AWS Security Incident Response ユーザーガイド

Version March 27, 2026

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Security Incident Response ユーザーガイド:

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

AWS Security Incident Response とは?

AWS Security Incident Response は、セキュリティインシデントへの迅速な準備、対応、復旧に向けたガイダンスの提供を支援します。これには、アカウント乗っ取り、データ侵害、ランサムウェア攻撃などのインシデントが含まれます。

AWS Security Incident Response は脅威検出結果のトリアージ、セキュリティイベントのエスカレーション、即時対応が必要なケースの管理を行います。さらに、影響を受けたリソースを調査するセキュリティインシデント対応エンジニアにアクセスできます。

> **Note**
>
> 影響を受けたリソースを復旧できる保証はありません。ビジネス要件に影響を与える可能性のあるリソースのバックアップを確立して維持することをお勧めします。

AWS Security Incident Response は、他の AWS Detection and Response サービスと連携し、検出から復旧まで、インシデントのライフサイクル全体をガイドします。

内容

サポートされている設定

AWS Security Incident Response では、以下の言語とリージョンの設定がサポートされています。

- 言語: AWS Security Incident Response は専用の英語サポートを提供します。日本語サポートは日本標準時の営業時間に制限されており、特定の制限があります。
-
  > **Note**
  >
  > 日本語サポートは、営業時間内 (月曜日から金曜日の午前 9 時 ~ 午後 5 時、祝日を除く) にベストエフォートベースで提供されます
- サポート対象の AWS リージョン:

AWS Security Incident Response は、AWS リージョン のサブセットで使用できます。これらのサポートされているリージョンでは、メンバーシップの作成、ケースの作成と表示、ダッシュボードへのアクセスが可能です。

- 米国東部 (オハイオ)
- 米国西部 (オレゴン)
- 米国東部 (バージニア)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (ミラノ)
- 欧州 (パリ)
- 欧州 (スペイン)
- 欧州 (ストックホルム)
- 欧州 (チューリッヒ)
- アジアパシフィック (香港)
- アジアパシフィック (ハイデラバード)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (メルボルン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- カナダ (中部)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)
- 南米 (サンパウロ)
- アフリカ (ケープタウン)

モニタリングおよび調査機能を有効にすると、AWS Security Incident Response はすべてのアクティブな商用 AWS リージョン からの Amazon GuardDuty の検出結果をモニタリングします。セキュリティのベストプラクティスとして、AWS では、サポートされているすべての AWS リー

ジョンで GuardDuty を有効にすることをお勧めします。この設定により、GuardDuty は、リソースをアクティブにデプロイしない AWS リージョン でも、許可されていないアクティビティや異常なアクティビティに関する検出結果を生成できます。これにより、全体的なセキュリティ体制を強化し、AWS 環境全体で包括的な脅威検出カバレッジを維持できます。

> **Note**
>
> Amazon GuardDuty は、設定されたリージョンの検出結果をレポートします。特定のリージョンでサービスを有効にしない場合、アラートは使用できません。

機能の概要

モニタリングと調査

AWS Security Incident Response は、Amazon GuardDuty および AWS Security Hub CSPM とのサードパーティー統合からのセキュリティ脅威アラートを迅速にレビューし、チームが分析する必要のあるアラートの数を減らします。環境に基づいて抑制ルールを設定し、トリアージと調査に必要な脅威アラートを減らします。

インシデント対応の効率化

関連するステークホルダー、サードパーティーのサービス、ツールを使用して、インシデント対応を数分以内にスケールして実行します。

セルフサービスのセキュリティソリューション

AWS Security Incident Response は統合するための API を提供し、独自のカスタマイズされたセキュリティソリューションを構築することができます。

可視性のためのダッシュボード

インシデント対応の準備状況をモニタリングして測定します。

セキュリティ体制

セキュリティ評価と迅速なインシデント対応調査のための AWS ベストプラクティスと精査されたツールにアクセスします。

迅速なサポート

セキュリティインシデント対応エンジニアに連絡して、セキュリティイベントを調査し、封じ込め、復旧方法に関するガイダンスを受け取ります。

準備状況と即応性

事前定義されたアクセス許可ポリシーを使用して、指定された個人またはグループにアラートをトリガーするインシデント対応チームを設定することで、効率的な通知を実装します。

概念と用語

以下の用語と概念は、AWS Security Incident Response サービスとその仕組みを理解する上で重要です。

スコープ: AWS Security Incident Response は、米国国立標準技術研究所 (NIST) の「800-61 Computer Security Incident Handling Guide」に準拠しており、業界のベストプラクティスに基づいたセキュリティイベント管理の一貫したアプローチを提供します。

分析: セキュリティイベントの範囲、影響、根本原因を理解するための詳細な調査と検討。

AWS Security Incident Response サービスポータル: セキュリティイベントケースを開始および管理するためのセルフサービスポータル。チケットシステム、自動通知、サービスチームとの直接的な関与を通じて、継続的なコミュニケーションと報告が促進されます。

コミュニケーション: インシデント対応プロセス中の AWS Security Incident Response チームとお客様間の継続的な対話と情報共有。

封じ込め、根絶、復旧: 追加の不正なアクティビティの防止 (封じ込め)、不正なリソースと元の脆弱性の削除 (根絶)、および通常の業務に復帰するためのリソースの復旧。

継続的改善: AWS Security Incident Response は、以前のエンゲージメントから学んだフィードバックと教訓を取り入れて、検出機能、調査プロセス、修復アクションを強化します。また、AWS Security Incident Response は、進化するセキュリティ課題に対処するため、最新のセキュリティ脅威とベストプラクティスを常に把握します。

サイバーセキュリティイベント: 情報システムまたはネットワークを使用して、システム、ネットワーク、またはそこに含まれる情報に悪影響を及ぼすアクション。

サイバーセキュリティインシデント: コンピュータセキュリティポリシー、許容可能な使用ポリシー、または標準セキュリティプラクティスの違反または差し迫った違反の脅威。

セキュリティインシデント対応エンジニア: アクティブなセキュリティイベント中にサポートを提供する個人のグループ。AWS がサポートするケースでは、これはセキュリティインシデント対応エンジニアです。

インシデント対応ワークフロー: NIST 800-61 標準に沿った、セキュリティイベントのエンドツーエンドの管理に関連する定義された一連のステップとアクティビティ。

調査ツール: アカウントとリソースの運用状態を確認するために使用される AWS Security Incident Response ツールとサービスにリンクされたロール。

教訓: セキュリティイベント対応のレビューとドキュメント。改善すべき分野を特定し、今後のインシデント対応計画に役立てます。

モニタリングと調査: AWS Security Incident Response は Amazon GuardDuty のセキュリティアラートを迅速にレビューし、チームが分析する必要がある最も重要なアラートを優先的に表示します。不要なアラートを防ぐために、環境の詳細に基づいて抑制ルールを設定します。

準備: インシデント対応計画やテスト手順の策定など、組織がセキュリティイベントに効果的に対応および管理するための準備を整えるために行われるアクティビティ。

レポートとコミュニケーション: 自動通知、コールブリッジ、調査アーティファクトの配信など、インシデント対応プロセス全体を通じて最新情報を把握するために使用されるプロセス。AWS Security Incident Response では、すべての AWS Security Incident Response の作業を管理するための一元化された単一のダッシュボードが AWS マネジメントコンソール で提供されます。

対応者が生成したインテリジェンス: 侵害の指標、戦術、手法、手順、および AWS 調査で観察された関連パターン。

セキュリティイベントの専門知識: 特に AWS クラウドのコンテキストにおいて、セキュリティイベントに効果的に対応し、管理するために必要な専門知識とスキル。

責任共有モデル: AWS とお客様の間のセキュリティ責任分担。AWS はクラウドのセキュリティに責任を持ち、お客様はクラウド内のセキュリティに責任を持ちます。

脅威インテリジェンス: 進化するセキュリティ脅威の特定と対応に役立つ、不正なアクティビティの詳細を含む内部および外部のデータフィード。

チケットシステム: セキュリティイベントケースのオンボーディングと管理、添付ファイルの追加、インシデント対応ライフサイクルの追跡を可能にする専用のケース管理プラットフォーム。

トリアージ: 適切な対応と次のステップを決定するためのセキュリティイベントの初期評価と優先順位付け。

ワークフロー: セキュリティイベントのエンドツーエンドの管理に関連するステップとアクティビティの定義されたシーケンス。

はじめに

AWS Security Incident Response の利用を開始する

内容

オンボーディングガイド

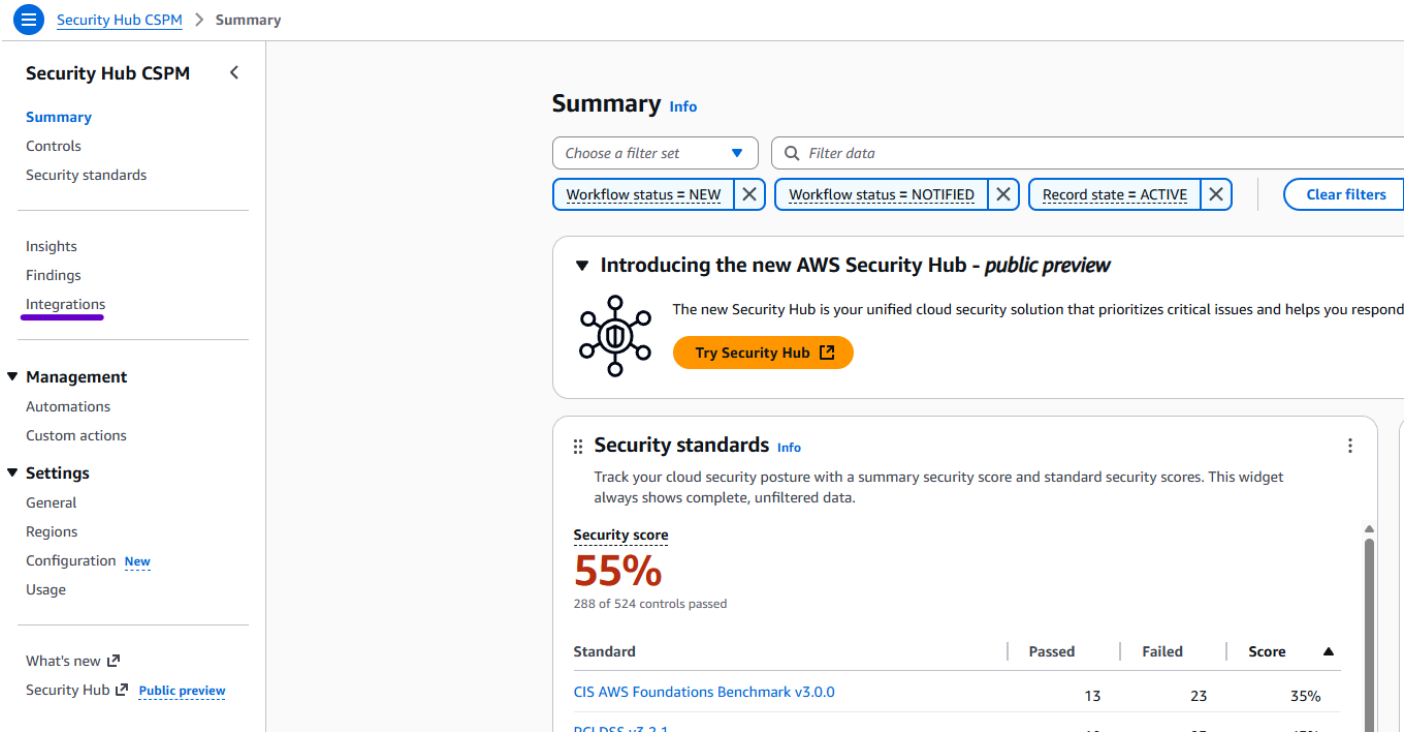
AWS Security Incident Response オンボーディングガイドでは、前提条件、 オンボーディング、封じ込めアクションについて説明します。

> **Important**
>
> 前提条件
>
> 1. デプロイにおける唯一の前提条件は、AWS Organizations を有効にすることです。
> 2. 必須ではありませんが、Security Incident Response のメリットを最大化するためにも、すべてのアカウントとアクティブ AWS リージョン で Amazon GuardDuty と AWS Security Hub CSPM を有効にすることをお勧めします。
> 3. GuardDuty とセキュリティインシデント対応を確認します。
> 4. GuardDuty ベストプラクティスガイド を確認します。

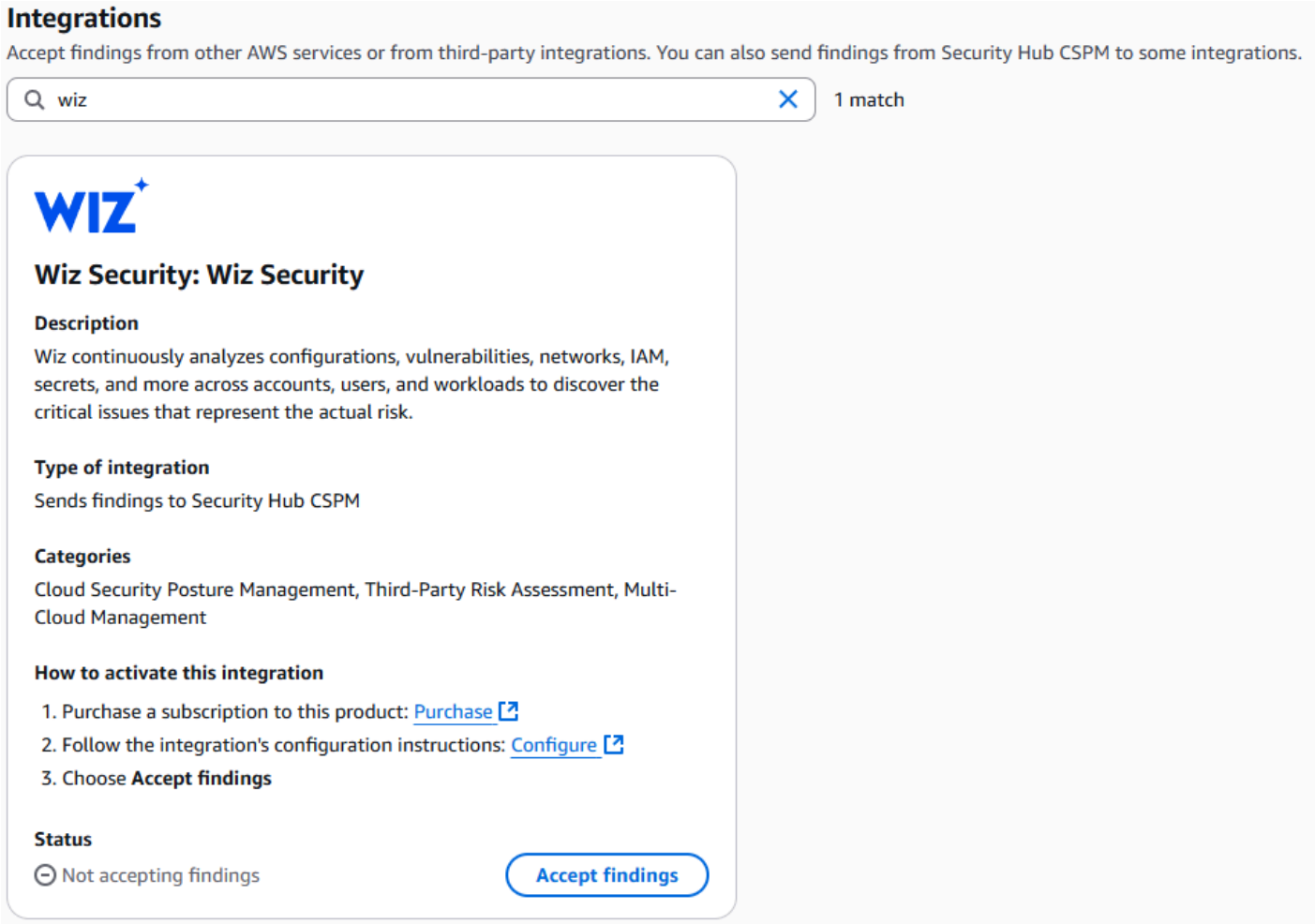
AWS Security Hub CSPM は、サードパーティーのエンドポイント検出および対応 (EDR) ベンダー (CrowdStrike、FortinetCNAPP (Lacework)、Trend Micro など) からの検出結果を取り込みます。これらの検出結果が Security Hub CSPM に取り込まれると、Security Incident Response によって自動的にトリアージされ、プロアクティブなケースが作成されます。Security Hub CSPM でサードパーティー EDR を設定するには、検出と分析 を参照してください。

Security Hub CSPM でサードパーティー EDR を設定するには:

1. Security Hub の CSPM 統合ページに移動して、サードパーティーの統合が存在することを確認します。
2. コンソールから、Security Hub CSPM サービスページに移動します。
3. 統合 (例として Wiz.IO を使用) を選択します。



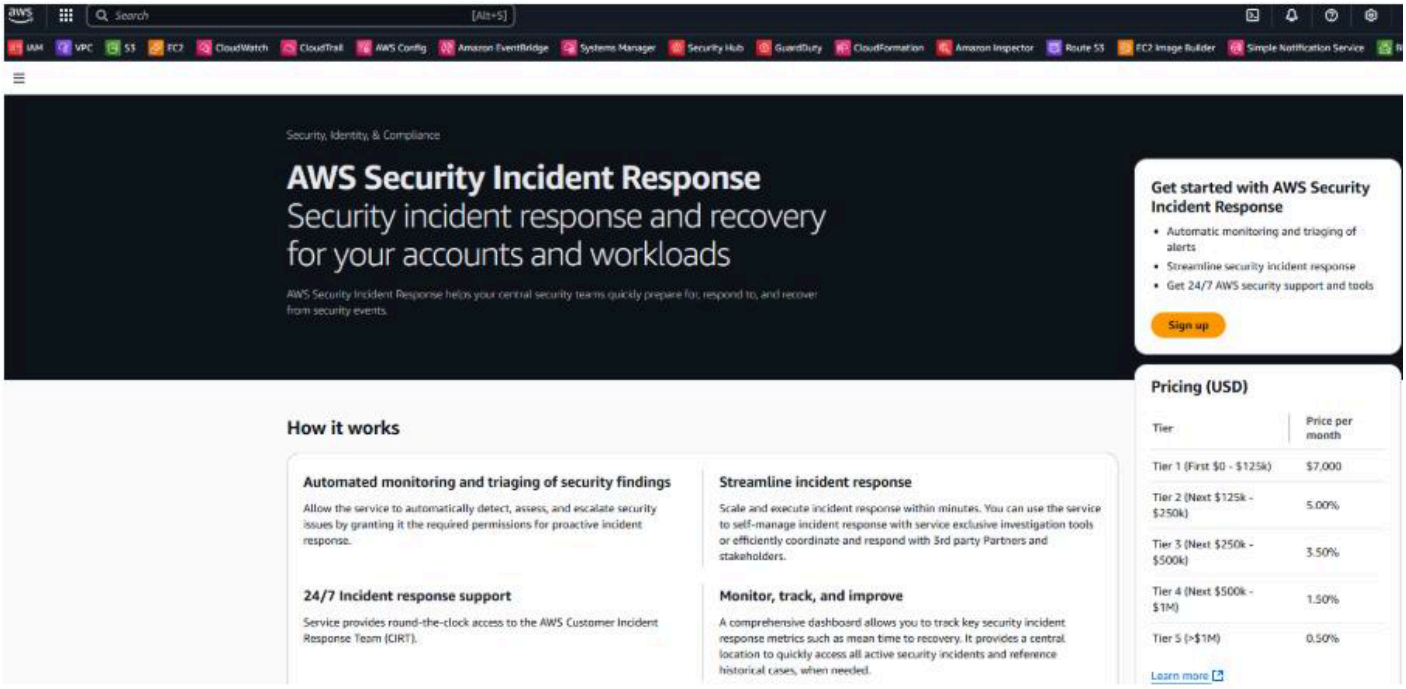
4. 統合するベンダーを検索する



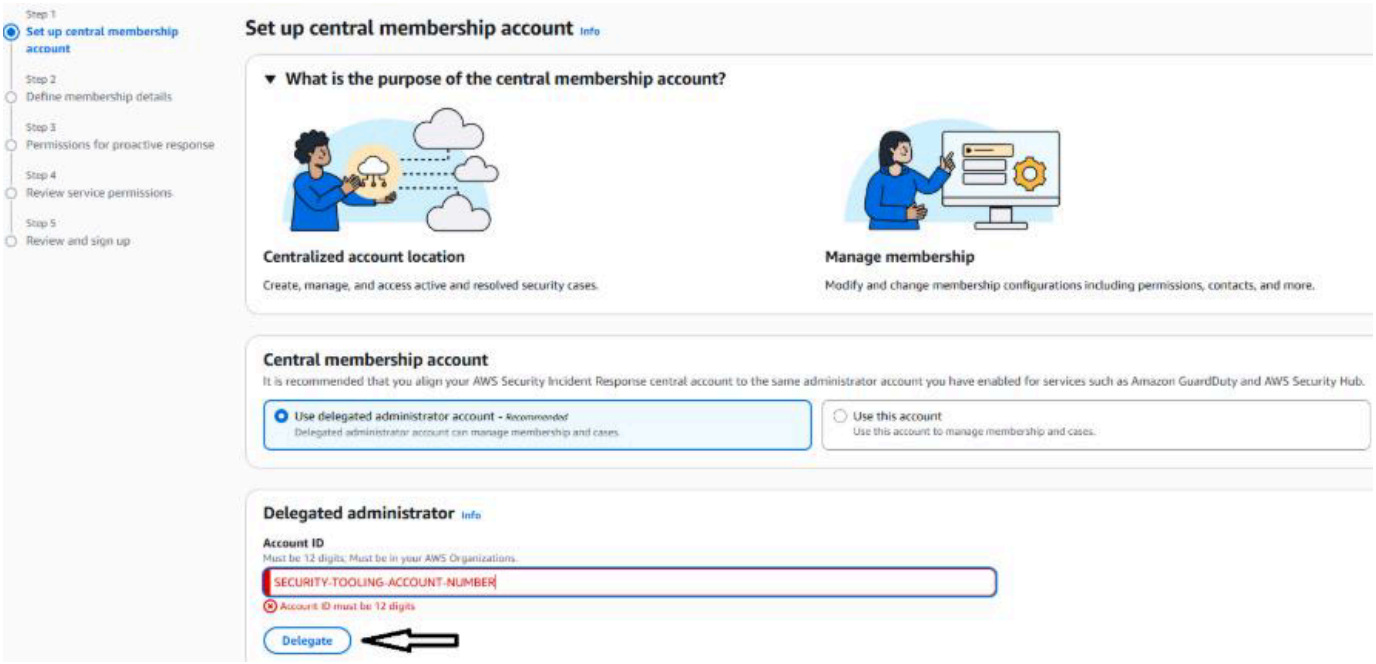
> **Note**
>
> プロンプトが表示されたら、アカウントまたはサブスクリプション情報を入力します。この情報を入力すると、Security Incident Response がサードパーティーの検出結果を取り込みます。サードパーティー検出結果の取り込みに対する料金を確認するには、Security Hub CSPM の「統合」ページを参照してください。

