AWS での自動化されたセキュリティ対応

AWS 実装ガイド

最終更新日：*2022* 年 *6* 月（改訂）

目次

はじめに

セキュリティ脅威の継続的な進化は、セキュリティチームによる対応を困難なものとし、その対応には費用と時間がかかります。「AWS での自動化されたセキュリティ対応」ソリューションは、業界のコンプライアンス標準とベストプラクティスに基づいて事前定義された応答と修復アクションを提供することにより、これらの脅威に迅速に対応するのに役立ちます。

このソリューションは、AWS Security Hub に自動化されたプレイブックのライブラリを提供するアドオンのソリューションで、すぐにデプロイ可能なアーキテクチャで構成されています。このソリューションにより、AWS Security Hub のユーザーは、一般的なセキュリティの検出結果を解決し、AWS でのセキュリティ体制を改善することが容易になります。

特定のプレイブックを選択して、AWS Security Hub のプライマリアカウントにデプロイできます。各プレイブックには、単一の AWS アカウント内または複数の AWS アカウント間で修復ワークフローを開始するために必要な、カスタムアクション、AWS Identity and Access Management (IAM) ロール、Amazon CloudWatch Events、AWS Systems Manager オートメーションランブック、AWS Lambda 関数、AWS Step Functions が含まれています。修復は AWS Security Hub のアクションメニューから機能し、承認されたユーザーがワンクリックで AWS Security Hub が管理するすべてのアカウントの検出結果を修復できるようにします。例えば、AWS リソースを保護するためのコンプライアンス標準である Center for Internet Security (CIS) AWS Foundations Benchmark の推奨事項を適用して、パスワードの有効期限を 90 日以内にしたり、AWS に保存されたイベントログの暗号化を強制したりすることができます。

> **注意**: 修復は、早急な対処が必要な緊急事態を対象としています。このソリューションでは、AWS Security Hub コンソールから開始された場合にのみ、検出結果を修正するための変更を行います。これらの変更を元に戻すには、リソースを手動で元の状態に戻す必要があります。
>
> AWS CloudFormation スタックの一部としてデプロイされた AWS リソースを修正する場合は、ドリフトが発生する可能性があることに注意してください。可能な場合は、スタックのリソースを定義するコードを変更し、スタックを更新して、スタックのリソースを修正してください。詳細については、 *AWS CloudFormation* ユーザーガイドの「ドリフトとは」を参照してください。

「AWS での自動化されたセキュリティ対応」ソリューションには、「CIS (Center for Internet Security) AWS Foundations Benchmark v1.2.0」、「AWS の基本的なセキュリティのベストプラクティス (AFSBP) v.1.0.0」、「Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1」の一部として定義されているセキュリティ基準のプレイブックによる修復が含まれています。詳細については、「プレイブック」セクションを参照してください。

この実装ガイドでは、アマゾン ウェブ サービス (AWS) クラウドに「AWS での自動化されたセキュリティ対応」ソリューションをデプロイするためのアーキテクチャ上の考慮事項と設定手順について説明します。セキュリティと可用性に関する AWS ベストプラクティスを使用して、このソリューションを AWS にデプロイするために必要な AWS のコンピューティング、ネットワーク、ストレージ、その他さまざまなサービスを起動、設定、実行する AWS CloudFormation テンプレートへのリンクが含まれています。

このガイドは、AWS クラウドにおけるアーキテクチャの設計の実務経験がある IT インフラストラクチャアーキテクト、管理者、DevOps プロフェッショナルを対象としています。

コスト

このソリューションの実行に使用した AWS のサービスのコストは、お客様の負担となります。2022 年 6 月の時点で、米国東部 (バージニア北部) の AWS リージョンでこのソリューションをデフォルト設定で実行するためのコストは、**1 か月あたり 300 回の修復で約 3.33 USD、1 か月あたり 3,000 回の修復で約 26.83 USD、1 か月あたり 30,000 回の修復で約 261.90 USD** です。料金は変更される可能性があります。詳細については、このソリューションで使用される各 AWS サービスの料金表ページを参照してください。

> **注意**: 多くの AWS のサービスには、無料で利用できるサービスの基準額である無料利用枠が含まれています。実際のコストは、提示しているコストの例よりも多い場合と少ない場合があります。

このソリューションを実行するための総コストは、次の要因によって異なります。

- AWS Security Hub のメンバーアカウントの数
- 自動的に呼び出されるアクティブな修復の数
- 修復の頻度

このソリューションでは、次の AWS コンポーネントを使用しており、設定に基づいてコストが発生します。小規模、中規模、大規模の組織向けのコスト例を示します。

AWS のサービス	無料利用枠	料金
AWS Systems Manager Automation - ステップカウント	AWS アカウントごと 1 か月あたり 100,000 ステップ	この無料利用枠を超えると、基本ステップごとに 1 ステップあたり 0.002 USD が課金されます。複数の AWS アカウントで自動化にする場合は、子 AWS アカウントで実行されるステップを含むすべてのステップは、オリジナル の AWS アカウントでのみカウントされます。
AWS Systems Manager Automation - ステップの実行時間	1 か月あたり 5,000 秒	この無料利用枠を超えると、`aws:executeScript` のアクションステップごとに、1 秒あたり 0.00003 USD が課金されます。
AWS Systems Manager Automation - ストレージ	無料利用枠なし	1 GB につき 1 か月あたり 0.046 USD

AWS のサービス	無料利用枠	料金
AWS Systems Manager Automation - データ転送	無料利用枠なし	転送される 1 GB あたり 0.900 USD (クロスアカウントまたは AWS リージョン外の場合)
AWS Security Hub - セキュリティチェック	無料利用枠なし	最初の 100,000 件のチェックに対するコスト (1 つの AWS アカウントごとで 1 つの AWS リージョンにつき 1 か月あたり) は、1 件のチェックにつき 0.0010 USD 次の 400,000 件のチェックに対するコスト (1 つの AWS アカウントごとで 1 つの AWS リージョンにつき 1 か月あたり) は、1 件のチェックにつき 0.0008 USD 500,000 件を超えるチェックに対するコスト (1 つの AWS アカウントごとで 1 つの AWS リージョンにつき 1 か月あたり) は、1 件のチェックにつき 0.0005 USD
AWS Security Hub - 検出結果の取り込みイベント	最初の 10,000 件のイベント (1 つの AWS アカウントごとで 1 つの AWS リージョンにつき 1 か月あたり) は無料。AWS Security Hub のセキュリティに関連する検出結果の取り込みイベントをチェックします。	10,000 件を超えるイベントに対するコスト (1 つの AWS アカウントごとで 1 つの AWS リージョンにつき 1 か月あたり) は、1 件のイベントにつき 0.00003 USD
Amazon CloudWatch - メトリクス	基本モニタリングのメトリクス (5 分間隔) 10 件の詳細モニタリングのメトリクス (1 分間隔) 100 万件の API リクエスト (GetMetricData と GetMetricWidgetImage には適用なし)	最初の 10,000 件のメトリクスのコストは、1 か月あたり 0.30 USD 次の 240,000 件のメトリクスのコストは、1 か月あたり 0.10 USD 次の 75,000 件のメトリクスのコストは、1 か月あたり 0.05 USD 1,000,000 件を超えるメトリクスのコストは、1 か月あたり 0.02 USD
Amazon CloudWatch - ダッシュボード	1 か月あたり最大 50 件のメトリクスに対応して、3 つのダッシュボード	1 か月あたり 1 つのダッシュボードごとに 3.00 USD
Amazon CloudWatch - アラーム	10 件のアラームメトリクス (高解像度のアラームには適用なし)	標準解像度 (60 秒) のコストは、アラームメトリクスごとに 0.10 USD 高解像度 (10 秒) のコストは、アラームメトリクスごとに 0.30 USD 標準解像度の異常検出のコストは、アラームごとに 0.30 ドル 高解像度の異常検出のコストは、アラームごとに 0.90 USD

AWS のサービス	無料利用枠	料金
		組み合わせた場合のコストは、アラームごとに 0.50 USD
Amazon CloudWatch - ログ収集	5 GB のデータ (取り込み、ストレージのアーカイブ、Logs Insights クエリでスキャンされたデータ)	1 GB あたり 0.50 USD
Amazon CloudWatch - ログのストレージ	5 GB のデータ (取り込み、ストレージのアーカイブ、Logs Insights クエリでスキャンされたデータ)	スキャンされたデータの 1 GB あたり 0.005 USD
Amazon CloudWatch - イベント	カスタマイズされたイベントを除く、すべてのイベントが対象	カスタマイズされたイベントで 100 万件のイベントにつき 1.00 USD クロスアカウントのイベントで、100 万件のイベントにつき 1.00 USD
AWS Lambda - リクエスト	1 か月あたり 100 万件の無料リクエスト	100 万件のリクエストあたり 0.20 USD
AWS Lambda - 実行時間	1 か月あたり 400,000 GB / 秒のコンピューティング時間	1 GB / 秒ごとに 0.0000166667 USD 実行時間に対する料金は、関数に割り当てたメモリ量により異なります。関数には、128 MB から 10,240 MB までの任意の量のメモリを 1 MB 単位の増分で割り当てることができます。
AWS Step Functions - 状態遷移	1 か月あたり 4,000 件の無料状態遷移	それ以後は、1,000 件の状態遷移につき 0.025 USD
Amazon EventBridge	AWS のサービスが発行するすべての状態変更イベントは無料	カスタマイズされたイベントで、100 万件の発行されたイベントにつき 1.00 USD サードパーティ製 (SaaS) のイベントで、100 万件の発行されたイベントにつき 1.00 USD クロスアカウントのイベントで、100 万件の送信されたイベントにつき 1.00 USD
Amazon SNS	最初の 100 万件 (1 か月あたり) の Amazon SNS リクエストは無料	それ以後は、100 万件のリクエストにつき 0.50 USD

料金の例 (1 か月あたり)

例 1: 1 か月あたり 300 件の修復

- 10 個の AWS アカウント、1 つの AWS リージョン
- 1 つの AWS アカウント / 1 つの AWS リージョン / 1 か月につき 30 件の修復
- 総コストは、1 か月あたり 3.33 USD

AWS のサービス	前提	月額料金
AWS Systems Manager Automation	ステップ: ~ 4 ステップ * 300 件の修復 * 0.002 USD = 2.40 USD 実行時間: 10 秒 * 300 件の修復 * 0.00003 USD = 0.09 USD	2.49 USD
AWS Security Hub	請求可能なサービスの利用なし	0 USD
Amazon CloudWatch Logs	300 件の修復 * 0.000002 USD = 0.0006 USD 0.0006 USD * 0.03 = 0.000018 USD	< 0.01 USD
AWS Lambda - リクエスト	300 件の修復 * 6 件のリクエスト = 1,800 件のリクエスト 0.20 USD * 1,000,000 件のリクエスト = 0.20 USD	0.20 USD
AWS Lambda - 実行時間	256M: 1.875 GB 秒 * 300 件の修復 * 0.0000167 USD = 0.009375 USD	< 0.01 USD
AWS Step Functions	15 件の状態遷移 * 300 件の修復 = 4,500 0.025 USD * (4,500/1,000) 状態遷移 = 0.1125 USD	< 0.12 USD
Amazon EventBridge のルール	ルールに対する課金なし	0 USD
Amazon SNS	0.50 USD * 1,000,000 件の通知 = 0.50 USD	0.50 USD
	合計	**3.33 USD**

