurora. Per informazioni su quale tipo di RDS protezione Regioni AWS supporta, consulta Regioni ed endpoint.	16 marzo 2023
GuardDuty annuncia l'attivazione della funzionalità	In passato, la configurazione GuardDuty API consentiva sia delle funzionalità che delle fonti di dati, ma ora tutti i nuovi tipi di GuardDuty protezione verranno configurati come funzionalità e non come fonti di dati. GuardDuty supporta ancora le fonti di dati via API ma non ne aggiungerà una nuovaAPI. L'attivazione delle funzionalità influisce sul comportamento dell'utente APIs che abilita GuardDuty o su un tipo di protezione interno GuardDuty. Se gestisci i tuoi GuardDuty account tramite APISDK, o CFN modello, vedi le GuardDuty APImodifiche a marzo 2023.	16 marzo 2023

GuardDuty La protezione da malware per EC2 è ora disponibile nella regione Medio Oriente (UAE)	La EC2 funzionalità Malware Protection for in GuardDuty è supportata nella regione Medio Oriente (UAE). Per ulteriori informazioni, consulta Regioni ed endpoint.	13 marzo 2023
Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi () SLR	GuardDuty ha aggiunto le seguenti nuove autorizzazioni per supportare la prossima funzionalità di monitoraggio del GuardDuty EKS runtime. • Usa EKS le azioni di Amazon per gestire e recuperare informazioni sui EKS cluster e gestire i EKS componenti aggiuntiv i sui cluster. EKS Le EKS azioni recuperano anche le informazioni sui tag associati a. GuardDuty `"eks:ListClusters", "eks:DescribeClu ster", "ec2:DescribeVpcEndp ointServices", "ec2:DescribeSecurity Groups"`	8 marzo 2023
Amazon GuardDuty ha aggiornato il ruolo collegato ai servizi () SLR	GuardDuty SLRÈ stato aggiornato per consentire la creazione di Malware Protectio n per EC2 SLR dopo l'attivaz ione di Malware Protection forEC2.	21 febbraio 2023

GuardDuty richiede la TLS versione 1.2 o successiva	Per comunicare con AWS le risorse, GuardDuty richiede e supporta la TLS versione 1.2 o successiva. Per ulteriori informazioni, consulta Protezione dei dati e Sicurezza dell'infrastruttura.	14 febbraio 2023
GuardDuty è ora disponibile nella regione Asia Pacifico (Hyderabad)	È stata aggiunta la regione Asia Pacifico (Hyderaba d) all'elenco delle Regioni AWS aree in cui è disponibi le. GuardDuty Per ulteriori informazioni, consulta Regioni ed endpoint.	14 febbraio 2023
Amazon GuardDuty User Guide è in linea con le IAM best practice	Guida aggiornata per allinears i alle IAM migliori pratiche. Per ulteriori informazioni, consulta le migliori pratiche di sicurezza in IAM.	10 febbraio 2023
GuardDuty è ora disponibile nella regione Europa (Spagna)	È stata aggiunta l'Europa (Spagna) all'elenco dei paesi Regioni AWS in cui GuardDuty è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint.	8 febbraio 2023
GuardDuty è ora disponibile nella regione Europa (Zurigo)	È stata aggiunta Europa (Zurigo) all'elenco dei paesi Regioni AWS in cui GuardDuty è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint.	12 dicembre 2022

Versione di anteprima di una nuova funzionalità: GuardDuty RDS Protezione	GuardDuty RDSLa protezion e monitora e profila l'attività di RDS accesso per identific are comportamenti di accesso sospetti sulle istanze di database Amazon Aurora. Attualmente, è disponibile per una versione di anteprima in cinque Regioni AWS. Per ulteriori informazioni, consulta Regioni ed endpoint.	30 novembre 2022
GuardDuty è ora disponibile nella regione Medio Oriente () UAE	È stato aggiunto Medio Oriente (UAE) all'elenco dei paesi Regioni AWS in cui GuardDuty è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint.	6 ottobre 2022