Security Incident Response のデプロイと設定

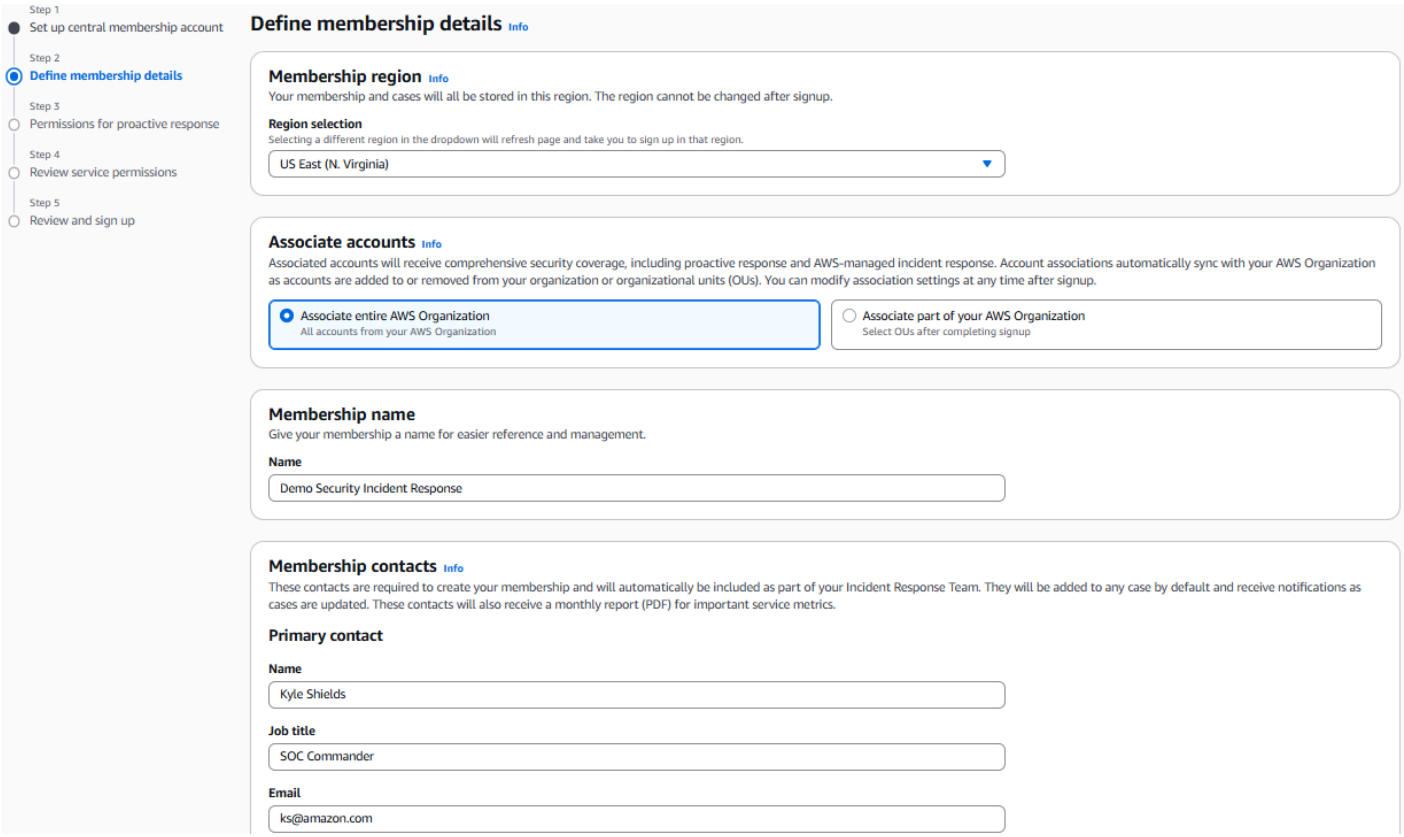
1. [サインアップ] を選択します。



2. 管理アカウントから委任管理者として セキュリティツール アカウントを選択します。
   - セキュリティリファレンスアーキテクチャ
   - 委任管理者のドキュメント



3. 委任された管理者のアカウントにログイン
4. メンバーシップの詳細を入力し、アカウントを関連付ける



Security Incident Response アクションを承認する

このページでは、セキュリティインシデント対応が AWS 環境で自動モニタリングと封じ込めアクションを実行することを承認する方法について説明します。プロアクティブ対応モニタリングと封じ込めアクション設定という 2 つの異なる認可機能を有効にすることができます。これらの機能は独立しており、セキュリティ要件に基づいて個別に有効にすることができます。

プロアクティブレスポンスを有効にする

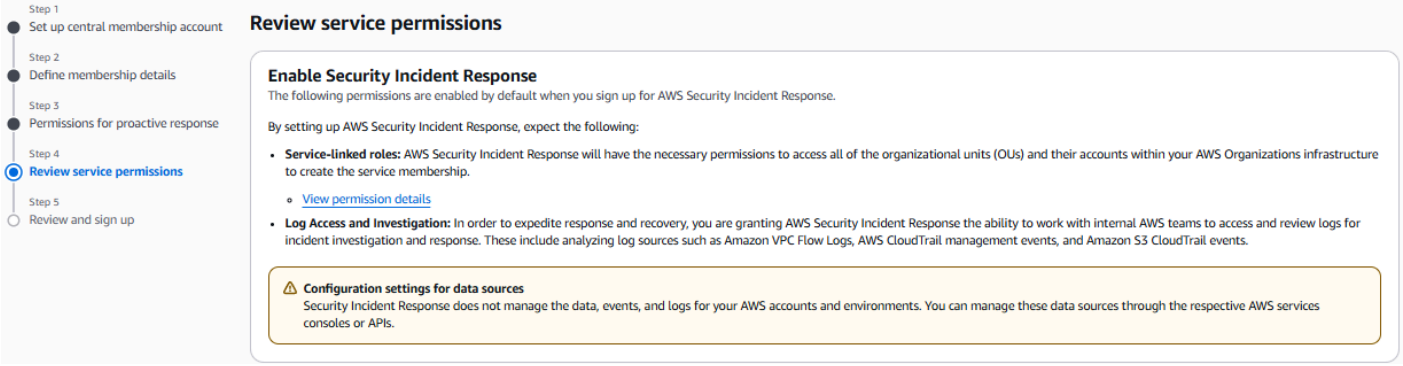
プロアクティブレスポンスは、組織全体での Amazon GuardDuty と AWS Security Hub CSPM の統合から生成されたアラートを Security Incident Response が監視して調査できるようにします。有効にすると、セキュリティインシデント対応は、サービス自動化を使用して優先度の低いアラートをトリアージし、チームが最も重要な問題に集中できるようにします。

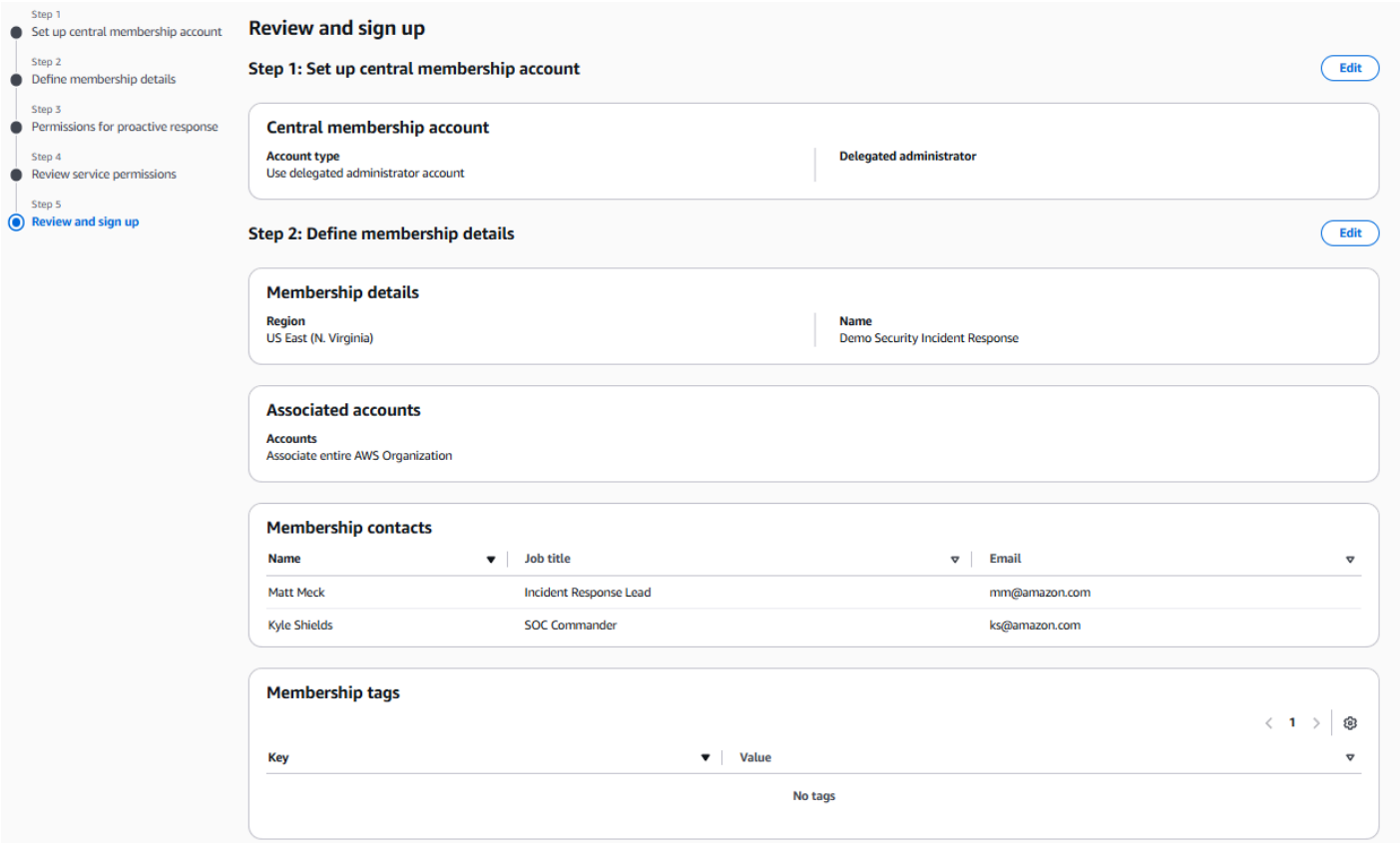
オンボーディング中にプロアクティブ対応を有効にするには:

1. セキュリティインシデント対応コンソールで、オンボーディングワークフローに移動します。

2. Security Incident Response が組織内のすべての対象アカウントとサポートされるアクティブな AWS リージョン リージョン全体での検出結果を監視できるようにするサービス許可を確認します。

3. [サインアップ] を選択して機能を有効にします。





この機能により、AWS Organizations 内のすべての対象メンバーアカウントにサービスリンクロールが自動的に作成されます。ただし、管理アカウントには AWS CloudFormation スタックセットを使用してサービスリンクロールを手動で作成する必要があります。

次のステップ: Security Incident Response の Amazon GuardDuty および AWS Security Hub CSPM との連動に関する詳細については、「AWS Security Incident Response ユーザーガイド」の「検出と分析」を参照してください。

封じ込めアクションの設定を定義する

封じ込めアクションにより、AWS Security Incident Response はアクティブなセキュリティインシデント中に迅速な対応策を実行できます。これらのアクションは、環境内のセキュリティインシデントの影響をすばやく軽減するのに役立ちます。

> **Important**
>
> Security Incident Response では、封じ込め機能がデフォルトで有効化されていません。封じ込め設定を使用して、封じ込めアクションを明示的に承認する必要があります。

AWS Security Incident Response エンジニアがユーザーに代わって封じ込めアクションを実行できるようにするには、必要な IAM ロールを作成する AWS CloudFormation StackSet をデプロイするだけでなく、組織またはアカウントレベルの封じ込め設定を定義する必要があります。アカウントレベルの設定は、組織レベルの設定よりも優先されます。

前提条件: AWS サポート ケースを作成する許可が必要です。

封じ込めオプション:

- 承認が必要 (デフォルト): 個別のケースごとに明示的な承認を得ることなくリソースのプロアクティブな封じ込めを実行しない。
- 確認されたリソースを封じ込める: 侵害されたことが確認されているリソースのプロアクティブな封じ込めを実行する。
- 疑わしいリソースを封じ込める: AWS Security Incident Response エンジニアリングが実行した分析に基づいて、侵害された可能性が高いリソースのプロアクティブな封じ込めを実行する。

封じ込め設定を定義するには:

1. Security Incident Response の封じ込めアクションの設定をリクエストする AWS サポート ケースを作成 します。
2. サポートケースで、以下を指定します:
   - 封じ込めアクションが承認される必要がある AWS Organizations ID または特定のアカウント ID

- ご希望の封じ込め方法 (承認が必要、封じ込め確定、または封じ込め疑い) を選択してください。
- 承認する封じ込めアクションのタイプ (EC2 インスタンスの分離、認証情報の更新、セキュリティグループの変更など)

3. AWS サポート がお客様と連携して封じ込めの設定を行います。必須の IAM ロールを作成するために不可欠な AWS CloudFormation StackSet をデプロイする必要があります。必要な場合は AWS サポート がサポートを提供できます。

設定されている場合、アクティブなセキュリティインシデント中に AWS Security Incident Response が承認された封じ込めアクションを実行し、環境を保護するための支援を提供します。

次のステップ: 封じ込め設定を行ったら、セキュリティインシデント対応コンソールでインシデント中に実行された封じ込めアクションをモニタリングできます。

Security Incident Response のデプロイ後

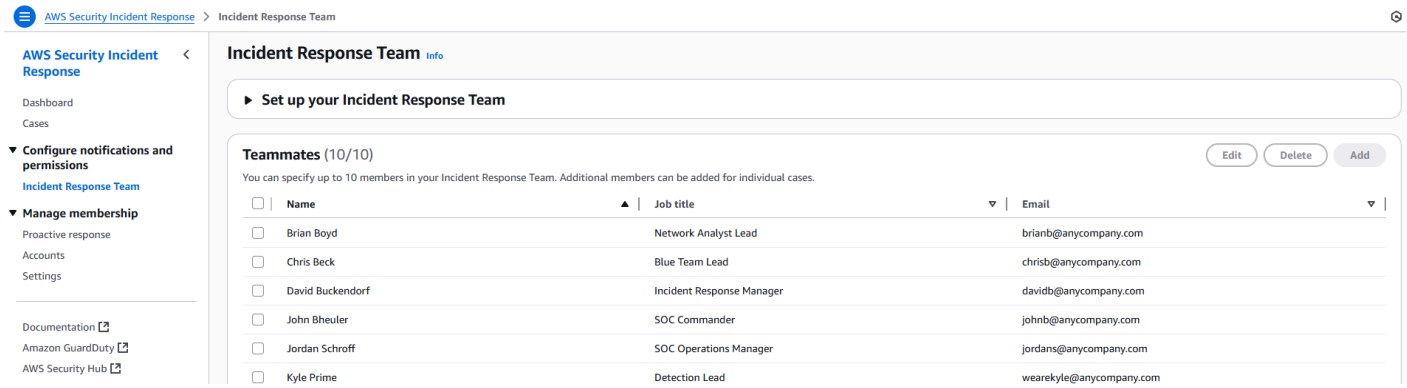
AWS は、既存のインシデント対応フレームワークを置き換える代わりに、それと統合します。

1. 運用統合機能を確認して、現在のプラクティスを強化してください。
2. OU レベルのメンバーシップサポートのデモ、EventBridge の活用、ならびに Jira-ITSM との統合を視聴して、より効率的なセキュリティ運用を実現してください。

   AWS Security Incident Response: New integrations and OU-level subscription

インシデント対応チームを更新する

1. サブスクライブ済みであることと、この オンボーディングガイド で説明されているオンボーディングステップが完了していることを確認します。
2. 左側のナビゲーションからインシデント対応チームを選択します。
3. チームに追加するチームメイトを選択します。



> **Note**
>
> チームには、組織のリーダーシップ、法律顧問、MDR パートナー、クラウドエンジニアなどが含まれます。最大 10 人のメンバーを追加できます。各メンバーの名前、タイトル、E メールアドレスのみを含めます。

AWS がサポートするケース

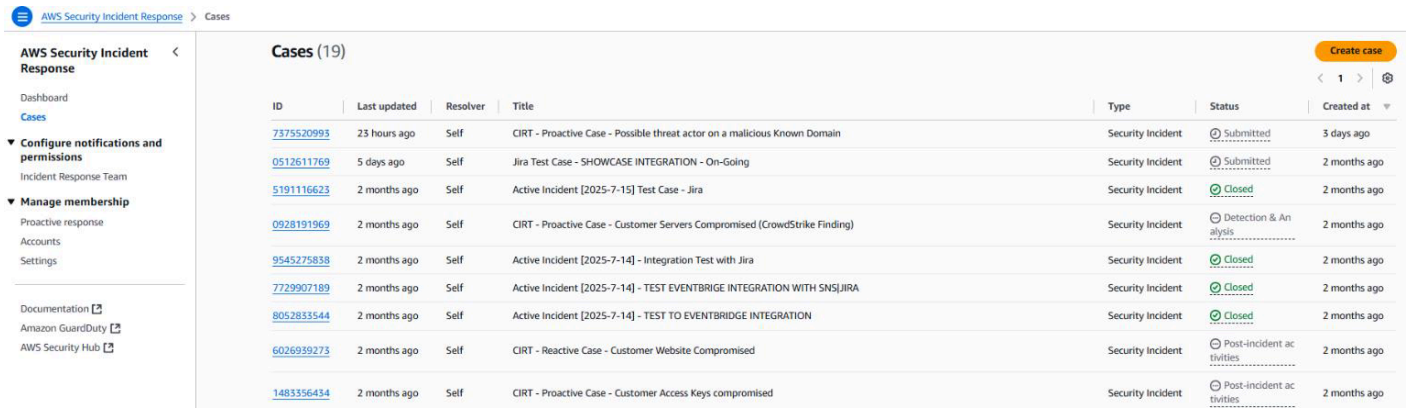
AWS Security Incident Response は、サブスクリプションベースのケース管理ポータルを提供します。ここでは、組織が Security Incident Response と直接やり取りします。15 分の SLO を使用して、セキュリティ調査とアクティブなインシデントを支援します。事後対応ケースに制限はありません。AWS サポート対象ケースの作成のドキュメントを参照してください。