例 2: 1 か月あたり 3,000 件の修復

- 100 個の AWS アカウント、1 つの AWS リージョン
- 1 つの AWS アカウント / 1 つの AWS リージョン / 1 か月につき 30 件の修復
- 総コストは、1 か月あたり 26.75 USD

AWS のサービス	前提	月額料金
AWS Systems Manager Automation	ステップ: ~4 ステップ * 3,000 件の修復 * 0.002 USD = 24.00 USD 実行時間: 10 秒 * 3,000 件の修復 * 0.00003 USD = 0.90 USD	24.90 USD
AWS Security Hub	請求可能なサービスの利用なし	0 USD
Amazon CloudWatch Logs	3,000 件の修復 * 0.000002 USD = 0.006 USD 0.006 USD * 0.03 = 0.00018 USD	< 0.01 USD
AWS Lambda - リクエスト	3,000 件の修復 * 6 件のリクエスト = 18,000 件のリクエスト 0.20 USD * 1,000,000 件のリクエスト = 0.20 USD	0.20 USD
AWS Lambda - 実行時間	256M: 1.875 GB 秒 * 3,000 件の修復 * 0.000167 USD = 0.09375 USD	0.09 USD
AWS Step Functions	15 件の状態遷移 * 3,000 件の修復 = 45,000 0.025 USD * (45,000/1,000) 状態遷移 = 1.125 USD	1.13 USD
Amazon EventBridge のルール	ルールに対する課金なし	0 USD
Amazon SNS	0.50 USD * 1,000,000 件の通知 = 0.50 USD	0.50 USD
	合計	**26.83 USD**

例 3: 1 か月あたり 30,000 件の修復

- 1000 個の AWS アカウント、1 つの AWS リージョン
- 1 つの AWS アカウント / 1 つの AWS リージョン / 1 か月につき 30 件の修復
- 総コストは、1 か月あたり 261.90 USD

AWS のサービス	前提	月額料金
AWS Systems Manager Automation	ステップ: ~ 4 ステップ * 30,000 件の修復 * 0.002 USD = 240.00 USD 実行時間: 10 秒 * 30,000 件の修復 * 0.00003 USD = 9.00 USD	249.00 USD
AWS Security Hub	請求可能なサービスの利用なし	0 USD
Amazon CloudWatch Logs	30,000 件の修復 * 0.000002 USD = 0.06 USD 0.06 USD * 0.03 = 0.0018 USD	< 0.01 USD
AWS Lambda - リクエスト	30,000 件の修復 * 6 件のリクエスト = 180,000 件のリクエスト 0.20 USD * 1,000,000 件のリクエスト = 0.20 USD	0.20 USD
AWS Lambda - 実行時間	256M: 1.875 GB 秒 * 30,000 件の修復 * 0.000167 USD = 0.9375 USD	0.94 USD
AWS Step Functions	15 件の状態遷移 * 30,000 件の修復 = 45,000 0.025 USD * (450,000/1,000) 状態遷移 = 11.25 USD	11.25 USD
Amazon EventBridge のルール	ルールに対する課金なし	0 USD
Amazon SNS	0.50 USD * 1,000,000 件の通知 = 0.50 USD	0.50 USD
	合計	**261.90**

アーキテクチャの概要

このソリューションを**デフォルトのパラメータで**デプロイすると、AWS クラウドに次の環境が構築されます。

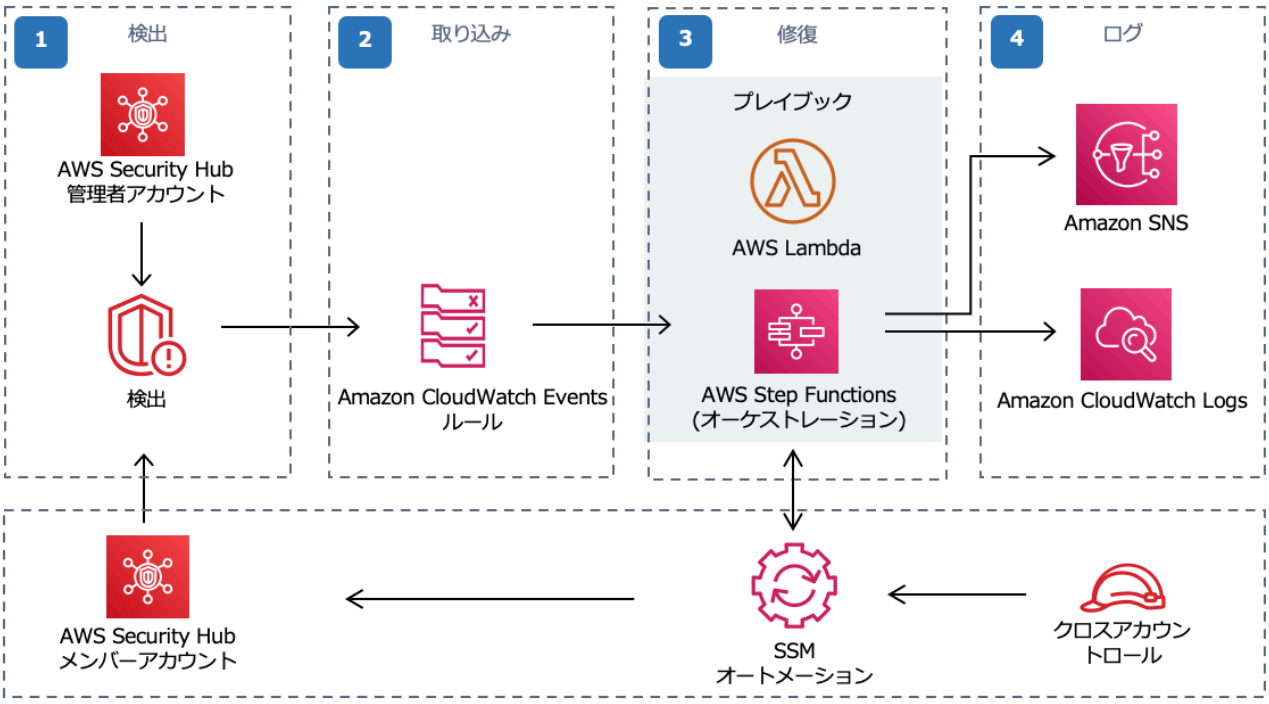


図 *1:* 「*AWS* での自動化されたセキュリティ対応」ソリューションのアーキテクチャ

「AWS での自動化されたセキュリティ対応」ソリューションには、検出、取り込み、修復、ログ、といった主なワークフローが含まれています。

1. 検出

AWS Security Hub は、AWS のセキュリティ状態の包括的なビューを提供します。セキュリティの業界標準とベストプラクティスに照らして環境を測定するのに役立ちます。これは、AWS Config、Amazon GuardDuty、AWS Firewall Manager などの他の AWS のサービスからイベントとデータを収集することで機能します。これらのイベントとデータは、CIS AWS Foundations Benchmark などのセキュリティ基準に照らして分析されます。準拠状況は、

AWS Security Hub コンソールで検出結果として表示されます。新しい検出結果は Amazon CloudWatch Events として送信されます。

2. 取り込み

カスタムアクションを使用して、検出結果に対してイベントを開始できます。これにより、Amazon CloudWatch Events が発生します。

AWS Security Hub のカスタムアクションと Amazon CloudWatch Events ルールは、「AWS での自動化されたセキュリティ対応」ソリューションのプレイブックを開始して、検出結果に対応します。このソリューションでサポートしている各コントロールに対して、2 つの Amazon CloudWatch Events ルールがデプロイされます。1 つはカスタムアクションのイベント (ユーザーが開始した修復) に一致するルール、もう 1 つはリアルタイムの検出イベントに一致するルール (デフォルトでは無効) です。

AWS Security Hub のカスタムアクションメニューを使用して自動修復を開始するか、非本番環境で慎重にテストした後で自動修復を有効にすることができます。これは修復ごとに有効にできます。すべての修復で自動開始を有効にする必要はありません。

3. 修復

クロスアカウントの AWS Identity and Access Management (IAM) ロールを使用して、自動修復では AWS の API を使用し、検出結果の修復に必要なタスクを実行します。このソリューションのすべてのプレイブックでは、AWS Lambda 関数が呼び出されます。一部の AWS Lambda 関数では、修復を直接実行します。その他では、AWS Systems Manager オートメーションランブックを使用して修復を実行します。

4. ログ

プレイブックでは、このソリューションの Amazon CloudWatch Logs グループに結果を記録し、Amazon Simple Notification Service (Amazon SNS) トピックに通知を送信して、AWS Security Hub の検出結果を更新します。実行されたアクションの監査証跡は、検出結果のメモに保持されます。AWS Security Hub のダッシュボードで、検出結果ワークフローのステータスが **NEW** から **NOTIFIED** または **RESOLVED** に変更されます。実行された修復を反映するように、セキュリティに関する検出結果のメモが更新されます。

ソリューションコンポーネント

AWS Security Hub の統合

`aws-sharr-deploy` スタックをデプロイすると、AWS Security Hub のカスタムアクション機能と統合されます。AWS Security Hub コンソールで **Remediate with SHARR** を選択すると、このソリューションでは AWS Step Functions を使用して、修復のために検出結果のレコードをルーティングします。

クロスアカウント権限と AWS Systems Manager のランブックは、`aws-sharr-member.template` と `aws-sharr-member-roles.template` の AWS CloudFormation テンプレートを使用して、すべての AWS Security Hub のアカウント (管理者およびメンバー) にデプロイする必要があります。詳細については、「プレイブック」セクションを参照してください。このテンプレートを使用すると、ターゲットアカウントでの自動修復が可能になります。

ユーザーは、Amazon CloudWatch Events ルールを使用して、修復ごとに自動修復を自動的に開始できます。このオプションは、AWS Security Hub に報告されるとすぐに検出結果の完全自動修復を起動します。自動開始はデフォルトでオフに設定されています。このオプションは、AWS Security Hub の管理者アカウントで Amazon CloudWatch Events ルールをオンにすることで、プレイブックのインストール中またはインストール後にいつでも変更できます。

クロスアカウントの修復

「AWS での自動化されたセキュリティ対応」ソリューションでは、クロスアカウントのロールを使用して、プライマリアカウントとセカンダリアカウント間で動作します。これらのロールは、このソリューションのインストール中にメンバーアカウントにデプロイされます。各修復には個別のロールが割り当てられます。プライマリアカウントの修復プロセスでは、修復が必要なアカウントの修復用のロールを引き受ける権限が付与されます。修復は、修復が必要なアカウントの AWS Systems Manager のランブックによって実行されます。

プレイブック

一連の修復は、プレイブックと呼ばれるパッケージにグループ化されます。プレイブックは、このソリューションのテンプレートを使用してインストール、更新、削除されます。このソリューションでは、現在、次のプレイブックをサポートしています。

- Center for Internet Security (CIS) Amazon Web Services Foundations benchmarks, version 1.2.0 (2018 年 5 月 18 日公開)
- AWS の基本的なセキュリティのベストプラクティス (AFSBP) version 1.0.0 (2021 年 3 月公開)
- Payment Card Industry Data Security Standards (PCI-DSS) version 3.2.1 (2018 年 5 月公開)

統合ログ管理

「AWS での自動化されたセキュリティ対応」ソリューションでは、単一の Amazon CloudWatch Logs グループ (SO0111-SHARR) にログを記録します。これらのログには、このソリューションのトラブルシューティングと管理のために、詳細なログ記録が含まれています。