Contenuto aggiunto per una nuova funzionalità: GuardDuty Malware Protection for EC2	GuardDuty Malware Protection for EC2 è un miglioramento opzionale di Amazon. GuardDuty Oltre a GuardDuty identificare le risorse a rischio, Malware Protection for EC2 rileva il malware che potrebbe essere all'origine della compromissione. Con Malware Protection for EC2 abilitata, ogni volta che GuardDuty rileva un comportamento sospetto su un'EC2istanza Amazon o un carico di lavoro di container indicativo di GuardDuty malware, Malware Protection for EC2 avvia una scansione senza agente sui EBS volumi collegati ai carichi di lavoro delle EC2 istanze o dei container interessati per rilevare la presenza di malware. Per informazioni sul EC2 funzionamento di Malware Protection for e sulla configurazione di questa funzionalità, consulta Malware Protection for. GuardDuty EC2 • Per informazioni su Malware Protection for EC2 findings, consulta Finding details. • Per informazioni sulla riparazione dell'EC2istanza compromessa e di un contenitore autonomo,	26 luglio 2022

	consulta Risolvere i problemi di sicurezza rilevati da. GuardDuty • Per informazioni sul controllo dei CloudWatch log per le scansioni antimalware e sui motivi per cui una risorsa viene ignorata durante la scansione antimalware, consulta Understanding Logs and Skip Reasons. CloudWatch • Per informazioni sui rilevamenti di minacce false positive, consulta Segnalazione di falsi positivi in Malware Protection for. GuardDuty EC2	
È stato ritirato un tipo di esito	Exfiltration:S3/ObjectRead.Unusual è stato ritirato.	5 luglio 2022

GuardDutySono stati aggiunti nuovi tipi di ricerca S3 che identificano i comportamenti anomali utilizzando il modello di machine learning (ML) per il rilevamento delle anomalie.	Sono stati aggiunti i nuovi tipi di esiti S3 seguenti. Questi tipi di risultati identificano se una API richiesta ha richiamato un'IAMentità in modo anomalo. Il modello ML valuta tutte le API richieste nell'account e identifica gli eventi anomali associati alle tecniche utilizzat e dagli avversari. Per ulteriori informazioni su ciascuno di questi nuovi esiti, consulta Tipi di esiti S3. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	5 luglio 2022

GuardDuty EKSAggiunto contenuto di protezione per GuardDuty	GuardDuty ora puoi generare risultati per le tue EKS risorse Amazon attravers o il monitoraggio dei log di EKS controllo. Per informazi oni su come configurare questa funzionalità, consulta EKSProtezione in Amazon GuardDuty. Per un elenco dei risultati che è GuardDuty possibile generare per EKS le risorse di Amazon, consulta i risultati di Kubernetes. Sono state aggiunte nuove linee guida sulla correzione di questi esiti nella Guida alla correzion e degli esiti di Kubernetes.	25 gennaio 2022
È stato aggiunto un nuovo esito	È stato aggiunto un nuovo esito UnauthorizedAccess :IAMUser/InstanceCredential Exfiltration.InsideAWS. Questo risultato ti informa quando un account esterno al tuo ambiente accede alle credenziali dell'istanza. AWS AWS	20 gennaio 2022

Sono stati aggiornati i tipi di esiti utili per identificare i problemi relativi a log4j	Amazon GuardDuty ha aggiornato i seguenti tipi di risultati per aiutare a identific are e dare priorità ai problemi relativi a CVE -2021-44228 e CVE -2021-45046: Backdoor: / C & .B; Backdoor: /C & .B! EC2 CActivity EC2 CActivity DNS; Comportamento:/. EC2 NetworkPortUnusual	22 dicembre 2021
Modifiche agli esiti	UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion è stato modificato in UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.OutsideAWS. Questa versione migliorata dell'esit o rileva le posizioni da cui vengono solitamente utilizzate le credenziali, riducendo così gli esiti del traffico instradato attraverso le reti on-premise. UnauthorizedAccess:IAMUser/ InstanceCredentialExfiltrat ion.OutsideAWS	7 settembre 2021
Aggiorna a GuardDuty SLR	GuardDuty SLRÈ stato aggiornato con nuove azioni per migliorare la precisione dei risultati.	3 agosto 2021
Sono state aggiunte informazi oni sull'origine dati per ogni tipo di esito.	Le descrizioni dei risultati ora contengono informazioni sulle fonti di dati GuardDuty utilizzat e per generare tale risultato.	10 maggio 2021

Sono stati ritirati 13 tipi di esiti.	13 risultati sono stati ritirati per essere sostituiti con nuovi AnomalousBehavoir risultati. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissions, Persistence:IAMUser/UserPermissions, PrivilegeEscalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissions, Recon:IAMUser/UserPermissions, ResourceConsumption:IAMUser/ComputeResources, Stealth:IAMUser/LoggingConfigurationModified, Discovery:S3/BucketEnumeration.UnusualImpact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual.	12 marzo 2021