調査チームの展開

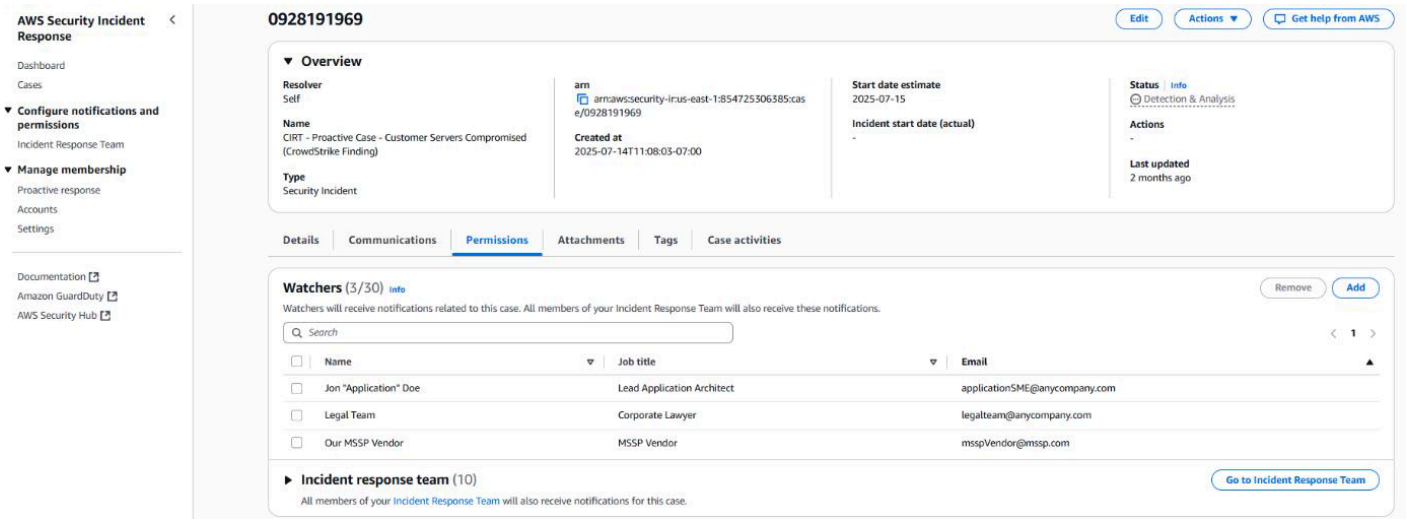
ケース管理ポータル経由でウォッチャーと IAM ポリシーを追加することで、ケースに対する可視性を外部関係者に付与できます。これらのオプションは、パートナー、法務チーム、または対象分野のエキスパートに使用します。

ウォッチャーをケースに追加するには:

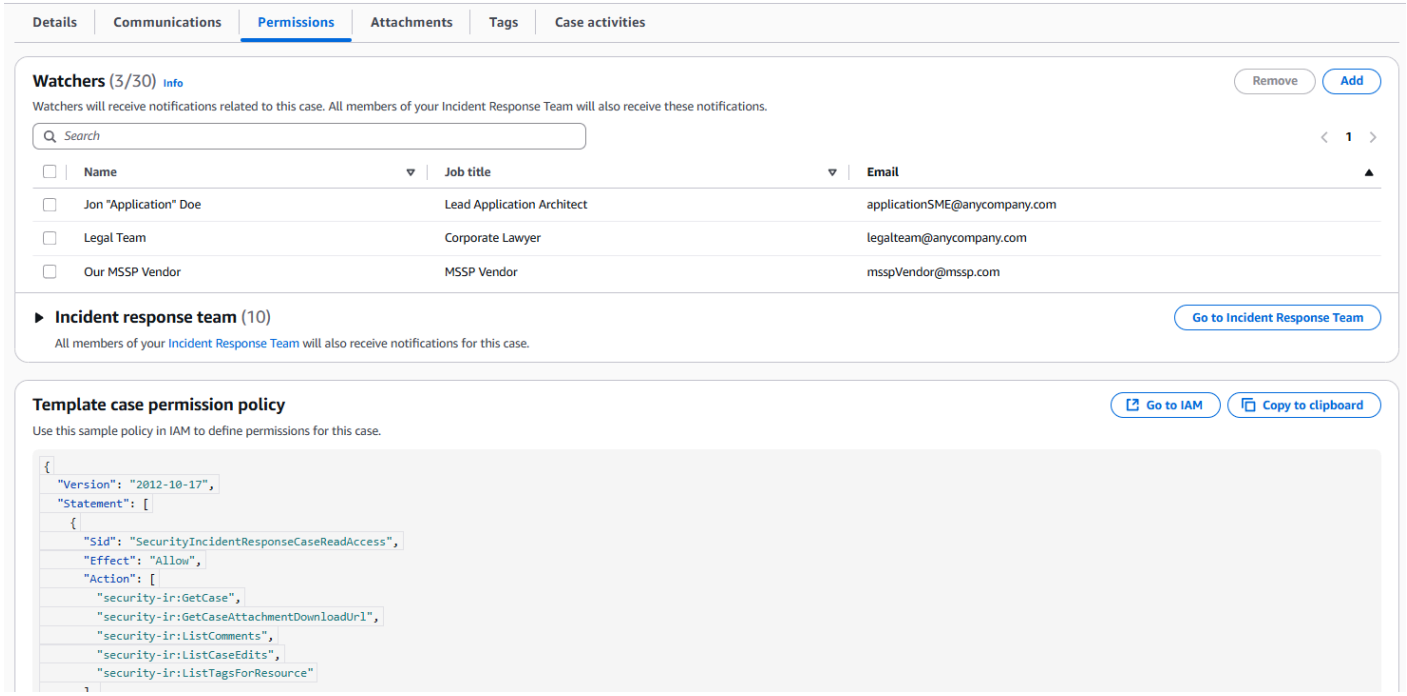
1. Security Incident Response ケースポータルから任意のケースを開きます。



2. [アクセス許可] タブを選択します。



3. [追加] を選択します。



> **Note**
>
> 各ケースには、当該ケースのみにアクセスを許可する事前設定済みの IAM ポリシーが含まれており、最小権限の原則が維持されます。このポリシーを、サードパーティの MDR パートナーや特定の調査チームが貢献できるように、IAM ロールまたはユーザーに直接コピー＆ペーストしてください。

GuardDuty の検出結果と抑制ルール

AWS Security Incident Response は、CrowdStrike、FortinetCNAPP (Lacework)、Trend Micro からのすべての Amazon GuardDuty 検出結果と AWS Security Hub CSPM 検出結果をプロアクティブに取り込み、トリアージして、応答します。当社の自動トリアージテクノロジーは、内部分析要件を排除します。このサービスは、GuardDuty と Security Hub で無害な検出結果に対する抑制ルールと自動アーカイブルールを作成します。Amazon GuardDuty コンソールの「検出結果」でこれらのルールを表示または変更します。

有効な GuardDuty 抑制ルールを確認するには、以下の手順を実行してください。

1. Amazon GuardDuty コンソールを開きます。
2. [検出結果] を選択します。
3. ナビゲーションペインで、[抑制ルール] を選択します。抑制ルール ページには、アカウントのすべての抑制ルールのリストが表示されます。
4. ルールの設定を確認または変更するには、ルールを選択し、アクション メニューから 抑制ルールの更新 を選択します。

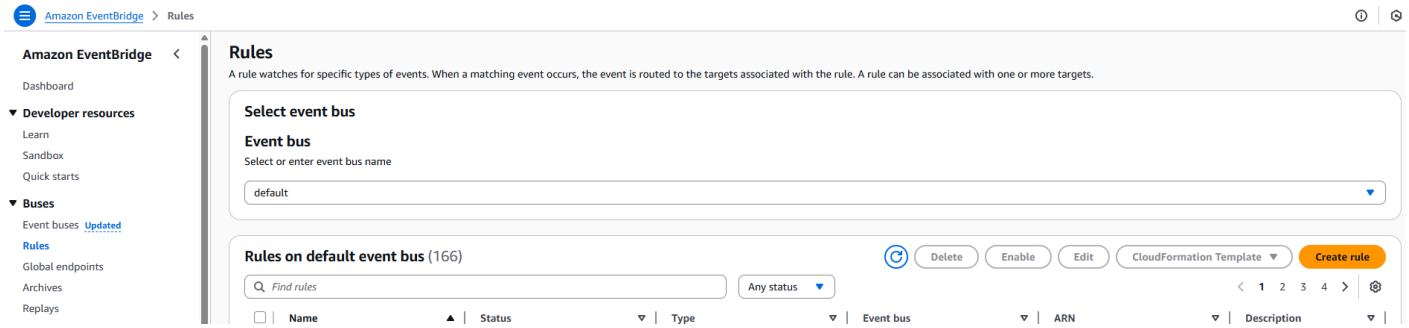
> **Note**
>
> SIEM テクノロジーを使用している組織では、GuardDuty 検出結果のボリュームが時間の経過とともに大幅に減少しており、Security Incident Response サービスと SIEM 両方の効率が向上しています。

Amazon EventBridge

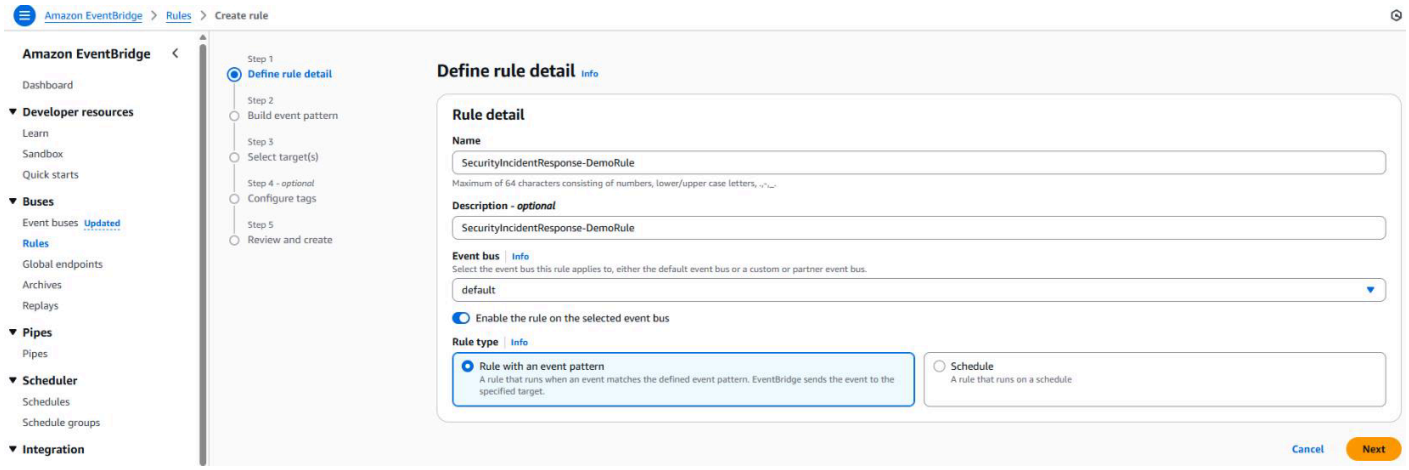
Amazon EventBridge は、セキュリティインシデント対応のイベント駆動型アーキテクチャを有効にし、ケースアクティビティがダウンストリームサービス (SNS、Lambda、SQS、Step-Functions) または外部ツール (Jira、ServiceNow、Teams、Slack、PagerDuty) をトリガーできるようにします。

EventBridge ルールを設定するには:

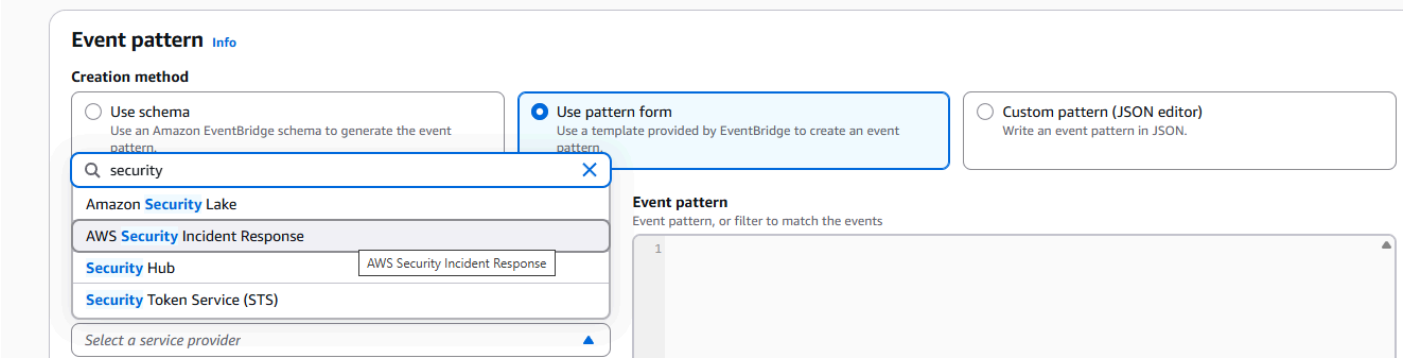
1. Amazon EventBridge にアクセスする
2. [バス] ドロップダウンから [ルール] を選択します。



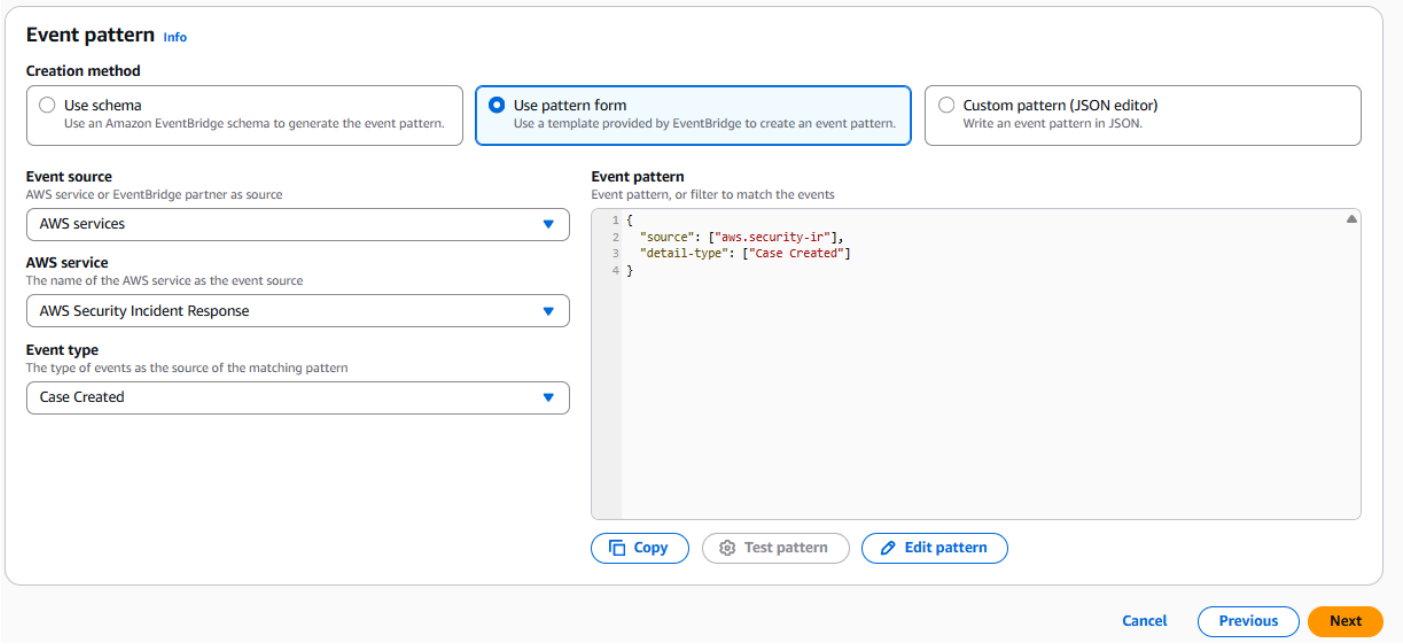
3. [Create Rule] (ルールの作成) を選択します。
4. ルールの詳細を入力します。
5. [次へ] を選択します。



6. [AWS サービス] にスクロールして、ドロップダウンメニューから [AWS Security Incident Response] を選択します。

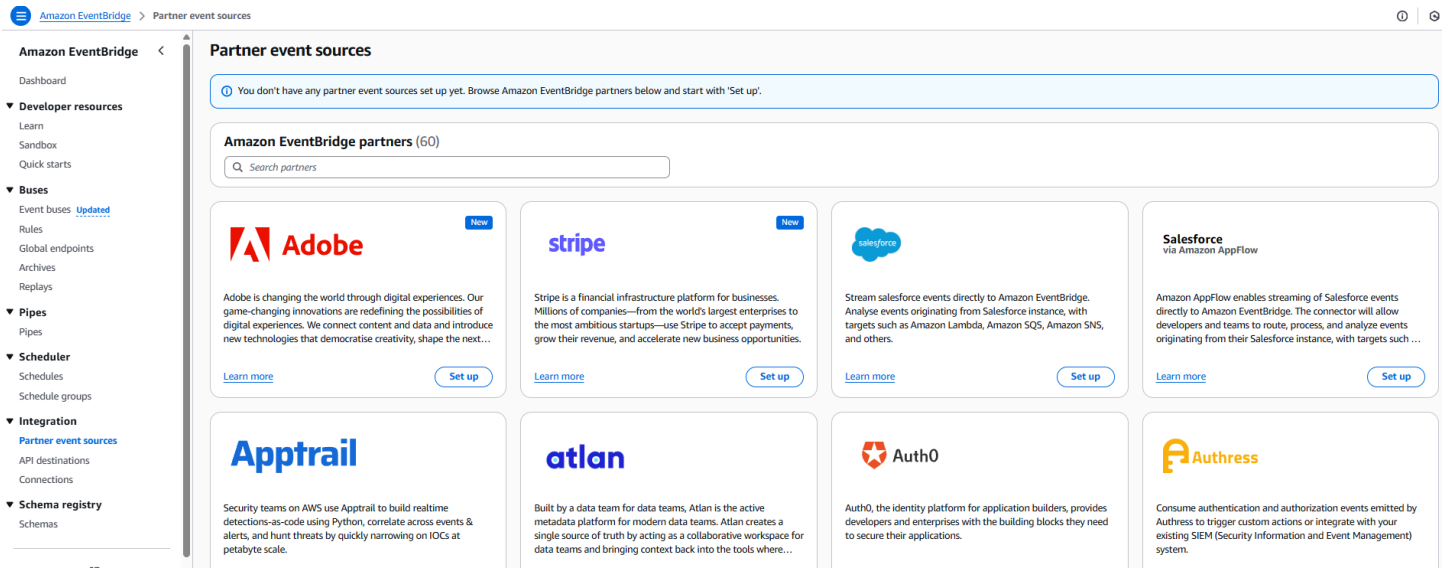


7. [イベントタイプ] ドロップダウンから、パターンを作成するイベントまたは API コールを選択します。
8. パターンは、手動で編集して複数のイベントを含めることができます。
9. [次へ] を選択します。



> **Note**
>
> イベントに 1 つ、または複数のターゲット (Amazon Simple Notification Service、AWS Lambda、SSM ドキュメント、Step-Function) を選択します。必要に応じて、クロスアカウントターゲットを設定します。