通知

このソリューションでは、Amazon Simple Notification Service (Amazon SNS) トピックを使用して修復結果を発行します。このトピックのサブスクリプションを使用して、このソリューションの機能を拡張できます。例えば、メール通知を送信したり、トラブルチケットを更新したりできます。

セキュリティ

AWS インフラストラクチャでシステムを構築する場合、セキュリティ上の責任はお客様と AWS の間で共有されます。この責任共有モデルにより、ホストオペレーティングシステムと仮想化レイヤーからサービスが運用されているシステムの物理的なセキュリティに至るまでのコンポーネントについて、AWS が運用、管理、および制御します。そのため、お客様の運用上の負担を軽減するのに役立ちます。AWS セキュリティの詳細については、AWS クラウドセキュリティを参照してください。

AWS IAM ロール

AWS Identity and Access Management (IAM) ロールにより、AWS クラウドのサービスとユーザーに対してアクセスポリシーとアクセス許可を詳細に割り当てることができます。このソリューションでは、各自動修復の機能ごとに、絞り込まれた範囲のアクセス権を付与する IAM ロールを作成します。

管理者アカウントの AWS Step Functions には、`SO0111-SHARR-Orchestrator-Admin` ロールが割り当てられます。このロールのみが、各メンバーアカウントの `SO0111-Orchestrator-Member` を引き受けることが許可されています。メンバーロールは、各修復ロールが AWS Systems Manager サービスに渡して、特定の修復ランブックを実行することを許可されています。修復ロール名は SO0111 で始まり、その後に修復ランブックの名前と一致する説明が続きます。
例えば、`SO0111-RemoveVPCDefaultSecurityGroupRules` は、`SHARR_RemoveVPCDefaultSecurityGroupRules` 修復ランブックのロールになります。

設計に関する考慮事項

AWS Security Hub のデプロイ

AWS Security Hub のデプロイと設定は、このソリューションの前提条件です。AWS Security Hub のセットアップに関する詳細は、*AWS Security Hub* ユーザーガイドの「AWS Security Hub のセットアップ」を参照してください。

少なくとも、プライマリアカウントで AWS Security Hub が動作するように設定されている必要があります。このソリューションは、AWS Security Hub のプライマリアカウントと同じ AWS アカウント (および AWS リージョン) にデプロイできます。各 AWS Security Hub のプライマリアカウントとセカンダリアカウントで、このソリューションの AWS Step Functions に対する `AssumeRole` アクセス権限がアカウントで修復ランブックを実行できるようにするメンバーテンプレートもデプロイする必要があります。

ソリューションのアップデート

このソリューションを v1.3.x 以前から最新バージョンにアップグレードするには、まず既存のスタックを削除してから、最新バージョンのスタックを再インストールする必要があります。削除の手順については、「ソリューションのアンインストール」セクションを参照してください。ログデータはすべて保持され、運用データが失われることはありません。v1.4.x からアップグレードする場合は、「ソリューションのアップデート」を参照してください。

スタックと StackSets のデプロイメント

StackSets では、1 つの AWS CloudFormation テンプレートを使用して、複数の AWS リージョンの AWS アカウントにスタックを作成できます。バージョン 1.4 以降、このソリューションはデプロイされる場所と方法に基づいてリソースを分割することにより、StackSets を用いたデプロイをサポートします。マルチアカウントのユーザーで、特に AWS Organizations を利用している場合は、StackSets を使用して多数のアカウントにデプロイすることでメリットを得られます。これにより、ソリューションのインストールとメンテナンスに必要な労力が軽減されます。StackSets の詳細については、「AWS CloudFormation StackSets の使用」を参照してください。

デプロイ可能な AWS リージョン

このソリューションは AWS Systems Manager を使用しますが、現在こちらは特定の AWS リージョンのみで利用可能です。このソリューションは、そのサービスをサポートするすべての AWS リージョンで動作します。AWS リージョンごとで利用可能な AWS サービスの最新情報については、「AWS リージョン別のサービス」を参照してください。

AWS CloudFormation テンプレート

このソリューションでは、AWS CloudFormation を使用して、AWS アカウントへの「AWS での自動化されたセキュリティ対応」ソリューションのデプロイを自動化します。これには、次の AWS CloudFormation テンプレートが含まれており、デプロイ前にダウンロードできます。

コアソリューション

テンプレートを表示

aws-sharr-deploy.template - このテンプレートを使用して、「AWS での自動化されたセキュリティ対応」ソリューションを起動します。このテンプレートには、このソリューションのコアコンポーネント、AWS Step Functions のログ用のネストされたスタック、選択したセキュリティ基準ごとに 1 つのネストされたスタックがインストールされます。
使用するサービスには、Amazon Simple Notification Service、AWS Key Management Service、AWS Identity and Access Management、AWS Lambda、AWS Step Functions、Amazon CloudWatch Logs、Amazon S3、AWS Systems Manager などがあります。

管理者アカウントのサポート

次のテンプレートが AWS Security Hub の管理者アカウントにインストールされ、サポートするセキュリティ基準が有効になります。`aws-sharr-deploy.template` をインストールするときに、インストールするテンプレートを次の中から選択できます。

aws-sharr-orchestrator-log.template - AWS Step Functions の Orchestrator 用の Amazon CloudWatch Logs グループの作成。

AFSBPStack.template - AWS の基本的なセキュリティのベストプラクティス v1.0.0 のルール。

CIS120Stack.template - CIS Amazon Web Services Foundations benchmarks、v1.2.0 のルール。

PCI321Stack.template - PCI-DSS v3.2.1 のルール。

メンバーアカウント

テンプレートを表示

aws-sharr-member.template - AWS Systems Manager のオートメーションランブックとアクセス権限を AWS Security Hub の各メンバーアカウント (管理者アカウントを含む) にインストールするためのコアソリューションをセットアップした後にこのテンプレートを使用します。このテンプレートを使用すると、インストールするセキュリティ基準のプレイブックを選択できます。

`aws-sharr-member.template` では、選択内容に基づいて次のテンプレートがインストールされます。

aws-sharr-remediations.template - 1 つ以上のセキュリティ基準で使用されている共通の修復コード。

afsbpMemberStack.template - AWS の基本的なセキュリティのベストプラクティス v1.0.0 の設定、アクセス許可、修復ランブック。

CIS120MemberStack.template - CIS Amazon Web Services Foundations benchmarks、v1.2.0 の設定、アクセス許可、修復ランブック。

PCI321MemberStack.template - PCI-DSS v3.2.1 の設定、アクセス許可、修復ランブック。

メンバーロール

テンプレートを表示

aws-sharr-member-roles.template - 各 AWS Security Hub のメンバーアカウントに必要な修復ロールを定義します。

自動デプロイ – StackSets

> **注意:** StackSets を使用してデプロイすることをお勧めします。ただし、単一アカウントへのデプロイやテストまたは評価目的の場合は、スタックのデプロイオプションを検討してください。

このソリューションを起動する前に、このガイドで説明しているアーキテクチャ、ソリューションコンポーネント、セキュリティ、および設計上の考慮事項を確認してください。このセクションの手順に従い、ソリューションを設定して AWS Organizations 内にデプロイします。詳細については、StackSets を参照してください。

デプロイ時間: StackSets パラメータによって、1 つのアカウントごとに約 15 分。

前提条件

AWS Organizations は、マルチアカウントの AWS 環境とリソースを一元的に管理するのに役立ちます。StackSets は AWS Organizations で最適に機能します。

既にこのソリューションの v1.3.x またはそれ以前のバージョンをデプロイしている場合は、既存のソリューションをアンインストールする必要があります。詳細については、「ソリューションのアップデート」セクションを参照してください。

このソリューションをデプロイする前に、AWS Security Hub のデプロイを確認してください。

- AWS Organization には、委任された AWS Security Hub の管理者アカウントが必要です。
- AWS Security Hub が、複数の AWS リージョンにわたって検出結果を集約するように設定する必要があります。詳細については、*AWS Security Hub* ユーザーガイドの「Aggregating findings across Regions」を参照してください。
- AWS を使用する各 AWS リージョンで、組織の AWS Security Hub をアクティブにする必要があります。

この手順では、AWS Organizations を使用する複数のアカウントがあり、AWS Organizations の管理アカウントと AWS Security Hub の管理者アカウントを委任していることを前提としています。

デプロイの概要

> **注意**: このソリューションの StackSets のデプロイでは、サービスマネージド型とセルフマネージド型の StackSets を組み合わせて使用しています。セルフマネージド型の StackSets では、サービスマネージド型の StackSets ではまだサポートされていないネストされた StackSets を使用しているため、今のところは使用する必要があります。

AWS Organizations の委任された管理アカウントから StackSets をデプロイしてください。

プランニング

次のフォームを使用して、StackSets のデプロイを支援することができます。データを準備し、デプロイ中に値をコピーして貼り付けてください。

AWS Organizations の管理者アカウント ID: _____

AWS Security Hub の管理者アカウント ID: _____

AWS CloudTrail のロググループ: _____

メンバーアカウント ID (カンマ区切りリスト):

_____,

_____,

_____,

_____,

_____

AWS Organizations の OU (カンマ区切りリスト):

_____,

_____,

_____,

_____,

_____

ステップ 1: 委任された AWS Security Hub の管理者アカウントで管理者スタックを起動

- セルフマネージド型の StackSets を使用して、AWS Security Hub の管理者と同じ AWS リージョンの AWS Security Hub の管理者アカウントで `aws-sharr-deploy.template` AWS CloudFormation テンプレートを起動します。このテンプレートでは、ネストされたスタックを使用しています。
- インストールするセキュリティ基準を選択します。デフォルトで、すべて選択されています (推奨)
- 使用する既存の Orchestrator ロググループを選択します。前回のインストールで `SO0111-SHARR-Orchestrator` がすでに存在する場合は、`Yes` を選択します。

セルフマネージド型 StackSets の詳細については、*AWS CloudFormation* ユーザーガイドの「Grant self-managed permissions」を参照してください。

ステップ 2: 各 AWS Security Hub のメンバーアカウントに修復ロールをインストール

ステップ 2 のテンプレートはステップ 1 で作成された IAM ロールを参照するため、ステップ 1 のデプロイが完了するまで待ちます。

- サービスマネージド型 StackSets を使用して、AWS Organizations の各アカウントの単一の AWS リージョンで `aws-sharr-member-roles.template` AWS CloudFormation テンプレートを起動します。
- 組織に新しいアカウントが追加された時に、このテンプレートを自動的にインストールするように選択します。
- AWS Security Hub の管理者アカウントのアカウント ID を入力します。

ステップ 3: 各 AWS Security Hub のメンバーアカウントと AWS リージョンでメンバースタックを起動

- セルフマネージド型 StackSets を使用して、同じ AWS Security Hub の管理者が管理する AWS Organizations のすべてのアカウントに AWS リソースがあるすべての AWS リージョンで、`aws-sharr-member.template` AWS CloudFormation テンプレートを起動します。

> **注意**: サービスマネージド型 StackSets がネストされたスタックがサポートされるまでは、組織に加わる新しいアカウントに対してこの手順を実行する必要があります。

- インストールするセキュリティ基準のプレイブックを選択します。
- AWS CloudTrail ロググループの名前を指定します (一部の修復で使用します)。
- AWS Security Hub の管理者アカウントのアカウント ID を入力します。