Sono stati aggiunti 8 nuovi tipi di esiti per comportamenti anomali.	Aggiunti 8 nuovi IAMUser tipi di risultati basati sul comportamento anomalo dei presidiIAM. CredentialAccess:IAMUser/AnomalousBehavior,, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior. Persistence:IAMUser/AnomalousBehaviorPrivilegeEscalation:IAMUser/AnomalousBehavior	12 marzo 2021
EC2Aggiunti risultati basati sulla reputazione del dominio.	Sono stati aggiunti 4 nuovi tipi di esiti Impatto basati sulla reputazione del dominio. Impact:EC2/AbusedDomainRequest.Reputation Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. È stata inoltre aggiunta una nuova EC2 scoperta per C&CActivity. Impact:EC2/SuspiciousDomainRequest.Reputation	27 gennaio 2021

Sono stati aggiunti 4 nuovi tipi di esiti.	Aggiunti 3 nuovi aliciousI PCaller risultati S3 M. Discovery:S3/MaliciousIPCaller, Exfiltration:S3/MaliciousIPCaller. Impact:S3/MaliciousIPCaller È stata inoltre aggiunta una nuova EC2 scoperta per C&CActivity. Backdoor:EC2/C&CActivity.B	21 dicembre 2020
È stato ritirato il tipo di esito UnauthorizedAccess:EC2/TorIPCaller.	Il tipo di UnauthorizedAccess :EC2/TorIPCaller ricerca è stato ora GuardDuty ritirato. Ulteriori informazioni.	1 ottobre 2020
È stato aggiunto il tipo di esito Impact:EC2/WinRmBruteForce.	È stato aggiunto un nuovo esito Impatto, ossia Impact:EC2/WinRmBruteForce. Ulteriori informazioni.	17 settembre 2020
È stato aggiunto il tipo di esito Impact:EC2/PortSweep.	È stato aggiunto un nuovo esito Impatto, ossia Impact:EC2/PortSweep. Ulteriori informazioni.	17 settembre 2020
GuardDuty è ora disponibile nelle regioni Africa (Città del Capo) ed Europa (Milano).	Aggiunte Africa (Città del Capo) ed Europa (Milano) all'elenco delle AWS regioni in cui GuardDuty è disponibile. Ulteriori informazioni	31 luglio 2020

Sono stati aggiunti nuovi dettagli di utilizzo per il monitoraggio GuardDuty dei costi.	Ora puoi utilizzare nuove metriche per interrogare i dati sui costi di GuardDuty utilizzo per il tuo account e gli account che gestisci. Una nuova panoramica dei costi di utilizzo è disponibile nella console all'indirizzo https://console.aws.amazon.com/guardduty/. È possibile accedere a informazioni più dettagliate tramiteAPI.	31 luglio 2020
Sono stati aggiunti contenuti riguardanti la protezione di S3 tramite il monitoraggio degli eventi dei dati di S3 in. GuardDuty	GuardDuty S3 Protection è ora disponibile tramite il monitoraggio degli eventi del piano dati S3 come nuova fonte di dati. Questa funzionalità sarà abilitata automaticamente per i nuovi account. Se lo stai già utilizzando, GuardDuty puoi abilitare la nuova fonte di dati per te o per i tuoi account membro.	31 luglio 2020
Sono stati aggiunti 14 nuovi esiti S3.	Sono stati aggiunti 14 nuovi tipi di esiti S3 per le origini del piano di controllo (control-plane) e del piano dati S3.	31 luglio 2020

È stato aggiunto il supporto per gli esiti S3 e sono stati modificati i nomi di 2 tipi di esiti esistenti.	GuardDuty i risultati ora includono maggiori dettagli sui risultati che coinvolgo no i bucket S3. I tipi di esiti esistenti correlati all'attività di S3 sono stati rinominati: Policy:IAMUser/S3BlockPubli cAccessDisabled è stato modificato in Policy:S3/ BucketBlockPublicAccessDis abled e Stealth:IAMUser/S3 ServerAccessLoggingDisabled è stato modificato in Stealth:S 3/ServerAccessLoggingDisabl ed.	28 maggio 2020
Contenuti aggiunti per l'integra zione AWS Organizations .	GuardDuty ora si integra con gli amministratori AWS Organizations delegati per consentirti di gestire gli GuardDuty account all'inter no della tua organizzazione. Quando imposti un amministr atore delegato come account GuardDuty amministratore, puoi abilitare automaticamente la gestione GuardDuty di qualsiasi membro dell'orga nizzazione da parte dell'acco unt amministratore delegato. È inoltre possibile abilitare automaticamente gli account GuardDuty dei nuovi AWS Organizations membri. Ulteriori informazioni.	20 aprile 2020