EventBridge 統合メニューの Partner Event Sources でパートナー統合パターンを確認できます。利用可能なパートナーには、Atlassian (Jira)、DataDog、New Relic、PagerDuty、Symantec、Zendesk などがあります。



統合と外部ツールワークフロー

JIRA または ServiceNow を Security Incident Response と統合するための AWS ソリューション

Jira および ServiceNow との双方向統合のために、完全に開発されたソリューションをデプロイします。これらの統合により、AWS Security Incident Response ケースと ITSM プラットフォーム間の双方向通信が可能になり、ケースの更新が対応する Jira タスクに自動的に反映されます。

統合の利点

既存の ITSM プラットフォームとの AWS Security Incident Response の統合は、インシデントの追跡と対応のワークフローを一元化することでセキュリティ運用を効率化します。これらの事前構築されたソリューションによってカスタム開発が不要になるため、セキュリティチームは AWS ネイティブなインシデント管理システムとエンタープライズ全体のインシデント管理システムの両方に対する可視性を維持できるようになります。イベント駆動の自動化向けの Amazon EventBridge を活用することで、更新がプラットフォーム間でリアルタイムかつシームレスに受け渡されるため、セキュリティインシデントがどこで発生しても、それらを一貫的に追跡できるようになります。この統合アプローチにより、セキュリティアナリストのコンテキスト切り替えが軽減され、対応時間が短縮され、インシデント対応ライフサイクル全体で包括的な監査証跡が提供されます。

EventBridge ルールを設定するには:

1. Amazon EventBridge にアクセスする

2. [バス] ドロップダウンから [ルール] を選択します。

外部ツールワークフロー

セキュリティインシデント対応は、複数の方法で外部ツールやパートナーと統合されます。

- SIEM 統合: Security Incident Response エンジニアは、AWS がサポートするケースが送信されたときに、お客様のチームと並行してこれらの検出結果を分析および調査するための支援を提供します。ハイブリッド環境とマルチクラウド環境間の相関関係を特定し、プロバイダー間の脅威アクターの動きをスコープするのに役立ちます。
- 既存のセキュリティオペレーションを強化: 従来の GuardDuty レスポンスワークフローをより効率的で並列なレスポンスモデルに置き換えます。現在、多くの組織がケース管理を通じた検出ワークフローに SIEM テクノロジーを利用しています。このサービスは、特に GuardDuty (および一部の Security Hub CSPM) の検出結果に対して効率的な代替手段を提供します。このソリューションは、高度な自動トリアージテクノロジーと人的監視を活用して、ポータルにプロアクティブケースを作成し、同時に対応チームに通知し、調整された修復作業のために当社のセキュリティインシデント対応エンジニアを関与させます。
- サードパーティーの調査チーム: 当社のセキュリティインシデント対応エンジニアは、パートナーや MDR プロバイダーと直接連携します。

付録 A: 連絡先

メタデータを事前にセキュリティインシデント対応エンジニアに提供いただくことで、プロファイル作成時間を短縮し、初期段階から当社のトリアージ技術の信頼性を向上させることができます。これは、脅威検出結果の取り込みとお客様の「既知の健全な環境」の作成を開始する際に特定される初期段階の誤検知を減らすために役立ちます。

IR および SOC 担当者連絡先情報

入力	IR | SOC 担当者: 役割、氏名、メールアドレス	プライマリエスカレーション連絡先とセカンダリエスカレーション連絡先	内部、既知の CIDR 範囲	外部、既知の CIDR 範囲	追加のクラウドサービスプロバイダー	作業 AWS リージョン	DNS サーバー IP (Amaz Route Resol 以外の場合)	VPN | リモートアクセスソリューションと IP アドレス	重要アプリケーション名 | アカウント番号	一般的ではないが広く使用されているポート	EDR | AV | 使用される脆弱性管理ツール	IDP | 拠点
1	SOC Commar 、John Smith、j	Prima	10.0.0 16	5.5.60 20 (Azure	Azure	us-east-1 、us-east-2	該当なし	Direct Connect パブリック VIF	Nginx Webserv (例: 重要) |	8080	CrowdSt ke Falcon	Entra、Azure

入力	IR | SOC 担当者: 役割、氏名、メールアドレス	プライマリエスカレーション連絡先とセカンダリエスカレーション連絡先	内部、既知の CIDR 範囲	外部、既知の CIDR 範囲	追加のクラウドサービスプロバイダー	作業 AWS リージョン	DNS サーバー IP (Amaz Route Resol 以外の場合)	VPN | リモートアクセスソリューションと IP アドレス	重要アプリケーション名 | アカウント番号	一般的ではないが広く使用されているポート	EDR | AV | 使用される脆弱性管理ツール	IDP | 拠点
	ith@exale.com							116.32.87	12345670			

入力	IR | SOC 担当者: 役割、氏名、メールアドレス	プライマリエスカレーション連絡先とセカンダリエスカレーション連絡先	内部、既知の CIDR 範囲	外部、既知の CIDR 範囲	追加のクラウドサービスプロバイダー	作業 AWS リージョン	DNS サーバー IP (Amaz Route Resol 以外の場合)	VPN | リモートアクセスソリューションと IP アドレス	重要アプリケーション名 | アカウント番号	一般的ではないが広く使用されているポート	EDR | AV | 使用される脆弱性管理ツール	IDP | 拠点

環境のメタデータ情報を送信するには、 AWS サポートケース を作成します。

メタデータを送信するには

1. メタデータテーブルに環境情報を入力します。
2. 以下の詳細を含む AWS サポート ケースを作成します。
   - ケースタイプ: テクニカル
   - サービス: セキュリティインシデント対応サービス
   - カテゴリ: その他
3. 完成したメタデータテーブルをケースに添付します。

RACI マトリックス

次の RACI マトリックスは、セキュリティインシデント対応の実装プロセス全体のロールと責任を定義します。RACI は、責任 (Responsible (R))、説明責任 (Accountable (A))、協議 (Consulted (C))、情報提供 (Informed (I)) の略です。

アクティビティ	お客様	AWS アカウントチーム	SIR チーム
オンボーディング前			
主要な利害関係者を特定する	R		I
検出結果のソースを検証する	R	C	I
[サードパーティー EDR 統合] Security Hub CSPM	R	C	I
GuardDuty 検証/ヘルスチェック	C	R	I
アカウントスコープを決定する	R		
エスカレーションプロトコルを確立する	R	I	C
AWS Organizations を有効にする	R	C	
アカウントを AWS Organizations に関連付ける	R	I	

アクティビティ	お客様	AWS アカウントチーム	SIR チーム
委任管理者/セキュリティツールアカウントを選択する	R	I	
オンボーディング			
メンバーシップの詳細を設定する	R	I	
チュートリアル (プロアクティブレスポンスとアラートのトリアージワークフローをセットアップする、サービスリンクロールを管理アカウントにデプロイする、封じ込めアクションを承認する)	R	C	I
デプロイ後の設定			
運用上の統合機能を確認する	R	C	I
セキュリティインシデント対応の事後対応ケースを送信する	R		
Amazon EventBridge との統合を設定する	R	C	C
サードパーティーツールを接続する (Jira、ServiceNow、PagerDuty、Teams など)	R	I	C
サービスの詳細とデモ	A	R	C

RACI の定義:

- 責任 (Responsible (R)) - タスクを完了するために作業を実行する当事者
- 説明責任 (Accountable (A) - タスクの正しい完了について最終的に回答できる当事者
- 協議 (Consulted (C) - 意見が求められ、双方向のコミュニケーションがある当事者

- 情報提供 (Informed (I) - 進捗状況を最新の状態に維持し、一方向のコミュニケーションがある当事者

メンバーアカウントを選択する

メンバーシップアカウントは、アカウントの詳細の設定、インシデント対応チームの詳細の追加と削除、およびすべてのアクティブなセキュリティイベントと履歴セキュリティイベントの作成と管理に使用できる AWS アカウントです。AWS Security Incident Response メンバーシップアカウントは、Amazon GuardDuty や AWS Security Hub CSPM などのサービス向けに有効化したものと同じアカウントに一致させることをお勧めします。

AWS Organizations を使用した AWS Security Incident Response メンバーシップアカウントの選択には 2 つのオプションがあります。Organizations の管理アカウントまたは Organizations の委任管理者アカウントでメンバーシップを作成できます。

委任管理者アカウントを使用する: AWS Security Incident Response 管理タスクとケース管理は、委任管理者アカウント内にあります。他の AWS セキュリティおよびコンプライアンスサービスに設定したのと同じ委任管理者を使用することをお勧めします。12 桁の委任管理者アカウント ID を指定し、そのアカウントにログインして続行します。

Important

セットアップの一環として委任管理者アカウントを使用する場合、AWS Security Incident Response は必要なトリアージのサービスリンクロールを AWS Organizations 管理アカウントで自動作成できません。
IAM を使用して、AWS Organizations 管理アカウントにこのロールを作成できます

サービスにリンクされたロールを作成するには (コンソール)

1. AWS Organizations 管理アカウントにログインします。
2. AWS CloudShell ウィンドウにアクセスするか、任意の方法を使って CLI 経由でアカウントにアクセスします。
3. CLI コマンド `aws iam create-service-linked-role --aws-service-name "triage.security-ir.amazonaws.com" --no-cli-pager` を使用する
4. (オプション) コマンドが機能したことを確認するには、コマンド `aws iam get-role --role-name AWSServiceRoleForSecurityIncidentResponse_Triage` を実行できます

現在ログインしているアカウントを使用する: このアカウントを選択すると、現在のアカウントが AWS Security Incident Response メンバーシップの中心となるメンバーシップアカウントとして指定されます。組織内の個人は、このアカウントを通じてサービスにアクセスして、アクティブケースと解決済みケースを作成、アクセス、管理する必要があります。

AWS Security Incident Response を管理するための十分なアクセス許可があることを確認してください。

アクセス許可を追加する具体的な手順については、「IAM ID のアクセス許可の追加および削除」を参照してください。

「AWS Security Incident Response managed policies」を参照してください。

IAM アクセス許可を確認するには、以下の手順に従います。

- IAM ポリシーを確認する: ユーザー、グループ、またはロールに添付されている IAM ポリシーを確認して、必要なアクセス許可が付与されていることを確認します。これを行うには、https://console.aws.amazon.com/iam/ に移動し、`Users` オプションを選択し、特定のユーザーを選択し、概要ページで、添付されたすべてのポリシーのリストを表示できる `Permissions` タブに移動します。各ポリシー行を展開して詳細を表示できます。
- アクセス許可をテストする: アクセス許可を検証するために必要なアクションを実行してみてください。例えば、ケースにアクセスする必要がある場合は、`ListCases` を実行してみてください。必要なアクセス許可がない場合は、エラーメッセージが表示されます。
- AWS CLI または SDK を使用する: AWS Command Line Interface または、任意のプログラミング言語の AWS SDK を使用して、アクセス許可をテストできます。例えば、AWS Command Line Interface を使用している場合、`aws sts get-caller-identity` コマンドを実行して現在のユーザーのアクセス許可を確認できます。
- AWS CloudTrail ログを確認する: CloudTrail ログを確認 して、実行しようとしているアクションがログに記録されているかどうかを確認します。これにより、アクセス許可の問題を特定できます。
- IAM ポリシーシミュレーターを使用する: IAM ポリシーシミュレーターは、IAM ポリシーをテストし、それがアクセス許可に与える影響を確認できるツールです。

> **Note**
>
> 特定のステップは、AWS サービスや実行しようとしているアクションに応じて異なる場合があります。

メンバーシップの詳細を設定する

- メンバーシップとケースを保存する AWS リージョン を選択します。

> **Warning**
>
> 初回メンバーシップ登録後にデフォルトの AWS リージョン を変更することはできません。

- 完全なメンバーシップカバレッジを AWS Organizations 全体に提供するか、組織単位 (OU) を使用して AWS Organizations の一部に提供するかを選択します。
- オプションで、このメンバーシップの名前を選択できます。
- メンバーシップ作成ワークフローの一部としてプライマリ連絡先とセカンダリ連絡先を提供する必要があります。これらの連絡先は、インシデント対応チームの一部として自動的に含まれます。1 つのメンバーシップに対して少なくとも 2 つの連絡先が存在する必要があります。これにより、少なくとも 2 つの連絡先がインシデント対応チームに含まれるようになります。
- メンバーシップのオプションタグを定義します。タグは、AWS コストを追跡し、リソースを検索するのに役立ちます。

アカウントを AWS Organizations に関連付ける

セットアップ中に AWS Organizations 全体を関連付けることを選択した場合、組織内のすべてのメンバーアカウントにメンバーシップ資格が付与されます。関連付けられたアカウントは、アカウントが組織に追加または削除されると自動的に更新されます。

セットアップ中に AWS Organizations の一部を関連付けることを選択し、メンバーシップを特定の組織単位 (OU) に制限した場合、選択した OU 内すべてのアカウントにメンバーシップ資格が付与されます。これには、選択した OU のサブ OU の下にあるアカウントが含まれます。関連付けられたアカウントは、アカウントが OU に追加または削除されるたびに自動更新されます。

組織単位に関するベストプラクティスの詳細については、「Organizing Your AWS Environment Using Multiple Accounts」を参照してください。

プロアクティブレスポンスとアラートのトリアージワークフローを設定する

AWS Security Incident Response は、Amazon GuardDuty と Security Hub CSPM の統合から生成された脅威アラートを監視して調査します。この機能を使用するには、Amazon GuardDuty を有効にする必要があります。AWS Security Incident Response は、サービス自動化を使用して優先度の低いアラートをトリアージし、チームが最も重要な問題に集中できるようにします。AWS Security Incident Response が Amazon GuardDuty および AWS Security Hub CSPM とどのように連携するかの詳細については、ユーザーガイドの「検出と分析」セクションを参照してください。

オンボーディング問題が発生した場合は、AWS サポート ケースを作成して追加のサポートを受けてください。AWS アカウント ID やセットアッププロセス中に発生した可能性のあるエラーなどの詳細を必ず含めてください。

> **Note**
>
> Amazon GuardDuty 抑制ルール、アラートのトリアージ設定、またはプロアクティブレスポンスのワークフローに関する質問については、[調査と問い合わせ] ケースタイプを使用して AWS がサポートするケースを作成し、AWS Security Incident Response チームに相談することができます。詳細については、AWS でサポートされているケースを作成するを参照してください。

この機能を使用すると、AWS Security Incident Response は対象のすべてのアカウント、および組織でサポートされているアクティブな AWS リージョンの検出結果をモニタリングおよび調査できます。この機能を実現するために、AWS Security Incident Response は AWS Organizations 内の対象のすべてのメンバーアカウントのサービスにリンクされたロールを自動的に作成します。ただし、管理アカウントの場合、モニタリングを有効にするには、サービスにリンクされたロールを手動で作成する必要があります。

サービスは、サービスにリンクされたロールを管理アカウント内に作成できません。このロールは、AWS CloudFormation スタックセットを使用 して管理アカウント内に手動で作成する必要があります。

プロアクティブ対応による自動アーカイブを理解する

プロアクティブ対応とアラートのトリアージを有効にすると、AWS Security Incident Response が Amazon GuardDuty と Security Hub CSPM のセキュリティ検出結果を自動的にモニタリングしてト

リアージします。この自動トリアージワークフローの一環として、検出結果は次の基準に基づいて自動的にアーカイブされます:

自動アーカイブの動作:

- 無害な検出結果: 自動トリアージプロセスによって検出結果が無害 (真のセキュリティ脅威ではない) であると判断された場合、AWS Security Incident Response は検出結果を Amazon GuardDuty に自動的にアーカイブし、抑制ルールを作成して、今後同様の検出結果がアラートを生成しないようにします。
- 抑制ルール: このサービスは、環境の既知の正常なパターン (予想される IP アドレス、IAM エンティティ、通常の運用動作など) に一致する検出結果に対し、Amazon GuardDuty と Security Hub CSPM の両方で抑制ルールと自動アーカイブルールを作成します。
- アラートボリュームの削減: SIEM テクノロジーを使用している組織では、サービスが組織の環境を学習し、無害な検出結果を自動的にアーカイブしていくにつれて、Amazon GuardDuty の検出結果ボリュームが大幅に減少します。これにより、AWS Security Incident Response のサービスと SIEM の両方の効率が向上します。

アーカイブされた検出結果の表示:

自動的にアーカイブされた検出結果と、AWS Security Incident Response によって作成された抑制ルールを確認できます:

1. [Amazon GuardDuty コンソール] に移動する
2. [検出結果] を選択する
3. 検出結果フィルターから [アーカイブ済み] を選択する
4. 各ルールの横にある下矢印を選択して、抑制ルールを確認する

重要な考慮事項:

- アーカイブされた検出結果は 90 日間 Amazon GuardDuty に保持され、その期間中いつでも表示することができます
- 抑制ルールは、Amazon GuardDuty コンソールからいつでも変更または削除できます
- 自動トリアージプロセスは、継続的に環境に適応し、時間の経過とともに精度を向上させ、誤検出を削減します

封じ込め: セキュリティインシデントが発生した場合、AWS Security Incident Response は、侵害されたホストの分離や認証情報のローテーションなど、封じ込めアクションを実行して、影響を迅速に軽減できます。Security Incident Response では、封じ込め機能がデフォルトで有効化されていません。これらの封じ込めアクションを実行するには、まずサービスに必要なアクセス許可を付与する必要があります。これは、必要なロールを作成する AWS CloudFormation StackSet をデプロイすることで実行できます。

ユーザータスク

内容

ダッシュボード

AWS Security Incident Response コンソールでは、ダッシュボードにインシデント対応チームの概要、プロアクティブレスポンスのステータス、4 週間のケースのローリングカウントが表示されます。

インシデント対応チーム

[インシデント対応チームを表示] を選択すると、インシデント対応チームメイトの詳細にアクセスできます。

自分のケース

ダッシュボードの [My Cases] セクションには、オープンおよびクローズされた AWS でサポートされているケースの数と、定義された期間内に割り当てられたセルフマネージドケースが表示されます。また、クローズされたケースの解決にかかった平均時間を時間単位で示します。

インシデント対応チームの管理

インシデント対応チームには、インシデント対応プロセスのステークホルダーが含まれます。メンバーシップの一部として、最大 10 人のステークホルダーを設定できます。

内部ステークホルダーの例としては、インシデント対応チームのメンバー、セキュリティアナリスト、アプリケーション所有者、およびセキュリティリーダーシップチームなどがあります。

外部ステークホルダーの例としては、インシデント対応プロセスに含める独立系ソフトウェアベンダーやマネージドサービスプロバイダー (MSP) の個人が含まれます。

> **Note**
>
> インシデント対応チームをセットアップしても、チームメイトにメンバーシップやケースなどのサービスリソースへのアクセスは自動的に付与されません。AWS Security Incident

Response の AWS マネージドポリシーを使用して、リソースへの読み取りおよび書き込みアクセスを許可できます。詳細については、こちらをクリックしてください。

メンバーシップレベルで指定されたインシデント対応チームメイトは、すべてのケースに自動的に追加されます。ケースの作成後は、いつでも個々のチームメイトを追加または削除できます。