> **重要:** このソリューションには、匿名の運用メトリクスを AWS に送信するオプションが含まれています。当社はこのデータを使用して、お客様がこのソリューション、関連サービスおよび製品をどのように使用しているかをよりよく理解し、提供するサービスや製品の改善に役立てます。AWS は、このアンケートを通じて収集されたデータを所有します。データ収集には、AWS プライバシーポリシーが適用されます。
>
> この機能を無効にするには、テンプレートをダウンロードして、AWS CloudFormation のマッピングセクションを変更し、AWS CloudFormation コンソールを使用してテンプレートをアップロードし、このソリューションをデプロイします。詳細については、このガイドの「運用メトリックの収集」セクションを参照してください。

ステップ 1: 委任された AWS Security Hub の管理者アカウントで管理者スタックを起動

1. AWS Security Hub の管理者アカウントで、管理スタック (`aws-sharr-deploy.template`) をデプロイします。通常、単一の AWS リージョンの組織ごとに 1 つ指定します。このスタックはネストされたスタックを使用するため、このテンプレートをセルフマネージド型の StackSets としてデプロイする必要があります。

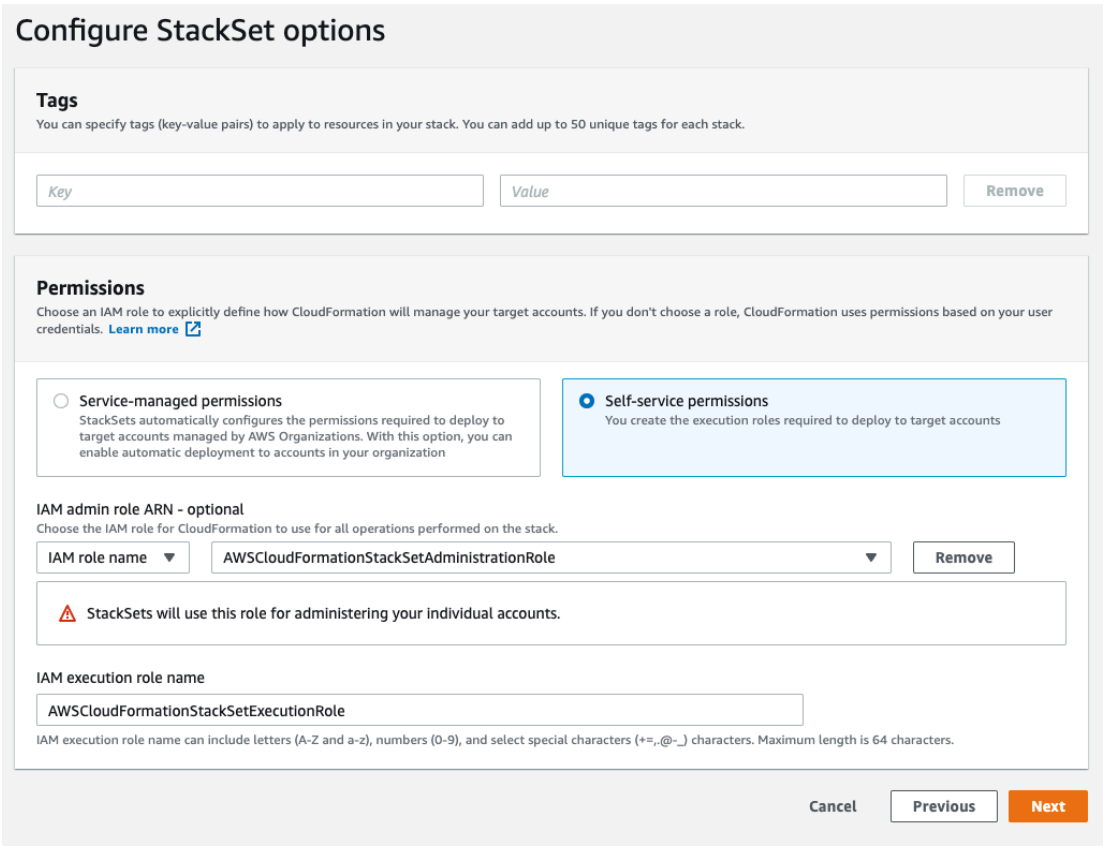


図 *2: StackSets* オプションの設定

2. **Account numbers** パラメータに、AWS Security Hub の管理者アカウントのアカウント ID を入力します。
3. **Specify regions** パラメータで、AWS Security Hub の管理者がオンになっている AWS リージョンのみを選択します。この手順が完了するのを待ってから、ステップ 2 に進みます。

ステップ 2: 各 AWS Security Hub のメンバーアカウントに修正ロールをインストール

サービスマネージド型 StackSets を使用して、メンバーロールのテンプレート (`aws-sharr-member-roles.template`) をデプロイします。この StackSets は、メンバーアカウントごとに 1 つの AWS リージョンにデプロイする必要があります。これにより、AWS Step Functions の SHARR Orchestrator からのクロスアカウント API コールを許可するグローバルロールが定義されます。

1. 組織のポリシーに従って、組織全体 (通常) または組織単位にデプロイします。
2. AWS Organizations の新しいアカウントにこれらのアクセス権限が付与されるように、自動デプロイをオンにします。
3. **Specify regions** パラメータで、単一の AWS リージョンを選択します。IAM ロールはグローバルです。この StackSets がデプロイされている間に、ステップ 3 に進むことができます。

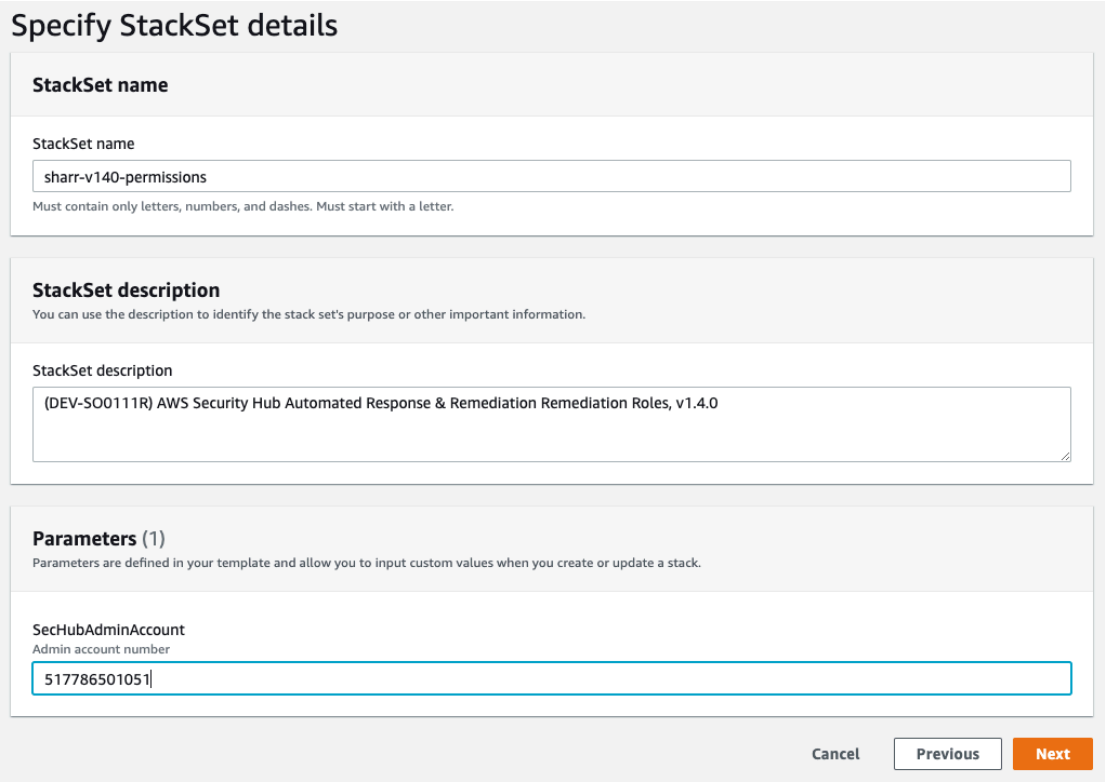


図 *3: StackSets* の詳細を指定

ステップ 3. 各 AWS Security Hub のメンバーアカウントと AWS リージョンでメンバースタックを起動

このスタックはネストされたスタックを使用するため、セルフマネージド型 StackSets としてデプロイする必要があります。AWS Organizations の新しいアカウントへの自動デプロイはサポートされていません。

パラメータ

LogGroup Configuration: AWS CloudTrail のログを受信するロググループを選択します。存在していない場合、またはロググループがアカウントごとに異なる場合は、適切な値を選択してください。アカウント管理者は、AWS CloudTrail のログ用に Amazon CloudWatch Logs のグループを作成した後に、AWS System Manager Parameter Store で /Solutions/SO0111/Metrics_LogGroupName パラメータを更新する必要があります。これは、API コールでメトリクスのアラームを作成する修復に必要です。

Standards: メンバーアカウントに読み込むセキュリティ基準を選択します。これにより、AWS Systems Manager のランブックがインストールされるだけで、セキュリティ基準は有効になりません。

SecHubAdminAccount: このソリューションの管理者テンプレートをインストールした AWS Security Hub の管理者アカウントのアカウント ID を入力します。

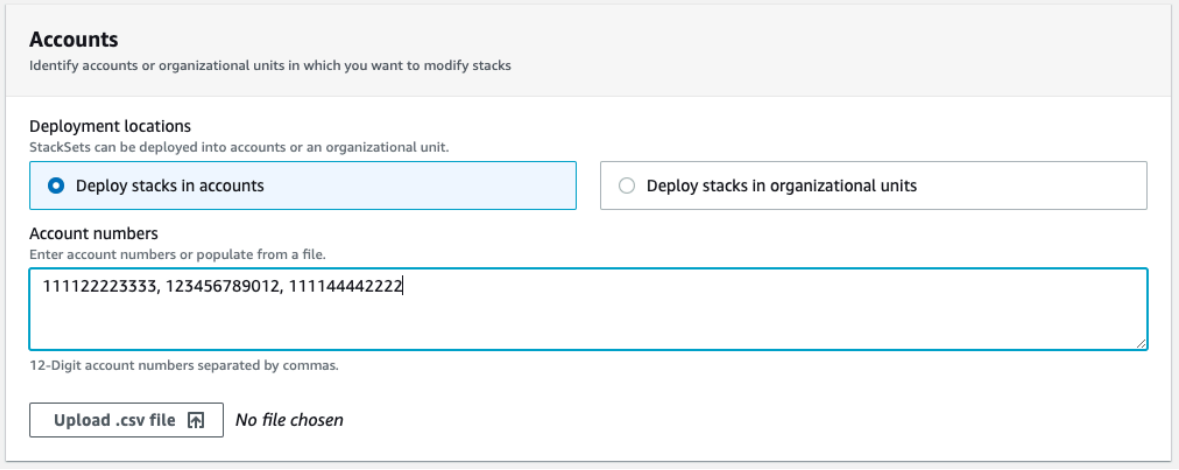


図 *4:* アカウント

Deployment locations: アカウント番号または組織単位のリストを指定できます。

Specify regions: 検出結果を修復する AWS リージョンをすべて選択します。アカウントと AWS リージョンの数に応じて、デプロイのオプションを調整できます。**リージョンの同時実行性**は並列化できます。