Sono stati aggiunti contenuti per la funzionalità di esportazione degli esiti.	Contenuto aggiunto che descrive la funzionalità Export Findings di GuardDuty.	14 novembre 2019
È stato aggiunto il tipo di esito UnauthorizedAccess:EC2/MetadataDNSRebind.	È stato aggiunto un nuovo esito Non autorizzato, ossia UnauthorizedAccess:EC2/MetadataDNSRebind. Ulteriori informazioni.	10 ottobre 2019
È stato aggiunto il tipo di esito Stealth:IAMUser/S3ServerAccessLoggingDisabled.	È stato aggiunto un nuovo esito Stealth, ossia Stealth:IAMUser/S3ServerAccessLoggingDisabled. Ulteriori informazioni.	10 ottobre 2019
È stato aggiunto il tipo di esito Policy:IAMUser/S3BlockPublicAccessDisabled.	È stato aggiunto un nuovo esito Policy, ossia Policy:IAMUser/S3BlockPublicAccessDisabled. Ulteriori informazioni.	10 ottobre 2019
È stato ritirato il tipo di esito Backdoor:EC2/XORDDOS.	Il tipo di Backdoor:EC2/XORDDOS risultato è stato ora ritirato da GuardDuty. Scopri di più	12 giugno 2019
È stato aggiunto il tipo di esito PrivilegeEscalation.	Il tipo di esito Privilege Escalation rileva quando gli utenti tentano di assegnare privilegi di escalation più permissivi ai loro account. Ulteriori informazioni	14 maggio 2019

GuardDuty è ora disponibile nella regione Europa (Stoccolma).	È stato aggiunto Europa (Stoccolma) all'elenco delle AWS regioni in cui GuardDuty è disponibile. Ulteriori informazioni	9 maggio 2019
È stato aggiunto un nuovo tipo di esito, ossia Recon:EC2/PortProbeEMRUnprotectedPort.	Questo risultato indica che una porta sensibile EMR correlata su un'EC2istanza non è bloccata e viene esaminata attivamente. Ulteriori informazioni	8 maggio 2019
Sono stati aggiunti 5 nuovi tipi di ricerca che rilevano se le EC2 istanze vengono potenzialmente utilizzate per attacchi Denial of Service (DoS).	Questi risultati forniscono informazioni sull'esistenza di EC2 istanze nell'ambiente che si comportano in un modo che potrebbe indicare che vengono utilizzate per eseguire attacchi Denial of Service (DoS). Ulteriori informazioni	8 marzo 2019
È stato aggiunto un nuovo tipo di esito: Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsagefinding type informa l'utente che le credenziali di accesso dell'utente root Account AWS vengono utilizzate per effettuare richieste programmatiche ai servizi. AWS Ulteriori informazioni	24 gennaio 2019

Il tipo di esito UnauthorizedAccess:IAMUser/UnusualASNCaller è stato ritirato	Il tipo di esito UnauthorizedAccess:IAMUser/UnusualASNCaller è stato ritirato. Ora riceverete una notifica sulle attività richiamate da reti insolite tramite altri tipi di ricerca attivi. GuardDuty Il tipo di ricerca generato si baserà sulla categoria di quelli richiamati da una rete insolita. API Ulteriori informazioni	21 dicembre 2018
Sono stati aggiunti due nuovi tipi di esiti: PenTest:IAMUser/ParrotLinux e PenTest:IAMUser/PentooLinux	PenTest:IAMUser/ParrotLinux finding type informa l'utente che un computer che esegue Parrot Security Linux sta effettuando API chiamate utilizzando le credenziali che appartengono al proprio account. AWS PenTest:IAMUser/PentooLinux finding type ti informa che una macchina su cui è in esecuzione Pentoo Linux sta effettuando API chiamate utilizzando credenziali che appartengono al tuo account. AWS Ulteriori informazioni	21 dicembre 2018