インシデント対応チームは、[コミュニケーション設定] に記載されているイベントに関する E メール通知を受け取ります。

通信設定

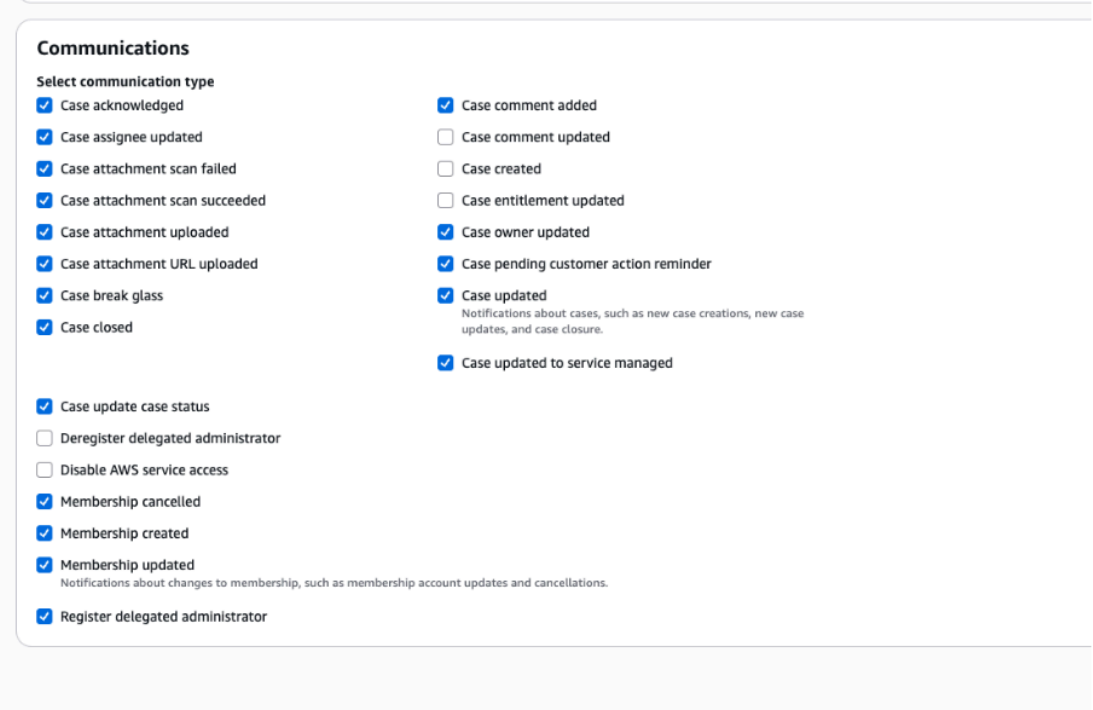
セキュリティインシデント発生時に通知の受信方法やインシデント対応システムとの連携方法を制御するため、通信設定を構成してください。

チームコミュニケーション設定の管理

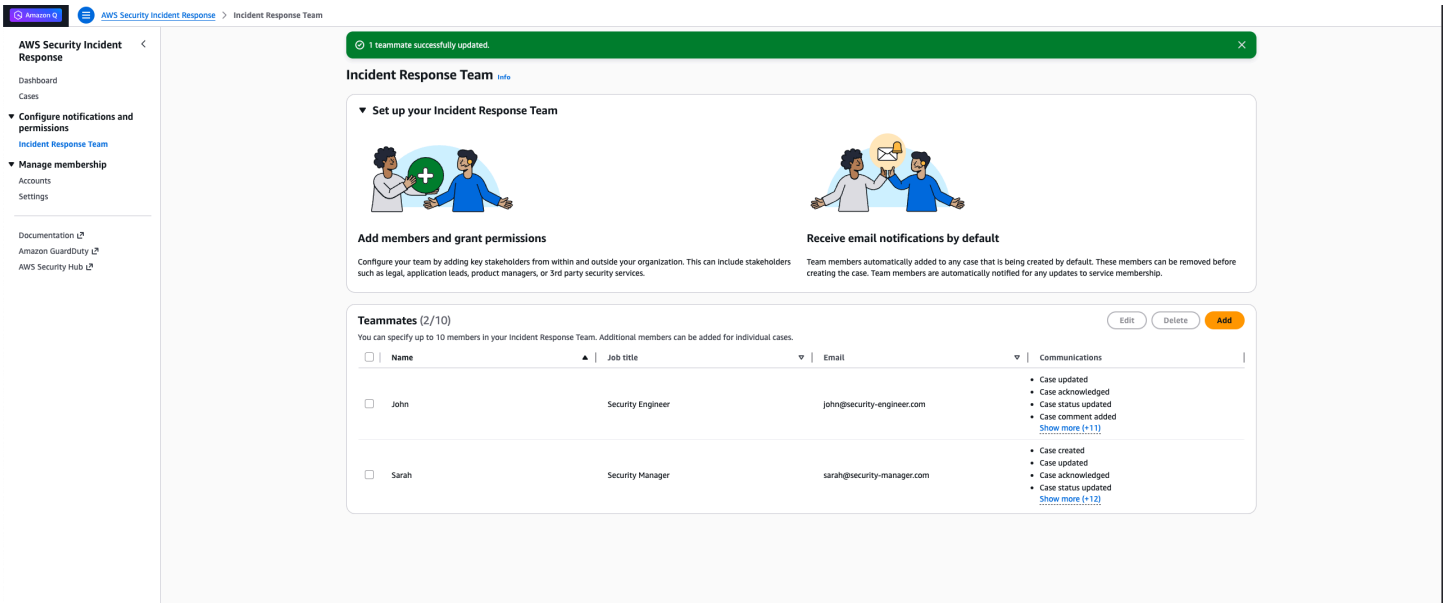
インシデント対応チームのメンバーごとに、ダッシュボードページから連絡先の設定を変更できます。

チームメンバーのコミュニケーション設定を管理するには、次の手順に従います。

1. ダッシュボードからインシデント対応チームページに移動する
2. 次のいずれかを行います。
   - 既存のチームメンバーを更新するには: コミュニケーション設定を変更するチームメイトを選択し、[編集] を選択します
   - 新しいチームメンバーを追加するには: [追加] を選択します
3. フォームの下部に「通信」が表示されます
   a. 受信する通信のチェックボックスをオンにします。
   b. 受信しない通信のチェックボックスをオフにします。



4. 変更内容を保存します。



デフォルトの通信設定

デフォルトでは、インシデント対応チームのメンバーはすべてのコミュニケーションを有効にします。上記の手順を使用して、この設定はいつでも変更することができます。

通信オプション

コミュニケーション設定は、インシデント対応システムとのやり取り方法と、セキュリティインシデント発生時の通知の配信方法を制御します。

> **Note**
>
> これらの設定は、セキュリティインシデント対応システム内の今後のすべての通信に適用されます。上記の手順を繰り返すことで、これらの設定をいつでも変更できます。

AWS Organizations へのアカウントの関連付け

AWS Security Incident Response を有効にすると、組織全体または特定の組織単位 (OU) を選択するオプションが表示されます。特定の OU が選択されている場合、メンバーシップは選択された OU 内に存在するアカウントのみを対象とします。組織全体が選択されている場合、メンバーシップは組織内のすべてのアカウントを対象とします。

詳細については、「AWS Organizations を使用した AWS Security Incident Response アカウントの管理」を参照してください。

メンバーシップカバレッジの管理

組織全体のカバレッジから特定の OU への切り替えなど、メンバーシップカバレッジオプションはいつでも変更できます。

OU 関連付けの更新

メンバーシップカバレッジを管理するには:

1. [アカウント関連付け設定] ページに移動します
2. [OU を追加] を選択して、メンバーシップに関連付ける OU を選択します
3. メンバーシップに関連付ける OU を選択します
4. [関連付けを更新] をクリックして、メンバーシップの OU の関連付けを保存します

関連付けを更新したら、同じページに戻り、メンバーシップから関連付けを解除する OU を削除できます。この柔軟性は、最初に組織全体を選択した場合でも適用されます。後でメンバーシップを更

新して、サービスをキャンセルして再度有効にすることなく、特定の OU のみを対象にすることができます。

詳細については、「組織単位 (OU) によるメンバーシップの管理」を参照してください。

重要な考慮事項

ルート直下のアカウント: メンバーシップの特定の OU を選択する場合、組織ルートの直下にあるアカウント (OU の一部ではない) はメンバーシップに関連付けられることはありません。これらのアカウントをメンバーシップカバレッジに含めるには、まずアカウントを OU に追加してから、その OU をメンバーシップに関連付ける必要があります。

> **Note**
>
> 当社では OU 関連付けのユーザーエクスペリエンスを継続的に改善し、プロセスをより直感的でわかりやすいものにしています。

モニタリングと調査

AWS セキュリティインシデント対応は、Amazon GuardDuty と AWS Security Hub CSPM のセキュリティアラートを確認してトリアージし、環境に基づいて抑制ルールを設定して不要なアラートを防ぎます。AWS Security Incident Response エンジニアリング (SIRE) チームは、検出結果を調査し、問題を迅速にエスカレートするとともに、潜在的な問題を迅速に封じ込めるようにユーザーのチームをガイドします。必要に応じて、ユーザーに代わって封じ込めアクションを実装する AWS Security Incident Response アクセス許可を付与できます。

AWS Security Incident Response は、NIST 800-61r2 Computer Security event Handling Guide for Security event Response に準拠しています。この業界標準に準拠することで、AWS Security Incident Response はセキュリティイベント管理に一貫したアプローチを提供し、AWS 環境内のセキュリティイベントの保護と対応に関するベストプラクティスに従います。

AWS Security Incident Response がセキュリティアラートを特定するか、セキュリティ支援をリクエストすると、AWS SIRE が調査します。チームは、GuardDuty アラートなどの口グイベントとサービスデータを収集し、そのデータをトリアージして分析し、修復と封じ込めのアクティビティを実行し、インシデント後のレポートを提供します。

内容

- 検出と分析
- AI 調査エージェント
- 封じ込め
- 根絶
- 復旧
- インシデント後レポート

準備

AWS Security Incident Response チームは、セキュリティイベント対応ライフサイクル全体を通じて調査を行い、お客様と提携します。セキュリティイベントが発生する前に、このチームを設定し、必要なアクセス許可を割り当てることをお勧めします。

検出と分析

イベントの報告

AWS Security Incident Response ポータルからセキュリティイベントを報告できます。セキュリティイベントの発生中は待機しないことが重要です。AWS Security Incident Response は自動および手動の手法を使用して、セキュリティイベントを調査し、ログを分析し、異常なパターンを探します。お客様の協力と環境の理解は、この分析を加速させます。

サポートされている検出ソースの有効化

> **Note**
>
> AWS Security Incident Response サービスコストには、サポートされている検出ソースや他の AWS サービスの使用に関連する使用料やその他のコスト、料金は含まれません。コストの詳細については、個々の機能またはサービスページを参照してください。

Amazon GuardDuty

組織全体で GuardDuty を有効にするには、「Amazon GuardDuty ユーザーガイド」の「`Setting up GuardDuty`」セクションを参照してください。

サポートされているすべての AWS リージョン で GuardDuty を有効にすることを強くお勧めします。これにより、GuardDuty はアクティブに使用されていないリージョンでも、許可されていな

いアクティビティや異常なアクティビティに関する検出結果を生成できます。詳細については、「Amazon GuardDuty Regions and endpoints」を参照してください

GuardDuty を有効にすると、AWS Security Incident Response は重大な脅威検出データにアクセスし、AWS 環境内の潜在的なセキュリティ問題を特定して対応できるようになります。

AWS Security Hub CSPM

Security Hub CSPM は、複数の AWS サービスおよびサポートされているサードパーティーのセキュリティソリューションからセキュリティ検出結果を取り込むことができます。これらの統合により、AWS Security Incident Response は他の検出ツールからの検出結果をモニタリングおよび調査できるようになります。

Security Hub CSPM と Organizations の統合を有効にするには、「AWS Security Hub CSPM ユーザーガイド」を参照してください。

Security Hub CSPM で統合を有効にするには、複数の方法があります。サードパーティー製品の統合では、AWS Marketplace から統合を購入して設定することが必要になる場合があります。統合情報には、これらのタスクを完了するためのリンクが含まれます。AWS Security Hub CSPM 統合を有効にする方法の詳細については、こちら をご覧ください。

AWS Security Incident Response は、AWS Security Hub CSPM と統合されている場合、次のツールからの検出結果をモニタリングおよび調査できます。

- CrowdStrike – CrowdStrike Falcon
- Lacework – Lacework
- Trend Micro – Cloud One

これらの統合を有効にすることで、AWS Security Incident Response のモニタリングおよび調査機能の範囲と有効性を大幅に強化できます。

検出

「プロアクティブ対応」が有効になっている場合 (https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html)、AWS Security Incident Response はオンボーディング中にアカウントにデプロイされる Amazon EventBridge ルールを通じて、Amazon GuardDuty と AWS Security Hub CSPM の検出結果を取り込みます。

AWS Security Incident Response は、自動トリアージ中に、良性である、または予想されるアクティビティに関連付けられていると判断された Amazon GuardDuty の検出結果を自動的にアーカイブし

ます。Amazon GuardDuty コンソールでアーカイブされた検出結果を表示するには、検出結果のステータスフィルターから [アーカイブ済み] を選択します。詳細については、「Amazon GuardDuty ユーザーガイド」の「GuardDuty コンソールで生成された検出結果を表示する」を参照してください。

AWS Security Incident Response は、自動トリアージ中に、良性である、または予想されるアクティビティに関連付けられていると判断された Amazon GuardDuty の検出結果を自動的にアーカイブします。このアーカイブは、トリアージされ、結果が「アーカイブ」と指定された検出結果に対してのみ発生します。アクティブな調査の検出結果は、調査が終了した後も Amazon GuardDuty コンソールに表示されます。Amazon GuardDuty コンソールでアーカイブされた検出結果を表示するには、検出結果フィルターから [アーカイブ済み] を選択します。アーカイブされた検出結果の使用の詳細については、「Amazon GuardDuty ユーザーガイド」の「検出結果を使用する」を参照してください。

AWS Security Hub CSPM がセキュリティ検出結果を取り込むと、システムは自動トリアージが開始されたことを示すメモを使用して各検出結果を更新します。ワークフローの状態が NEW (新規) から NOTIFIED (通知済み) に変更され、その検出結果がデフォルトの AWS Security Hub CSPM 検出結果ビューから削除されます。トリアージにより、検出結果が良性である、または予想されるアクティビティに関連付けられていると判断された場合、システムは検出結果にメモを追加し、ワークフローの状態を SUPPRESSED (抑制) に更新します。

分析: 自動トリアージ

AWS Security Incident Response は、セキュリティ検出結果を自動的にトリアージします。トリアージプロセスでは、検出結果のペイロード、AWS サービスメタデータ、AWS ログ記録とモニタリングデータ (AWS CloudTrail や VPC フローログなど)、AWS 脅威インテリジェンス、および AWS とオンプレミス環境に関して提供するよう招待されたコンテキストなど、複数のソースからのデータを分析することで、検出されたアクティビティが予想される動作を表すかどうかを決定します。

自動トリアージが、検出されたアクティビティが予想されると判断した場合、システムはそれ以上の調査アクションを実行しません。

分析: インシデント対応セキュリティ調査

AWS Security Incident Response エンジニアリングは、AWS とセキュリティインシデント対応に関する専門知識を持つ、グローバルで常に利用可能なセキュリティプロフェッショナルのチームです。自動トリアージが、アクティビティが予想されると判断できない場合、AWS Security Incident Response エンジニアリングはセキュリティ調査を実行します。イベントが Security Hub から取り込まれた場合、AWS Security Incident Response エンジニアリングの調査が進行中であることを示すメモが関連する検出結果に投稿されます。

AWS Security Incident Response エンジニアリングは、追加のサービスメタデータと脅威インテリジェンスを分析し、ユーザーの環境での過去の検出結果と調査からのインサイトを確認し、インシデント対応の専門知識を適用することで、実践的なセキュリティ調査を行います。封じ込めの設定に応じて (「封じ込め」を参照)、AWS セキュリティインシデント対応エンジニアリングは、検出されたアクティビティが予想され承認されているかどうかを確認するために、AWS Security Incident Response コンソールのセキュリティインシデント対応ケースを通じて組織のインシデント対応チームを関与させる場合があります (AWS 生成されたケースへの対応)。

コミュニケーションを行う

AWS セキュリティインシデント対応は、セキュリティインシデント対応ケースを通じてインシデント対応チームを関与させることで、セキュリティ調査中に情報を提供します。複数の AWS Security Incident Response エンジニアリングメンバーが調査をサポートしている場合があります。コミュニケーションには、セキュリティ調査の作成の確認または通知、通話ブリッジの確立、ログファイルなどのアーティファクトの分析、予想されるアクティビティの確認のリクエスト、および調査結果の共有が含まれる場合があります。

AWS Security Incident Response がインシデント対応チームをプロアクティブに関与させると、AWS Security Incident Response メンバーシップアカウントにケースが作成され、すべての組織アカウントのコミュニケーションが 1 か所に一元化されます。これらのケースには、タイトルに「[Proactive case]」プレフィックスが含まれており、AWS Security Incident Response によって開始されたものとして識別されます。これらのコミュニケーションに積極的に関与し、タイムリーに対応することで、インシデント対応チームは以下の作業を行うために AWS Security Incident Response を支援できます:

- 実際のセキュリティインシデントに迅速に対応できます。
- 環境と予想される動作を理解する。
- 時間の経過とともに誤検出の検知を削減する。

AWS Security Incident Response の有効性はユーザーの協力によって向上し、より効率的にモニタリングされる安全な AWS 環境につながります。

検出結果の更新

AWS Security Incident Response は、ソースとトリアージの結果に応じて、検出結果を異なる方法で管理します。

サービスチューニング

アカウントサービスクォータで許可されている場合、AWS Security Incident Response は Amazon GuardDuty 抑制ルール または AWS Security Hub CSPM 自動化ルールのデプロイを試みます。これらのルールは、既知の承認されたアクティビティのタイプとソース (送信元 IP アドレス、ASN、ID プリンシパル、リソースなど) に一致する今後の検出結果を抑制します。AWS Security Hub CSPM ルールは優先度 10 でデプロイされるため、必要に応じてこれらの自動化を自己定義ルールで上書きできます。

このようにして、AWS Security Incident Response は AWS 環境で予想される動作に基づいて検出ソースを調整します。これらのルールセットの変更は、インシデント対応チームに通知され、変更はリクエストに応じてロールバックされます。

AI 調査エージェント

概要:

AI 搭載の調査エージェントは、お客様や AWS Security Incident Response エンジニアと協力してセキュリティ調査を迅速化します。お客様が AWS がサポートするケースを作成すると、エージェントはセキュリティインシデント対応エンジニアの関与と並行して自動的にアクティブ化され、解決時間が数日から数時間に短縮されます。

お客様からのエスカレーション中に、セキュリティインシデント対応ケースは、ユーザーによって作成されるか、AWS Security Incident Response によってプロアクティブに作成される場合があります。新しい AWS がサポートするケースが作成されると、調査エージェントが自動的にトリガーされます。すべてのケースは、コンソール、API、または Amazon EventBridge 統合を通じて管理できます。

主な利点

- 並列調査 – エージェントは対応者と同時に活動し、AI による自動化と人間の専門知識の両方を提供します。
- 自動化された証拠収集 – AWS CloudTrail、IAM、Amazon EC2、および Cost Explorer を自動的にクエリすることで、手動ログ分析を排除します。
- 自然言語インターフェイス – AWS ログ形式に関する専門知識を必要とせずに、セキュリティ上の懸念を平易な言語で記述します。
- より迅速な対応 — 調査タブで数分以内に調査概要を確認できます。
- 完全な監査可能性 – すべてのエージェントアクションは、AWS CloudTrail ロールのもとで `AWSServiceRoleForSupport` ログとして記録されます。

> **Important**
>
> この機能は、 AWSがサポートするケースでのみ利用可能です。セルフマネージドケースには AI 調査機能は含まれません。

仕組み

AI 調査エージェントは、AWS がサポートするセキュリティケースを分析する際に、構造化されたワークフローに従います:

調査ワークフロー

1. ケース作成 – お客様は、セキュリティ上の懸念を説明する AWS がサポートするケースをセキュリティインシデント対応コンソールに作成します。
2. 並列アクティベーション
   - セキュリティインシデント対応エンジニアがケースに関与します。
   - 同時に、AI エージェントは調査ワークフローを開始します。
3. コンテキストの質問 (オプション) – エージェントは具体的な詳細を収集するため、確認のための質問を行う場合があります。
   - 影響を受けた AWS アカウント ID
   - 関連する IAM プリンシパル (ユーザー、ロール、アクセスキー)
   - 特定のリソース識別子 (S3 バケット、EC2 インスタンス、ARN)
   - 不審な活動の発生時期
4. 証拠収集 – エージェントは AWS データソースを自動的にクエリします。
   - AWS CloudTrail – インシデントに関連する API 呼び出しおよびアクティビティ
   - IAM – ユーザーとロールのアクセス許可、ポリシーの変更、および新しい ID の作成
   - Amazon EC2 インスタンス API – 関連する場合のコンピューティングリソースに関する情報
   - Cost Explorer – 異常なリソース消費に関するコストと使用状況の指標
5. 分析と相関 — エージェントはサービス間で証拠を関連付け、パターンを識別し、イベントのタイムラインを構築します。
6. 概要の生成 – 数分以内に、エージェントは調査タブで包括的な調査概要を提示します。