自動デプロイ – スタック

> **注意:** マルチアカウントのユーザーには、StackSets を使用したデプロイを強くお勧めします。

このソリューションを起動する前に、このガイドで説明しているアーキテクチャ、ソリューションコンポーネント、セキュリティ、および設計上の考慮事項を確認してください。このセクションの手順に従って、このソリューションを設定して AWS アカウントにデプロイします。

デプロイ時間：約 15 分

前提条件

このソリューションをデプロイする前に、AWS Security Hub がプライマリアカウントおよびセカンダリアカウントと同じ AWS リージョンにあることを確認してください。既にこのソリューションをデプロイしている場合は、既存のソリューションをアンインストールする必要があります。詳細については、「ソリューションのアップデート」セクションを参照してください。

デプロイの概要

次の手順を使用して、このソリューションを AWS にデプロイします。

ステップ 1. 管理者スタックの起動

- `aws-sharr-deploy.template` AWS CloudFormation テンプレートを AWS Security Hub の管理者アカウントで起動します。
- インストールするセキュリティ基準を選択します。
- 使用する既存の `Orchestrator` ロググループを選択します (以前のインストールで `SO0111-SHARR-Orchestrator` が既に存在している場合は `Yes` を選択してください)。

ステップ 2. メンバースタックの起動

- CIS 3.1-3.14 の修復で使用する Amazon CloudWatch Logs グループの名前を指定します。AWS CloudTrail のログを受け取る Amazon CloudWatch Logs のロググループの名前である必要があります。
- 修復ロールをインストールするかどうかを選択します。このロールは、アカウントごとに 1 回だけインストールしてください。
- インストールするプレイブックを選択します。
- AWS Security Hub の管理者アカウントのアカウント ID を入力します。

ステップ 3. 使用可能な修復の調整 (オプション)

- メンバーアカウントごとに修復をすべて削除します。この手順は省略可能です。

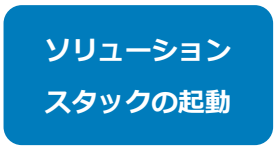
ステップ 1. 管理者スタックの起動

> **重要:** このソリューションには、匿名の運用メトリクスを AWS に送信するオプションが含まれています。当社はこのデータを使用して、お客様がこのソリューション、関連サービスおよび製品をどのように使用しているかをよりよく理解し、提供するサービスや製品の改善に役立てます。AWS は、このアンケートを通じて収集されたデータを所有します。データ収集には、AWS プライバシーポリシーが適用されます。
>
> この機能を無効にするには、テンプレートをダウンロードして、AWS CloudFormation のマッピングセクションを変更し、AWS CloudFormation コンソールを使用してテンプレートをアップロードし、このソリューションをデプロイします。詳細については、このガイドの「運用メトリックの収集」セクションを参照してください。

この自動化された AWS CloudFormation テンプレートは、「AWS Security Hub での自動化されたセキュリティ対応」ソリューションを AWS クラウドにデプロイします。スタックを起動する前に、AWS Security Hub を有効にして、前提条件を確認する必要があります。

> **注意:** このソリューションの実行中に使用した AWS のサービスのコストは、お客様の負担となります。詳細については、このガイドの「コスト」セクションで、このソリューションで使用されている各 AWS のサービスの料金表ページを参照してください。

1. AWS Security Hub が現在設定されている AWS アカウントの AWS マネジメントコンソールにサインインしてから、`aws-sharr-deploy.template` AWS CloudFormation テンプレートを起動するボタンを選択します。独自にカスタマイズするためにテンプレートをダウンロードすることもできます。



2. テンプレートは、デフォルトで米国東部 (バージニア北部) リージョンで起動されます。別の AWS リージョンでこのソリューションを起動するには、AWS マネージメントコンソールのナビゲーションバーでリージョンセレクターを使用します。

> **注意**:このソリューションでは AWS Systems Manager を使用します。このサービスは、現在、一部の AWS リージョンでのみ利用可能です。このソリューションは、AWS Systems Manager が利用可能な AWS リージョンで起動する必要があります。AWS リージョンごとで利用可能な AWS サービスの最新情報については、「AWS リージョン別のサービス」をご参照ください。

3. **スタックの作成**ページで、正しいテンプレート URL が **Amazon S3 URL** テキストボックスに入力されていることを確認し、[**次へ**] を選択します。
4. **スタックの詳細を指定**ページで、このソリューションのスタックに名前を割り当てます。名前の文字数制限に関する詳細は、*AWS Identity and Access Management* ユーザーガイドの「IAM および AWS STS クォータ」を参照してください。
5. **パラメータ**ページで、次のパラメータを指定して [**次へ**] を選択します。

パラメータ	デフォルト	説明
Load AFSBP Admin Stack	`yes`	AFSBP コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
Load CIS120 Admin Stack	`yes`	CIS120 コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
Load PC1321Admin Stack	`yes`	PC1321 コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。

パラメータ	デフォルト	説明
Reuse Orchestrator Log Group	no	既存の Amazon CloudWatch Logs の SO0111-SHARR-Orchestrator グループを再利用するかどうかを選択します。これにより、以前のバージョンのログデータを失うことなく、再インストールとアップグレードが簡単に行えます。v1.2 以降からアップグレードする場合は、yes を選択してください.

6. **スタックオプションの設定**ページで、[**次へ**] を選択します。
7. **レビュー**ページで、設定を確認します。テンプレートが AWS Identity and Access Management (IAM) リソースを作成することを承認するチェックボックスを必ずオンにします。
8. [**スタックの作成**] を選択してスタックをデプロイします。

   スタックのステータスは、AWS CloudFormation コンソールの**ステータス**列で確認できます。約 10 分で CREATE_COMPLETE ステータスが表示されます。

ステップ 2. 各 AWS Security Hub のメンバーアカウントに修正ロールをインストール

aws-sharr-member-roles.template StackSets は、メンバーアカウントごとに 1 つのリージョンにのみデプロイする必要があります。これにより、AWS Step Functions の SHARR Orchestrator からのクロスアカウント API コールを許可するグローバルロールが定義されます。

1. AWS Security Hub のメンバーアカウント (メンバーでもある管理者アカウントを含む) ごとに AWS マネジメントコンソールにサインインします。aws-sharr-member-roles.template AWS CloudFormation テンプレートを起動するボタンを選択します。独自にカスタマイズするためにテンプレートをダウンロードすることもできます。

   ロールスタックの起動
2. テンプレートは、デフォルトで米国東部 (バージニア北部) リージョンで起動されます。別の AWS リージョンでこのソリューションを起動するには、AWS マネージメントコンソールのナビゲーションバーでリージョンセレクターを使用します。

3. **スタックの作成**ページで、正しいテンプレート URL が **Amazon S3 URL** テキストボックスに入力されていることを確認し、[**次へ**] を選択します。
4. **スタックの詳細を指定**ページで、ソリューションスタックに名前を付けます。名前の文字数制限に関する詳細は、*AWS Identity and Access Management* ユーザーガイドの「IAM および AWS STS クォータ」を参照してください。
5. **パラメータ**ページで、次のパラメータを指定して [**次へ**] を選択します。

パラメータ	デフォルト	説明
Sec Hub Account Admin	<入力が必須>	AWS Security Hub の管理者アカウントの 12 桁のアカウント ID を入力します。この値により、管理者アカウントのソリューションのロールに権限が付与されます。

6. **スタックオプションの設定**ページで、[**次へ**] を選択します。
7. **レビュー**ページで、設定を確認します。テンプレートが AWS Identity and Access Management (IAM) リソースを作成することを承認するチェックボックスを必ずオンにします。
8. [**スタックの作成**] を選択してスタックをデプロイします。

   スタックのステータスは、AWS CloudFormation コンソールの**ステータス**列で確認できます。約 5 分で CREATE_COMPLETE ステータスが表示されます。このスタックが読み込まれている間は、次のステップに進むことができます。

ステップ 3. メンバースタックの起動

重要: このソリューションには、匿名の運用メトリクスを AWS に送信するオプションが含まれています。当社はこのデータを使用して、お客様がこのソリューション、関連サービスおよび製品をどのように使用しているかをよりよく理解し、提供するサービスや製品の改善に役立てます。AWS は、このアンケートを通じて収集されたデータを所有します。データ収集には、AWS プライバシーポリシーが適用されます。

この機能を無効にするには、テンプレートをダウンロードして、AWS CloudFormation のマッピングセクションを変更し、AWS CloudFormation コンソールを使用してテンプレートをアップロード

> し、このソリューションをデプロイします。詳細については、このガイドの「運用メトリックの収集」セクションを参照してください。

`aws-sharr-member` スタックは、各 AWS Security Hub のメンバーアカウントにインストールする必要があります。このスタックは、自動修復用のランブックを定義します。各メンバーアカウントの管理者は、このスタック経由で利用可能な修復をコントロールできます。

1. AWS Security Hub のメンバーアカウント (メンバーでもある管理者アカウントを含む) ごとに AWS マネジメントコンソールにサインインします。`aws-sharr-member.template` AWS CloudFormation テンプレートを起動するボタンを選択します。独自にカスタマイズするためにテンプレートをダウンロードすることもできます。

   メンバースタックの起動

2. テンプレートは、デフォルトで米国東部 (バージニア北部) リージョンで起動されます。別の AWS リージョンでこのソリューションを起動するには、AWS マネージメントコンソールのナビゲーションバーでリージョンセレクターを使用します。

> **注意**: このソリューションでは AWS Systems Manager を使用します。このサービスは、現在、ほとんどの AWS リージョンで利用可能です。このソリューションは、AWS Systems Manager が利用可能な AWS リージョンで起動する必要があります。AWS リージョンごとで利用可能な AWS サービスの最新情報については、「AWS リージョン別のサービス」をご参照ください。

3. **スタックの作成**ページで、正しいテンプレート URL が **Amazon S3 URL** テキストボックスに入力されていることを確認し、[**次へ**] を選択します。
4. **スタックの詳細を指定**ページで、このソリューションのスタックに名前を割り当てます。名前の文字数制限に関する詳細は、*AWS Identity and Access Management* ユーザーガイドの「IAM および AWS STS クォータ」を参照してください。
5. **パラメータ**ページで、次のパラメータを指定して [**次へ**] を選択します。

パラメータ	デフォルト	説明
Provide the name of the LogGroup to be used to create Metric Filters and Alarms	<入力が必須>	AWS CloudTrail が API コールを記録する Amazon CloudWatch Logs グループの名前を指定します。これは CIS 3.1-3.14 の修復に使用されます。

パラメータ	デフォルト	説明
Load AFSBP Member Stack	`yes`	AFSBP コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
Load CIS120 Member Stack	`yes`	CIS120 コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
Load PCI321 Member Stack	`yes`	PC1321 コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
Create S3 Bucket For Redshift Audit Logging	`no`	AFSBP Redshift.4 修復用に Amazon S3 バケットを作成する必要がある場合は、`yes` を選択します。Amazon S3 バケットと修復の詳細については、*AWS Security Hub* ユーザーガイドの「[Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります」を参照してください。
Sec Hub Admin Account	<入力が必須>	AWS Security Hub の管理者アカウントの 12 桁のアカウント ID を入力します。

6. **スタックオプションの設定**ページで、[**次へ**] を選択します。
7. **レビュー**ページで、設定を確認します。テンプレートが AWS Identity and Access Management (IAM) リソースを作成することを承認するチェックボックスを必ずオンにします。
8. [**スタックの作成**] を選択してスタックをデプロイします。