È stato aggiunto il supporto per l'argomento degli GuardDuty annunci SNS di Amazon	Ora puoi iscriverti all'SNSargomento GuardDuty degli annunci per ricevere notifiche sui nuovi tipi di risultati rilasciati, aggiornamenti ai tipi di risultati esistenti e altre modifiche alle funzionalità. Le notifiche sono disponibili in tutti i formati supportati da AmazonSNS. Ulteriori informazioni	21 novembre 2018
Sono stati aggiunti due nuovi tipi di esiti: UnauthorizedAccess:EC2/TorClient e UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClientfinding type ti informa che un'EC2istanza nel tuo AWS ambiente sta effettuando connessioni a un nodo Tor Guard o a un nodo Authority. UnauthorizedAccess:EC2/TorRelayfinding type ti informa che un'EC2istanza nel tuo AWS ambiente sta effettuando connessioni a una rete Tor in un modo che suggerisce che stia agendo come un relè Tor. Ulteriori informazioni	16 novembre 2018
È stato aggiunto un nuovo tipo di esito: CryptoCurrency:EC2/BitcoinTool.B	Questa scoperta ti informa che un'EC2istanza nel tuo AWS ambiente sta interrogando un nome di dominio associato a Bitcoin o ad altre attività legate alle criptovalute. Ulteriori informazioni	9 novembre 2018

È stato aggiunto il supporto per l'aggiornamento della frequenza delle notifiche inviate a Events CloudWatch	Ora puoi aggiornare la frequenza delle notifiche inviate a CloudWatch Events per le successive occorrenz e di risultati esistenti. I valori possibili sono 15 minuti, 1 ora o 6 ore (impostazione predefini ta). Ulteriori informazioni	9 ottobre 2018
È stato aggiunto il supporto per una regione	È stato aggiunto il supporto regionale per AWS GovCloud (Stati Uniti occidentali) Ulteriori informazioni	25 luglio 2018
È stato aggiunto il supporto per in AWS CloudFormation StackSets GuardDuty	Puoi utilizzare il GuardDuty modello Enable Amazon per eseguire l'attivazione GuardDuty simultanea in più account. Ulteriori informazioni	25 giugno 2018
Aggiunto il supporto per le regole di GuardDuty archiviaz ione automatica	I clienti possono ora creare regole di archiviazione automatica granulari per la soppressione dei risultati. I risultati che corrispondono a una regola di archiviazione automatica, li contrassegna GuardDuty automaticamente come archiviati. Ciò consente ai clienti di effettuare ulteriori ottimizzazioni GuardDuty per conservare solo i risultati pertinenti nella tabella dei risultati corrente. Ulteriori informazioni	4 maggio 2018

GuardDuty è disponibile nella regione Europa (Parigi)	GuardDuty è ora disponibile in Europa (Parigi) e consente di estendere il monitoraggio continuo della sicurezza e il rilevamento delle minacce in questa regione. Ulteriori informazioni	29 marzo 2018
AWS CloudFormation È ora supportata la creazione di account GuardDuty amministratore e account membro tramite.	Per ulteriori informazioni, consulta `AWS::GuardDuty::master` e `AWS::GuardDuty::member`.	6 marzo 2018
Sono stati aggiunti nove nuovi rilevamenti di anomalie CloudTrail basati.	Questi nuovi tipi di ricerca vengono abilitati automaticamente GuardDuty in tutte le regioni supportate. Ulteriori informazioni	28 febbraio 2018
Aggiunti tre nuovi tipi di rilevamento intelligente delle minacce (tipi di ricerca).	Questi nuovi tipi di ricerca vengono abilitati automaticamente GuardDuty in tutte le regioni supportate. Ulteriori informazioni	5 febbraio 2018
Aumento del limite per GuardDuty gli account dei membri.	Con questa versione, è possibile aggiungere fino a 1000 account GuardDuty membro per AWS account (account GuardDuty amministratore). Ulteriori informazioni	25 gennaio 2018

Modifiche al caricamento e ulteriore gestione degli elenchi di IP affidabili e degli elenchi di minacce per gli account GuardDuty amministratore e gli account dei membri.	Con questa versione, gli utenti degli GuardDuty account di amministratore possono caricare e gestire elenchi di IP affidabili ed elenchi di minacce. Gli utenti degli GuardDuty account membri non possono caricare e gestire elenchi. Gli elenchi di IP affidabili e gli elenchi di minacce caricati dall'account amministratore sono soggetti a restrizioni di GuardDuty funzionalità negli account dei membri. Ulteriori informazioni	25 gennaio 2018

Aggiornamenti precedenti

Modifica	Descrizione	Data
Pubblicazione iniziale	Pubblicazione iniziale della Amazon GuardDuty User Guide.	28 novembre 2017

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.