> **Note**
>
> すべてのフィールドはオプションです。10 分以内に回答がない場合、調査は自動的に開始されます。場合によっては、十分な情報が既に利用可能な場合、エージェントは任意の質問を完全にスキップすることがあります。

調査結果へのアクセス

AI 分析を表示する。

1. セキュリティインシデント対応コンソールで該当のケースに移動してください。
2. 調査タブを選択してください。
3. 調査結果、タイムライン、コンテキストを含む調査概要を確認します。

AI 調査エージェントの概要は、ケースの [コミュニケーション] セクションにコメントとして自動的に投稿されるため、他のケースの更新情報と併せて簡単に確認できます。

データアクセスと許可

AI 調査エージェントは、`AWSServiceRoleForSupport` サービス関連ロールを使用して AWS リソースにアクセスします。このロールは、証拠収集に必要な読み取り専用アクセス許可を提供します。

エージェントによって実行されたすべてのアクションは AWS CloudTrail に記録されるため、顧客は調査中にアクセスされたデータを正確に監査できます。AWS CloudTrail ログでは、これらのアクションは `AWSServiceRoleForSupport` に属性付けられます。

前提条件

AI を活用した調査機能を使用する前に、以下の点を確認してください。

必要なセットアップ

- AWS Security Incident Response有効化済み – サービスは AWS Organizations 管理アカウントを通じて有効化する必要があります。
- AWS がサポートするケースのタイプ – AI 調査は、AWS がサポートするケースでのみ使用できます (セルフマネージドケースでは使用できません)。
- AWSServiceRoleForSupport – このサービス関連ロールは自動的に作成され、調査エージェントに必要な権限を提供します。