   スタックのステータスは、AWS CloudFormation コンソールの**ステータス**列で確認できます。約 15 分で CREATE_COMPLETE ステータスが表示されます。

ステップ 4: 使用可能な修復の調整 (オプション)

メンバーアカウントから特定の修復を削除する場合は、ネストされたスタックをセキュリティ基準に合わせて更新することで削除できます。シンプルにするために、ネストされたスタックのオプションはルートスタックには伝播されません。

1. AWS CloudFormation コンソールにサインインして、ネストされたスタックを選択します。
2. [**更新**] を選択します。

3. [**ネストされたスタックを更新**] を選択して [**スタックの更新**] を選択します。

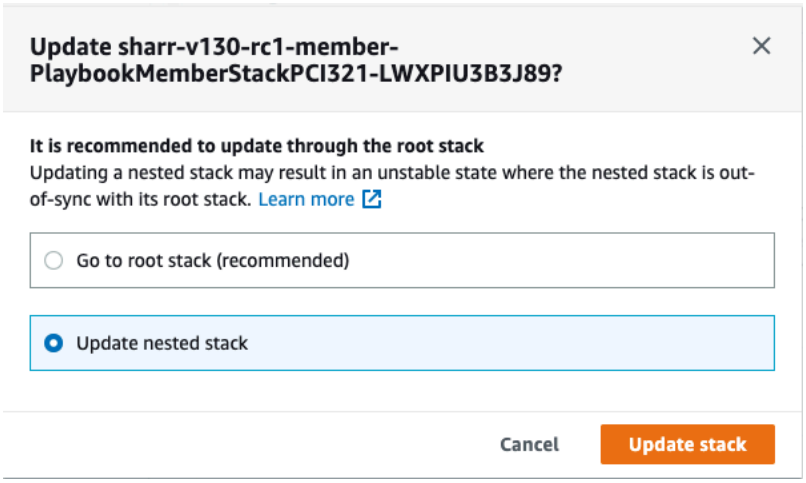


図 *5:* ネストされたスタックの更新

4. [**現在のテンプレートを使用**] を選択し、[**次へ**] を選択します。
5. 使用可能な修復を調整します。必要なコントロールの値は `Available` に、不要なコントロールは `Not available` に変更してください。

> **注意**: 修復をオフにすると、セキュリティ基準とコントロール用のソリューションの修復ランブックが削除されます。

6. **スタックオプションの設定**ページで、[**次へ**] を選択します。
7. **レビュー**ページで、設定を確認します。テンプレートが AWS Identity and Access Management (IAM) リソースを作成することを承認するチェックボックスを必ずオンにします。
8. [**スタックの更新**] を選択します。

スタックのステータスは、AWS CloudFormation コンソールの**ステータス**列で確認できます。約 15 分で UPDATE_COMPLETE ステータスが表示されます。

その他のリソース

AWS のサービス

- AWS Security Hub
- AWS CloudFormation
- AWS Key Management Service
- AWS Lambda
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- AWS Step Functions
- AWS Systems Manager
- Amazon Simple Notification Service
- AWS Identity and Access Management
- AWS CDK

関連リソース

- Automated Response and Remediation with AWS Security Hub
- CIS Amazon Web Services Foundations benchmarks, version 1.2.0
- AWS の基本的なセキュリティのベストプラクティス標準
- Payment Card Industry Data Security Standard (PCI DSS)

プレイブック

このソリューションには、Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0、AWS の基本的なセキュリティのベストプラクティス (AFSBP) v.1.0.0、Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1 の一部として定義されているセキュリティ基準のプレイブックの修復が含まれています。

特定の修復の詳細については、AWS アカウントにこのソリューションによってデプロイされた名前の AWS Systems Manager ランブックを参照してください。AWS Systems Manager コンソールに移動し、ナビゲーションペインで [**ドキュメント**] を選択してください。

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1
SHARR-EnableAutoScalingGroupELBHealthCheck ロードバランサーに関連付けられた Auto Scaling グループは、ロードバランサーのヘルスチェックを使用します。	Autoscaling.1		Autoscaling.1
SHARR-CreateCloudTrailMultiRegionTrail AWS CloudTrail を有効にし、少なくとも 1 つのマルチリージョンの証跡で設定します。	CloudTrail.1	2.1	CloudTrail.2
SHARR-EnableCloudTrailEncryption AWS CloudTrail は、保管時の暗号化を有効にします。	CloudTrail.2	2.7	CloudTrail.1
SHARR-EnableCloudTrailLogFileValidation AWS CloudTrail のログファイルの整合性検証がアクティブになっていることを確認します。	CloudTrail.4	2.2	CloudTrail.3
SHARR-EnableCloudTrailToCloudWatchLogging AWS CloudTrail のトレイルが Amazon CloudWatch Logs と統合されていることを確認します。	CloudTrail.5	2.4	CloudTrail.4
SHARR-ReplaceCodeBuildClearTextCredentials AWS CodeBuild プロジェクトの環境変数にクリアテキストの認証情報を含ませません。	CodeBuild.2		CodeBuild.2

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1
SHARR-EnableAWSConfig AWS Config がアクティブになっていることを確認します。	Config.1	2.5	Config.1
SHARR-MakeEBSSnapshotsPrivate Amazon EBS のスナップショットをパブリックで復元可能にしません。	EC2.1		EC2.1
SHARR-RemoveVPCDefaultSecurityGroupRules Amazon VPC のデフォルトセキュリティグループでインバウンドとアウトバウンドのトラフィックを禁止します。	EC2.2	4.3	EC2.2
SHARR-EnableVPCFlowLogs Amazon VPC フローログをすべての Amazon VPC で有効にします。	EC2.6	2.9	EC2.6
SHARR-EnableEbsEncryptionByDefault Amazon EBS の暗号化をデフォルトで有効にします。	EC2.7		
SHARR-RevokeUnrotatedKeys AWS IAM ユーザーのアクセスキーを 90 日以内でローテーションさせます。	IAM.3	1.4	
SHARR-SetIAMPasswordPolicy AWS IAM のデフォルトのパスワードポリシー	IAM.7	1.5-1.11	IAM.8
SHARR-RevokeUnusedIAMUserCredentials 事前定義された日数以内に使用されない場合に、AWS IAM ユーザーの認証情報をオフにします。	IAM.8	1.3	IAM.7
SHARR-RemoveLambdaPublicAccess AWS Lambda 関数のパブリックアクセスを禁止します。	Lambda.1		Lambda.1
SHARR-MakeRDSSnapshotPrivate Amazon RDS のスナップショットのパブリックアクセスを禁止します。	RDS.1		RDS.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1
SHARR-DisablePublicAccessToRDSInstance Amazon RDS の DB インスタンスのパブリックアクセスを禁止します。	RDS.2		RDS.2
SHARR-EncryptRDSSnapshot Amazon RDS のクラススナップショットとデータベーススナップショットを保管時に暗号化します。	RDS.4		
SHARR-EnableMultiAZOnRDSInstance Amazon RDS の DB インスタンスを複数のアベイラビリティーゾーンに設定します。	RDS.5		
SHARR-EnableEnhancedMonitoringOnRDSInstance 拡張モニタリングを Amazon RDS の DB インスタンスとクラスターに設定します。	RDS.6		
SHARR-EnableRDSClusterDeletionProtection Amazon RDS クラスターの削除保護を有効にします。	RDS.7		
SHARR-EnableRDSInstanceDeletionProtection Amazon RDS の DB インスタンスの削除保護を有効します。	RDS.8		
SHARR-EnableMinorVersionUpgradeOnRDSDBInstance Amazon RDS の自動マイナーバージョンのアップグレードを有効にします。	RDS.13		
SHARR-EnableCopyTagsToSnapshotOnRDSCluster Amazon RDS の DB クラスターのタグをスナップショットにコピーして設定します。	RDS.16		
SHARR-DisablePublicAccessToRedshiftCluster Amazon Redshift クラスターのパブリックアクセスを禁止します。	Redshift.1		Redshift.1
SHARR-EnableAutomaticSnapshotsOnRedshiftCluster Amazon Redshift クラスターの自動スナップショットをアクティブにします。	Redshift.3		

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1
SHARR-EnableRedshiftClusterAuditLogging Amazon Redshift クラスターの監査ログを有効にします。	Redshift.4		
SHARR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift のメジャーバージョンへの自動アップグレードを有効にします。	Redshift.6		
SHARR-ConfigureS3PublicAccessBlock Amazon S3 のパブリックアクセスをブロックする設定をアクティブにします。	S3.1		S3.6
SHARR-ConfigureS3BucketPublicAccessBlock Amazon S3 バケットのパブリックの読み取りアクセスを禁止します。	S3.2		S3.2
Amazon S3 バケットのパブリックの書き込みアクセスを禁止します。	S3.3		S3.1
SHARR-EnableDefaultEncryptionS3 Amazon S3 バケットのサーバーサイドの暗号化を有効にします。	S3.4		S3.4
SHARR-SetSSLBucketPolicy Amazon S3 バケットが SSL を使用するためのリクエストを要求します。	S3.5		S3.5
SHARR-S3BlockDenylist バケットポリシーで他の AWS アカウントに付与される Amazon S3 のアクセス許可を制限します。	S3.6		
Amazon S3 の Block Public Access 設定をバケットレベルでアクティブにします。	S3.8		
SHARR-ConfigureS3BucketPublicAccessBlock AWS CloudTrail のログ用の Amazon S3 バケットがパブリックにアクセスできないことを確認します。		2.3	

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1
SHARR-CreateAccessLoggingBucket AWS CloudTrail で、Amazon S3 バケットのアクセスログがアクティブになっていることを確認します。		2.6	
SHARR-EnableKeyRotation 作成した AWS KMS key のローテーションがアクティブになっていることを確認します。		2.8	KMS.1
SHARR-CreateLogMetricFilterAndAlarm 不正な API コールに関するログメトリクスのフィルタとアラームが存在することを確認します。		3.1	
SHARR-CreateLogMetricFilterAndAlarm MFA を使用しない AWS マネジメントコンソールへのサインインに関するログメトリクスのフィルタとアラームが存在することを確認します。		3.2	
SHARR-CreateLogMetricFilterAndAlarm ルートユーザーの使用に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.3	CW.1
SHARR-CreateLogMetricFilterAndAlarm AWS IAM ポリシーの変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.4	
SHARR-CreateLogMetricFilterAndAlarm AWS CloudTrail の設定変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.5	
SHARR-CreateLogMetricFilterAndAlarm AWS マネジメントコンソールの認証の失敗に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.6	
SHARR-CreateLogMetricFilterAndAlarm ユーザーが作成した AWS KMS key の無効化と削除に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.7	

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1
SHARR-CreateLogMetricFilterAndAlarm Amazon S3 バケットのポリシー変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.8	
SHARR-CreateLogMetricFilterAndAlarm AWS Config の設定変更に関するログメトリックスのフィルタとアラームが存在することを確認します。		3.9	
SHARR-CreateLogMetricFilterAndAlarm セキュリティグループの変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.10	
SHARR-CreateLogMetricFilterAndAlarm ネットワークアクセスコントロールリスト（NACL）の変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.11	
SHARR-CreateLogMetricFilterAndAlarm ネットワークゲートウェイに対する変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.12	
SHARR-CreateLogMetricFilterAndAlarm ルートテーブルの変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.13	
SHARR-CreateLogMetricFilterAndAlarm Amazon VPC の変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.14	
AWS-DisablePublicAccessForSecurityGroup セキュリティグループが、0.0.0.0/0 からポート 3389 へのインバウンドアクセスを許可しないことを確認します。		4.1	EC2.5
AWS-DisablePublicAccessForSecurityGroup セキュリティグループが、0.0.0.0/0 からポート 3389 へのインバウンドアクセスを許可しないことを確認します。		4.2	

新しい修復の追加

既存のプレイブックに新しい修復を追加するために、このソリューション自体を変更する必要はありません。

> **注意:** この後の説明では、このソリューションによってインストールされたリソースを開始点として活用します。慣例により、ほとんどのソリューションのリソース名には **SHARR** や **SO0111** が含まれ、見つけやすく、識別し易いようになっています。

概要

「AWS での自動化されたセキュリティ対応」ソリューションのランブックは、次の標準的な命名規則に従う必要があります。

`SHARR-<standard>-<version>-<control>`

Standard: セキュリティ基準の略称です。これは SHARR がサポートするセキュリティ基準に一致する必要があります。「CIS」、「AFSBP」、「PCI」のいずれかである必要があります。

Version: セキュリティ基準のバージョン。この場合も、SHARR がサポートするバージョンと検出結果データのバージョンが一致している必要があります。

Control: 修復するコントロールのコントロール ID。これは検出結果データと一致する必要があります。

1. メンバーアカウントにランブックを作成します。
2. メンバーアカウントに IAM ロールを作成します。
3. (オプション) 管理者アカウントで自動修復ルールを作成します。

ステップ 1. メンバーアカウントでランブックを作成

1. AWS Systems Manager コンソールにサインインし、JSON の検出結果の例を取得します。
2. 検出結果を修復するランブックを作成します。**自己所有** タブで、**ドキュメント**セクションの下にある任意の `SHARR-` ドキュメントを開始点として使用します。

3. 管理者アカウントの AWS Step Functions がランブックを実行します。ランブックをコールしたときにロールを渡すために、ランブックで修復ロールを指定する必要があります。

ステップ 2. メンバーアカウントで IAM ロールを作成

1. AWS Identity and Access Management コンソールにサインインします。
2. IAM ロールの **SO0111** から例を取得し、新しいロールを作成します。このロール名は `SO0111-Remediate-<standard>-<version>-<control>` で始まる必要があります。例えば、CIS v1.2.0 のコントロール 5.6 を追加する場合は、このロールは `SO0111-Remediate-CIS-1.2.0-5.6` である必要があります。
3. この例を使用して、必要な API コールのみに修復の実行を許可する、適切な範囲が設定されたロールを作成します。

この時点で、修復はアクティブになり、AWS Security Hub の SHARR カスタムアクションからの自動修復が可能になります。

ステップ 3: (オプション) 管理者アカウントで自動修復ルールを作成

自動修復とは、AWS Security Hub が結果を受け取るとすぐに修復を実行することです。このオプションを使用する前に、慎重にリスクを検討するようにしてください。

1. Amazon CloudWatch Events で同じセキュリティ基準のルール例を確認してください。ルールの命名規則は、`standard_control_`**`AutoTrigger`** になります。
2. 使用する例からイベントパターンをコピーします。
3. `GeneratorId` の値を、JSON の検出結果の `GeneratorId` と一致するように変更します。
4. ルールを保存してアクティブにします。

新しいプレイブックの追加

「AWS での自動化されたセキュリティ対応」ソリューションのプレイブックとデプロイ用のソースコードを GitHub リポジトリからダウンロードしてください。

AWS CloudFormation のリソースは AWS CDK のコンポーネントから作成され、そのリソースには、新しいプレイブックの作成と設定に使用できるプレイブックのテンプレートコードが含まれています。プロジェクトのセットアップとプレイブックのカスタマイズの詳細については、GitHub の README.md をご参照ください。

AWS Systems Manager Parameter Store

「AWS での自動化されたセキュリティ対応」ソリューションでは、運用データの格納に AWS Systems Manager Parameter Store を使用しています。次のパラメータが AWS Systems Manager Parameter Store に格納されます。

名前	値	使用
/Solutions/SO0111/CMK_REMEDIATION_ARN	AFSBP の修復でデータを暗号化する AWS KMS key	修復の一環として、AWS CloudTrail ログなどの顧客データを暗号化します。
/Solutions/SO0111/CMK_ARN	SHARR がデータの暗号化に使用する AWS KMS key	このソリューションのデータを暗号化します。
/Solutions/SO0111/SNS_Topic_ARN	このソリューションの Amazon SNS トピックの ARN	修復イベントを通知します。
/Solutions/SO0111/SNS_Topic_Config.1	AWS Config の更新に関する Amazon SNS トピック	Config.1 の修復に使用します。
/Solutions/SO0111/sendAnonymousMetrics	Yes	匿名のメトリクスを収集します。
/Solutions/SO0111/version	ソリューションのバージョン	

名前	値	使用
/Solutions/SO0111/<security standard long name>/<version>/status	enabled	セキュリティ基準がこのソリューションで有効かどうかを示します。これを disabled に変更すると、自動修復に関するセキュリティ基準を無効にできます。
/Solutions/SO0111/<security standard long name>/shortname	文字列	セキュリティ基準の略称。(例: CIS、AFSBP、PCI)
/Solutions/SO0111/<security standard short name>/<version>/<control>/remap	文字列	あるコントロールが別のコントロールと同じ修復を使用している場合は、これらのパラメータによって再分類が行われます。

Amazon SNS トピック

「AWS での自動化されたセキュリティ対応」ソリューションでは、Amazon SNS トピック (SO0111-SHARR_Topic) が作成されます。このトピックは、修復の進行状況に関する更新を投稿するために使用されます。次がこのトピックに送信される 3 つの通知です。

```
Remediation queued for <standard> control <control_ID> in account
<account_ID>
```

```
Remediation failed for <standard> control <control_ID> in account
<account_ID>
```

```
<control_ID> remediation was successfully invoke via AWS Systems
Manager in account <account_ID>
```

これは完了メッセージです。修復がエラーなしで完了したことを示していますが、修復を成功させるための決定的なテストは、AWS Config のチェックまたは手動検証になります。

トラブルシューティング

ソリューションのログ

このソリューションは、AWS Systems Manager で実行される修復ランブックから出力を収集し、その結果を AWS Security Hub の管理者アカウントの Amazon CloudWatch Logs グループ (`SO0111-SHARR`) に記録します。コントロールおよび日ごとに 1 つのストリームが作成されます。

AWS Step Functions の Orchestrator は、AWS Security Hub の管理者アカウントで Amazon CloudWatch Logs の `SO0111-SHARR-Orchestrator` グループにすべてのステップの遷移を記録します。このログは、AWS Step Functions の各インスタンスの状態遷移を記録する監査証跡です。AWS Step Functions の実行ごとに 1 つのログストリームが作成されます。

どちらのロググループも AWS KMS key を使用して暗号化されます。

次のトラブルシューティング情報では、`SO0111-SHARR` ロググループを使用しています。このログに加えて、AWS Systems Manager Automation コンソール、オートメーションの実行ログ、AWS Step Functions コンソール、AWS Lambda のログを使用して、問題のトラブルシューティングを行います。

修復が失敗すると、次のようなメッセージが `SO0111-SHARR` に基準、コントロール、日付用のログストリームに記録されます。(例: **CIS-2.9-2021-08-12**)

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc vpc-0e92bbe911cf08acb)
```

次のメッセージに詳細が記載されています。この出力は、セキュリティ基準とコントロールに関する SHARR のランブックからのものです。(例: **SHARR-CIS_1.2.0_2.9**)

```
Step fails when it is Execution complete: verified.Failed to run automation with executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :

{Status=[Failed], Output=[No output available yet because the step is not successfully executed], ExecutionId=[eecdef79-9111-4532-921a-
```