必要なアクセス許可

AWS がサポートするケースを作成し、調査結果にアクセスするには、IAM プリンシパルに以下のアクセス許可が必要です:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "security-ir:CreateCase",
                "security-ir:GetCase",
                "security-ir:ListCases",
                "security-ir:UpdateCase"
            ],
            "Resource": "*"
        }
    ]
}
```

調査エージェントの使用

AI 調査エージェントは、AWS がサポートするケースを作成するときに自動的に起動します。

AI 調査の進行状況をモニタリングする

1. AWS Security Incident Response コンソールでケースを開きます。
2. 調査タブ を選択してください。
3. 調査ステータス (進行中または完了) を表示します。
4. 完了後、調査結果、タイムライン、および提言を含む包括的な調査概要を確認してください。

責任ある AI の開示

調査の概要は AWS 生成 AI 機能を使用して生成されます。AI が生成した推奨事項を特定の状況下で評価し、適切な監視メカニズムを導入し、結果を独自に検証し、すべてのセキュリティ決定に対する人間の監視を維持する責任は貴方にあります。

顧客データの使用

「AI 調査エージェント」は、モデルトレーニングに顧客データを使用せず、また、サードパーティーと顧客データを共有しません。

封じ込め

AWS セキュリティインシデント対応は、ユーザーと協力してイベントを封じ込めます。セキュリティの検出結果に応じて、アカウントでプロアクティブ封じ込めアクションを実行するようにサービスを設定できます。サポートされている封じ込めアクション に記載されている SSM ドキュメント を使用して、ユーザー自身で、またはサードパーティーと協力して封じ込めを実行することもできます。

> **Important**
>
> AWS セキュリティインシデント対応では、デフォルトでは封じ込め機能は有効になりません。
> プロアクティブ封じ込め機能を有効にするには、次の 2 つのステップが必要です:
>
> 1. IAM ロールを使用して、サービスに 必要なアクセス許可を付与する。これらのロールは、必要なロールを作成する AWS CloudFormation スタックセットを使用して、アカウントごと、または組織全体で個別に作成できます。
> 2. アカウントごと、またはユーザーの組織全体で封じ込め設定を定義して、プロアクティブ封じ込めアクションを承認します。アカウントレベルの設定は、組織レベルの設定よりも優先されます。AWS サポートケース (技術: セキュリティインシデント対応サービス/その他) を作成して、これを行うことができます。使用可能な封じ込め設定は次のとおりです:
>   - 承認が必要 (デフォルト): ケースバイケースで、明示的な承認なしにリソースのプロアクティブ封じ込めを実行しない。
>   - 確認されたものを封じ込める: 侵害されたことが確認されているリソースのプロアクティブ封じ込めを実行する。
>   - 疑わしいものを封じ込める: AWS セキュリティインシデント対応エンジニアリングによって実行された分析に基づいて、侵害された可能性が高いリソースのプロアクティブ封じ込めを実行する。

封じ込めの意思決定

封じ込めの重要な部分は、システムをシャットダウンするか、ネットワークからリソースを分離するか、アクセスをオフにするか、セッションを終了するかなどの意思決定です。これらの決定は、イベントを封じ込めるための事前定義された戦略と手順がある場合に容易になります。AWSセキュリティインシデント対応は、封じ込め戦略を提供し、潜在的な影響の情報を提供し、関連するリスクを検討して同意した後にのみソリューションの実装をガイドします。

サポートされている封じ込めアクション

AWS Security Incident Response は、サポートされている封じ込めアクションをユーザーに代わって実行して、対応を迅速化し、脅威アクターが環境に損害を引き起こす可能性のある時間を短縮します。この機能を使用すると、特定された脅威を迅速に軽減し、潜在的な影響を最小限に抑え、全体的なセキュリティ体制を強化できます。分析対象のリソースに応じて、さまざまな封じ込めオプションがあります。サポートされている封じ込めアクションについては、以下のサブセクションで説明します。

EC2 封じ込め

`AWSSupport-ContainEC2Instance` 封じ込め自動化は、EC2 インスタンスの可逆的なネットワーク封じ込めを実行し、インスタンスをそのまま実行したままにしますが、新しいネットワークアクティビティから分離して、VPC 内外のリソースとの通信を防止します。

> **Important**
>
> セキュリティグループを変更しても、既存の追跡された接続はシャットダウンされないことに注意してください。将来のトラフィックのみが、新しいセキュリティグループとこの SSM ドキュメントによって効果的にブロックされます。詳細については、サービステクニカルガイドの「ソースの封じ込め」セクションを参照してください。

IAM 封じ込め

`AWSSupport-ContainIAMPrincipal` 封じ込め自動化は、IAM ユーザーまたはロールの可逆的なネットワーク封じ込めを実行し、ユーザーまたはロールをIAMに残しますが、アカウント内のリソースとの通信を隔離します。

S3 封じ込め

`AWSSupport-ContainS3Resource` 封じ込め自動化は、S3 バケットの可逆的な封じ込めを実行し、バケットにオブジェクトを残し、アクセスポリシーを変更して Amazon S3 バケットまたはオブジェクトを分離します。

封じ込め戦略の開発

AWS Security Incident Response では、主要なイベントタイプごとに、リスク選好度に適合する封じ込め戦略を検討することをお勧めします。イベント中の意思決定に役立つ明確な基準を文書化してください。考慮すべき基準は次のとおりです。

- リソースへの潜在的な損害

- 証拠と規制要件の保存
- サービスの利用不能状態 (ネットワーク接続、外部関係者に提供されるサービスなど)
- 戦略の実装に必要な時間とリソース
- 戦略の有効性 (部分的封じ込めまたは完全封じ込めなど)
- ソリューションの永続性 (可逆的または不可逆的など)
- ソリューションの期間 (緊急回避策、一時的な回避策、永続的なソリューションなど)

リスクを軽減し、より効果的な封じ込め戦略を定義して実装する時間を確保できるセキュリティコントロールを適用します。

段階的封じ込めアプローチ

AWS Security Incident Response は、リソースタイプに基づく短期戦略と長期戦略を含む、効率的で効果的な封じ込めを実現するための段階的なアプローチを提案します。

封じ込め戦略

AWS Security Incident Response はセキュリティイベントの範囲を特定できますか?

- できる場合は、すべてのリソース (ユーザー、システム、リソース) を特定します。
- できない場合は、特定されたリソースに対する次のステップの実行と並行して調査します。

リソースは分離できますか?

- できる場合は、影響を受けるリソースの分離に進みます。
- できない場合は、システム所有者とマネージャーと協力して、問題を封じ込めるために必要な追加のアクションを決定します。

影響を受けたすべてのリソースは、影響を受けていないリソースから分離されていますか?

- されている場合は、次のステップに進みます。
- されていない場合、影響を受けるリソースを引き続き分離して短期的な封じ込めを完了し、イベントがさらにエスカレートするのを防ぎます。

システムバックアップ

影響を受けたシステムのバックアップコピーは、さらなる分析のために作成されましたか?

フォレンジックコピーは暗号化され、安全な場所に保存されていますか?

- されている場合は、次のステップに進みます。
- されていない場合は、フォレンジックイメージを暗号化し、誤って使用、損傷、改ざんされないように安全な場所に保存します。

封じ込め設定を送信

アカウントまたは組織の封じ込め設定を設定するには、 AWS サポート ケース を作成します。

サポートケースには、以下の情報を明記してください。

設定されている場合、アクティブなセキュリティインシデント中に AWS Security Incident Response が承認された封じ込めアクションを実行し、環境を保護するための支援を提供します。

- 封じ込めアクションが承認される必要がある AWS Organizations ID または特定のアカウント ID。
- ご希望の封じ込めオプション。

> **Note**
>
> AWS Security Incident Response は、適切な設定で設定され、必要なアクセス許可を付与するために必要な AWS CloudFormation StackSet がデプロイされた後にのみ、封じ込めアクションを実行します。

根絶

根絶フェーズでは、マルウェアの削除、侵害されたユーザーアカウントの削除、検出された脆弱性の軽減など、影響を受けるすべてのアカウント、リソース、インスタンスを特定して対処し、環境全体に均一な修復を適用することが重要です。

ベストプラクティスは、段階的なアプローチを使用して根絶と復旧を行い、修復ステップを優先することです。初期フェーズの目的は、将来のイベントを防ぐために、価値の高い変更で全体的なセキュリティを迅速に (数日から数週間) 向上させることです。後のフェーズでは、長期的な変更 (インフラストラクチャの変更など) と、エンタープライズを可能な限り安全に保つための継続的な作業に集中できます。各ケースは一意であり、AWS セキュリティインシデント対応エンジニアはユーザーと協力して必要なアクションを評価します。

以下の点を考慮してください。

- システムのイメージを再作成し、パッチやその他の対策で強化して、攻撃のリスクを防止または軽減できますか?
- 感染したシステムを新しいインスタンスまたはリソースに置き換えて、感染した項目を終了しながらクリーンベースラインを有効にできますか?
- 不正使用によって残されたマルウェアやその他のアーティファクトをすべて削除し、影響を受けたシステムをさらなる攻撃から保護しましたか?
- 影響を受けるリソースに対するフォレンジックの要件はありますか?

復旧

AWS Security Incident Response は、システムを通常のオペレーションに復元し、正常に機能していることを確認し、脆弱性を修正して、将来の同様のイベントを防ぐのに役立つガイダンスを提供します。AWS Security Incident Response は、システムの復旧を直接支援するものではありません。主な考慮事項は次のとおりです。

- 影響を受けたシステムにパッチが適用され、最近の攻撃に対して強化されていますか?
- システムを本番環境に復元するための実行可能なタイムラインはどのようなものですか?
- 復元されたシステムをテスト、モニタリング、検証するには、どのようなツールを使用しますか?

インシデント後レポート

AWS Security Incident Response は、チームと当社の間のセキュリティアクティビティが終了した後のイベントの概要を提供します。

毎月月末に、AWS Security Incident Response サービスは毎月のレポートを各お客様の主要な連絡先に E メールで送信します。レポートは、以下に説明するメトリクスを使用して PDF 形式で配信されます。お客様は、AWS Organizations ごとに 1 つのレポートを受け取ります。

ケースメトリクス

- 作成されたケース
  - ディメンション名: タイプ
  - ディメンション値: AWS サポート、セルフサポート
  - 単位: 数
  - 説明: 作成されたケースの数。
- クローズされたケース

  - ディメンション名: タイプ
  - ディメンション値: AWS サポート、セルフマネージド
  - 単位: 数
  - 説明: クローズされたケースの合計数の測定値。
- オープンケース
  - ディメンション名: タイプ
  - ディメンション値: AWS サポート、セルフサポート
  - 単位: 数
  - 説明: オープンケースの数。

メトリクスのトリアージ

- 受け取った検出結果
  - 単位: 数
  - 説明: トリアージに送信された検出結果の数。
- アーカイブされた検出結果
  - 単位: 数
  - 説明: 手動調査なしで処理された後にアーカイブされた検出結果の数。
- 手動で調査された検出結果
  - 単位: 数
  - 説明: 手動調査が実行された検出結果の数。
- アーカイブされた調査
  - 単位: 数
  - 説明: 誤検出が発生し、アーカイブのために送信された手動調査の数
- エスカレーションされた調査
  - 単位: 数
  - 説明: セキュリティインシデントにつながる手動調査の数

事例

AWS Security Incident Response では、AWS でサポートされているケースまたはセルフマネージドケースの 2 種類のケースを作成できます。

AWS でサポートされているケースを作成する

AWS Security Incident Response の AWS がサポートするケースは、コンソール、API、または AWS Command Line Interface を使用して作成できます。AWS がサポートするケースでは、セキュリティインシデント対応エンジニアからサポートを受けることができます。

> **Important**
>
> デモ/シミュレーションケースは 90 日後に終了します。

> **Note**
>
> AWS セキュリティインシデント対応エンジニアは 15 分以内にケースに対応します。対応時間は、AWS セキュリティインシデント対応エンジニアからの最初の対応のものです。お客様の初回のリクエストには、この時間内に応答するよう取り組んでいます。この応答時間は、後続の応答には適用されません。

> **Note**
>
> アクティブなセキュリティインシデントや調査のためだけでなく、AWS セキュリティインシデント対応機能に関する問い合わせのためにも、AWS がサポートするケースを作成できます。これには、GuardDuty 抑制ルールに関する質問、アラートのトリアージ設定、プロアクティブ対応ワークフロー、およびセキュリティ体制に関する一般的なガイダンスが含まれます。これらの目的のために、[調査と問い合わせ] ケースタイプを選択します。

AWS Security Incident Response に連絡するタイミング

ニーズに応じて、さまざまな目的で AWS セキュリティインシデント対応に連絡できます。次の表は、さまざまなシナリオとそれぞれの適切な問い合わせ方法を示しています。

シナリオ	次を使用する場合	応答時間	ケースのタイプ
アクティブなセキュリティインシデント	即時のインシデント対応のサポートとサービスを必要とす	15 分 (最初の対応)	アクティブなセキュリティインシデント

シナリオ	次を使用する場合	応答時間	ケースのタイプ
	る緊急のセキュリティインシデントが発生している		
調査	セキュリティインシデントが認識されており、ログ分析およびインシデント対応調査のセカンダリ確認のサポートが必要である	15 分 (最初の対応)	調査と問い合わせ
問い合わせとガイダンス	Amazon GuardDuty の検出結果、抑制ルール、アラートのトリアージ設定、プロアクティブ対応ワークフロー、または AWS Security Incident Response 機能に関連する一般的なセキュリティ体制について質問がある	15 分 (最初の対応)	調査と問い合わせ
オンボーディングの問題	AWS セキュリティインシデント対応のオンボーディングプロセス中に技術的な問題が発生している	サポートプランによって異なります	AWS サポート ケース

AWS がサポートするすべてのケース (アクティブなセキュリティインシデントおよび調査と問い合わせ) について、AWS セキュリティインシデント対応エンジニアは、最初の対応では 15 分以内に対応します。この対応時間は最初の連絡 (対応) にのみ適用され、後続の対応には適用されません。

次の例では、コンソールの使用について説明します。

1. AWS マネジメントコンソール 経由で AWS Security Incident Response にサインインします。
2. [ケースを作成] を選択します
3. [AWS を利用してケースを解決] を選択します
4. リクエストのタイプを選択します
   a. アクティブなセキュリティインシデント: このタイプは、緊急のインシデント対応サポートとサービスのためのものです。

b. 調査と問い合わせ: AWS セキュリティインシデント対応エンジニアがログ分析およびインシデント対応調査のセカンダリ確認をサポートできる、認識されたセキュリティインシデントには、このタイプを使用します。GuardDuty の検出結果、抑制ルール、アラートのトリアージ設定、プロアクティブ対応ワークフロー、および AWS セキュリティインシデント対応機能に関連する一般的なセキュリティ体制についての質問には、このタイプを使用できます。

5. 開始日の見積もりを、インシデントの最も早い兆候が確認された日付に設定します。例えば、初めて異常な動作が発生したときや、関連する最初のセキュリティアラートを受け取ったときなどです。
6. ケースのタイトルを定義します
7. ケースの詳細な説明を提供してください。 インシデントレスポンダーがケースを解決するのに役立つ以下の側面を考慮してください。
   a. 何が起きたのか。
   b. インシデントを発見して報告したのは誰ですか?
   c. ケースの影響を受けるのは誰ですか?
   d. 既知の影響は何ですか?
   e. このケースの緊急性はどれくらいですか?
   f. ケースの範囲内にある 1 つ以上の AWS アカウント ID を追加します。
8. オプションで、ケース詳細を追加します。
   a. ドロップダウンリストから、影響を受ける主なサービスを選択します。
   b. ドロップダウンリストから、影響を受ける主なリージョンを選択します。
   c. このケースの一部として特定した 1 つ以上の脅威アクター IP アドレスを追加します。
9. オプションで、通知を受け取る追加のインシデントレスポンダーをケースに追加します 個人を追加するには、以下を実行します。
   a. E メールアドレスを追加します。
   b. オプションで、姓名を追加します。
   c. [新規追加] を選択して、別の個人を追加します。
   d. 個人を削除するには、個人の [削除] オプションを選択します。
   e. [追加] を選択して、リストされているすべての個人をケースに追加します。
      i. 複数の個人を選択し、[削除] を選択してリストから削除できます。
10. オプションで、ケースにタグを追加します。
    a. タグを追加するには、次の操作を行います。
    b. [新しいタグを追加] をクリックします。

c. [Key] (キー) で、タグの名前を入力します。

d. [Value] (値) で、タグの値を入力します。

e. タグを削除するには、そのタグの [Remove] (削除) オプションを選択します。

AWS がサポートするケースが作成されると、AWS セキュリティインシデント対応エンジニアとインシデント対応チームにすぐに通知されます。

AI 調査で AWSがサポートするケースを作成する

1. AWS Security Incident Response コンソール (console.aws.amazon.com/) を開きます。
2. ナビゲーションペインから [ケース] を選択します。
3. [ケースを作成] を選択します。
4. Case type で、AWS がサポートするケース を選択します。
5. タイトル、発生開始日、影響を受けた AWS アカウント ID を含むケースの詳細情報を提供してください。
6. セキュリティイベントの説明 セクションでは、インシデントについて詳細な説明を提供してください。
7. 影響を受けた AWS サービス、リージョン、およびその他の関連する詳細に関する追加情報を提供してください。
8. [ケースを作成] を選択します。

ケースの作成後、セキュリティインシデント対応エンジニアと AI エージェントの両方が同時に作業を開始します。

AI の明確化に関する質問に回答する (オプション)

1. ケースの 調査 タブに移動してください。
2. AI エージェントから提示された明確化のための質問を確認します。
3. 質問に応答するか、回答しない場合はスキップを選択してください。
4. 送信を選択して続行します。すべてのフィールドはオプションです。

責任ある AI の開示

調査の概要は AWS 生成 AI 機能を使用して生成されます。AI が生成した推奨事項を特定の状況下で評価し、適切な監視メカニズムを導入し、結果を独自に検証し、すべてのセキュリティ決定に対する人間の監視を維持する責任は貴方にあります。

セルフマネージドケースを作成する

AWS Security Incident Response のセルフマネージドは、コンソール、API、または AWS Command Line Interface を使用して作成できます。このタイプのケースでは、AWS セキュリティインシデント対応エンジニアは関与しません。次の例では、コンソールの使用について説明します。

1. https://console.aws.amazon.com/security-ir/ で AWS マネジメントコンソール から AWS Security Incident Response にサインインします。
2. [Create Case] を選択します。
3. [自分のインシデント対応チームでケースを解決する] を選択します。
4. 開始日の見積もりを、インシデントの最も早い兆候が確認された日付に設定します。例えば、初めて異常な動作が発生したときや、関連する最初のセキュリティアラートを受け取ったときなどです。
5. ケースのタイトルを定義します。[タイトルを生成] オプションを選択するときは、提案されるように、ケースタイトルにデータを含めることをお勧めします。
6. ケースの一部である AWS アカウント ID を入力します。アカウント ID を追加するには、次の手順を実行します。
   a. 12 桁のアカウント ID を入力し、[アカウントを追加] を選択します。
   b. アカウントを削除するには、ケースから削除するアカウントの横にある [削除] を選択します。
7. ケースの詳細な説明を提供してください。
   a. インシデントレスポンダーがケースを解決するのに役立つ以下の側面を考慮してください。
      i. 何が起きたのか。
      ii. インシデントを発見して報告したのは誰ですか?
      iii. ケースの影響を受けるのは誰ですか?
      iv. 既知の影響は何ですか?
      v. このケースの緊急性はどれくらいですか?
8. オプションで、ケース詳細を追加します。
   a. ドロップダウンリストから、影響を受ける主なサービスを選択します。
   b. ドロップダウンリストから、影響を受ける主なリージョンを選択します。
   c. このケースの一部として特定した 1 つ以上の脅威アクター IP アドレスを追加します。

9. オプションで、通知を受け取る追加のインシデントレスポンダーをケースに追加します 個人を追加するには、以下を実行します。
   a. E メールアドレスを追加します。
   b. オプションで、姓名を追加します。
   c. [新規追加] を選択して、別の個人を追加します。
   d. 個人を削除するには、個人の [削除] オプションを選択します。
   e. [追加] を選択して、リストされているすべての個人をケースに追加します。複数の個人を選択し、[削除] を選択してリストから削除できます。
10. オプションで、ケースにタグを追加します。タグを追加するには、次の操作を行います。
   a. [新しいタグを追加] をクリックします。
   b. [Key] (キー) で、タグの名前を入力します。
   c. [Value] (値) で、タグの値を入力します。
   d. タグを削除するには、そのタグの [Remove] (削除) オプションを選択します。

ケースが作成されると、インシデント対応チームに E メールで通知されます。

AWS セキュリティインシデント対応エンジニアとの協力

セキュリティインシデントケースを開くと、AWS セキュリティインシデント対応エンジニアがインシデントの処理を開始します。このセクションでは、調査中に予想されることと、チームと効果的にコラボレーションする方法について説明します。

AWS セキュリティインシデント対応エンジニアに期待すること

AWS がサポートするケースを開くと、セキュリティインシデント対応エンジニアがインシデントに割り当てられます。割り当てられた対応者は以下を行います:

- ケースで提供された初期情報を確認する
- 関連する AWS サービスログとセキュリティ検出結果を分析する
- セキュリティインシデントのスコープと影響を特定する
- 状況に合わせた調査と対応計画を策定する

対応タイムライン: AWS Security Incident Response エンジニアが新しいケースの受け付けを確認するためのサービスレベル目標 (SLO) は 15 分以内です。初期評価のタイムラインは、ケースの重大性と複雑性に応じて異なる場合があります。AWS Security Incident Response エンジニアが 5 営業日以内にお客様からの応答や重要情報を受け取らない場合、ケースはクローズされます。

調査ワークフロー

AWS セキュリティインシデント対応エンジニアは、NIST 800-61r2 フレームワークに沿った構造化されたインシデント対応プロセスに従います。調査中、次のフェーズが期待できます:

1. 初期トリアージ - セキュリティインシデント対応エンジニアは、ケースの詳細を確認し、インシデントのスコープを確認します
2. 調査 - セキュリティインシデント対応エンジニアが、ログを分析し、侵害のインジケーターを特定し、根本原因を確認します
3. 封じ込め - セキュリティインシデント対応エンジニアが、インシデントの影響を制限するためのアクションを推奨します
4. 根絶と復旧 - セキュリティインシデント対応エンジニアが、脅威の排除と通常の運用の復元を支援します
5. インシデント後のレビュー - セキュリティインシデント対応エンジニアが、今後のインシデントを防ぐための検出結果と推奨事項を提供します

これらのフェーズを通じて、セキュリティインシデント対応エンジニアがケースの更新を通じてユーザーに情報を提供し、追加情報やアクションをリクエストする場合があります。

情報セキュリティインシデント対応エンジニアがリクエストする場合がある

インシデントを効果的に調査するために、AWS セキュリティインシデント対応エンジニアから以下の提供を求められる場合があります:

- タイムラインの詳細 - インシデントとそのインシデントにつながる関連イベントを初めて検出したタイミング
- 影響を受けたリソース - 関連する特定の AWS アカウント ID、サービス、リージョン、リソース ARN
- アクセス情報 - 影響を受けたリソースにアクセスできるユーザーと最近のアクセス変更に関する詳細
- ビジネスコンテキスト - 影響を受けたリソースの使用方法と潜在的なビジネスへの影響
- ログと証拠 - 調査に役立つ可能性のある追加のログ、スクリーンショット、またはアーティファクト
- 承認 - ユーザーに代わって特定の封じ込めまたは修復アクションを実行するための承認

セキュリティインシデント対応エンジニアが、各情報が必要な理由と、それが調査にどのように役立つかを説明します。

コミュニケーションのベストプラクティス

効果的なコミュニケーションにより、インシデントの解決が加速します。AWS セキュリティインシデント対応エンジニアと協力するときは、次のプラクティスに従ってください:

- セキュリティインシデント対応エンジニアからの情報のリクエストに 迅速に対応する
- 関連性が不明な場合でも、完全な情報を提供する
- 推奨事項を理解できない場合や明確化が必要な場合に 質問する
- インシデントの新たな進展や変更点で ケースを更新する
- セキュリティインシデント対応エンジニアと調整するために、チームから 主要な連絡先を指定する

> **Important**
>
> AWS Security Incident Response エンジニアが 5 営業日以内に重要な情報リクエストへの応答を受け取らなかった場合は、ケースのクローズに向けて作業を行います。新しい情報が使用可能になった場合は、ケースを再開できます。

調査中のロール

AWS Security Incident Response エンジニアが調査を主導するときは、お客様の参加が不可欠です。次のアクションはお客様の責任となります。

- 情報リクエストにタイムリーに対応する
- 推奨される封じ込めおよび修復アクションを AWS 環境に実装する
- Security Incident Response エンジニアがお客様に代わってアクションを実行することを承認する (プロアクティブレスポンスを有効にしている場合)
- 必要に応じて内部チーム (セキュリティ、法務、コンプライアンス) と調整する
- インシデント対応の優先順位とトレードオフに関するビジネス上の意思決定を行う

AWS Security Incident Response エンジニアは専門知識と推奨事項を提供しますが、AWS リソースの継続的な制御と、対応アクションに関する最終決定はお客様が行います。

ケースのクローズ

AWS Security Incident Response エンジニアは、次の場合にケースをクローズします。

- インシデントが封じ込められ、修正されている
- すべての調査結果がユーザーと共有されている
- セキュリティインシデント対応エンジニアのさらなるサポートは必要ない
- ユーザーがケースのクローズをリクエストしている

ケースをクローズする前に、セキュリティインシデント対応エンジニアは、検出結果、実行されたアクション、およびセキュリティ体制を改善するための推奨事項の概要を提供します。

ケースのクローズ後に追加のサポートが必要な場合は、新しいケースを開始する、または AWS サポート に問い合わせることができます。

AWS が生成したケースへの対応

AWS Security Incident Response は、アカウントまたはリソースに影響を及ぼす可能性のある事柄に対処する必要がある、またはそれらに注意する必要があるときに、アウトバウンド通知またはケースを作成する場合があります。これは、サブスクリプションの一環としてプロアクティブレスポンスとアラートのトリアージワークフローを有効にした場合にのみ行われます。

これらの通知は AWS Security Incident Response コンソールに Security Incident Response ケースとして表示され、「[Proactive case]」というプレフィックスが付けられます。これらのケースを表示して管理するには、次の手順を実行します。

- https://console.aws.amazon.com/security-ir/ の Security Incident Response コンソールを開きます
- [ケース] を選択します。
- 「[Proactive case]」というプレフィックスが付いたケースを含む、すべてのケースが表示されます。

これらのケースは、必要に応じて更新、解決、再開することができます。これらのケースを通じて AWS Security Incident Response チームと直接コミュニケーションをとることができるため、潜在的なセキュリティ問題を効率的に処理できます。

ケースの管理

内容

- ケースステータスの変更
- リゾルバーの変更
- アクション項目
- ケースを編集する
- 通信
- アクセス許可
- アタッチメント
- タグ
- ケースアクティビティ
- ケースを閉じる

ケースステータスの変更

ケースは次のいずれかの状態になっています。

- 送信済み: これはケースの初期ステータスです。このステータスのケースは、リクエスト者によって送信されていますが、まだ処理されていません。
- 検出と分析: このステータスは、インシデントレスポンダーがケースの作業を開始したことを示します。このフェーズには、データ収集、イベントのトリアージ、データに基づく結論を作成するための分析の実行が含まれます。
- 封じ込め、根絶および復旧: このステータスでは、インシデントレスポンダーは、削除に追加の労力を必要とする疑わしいアクティビティを特定しました。インシデントレスポンダーは、ビジネスリスク分析と追加のアクションに関する推奨事項を提供します。サービスのオプトイン機能を有効にしている場合、AWS インシデントレスポンダーは、影響を受けるアカウントで SSM ドキュメントを使用して封じ込めアクションを実行するための同意を求めます。
- インシデント後アクティビティ: このステータスでは、プライマリセキュリティイベントが封じ込められています。現在の焦点は、ビジネスオペレーションを回復し、正常に戻すことです。ケースのリゾルバーが AWS でサポートされている場合、概要と根本原因の分析が提供されます。
- クローズ: これはワークフローの最終ステータスです。クローズステータスのケースは、作業が完了したことを示します。クローズしたケースは再開できないため、このステータスに移行する前にすべてのアクションが完了していることを確認してください。

[アクション/更新ステータス] を選択して、セルフマネージドケースのステータスを変更します。AWS がサポートするケースの場合、ステータスは AWS セキュリティインシデント対応エンジニアによって設定されます。

リゾルバーの変更

セルフマネージドケースの場合、インシデント対応チームは AWS にサポートをリクエストできます。[AWS からサポートを受ける] を選択して、このケースのリゾルバーを AWS に変更します。ケースが AWS サポート対象に更新されると、ステータスは [送信済み] に変更されます。既存のケース履歴は、AWS セキュリティインシデント対応エンジニアが利用できます。AWS にヘルプをリクエストすると、セルフマネージドに戻すことはできません。

アクション項目

ケースを処理する AWS セキュリティインシデント対応エンジニアは、内部チームにアクションをリクエストする場合があります。

ケースの作成後に表示されるアクション項目には以下のものが含まれます。

- インシデントレスポンダーがケースにアクセスするためのアクセス許可を付与するリクエスト
- ケースに関する詳細情報を提供するリクエスト

ケースをクローズする準備ができたときのアクション項目:

- ケースレポートの確認リクエスト
- ケースをクローズするリクエスト

ケースを編集する

ケースの詳細を変更するには、[編集] を選択します。

AWS でサポートされているケースとセルフマネージドケースの場合:

ケースの作成後に、以下のケースの詳細を変更できます。

- タイトル
- 説明

AWS でサポートされているケースのみ:

以下の追加フィールドを変更できます。

- リクエストタイプ:
  - アクティブなセキュリティインシデント: このタイプは、緊急のインシデント対応サポートとサービス用です。
  - 調査: 調査により、認識されたセキュリティインシデントのサポートを受けることができます。ここでは、AWS セキュリティインシデント対応エンジニアがログダイブとセキュリティイベントの二次確認をサポートできます。
- 開始日の見積もり: 最初に提供された開始日よりも前にケースに関する兆候を確認した場合は、このフィールドを変更してください。説明フィールドに新しく検出された兆候に関する追加の詳細を入力するか、コミュニケーションタブにコメントを追加することを検討してください。

通信

AWS セキュリティインシデント対応エンジニアは、ケースを処理する際のアクティビティを文書化するコメントを追加できます。異なる AWS セキュリティインシデント対応エンジニアがケースを同時に処理できます。これらはコミュニケーションログ内で [AWS レスポンダー] として表されます。

アクセス許可

アクセス許可タブには、ケースの変更について通知されるすべての個人が一覧表示されます。ケースがクローズされるまで、リストから個人を追加または削除できます。

> **Note**
>
> 個々のケースでは、最大 30 人のステークホルダーを含めることができます。これらのステークホルダーにケースレベルのアクセス権を付与するには、追加のアクセス許可設定が必要です。

コンソールでケースへのアクセスを提供する

AWS マネジメントコンソール でケースへのアクセスを提供するには、IAM アクセス許可ポリシーテンプレートをコピーし、このアクセス許可をユーザーまたはロールに追加します。

IAM ポリシーをユーザーまたはロールに追加する:

1. IAM アクセス許可ポリシーをコピーします。
2. https://console.aws.amazon.com/iam/ から IAM を開きます。

3. ナビゲーションペインで、[ユーザー] または [ロール] を選択します。
4. ユーザーまたはロールを選択して、詳細ページを開きます。
5. [アクセス許可] タブで、[アクセス許可の追加] を選択します。
6. [Attach policy] (ポリシーのアタッチ) を選択します。
7. 適切な AWS Security Incident Response マネージドポリシーを選択します。
8. [Add policy] (ポリシーの追加) を選択します。

アタッチメント

インシデントレスポンダーは、セルフマネージドケースの調査で他のインシデントレスポンダーを支援する添付ファイルをケースに追加できます。

> **Note**
>
> AWS でサポートされているケースを選択した場合、AWS は添付ファイルを表示できません。AWS でサポートされているケースのすべての詳細は、ケースコメントを通じて、または任意の通信技術を使用して画面共有を提供することによって共有する必要があります。

[アップロード] を選択して、ケースに追加するファイルをコンピュータから選択します。

> **Note**
>
> アップロードされた添付ファイルは、ケースが `Closed` 状態になってから 7 日後に削除されます。

タグ

タグは、そのリソースに関するメタデータを保持するためにケースに割り当てることができるオプションのラベルです。タグは、キーとオプションの値で構成されるラベルです。タグを使用して、リソースの検索、コストの割り当て、およびアクセス許可の認証を行うことができます。

タグを追加するには、次の操作を行います。

1. [新しいタグを追加] をクリックします。
2. [Key] (キー) で、タグの名前を入力します。
3. [Value] (値) で、タグの値を入力します。

タグを削除するには、そのタグの [Remove] (削除) オプションを選択します。

ケースアクティビティ

監査証跡は、すべてのケースアクティビティの詳細な時系列レコードを提供します。イベント後のアクティビティで重要な情報を提供し、潜在的な改善点を特定するのに役立ちます。ケース変更の時間、ユーザー、アクション、および詳細は、ケース監査証跡に記録されます。

ケースを閉じる

AWS でサポートされているケースについては、ケースの詳細ページで [ケースをクローズ] を選択し、ステータスに関係なくケースを完全にクローズします。通常、ケースは完全にクローズされる前に [クローズする準備が完了] ステータスになります。[クローズする準備が完了] 以外のステータスでケースを早期にクローズすると、AWS セキュリティインシデント対応エンジニアがこの AWS がサポートするケースの処理を停止するようにリクエストすることになります。

インシデント対応チームがレスポンダーである場合は、ケースの詳細ページで [アクション/ケースを閉じる] を選択します。

> **Note**
>
> [クローズする準備が完了] ステータスは、ケースを完全にクローズでき、ケースに対して追加の作業を行う必要がないことを示します。

ケースは、完全にクローズされた後に再度開くことはできません。すべての情報は読み取り専用になります。誤ってクローズされないようにするため、ケースをクローズすることを確認するように求められます。

CloudFormation StackSets の操作

> **Important**
>
> AWS Security Incident Response は、デフォルトで封じ込め機能を有効にしません。これらの封じ込めアクションを実行するには、AWS Identity and Access Management ロールを使用してサービスに必要なアクセス許可を付与する必要があります。これらのロールは、アカウントごとに個別に作成することも、CloudFormation StackSet をデプロイすることで組織全体にわたって作成することもできます。StackSets は必要なロールを作成します。

サービスマネージド型のアクセス許可を使用して StackSet を作成する具体的な手順については、AWS CloudFormationユーザーガイド の サービスマネージド型のアクセス許可を使用して CloudFormation StackSets を作成する を参照してください。

以下は、AWSSecurityIncidentResponseContainment ロールと AWSSecurityIncidentResponseContainmentExecution ロールを作成するためのテンプレートです。

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for production SIR containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
 '${AWS::AccountId}' } },
              },
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Effect': 'Allow',
                    'Action': ['ssm:StartAutomationExecution'],
```

```
                    'Resource':
                      [
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainEC2Instance:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainS3Resource:$DEFAULT',
                        !Sub 'arn:${AWS::Partition}:ssm:*:*:automation-definition/
AWSSupport-ContainIAMPrincipal:$DEFAULT',
                      ],
                  },
                  {
                    'Effect': 'Allow',
                    'Action':
                      ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
 'ssm:ListCommandInvocations'],
                    'Resource': '*',
                  },
                  {
                    'Effect': 'Allow',
                    'Action': ['iam:PassRole'],
                    'Resource': !GetAtt
 AWSSecurityIncidentResponseContainmentExecution.Arn,
                    'Condition': { 'StringEquals': { 'iam:PassedToService':
 'ssm.amazonaws.com' } },
                  },
                ],
            }
  AWSSecurityIncidentResponseContainmentExecution:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainmentExecution
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
 'Action': 'sts:AssumeRole' }],
        }
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
          PolicyDocument:
            {
```

```
            'Version': '2012-10-17',
            'Statement':
              [
                {
                  'Sid': 'AllowIAMContainment',
                  'Effect': 'Allow',
                  'Action':
                    [
                      'iam:AttachRolePolicy',
                      'iam:AttachUserPolicy',
                      'iam:DeactivateMFADevice',
                      'iam:DeleteLoginProfile',
                      'iam:DeleteRolePolicy',
                      'iam:DeleteUserPolicy',
                      'iam:GetLoginProfile',
                      'iam:GetPolicy',
                      'iam:GetRole',
                      'iam:GetRolePolicy',
                      'iam:GetUser',
                      'iam:GetUserPolicy',
                      'iam:ListAccessKeys',
                      'iam:ListAttachedRolePolicies',
                      'iam:ListAttachedUserPolicies',
                      'iam:ListMfaDevices',
                      'iam:ListPolicies',
                      'iam:ListRolePolicies',
                      'iam:ListUserPolicies',
                      'iam:ListVirtualMFADevices',
                      'iam:PutRolePolicy',
                      'iam:PutUserPolicy',
                      'iam:TagMFADevice',
                      'iam:TagPolicy',
                      'iam:TagRole',
                      'iam:TagUser',
                      'iam:UntagMFADevice',
                      'iam:UntagPolicy',
                      'iam:UntagRole',
                      'iam:UntagUser',
                      'iam:UpdateAccessKey',
                      'identitystore:CreateGroupMembership',
                      'identitystore:DeleteGroupMembership',
                      'identitystore:IsMemberInGroups',
                      'identitystore:ListUsers',
                      'identitystore:ListGroups',
```

```
                        'identitystore:ListGroupMemberships',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowOrgListAccounts',
                    'Effect': 'Allow',
                    'Action': 'organizations:ListAccounts',
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSOContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'sso:CreateAccountAssignment',
                        'sso:DeleteAccountAssignment',
                        'sso:DeleteInlinePolicyFromPermissionSet',
                        'sso:GetInlinePolicyForPermissionSet',
                        'sso:ListAccountAssignments',
                        'sso:ListInstances',
                        'sso:ListPermissionSets',
                        'sso:ListPermissionSetsProvisionedToAccount',
                        'sso:PutInlinePolicyToPermissionSet',
                        'sso:TagResource',
                        'sso:UntagResource',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSORead',
                    'Effect': 'Allow',
                    'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Read',
                    'Effect': 'Allow',
                    'Action':
                      [
                        's3:GetAccountPublicAccessBlock',
                        's3:GetBucketAcl',
                        's3:GetBucketLocation',
```

```
                    's3:GetBucketOwnershipControls',
                    's3:GetBucketPolicy',
                    's3:GetBucketPolicyStatus',
                    's3:GetBucketPublicAccessBlock',
                    's3:GetBucketTagging',
                    's3:GetEncryptionConfiguration',
                    's3:GetObject',
                    's3:GetObjectAcl',
                    's3:GetObjectTagging',
                    's3:GetReplicationConfiguration',
                    's3:ListBucket',
                    's3express:GetBucketPolicy',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowS3Write',
                'Effect': 'Allow',
                'Action':
                  [
                    's3:CreateBucket',
                    's3:DeleteBucketPolicy',
                    's3:DeleteObjectTagging',
                    's3:PutAccountPublicAccessBlock',
                    's3:PutBucketACL',
                    's3:PutBucketOwnershipControls',
                    's3:PutBucketPolicy',
                    's3:PutBucketPublicAccessBlock',
                    's3:PutBucketTagging',
                    's3:PutBucketVersioning',
                    's3:PutObject',
                    's3:PutObjectAcl',
                    's3express:CreateSession',
                    's3express:DeleteBucketPolicy',
                    's3express:PutBucketPolicy',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowAutoScalingWrite',
                'Effect': 'Allow',
                'Action':
                  [
                    'autoscaling:CreateOrUpdateTags',
```

```
                'autoscaling:DeleteTags',
                'autoscaling:DescribeAutoScalingGroups',
                'autoscaling:DescribeAutoScalingInstances',
                'autoscaling:DescribeTags',
                'autoscaling:EnterStandby',
                'autoscaling:ExitStandby',
                'autoscaling:UpdateAutoScalingGroup',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowEC2Containment',
            'Effect': 'Allow',
            'Action':
              [
                'ec2:AuthorizeSecurityGroupEgress',
                'ec2:AuthorizeSecurityGroupIngress',
                'ec2:CopyImage',
                'ec2:CreateImage',
                'ec2:CreateSecurityGroup',
                'ec2:CreateSnapshot',
                'ec2:CreateTags',
                'ec2:DeleteSecurityGroup',
                'ec2:DeleteTags',
                'ec2:DescribeImages',
                'ec2:DescribeInstances',
                'ec2:DescribeSecurityGroups',
                'ec2:DescribeSnapshots',
                'ec2:DescribeTags',
                'ec2:ModifyNetworkInterfaceAttribute',
                'ec2:RevokeSecurityGroupEgress',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowKMSActions',
            'Effect': 'Allow',
            'Action':
              [
                'kms:CreateGrant',
                'kms:DescribeKey',
                'kms:GenerateDataKeyWithoutPlaintext',
                'kms:ReEncryptFrom',
                'kms:ReEncryptTo',
```

```
                ],
              'Resource': '*',
            },
            {
              'Sid': 'AllowSSMActions',
              'Effect': 'Allow',
              'Action': ['ssm:DescribeAutomationExecutions'],
              'Resource': '*',
            },
          ],
        }
```