```
e098549f5259]}.Please refer to Automation Service Troubleshooting Guide for
more diagnosis details.
```

この情報は失敗箇所を示しています。この場合は、メンバーアカウントで実行されている子オートメーションになります。この問題をトラブルシューティングするには、(上記のメッセージより) メンバーアカウントで AWS マネジメントコンソールにログインし、AWS Systems Manager に移動して **Automation** に移動し、実行 ID (`eecdef79-9111-4532-921a-e098549f525`) のログ出力を調べる必要があります。

問題と解決策

- **問題:** このソリューションのデプロイは、リソースが Amazon CloudWatch で既に使用可能であることを示すエラーで失敗します。

  解決策: AWS CloudFormation のリソース / イベントのセクションで、ロググループが既に存在することを示すエラーメッセージがないか確認します。SHARR のデプロイ用のテンプレートを使用すると、既存のロググループを再利用できます。再利用を選択したことを確認します。

- **問題**: 同じ AWS アカウントで、AWS Security Hub を複数の AWS リージョンで実行しています。このソリューションを複数の AWS リージョンにデプロイしたいです。

  解決策: AWS Security Hub の管理者と同じアカウントおよび AWS リージョンに管理者スタックをデプロイする必要があります。AWS Security Hub のメンバーが設定されている各アカウントと AWS リージョンに、メンバーテンプレートをインストールします。AWS Security Hub で集約を有効にします。

- **問題**: デプロイ直後に、**SO0111-SHARR-Orchestrator** が次の 502 エラーで Get Automation Document State を失敗します。「*Lambda was unable to decrypt the environment variables because KMS access was denied. Please check the function's KMS key settings. KMS Exception: UnrecognizedClientExceptionKMS Message: The security token included in the request is invalid. (Service: AWSLambda; Status Code: 502; Error Code: KMSAccessDeniedException; Request ID: …*」

解決策: 修復を実行する前に、このソリューションが安定するまで約 10 分待ちます。問題が解決しない場合は、サポートチケットを切るか、GitHub の Issue に登録してください。

- **問題**: 検出結果を修正しようとしたが、何も起こりませんでした。

  解決策: 修復されなかった理由がないか、検出結果のメモを確認してください。一般的な原因は、この検出結果に自動修復機能がないことです。現時点では、メモ以外に修復が存在しない場合は、ユーザーに直接フィードバックを提供する方法はありません。

  このソリューションのログを確認してください。コンソールで Amazon CloudWatch Logs を開いてください。Amazon CloudWatch Logs のグループである SO0111-SHARR を見つけます。最近更新されたストリームが最初に表示されるようにリストを並べ替えてください。実行しようとした検出結果のログストリームを選択します。そこでエラーが見つかるはずです。失敗の原因としては、検出結果の制御と修復の制御の不一致、クロスアカウントの修復 (まだサポートされていない) 、または検出結果がすでに修復されていることが考えられます。失敗の原因を特定できなかった場合は、ログを収集し、サポートチケットを切ってください。

- **問題**: 修復を開始した後に、AWS Security Hub コンソールのステータスが更新されていません。

  解決策: AWS Security Hub コンソールでは、自動的に更新されません。現在のビューを更新してください。検出結果のステータスが更新されます。

  検出結果が **Failed** から **Passed** に移行するまでに数時間かかる場合があります。検出結果は、AWS Config などの他のサービスから AWS Security Hub に送信されたイベントデータから作成されます。ルールが再評価されるまでの時間は、基盤となるサービスによって異なります。

  これで問題が解決しない場合は、上記の「検出結果を修正しようとしたが、何も起こりませんでした」の解決方法を参照してください。

- **問題**: AWS Step Functions の Orchestrator で、**Get Automation Document State** が失敗します。「*An error occurred (AccessDenied) when calling the AssumeRole operation*.」

  解決策: SHARR が検出結果の修復を試みているメンバーアカウントにメンバーのテンプレートがインストールされていません。メンバーのテンプレートをデプロイするための手順に従ってください。

- **問題**: レコーダーまたは配信チャネルがすでに存在するため、Config.1 のランブックが失敗します。

  解決策: AWS Config の設定を慎重に調べて、AWS Config が正しくセットアップされていることを確認してください。自動修復では、場合によって、既存の AWS Config の設定を修復できません。

- **問題**: 修復は成功しているが、`"No output available yet because the step is not successfully executed."` のメッセージが返される

  解決策: これは、「特定の修復ランブックがレスポンスを返さない」というこのリリースの既知の問題です。修復ランブックは正常に失敗し、動作しない場合にこのソリューションに通知します。

- **問題**: 解決に失敗して、スタックトレースが送信される

  解決策: 場合によっては、エラーメッセージではなくスタックトレースになるエラー状態に対処する機会を逃すことがあります。トレースデータから問題のトラブルシューティングを試みてください。サポートが必要な場合は、サポートチケットを切ってください。

- **問題**: カスタムアクションのリソースで v1.3.0 のスタックを削除できませんでした。

  解決策: カスタムアクションを削除すると、管理者用テンプレートの削除が失敗することがあります。これは既知の問題で、次のリリースで修正される予定です。このような場合は、次のようになります。

  1. AWS Security Hub マネジメントコンソールにサインインします。
  2. 管理者用のアカウントで、**設定**に移動します。
  3. [**カスタムアクション**] タブを選択します。
  4. **Remediate with SHARR** のエントリを手動で削除します。
  5. 再度、スタックを削除します。

- **問題:** 管理者スタックを再度デプロイした後に、`AssumeRole` で AWS Step Functions が失敗します。

解決策: 管理者スタックを再度デプロイすると、管理者アカウントの管理者ロールとメンバーアカウントのメンバーロール間の信頼関係が切断されます。メンバーロールスタックをすべてのメンバーアカウントに再度デプロイする必要があります。

- **問題**: 24 時間を超えても CIS 3.x の修復が `PASSED` と表示されません。

  解決策: これは、メンバーアカウントに `SO0111-SHARR_LocalAlarmNotification` Amazon SNS トピックへのサブスクリプションがない場合によく発生します。

ソリューションのアップデート

v1.4 以前のバージョンからのアップグレード

v1.4.x 以前のソリューションをデプロイしている場合は、アンインストールしてから最新バージョンをインストールしてください。

1. 以前にデプロイしたソリューションをアンインストールします。「ソリューションのアンインストール」を参照してください。
2. 最新のテンプレートを起動します。「自動デプロイ」を参照してください。

> **注意**: v1.2.1 以前から v1.3.0 以降にアップグレードする場合は、**Use existing Orchestrator Log Group** を `No` に設定してください。v1.3.0 以降を再インストールする場合は、このオプションで `Yes` を選択できます。このオプションを使用すると、AWS Step Functions の Orchestrator と同じロググループに引き続きログを記録できます。

v1.4 以降からのアップグレード

v1.4.x からアップグレードする場合は、すべてのスタックまたは StackSets を次のように更新します。

1. 最新のテンプレートを使用して、AWS Security Hub の管理者アカウントのスタックを更新します。
2. 各メンバーアカウントで、最新のテンプレートの権限を更新します

3. 現在デプロイしているすべての AWS リージョンの各メンバーアカウントで、最新のテンプレートのメンバースタックを更新します。

ソリューションのアンインストール

AWS マネジメントコンソールでこのソリューションをアンインストールするには、次の手順を使用します。

V1.0.0 – V1.2.1

リリース v1.0.0 ～ v1.2.1 では、サービスカタログを使用して CIS または AFSBP プレイブックをアンインストールします。v1.3.0 では、AWS Service Catalog は使用されなくなりました。

1. AWS CloudFormation コンソールにサインインし、AWS Security Hub の管理者アカウントに移動します。
2. [**Service Catalog**] を選択して、プロビジョニングされたプレイブックを終了し、セキュリティグループ、ロール、またはユーザーを削除します。
3. AWS Security Hub のメンバーアカウントから `CISPermissions.template` スポークテンプレートを削除します。
4. AWS Security Hub の管理者およびメンバーアカウントから `AFSBPMemberStack.template` スポークテンプレートを削除します。
5. AWS Security Hub の管理者アカウントに移動し、このソリューションのインストールスタックを選択して、[**削除**] を選択します。

> **注意:** Amazon CloudWatch Logs のグループログは保持されます。組織のログの保存ポリシーの要件に応じて、これらのログを保持することをお勧めします。

V1.3.x

1. 各メンバーアカウントから `aws-sharr-member.template` を削除します。
2. 管理者アカウントから `aws-sharr-admin.template` を削除します。

注意: v1.3.0 で管理者テンプレートを削除すると、カスタムアクションの削除に失敗する場合があります。これは既知の問題で、次のリリースで修正される予定です。次の手順を使用して、この問題を解決してください。

1. AWS Security Hub マネジメントコンソールにサインインします。
2. 管理者用のアカウントで、**設定**に移動します。
3. [**カスタムアクション**] タブを選択します。
4. **Remediate with SHARR** のエントリを手動で削除します。
5. 再度、スタックを削除します。

V1.4.0 以降

スタックのデプロイ

1. 各メンバーアカウントから `aws-sharr-member.template` を削除します。
2. 管理者アカウントから `aws-sharr-admin.template` を削除します。

StackSets のデプロイ

StackSets ごとにスタックを削除してから、デプロイとは逆の順序で StackSets を削除します。

テンプレートが削除されても `aws-sharr-member-roles.template` の IAM ロールは保持されることに注意してください。このロールを使用した修復が引き続き機能するようにするようにしています。この SO0111-* のロールは、AWS CloudTrail から Amazon CloudWatch へのロギングや Amazon RDS の拡張モニタリングなどのアクティブな修復で使用されていないことを確認した後に手動で削除できます。

運用メトリクスの収集

このソリューションには、匿名の運用メトリクスを AWS に送信するオプションが含まれています。当社はこのデータを使用して、お客様がこのソリューション、関連サービスおよび製品をどのように使用

しているかをよりよく理解し、提供するサービスや製品の改善に役立てます。有効にすると、次の情報が収集され、AWS に送信されます。

- **Solution ID -** AWS ソリューション識別子
- **Unique ID (UUID) -** 「AWS での自動化されたセキュリティ対応」ソリューションごとにランダムに生成された一意の識別子
- **Timestamp -** データ収集タイムスタンプ
- **Instance Data -** このスタックのデプロイに関する情報
- **Status -** デプロイのステータス (ソリューションの成功または失敗) または (修復の成功または失敗)
- **Error message -** ステータスのフィールドに表示される一般的なエラーメッセージ
- **Generator_id -** AWS Security Hub のルール情報
- **Type -** 修復のタイプと名前
- **productArn -** AWS Security Hub がデプロイされている AWS リージョン
- **finding_triggered_by -** 実行される修復のタイプ (カスタムアクションまたは自動トリガー)

AWS は、このアンケートを通じて収集されたデータを所有します。データ収集には、AWS プライバシーポリシーが適用されます。この機能を無効にするには、AWS CloudFormation テンプレートを起動する前に、次の手順を実施してください。

1. AWS CloudFormation テンプレートをローカルのハードドライブにダウンロードします。
2. テキストエディタで AWS CloudFormation テンプレートを開きます。
3. AWS CloudFormation テンプレートのマッピングセクションを次のように変更します。

```
Mappings:
  Solution:
    Data:
      SendAnonymousUsageData: 'Yes'
```

次のように変更します。

```
Mappings:
  Solution:
    Data:
      SendAnonymousUsageData: 'No'
```

4. AWS CloudFormation コンソールにサインインします。
5. [**スタックの作成**] を選択します。
6. **スタックの作成**ページの**テンプレートの指定**セクションで、[**テンプレートファイルのアップロード**] を選択します。
7. **テンプレートファイルのアップロード**で、[**ファイルの選択**] を選択し、ローカルドライブから編集したテンプレートを選択します。
8. [**次へ**] を選択し、このガイドの「自動デプロイメント」セクションの「スタックの起動」の手順に従います。

ソースコード

GitHub リポジトリにアクセスして、このソリューションのテンプレートとスクリプトをダウンロードし、カスタマイズした上で他のユーザーと共有できます。

改訂

日付	変更
2020 年 8 月	初回リリース
2020 年 10 月	プレイブックをカスタマイズするための追加のトラブルシューティング情報を追記
2020 年 11 月	中国リージョンのデプロイ手順を追加。AWS Security Hub の管理者アカウント用のソリューションのデプロイ手順を更新。詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。
2021 年 3 月	リリース v1.2.0: 新しいプレイブックのアーキテクチャと新しい AFSBP の修復を追加詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。
2021 年 5 月	リリース v1.2.1: EC2.2 と EC2.7 に影響する問題のバグ修正詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。

日付	変更
2021 年 8 月	リリース v1.3.0: PCI DSS v3.2.1 プレイブックを追加。CIS v1.2.0 に 17 の新しい修復を追加。AFSBP に 4 つの新しい修復を追加。SSM のランブックに基づく新しいプレイブックのアーキテクチャを使用するように CIS を変換します。既存のプレイブックをユーザー定義の修復で拡張する手順を追加。詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。
2021 年 9 月	リリース v1.3.1: CreateLogMetricFilterAndAlarm.py を変更して、アクションをアクティブにするように変更し、Amazon SNS 通知を SO0111-SHARR-LocalAlarmNotification に追加。CIS 2.8 の修復を新しい検出結果のデータ形式に一致するように変更。詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。
2021 年 11 月	リリース v1.3.2: CIS v1.2.0 コントロール 3.1 - 3.14 のバグ修正。詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。
2021 年 12 月	リリース v1.4.0: StackSets を使用してこのソリューションがデプロイできるようになりました。クロスアカウントに加えて、クロスリージョンの修復もサポートしています。スタックが削除されてもメンバーアカウントの IAM ロールは保持されます。詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。
2022 年 1 月	リリース v1.4.1: バグ修正。詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。
2022 年 1 月	リリース v1.4.2: バグ修正。詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。
2022 年 6 月	リリース v1.5.0: 修復の追加。詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。

寄稿者

- *Mike O'Brien*
- *Nikhil Reddy*
- *Max Granat*
- *Chandini Penmetsa*
- *Chaitanya Deolankar*

注意

お客様は、この文書に記載されている情報を独自に評価する責任を負うものとします。このドキュメントは、(a) 情報提供のみを目的としており、(b) AWS の現行製品とプラクティスを表したものであり、予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤー、またはライセンサーからの契約義務や確約を意味するものではありません。AWS の製品やサービスは、明示または暗示を問わず、いかなる保証、表明、条件を伴うことなく「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で行われるいかなる契約の一部でもなく、そのような契約の内容を変更するものでもありません。

「AWS での自動化されたセキュリティ対応」ソリューションは、Apache Software Foundation で閲覧可能な Apache ライセンスバージョン 2.0 の条項に基づいてライセンスされています。