メンバーシップをキャンセルする

AWS Security Incident Response の CancelMembership アクセス許可を持つロールは、コンソール、API、または AWS Command Line Interface からメンバーシップをキャンセルできます。

> **Important**
>
> メンバーシップがキャンセルされると、過去のケースデータを表示できなくなります。メンバーシップをキャンセルすると、メンバーシップはすぐに削除され、メンバーシップのケースにはそれ以上アクセスできなくなります。`Active` または `ready to close` に該当するリソースや調査も、メンバーシップのキャンセル時に終了します。

メンバーシップをキャンセルする場合

メンバーシップは削除され、メンバーシップのケースにはそれ以上アクセスできなくなります。

> **Important**
>
> サービスに再サブスクライブすると、新しいメンバーシップが作成され、以前のメンバーシップにあったケースリソースは、キャンセル前にダウンロードした場合にのみアクセスできます。

メンバーシップがキャンセルされると、メンバーシップインシデント対応チームの全員に E メールで通知されます。

Important

委任管理者アカウントを使用してメンバーシップを作成し、AWS Organizations API を使用してアカウントから委任管理者の指定を削除すると、メンバーシップは直ちに終了します。

AWS Security Incident Response リソースのタグ付け

タグとは、ユーザーまたは AWS が AWS リソースに割り当てるメタデータラベルです。各タグは、キーと値から構成されます。ユーザーが割り当てるタグでは、ユーザーがキーと値を定義します。たとえば、1 つのリソースのキーを `stage` と定義し、値を `test` と定義します。

タグは、以下のことに役立ちます。

- AWS リソースを識別および整理します。多くの AWS のサービス ではタグ付けがサポートされているため、各種のサービスからリソースに同じタグを割り当てて、リソースの関連を示すことができます。
- AWS のコストの追跡。これらのタグは、AWS Billing ダッシュボードで有効にします。AWS では、タグを使用してコストを分類し、毎月のコスト配分レポートを提供します。詳細については、「AWS Billing ユーザーガイド」の「Use cost allocation tags」を参照してください。
- AWS リソースへのアクセスを制御します。詳細については、IAM ユーザーガイドの「タグを使用したアクセス制御」を参照してください。

「AWS Security Incident Response API reference for tagging」を参照してください。

AWS CloudShell を使用して AWS Security Incident Response を操作する

AWS CloudShell はブラウザベースの事前に認証されたシェルで、AWS マネジメントコンソール から直接起動できます。任意のシェル (Bash、PowerShell または Z シェル) を使用して、AWS サービス (AWS Security Incident Response など) に対して AWS CLI コマンドを実行できます。この手順は、コマンドラインツールのダウンロードもインストールも不要です。

AWS マネジメントコンソール から AWS CloudShell を起動すると、コンソールへのサインインに使用した AWS 認証情報は、新しいシェルセッションで自動的に利用できます。AWS CloudShell ユーザーのこの事前認証により、AWS CLI バージョン 2 (シェルのコンピューティング環境にプリインストール済み) を使用している Security Incident Response など AWS サービスとやり取りするときに、認証情報の設定をスキップできます。

内容

AWS CloudShell の IAM アクセス許可の取得

AWS Identity and Access Management 管理者によって提供されるアクセス管理リソースを使用して、管理者は IAM ユーザーが AWS CloudShell にアクセスして環境の機能を使用できるアクセス許可を付与します。

管理者がユーザーにアクセス権を付与する最も簡単な方法は、AWS マネージドポリシーを介した方法です。AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。CloudShell 用に次の AWS マネージドポリシーを IAM アイデンティティにアタッチできます。

- `AWSCloudShellFullAccess`: すべての機能へのフルアクセス権のある AWS CloudShell を使用するためのアクセス許可を付与します。

IAM ユーザーが AWS CloudShell を使用して実行できるアクションの範囲を制限する場合、テンプレートとして `AWSCloudShellFullAccess` マネージドポリシーを使用するカスタムポリシーを作成できます。CloudShell でユーザーが使用できるアクションを制限する方法の詳細については、「AWS CloudShell ユーザーガイド」の「IAM ポリシーを使用して AWS CloudShell へのアクセスと使用を管理する」を参照してください。

> **Note**
>
> IAM アイデンティティには、Security Incident Response への呼び出しを行うアクセス許可を付与するポリシーも必要です。

AWS CloudShell を使用して Security Incident Response とやり取りする

AWS マネジメントコンソール から AWS CloudShell を起動すると、コマンドラインインターフェイスを使用して Security Incident Response とのやり取りをすぐに開始できます。

> **Note**
>
> AWS CloudShell で AWS Command Line Interface を使用する場合、追加のリソースをダウンロードまたはインストールする必要はありません。さらに、ユーザーはシェル内で既に認証されているので、呼び出しを行う前に認証情報を設定する必要はありません。

AWS CloudShell と Security Incident Response の使用

1. AWS マネジメントコンソールから、ナビゲーションバーに表示される次のオプションを選択して CloudShell を起動します。
   - CloudShell アイコンを選択する。
   - 検索ボックスに「cloudshell」を入力し始めて、表示された CloudShell オプションを選択する。
2. AWS Security Incident Response とのやり取りには、標準的な AWS Command Line Interface を使用します。利用可能な CLI コマンドの完全なリファレンスについては、「AWS Security Incident Response 向けの AWS CLI コマンドリファレンス」を参照してください。

AWS CloudTrail を使用した AWS Security Incident Response API コールのログ記録

AWS Security Incident Response は、ユーザー、ロール、または AWS サービスによって Security Incident Response で実行されたアクションを記録するサービスである AWS CloudTrail と統合されています。CloudTrail は、Security Incident Response のすべての API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、Security Incident Response コンソールからの呼び出しと Security Incident Response API オペレーションへのコード呼び出しが含まれます。追跡を作成すると、Security Incident Response のイベントなどを含む Amazon S3 バケットへの CloudTrail イベントの継続的な送信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Security Incident Response に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail の Security Incident Response 情報

CloudTrail は、AWS アカウントを作成すると、その中で有効になります。Security Incident Response でアクティビティが発生すると、そのアクティビティは [イベント履歴] 内の他の AWS のサービスのイベントと共に CloudTrail イベントに記録されます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、 CloudTrail イベント履歴でのイベントの表示を参照してください。

AWS アカウント で過去 90 日間のイベントを継続的に記録するには、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。AWS マネジメントコンソール を使用して作成した証跡はマルチリージョンです。AWS CLI を使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。アカウント内のすべて AWS リージョン でアクティビティを把握するため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョン に記録されたイベントのみを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウント の証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成すると、進行中の管理イベントのコピーを 1 つ無料で CloudTrail から Amazon S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

[CloudTrail Lake] を使用すると、イベントに対して SQL ベースのクエリを実行できます。CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントは、イベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基づいた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレクタが制御します。CloudTrail Lake の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS CloudTrail Lake の使用」を参照してください。

CloudTrail Lake のイベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

すべての Security Incident Response アクションは CloudTrail によってログに記録され、「AWS Security Incident Response API Reference」に記載されています。例えば、`CreateMembership`、`CreateCase`、`UpdateCase` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストが、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

Security Incident Response ログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、CreateCase アクションを示す CloudTrail ログエントリを示します。


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA0000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA0000000000000000",
                "arn": "arn:aws:iam::123412341234:role/Admin",
                "accountId": "123412341234",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-10-13T06:32:53Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-10-13T06:40:45Z",
    "eventSource": "security-ir.amazonaws.com",
    "eventName": "CreateCase",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/
arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/
installer#exe md/prompt#off md/command#security-ir.create-case",
    "requestParameters": {
        "impactedServices": [
            "Amazon GuardDuty"
```

```
        ],
        "impactedAccounts": [],
        "clientToken": "testToken112345679",
        "resolverType": "Self",
        "description": "***",
        "engagementType": "Investigation",
        "watchers": [
            {
                "email": "***",
                "name": "***",
                "jobTitle": "***"
            }
        ],
        "membershipId": "m-r1abcdabcd",
        "title": "***",
        "impactedAwsRegions": [
            {
                "region": "ap-southeast-1"
            }
        ],
        "reportedIncidentStartDate": 1711553521,
        "threatActorIpAddresses": [
            {
                "ipAddress": "***",
                "userAgent": "browser"
            }
        ]
    },
    "responseElements": {
        "caseId": "0000000001"
    },
    "requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
    "eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123412341234",
            "type": "AWS::SecurityResponder::Case",
            "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123412341234",
```

```
    "eventCategory": "Management"
}
```

AWS Organizations を使用した AWS Security Incident Response アカウントの管理

AWS Security Incident Response は AWS Organizations と統合されています。組織の AWS Organizations 管理アカウントは、AWS Security Incident Response の委任管理者としてアカウントを指定できます。このアクションにより、AWS Security Incident Response は AWS Organizations で信頼できるサービスとして有効になります。これらの許可が付与される方法については、「Using AWS Organizations with other AWS services」を参照してください。

以下のセクションでは、委任 Security Incident Response 管理者アカウントとして実行できるさまざまなタスクについて説明します。

内容

AWS Organizations を用いて AWS Security Incident Response を使用するための考慮事項とレコメンデーション

以下の考慮事項と推奨事項は、委任 Security Incident Response 管理者アカウントが AWS Security Incident Response でどのように機能するかを理解するのに役立ちます。

AWS Security Incident Response の委任管理者アカウント。

1 つのメンバーアカウントを委任 Security Incident Response 管理者アカウントとして指定できます。例えば、*## (######)* でメンバーアカウント *111122223333* を指定する場合、*### (##)* で別のメンバーアカウント *555555555555* を指定することはできません。他のすべてのリージョンで委任 Security Incident Response 管理者アカウントと同じアカウントを使用する必要があります。

委任 Security Incident Response 管理者アカウントを特定の AWS リージョン に設定します。

AWS リージョン 初期設定時に、委任 Security Incident Response 管理者アカウントとして指定できます。設定はリージョン限定ですが、AWS Security Incident Response はサポートされているすべての AWS リージョン において組織全体をカバーします。Amazon GuardDuty と AWS Security Hub CSPM のセキュリティ検出結果は、サポートされているすべての AWS リージョン から取り込まれ、ケースはサブスクリプションをアクティブ化したリージョンで一元管理されます。委任 Security Incident Response 管理者アカウントとメンバーアカウントは、AWS Organizations を通じて追加する必要があります。

組織の管理アカウントを委任 Security Incident Response 管理者アカウントとして設定することは推奨されません。

組織の管理アカウントは、委任 Security Incident Response 管理者アカウントとして使用できます。ただし、AWS のセキュリティのベストプラクティスは最小特権の原則に従っており、この設定は推奨されていません。

ライブサブスクリプションから委任 Security Incident Response 管理者アカウントを削除すると、サブスクリプションは直ちにキャンセルされます。

委任 Security Incident Response 管理者アカウントを削除すると、AWS Security Incident Response はこの委任 Security Incident Response 管理者アカウントに関連付けられているすべてのメンバーアカウントを削除します。AWS Security Incident Response は、すべてのメンバーアカウントで有効化されなくなります。

AWS アカウント管理 の信頼されたアクセスの有効化

AWS Security Incident Response の信頼されたアクセスを有効にすると、管理アカウントの委任管理者は、AWS Organizations の各メンバーアカウントに固有の情報とメタデータ (主要連絡先や代替連絡先の詳細など) を変更できるようになります。

組織内の AWS Security Incident Response の信頼されたアクセスを有効にするには、次の手順を使用します。

最小アクセス許可

これらのタスクを実行するには、以下の要件を満たす必要があります。

- これは、組織の管理アカウントからのみ実行できます。
- 組織で、すべての機能が有効になっている 必要があります。

Console

AWS Security Incident Response の信頼されたアクセスを有効にするには

1. AWS Organizations コンソールにサインインします。組織の管理アカウントで、IAM ユーザーとしてサインインするか、IAM ロールを引き受けるか、ルートユーザーとしてサインインする (推奨されません) 必要があります。
2. ナビゲーションペインで、[Services] (サービス) を選択します。
3. サービスのリストで [AWS Security Incident Response] を選択します。
4. [Enable trusted access (信頼されたアクセスを有効にする)] を選択します。
5. [AWS Security Incident Response の信頼されたアクセスを有効にする] ダイアログボックスで、[有効にする] と入力して確定し、[信頼されたアクセスを有効にする] を選択します。

API/CLI

AWS アカウント管理 の信頼されたアクセスを有効にするには

次のコマンドの実行後に、組織の管理アカウントの認証情報を使用して、`--accountId` パラメータを使用するアカウント管理 API オペレーションを呼び出し、組織内のメンバーアカウントを参照するすことができます。

- AWS CLI: enable-aws-service-access

  次の例では、呼び出し側アカウントの組織内の AWS Security Incident Response 用に信頼されたアクセスを有効にします。

```
$ aws organizations enable-aws-service-access \
                                        --service-principal security-
ir.amazonaws.com
```

  このコマンドは成功時に出力を生成しません。

委任 Security Incident Response 管理者アカウントの指定に必要なアクセス許可

AWS Organizations の委任管理者を使用して、AWS Security Incident Response メンバーシップを設定することもできます。これらの許可が付与される方法については、「Using AWS Organizations with other AWS services」を参照してください。

> **Note**
>
> AWS Security Incident Response は、コンソールを使用してセットアップや管理を行うときに、AWS Organizations 信頼関係を自動的に有効にします。CLI/SDK を使用する場合は、EnableAWSServiceAccess API を使用して `security-ir.amazonaws.com` を信頼することで、これを手動で有効にする必要があります。

AWS Organizations マネージャーとして、組織の委任 Security Incident Response 管理者アカウントを指定する前に、AWS Security Incident Response アクション `security-ir:CreateMembership` と `security-ir:UpdateMembership` を実行できることを確認します。これらのアクションにより、AWS Security Incident Response を使用して組織の委任 Security Incident Response 管理者アカウントを指定できます。また、組織に関する情報を取得するのに役立つ AWS Organizations アクションの実行が許可されていることも確認する必要があります。

これらの許可を与えるには、アカウントの AWS Identity and Access Management (IAM) ポリシーに以下のステートメントを含める：

```
{
    "Sid": "PermissionsForSIRAdmin",
    "Effect": "Allow",
    "Action": [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
```

```
            ],
            "Resource": "*"
        }
```

AWS Organizations 管理アカウントを委任 Security Incident Response 管理者アカウントとして指定する場合、アカウントには IAM アクション `CreateServiceLinkedRole` も必要です。アクセス許可の追加に進む前に、AWS Organizations を用いて AWS Security Incident Response を使用するための考慮事項とレコメンデーション を確認してください。

AWS Organizations 管理アカウントの委任 Security Incident Response 管理者アカウントとしての指定を続行するには、以下のステートメントを IAM ポリシーに追加し、*111122223333* を AWS Organizations 管理アカウントの AWS アカウント ID に置き換えます。

```
        {
         "Sid": "PermissionsToEnableSecurityIncidentResponse"
         "Effect": "Allow",
         "Action": [
          "iam:CreateServiceLinkedRole"
         ],
         "Resource": "arn:aws:iam::111122223333:role/aws-service-role/security-
ir.amazonaws.com/AWSServiceRoleForSecurityIncidentResponse",
         "Condition": {
          "StringLike": {
           "iam:AWSServiceName": "security-ir.amazonaws.com"
          }
         }
        }
```

AWS Security Incident Response の委任管理者を指定する

このセクションでは、AWS Security Incident Response 組織の委任管理者を指定する手順について説明します。

AWS 組織のマネージャーとして、委任 Security Incident Response 管理者アカウントの運用方法に関する 考慮事項とレコメンデーション を必ずお読みください。続行する前に、委任 Security Incident Response 管理者アカウントの指定に必要なアクセス許可 があることを確認してください。

任意のアクセス方法を選択して、組織の委任 Security Incident Response 管理者アカウントを指定します。管理アカウントのみがこの手順を実行できます。

Console

1. https://console.aws.amazon.com/security-ir/ の Security Incident Response コンソールを開きます

   サインインするには、AWS Organizations 組織の管理アカウントの認証情報を使用します。
2. ページの右上隅にある AWS リージョン セレクターを使用して、組織の委任 Security Incident Response 管理者アカウントを指定するリージョンを選択します。
3. セットアップウィザードに従って、委任管理者アカウントを含むメンバーシップを作成します。

API/CLI

- 組織の管理アカウントの AWS アカウント の認証情報を使用して CreateMembership を実行します。
  - あるいは、AWS Command Line Interface を使用してこれを実行することもできます。次の AWS CLI コマンドは、委任 Security Incident Response 管理者アカウントを指定します。メンバーシップの設定に使用できる文字列オプションは以下のとおりです。

```
                                    {
                                      "customerAccountId": "stringstring",
                                      "membershipName": "stringstring",
                                      "customerType": "Standalone",
                                      "organizationMetadata": {
                                        "organizationId": "string",
                                        "managementAccountId":
"stringstring",
                                        "delegatedAdministrators": [
                                          "stringstring"
                                        ]
                                      },
                                      "membershipAccountsConfigurations":
{
                                        "autoEnableAllAccounts": true,
                                        "organizationalUnits": [
                                          "string"
```

```
    ]
  },
  "incidentResponseTeam": [
    {
      "name": "string",
      "jobTitle": "stringstring",
      "email": "stringstring"
    }
  ],
  "internalIdentifier": "string",
  "membershipId": "stringstring",
  "optInFeatures": [
    {
      "featureName": "RuleForwarding",
      "isEnabled": true
    }
  ]
}
```

委任 Security Incident Response 管理者アカウントのために AWS Security Incident Response が有効になっていない場合、いかなるアクションも実行できません。まだそのようにしていない場合は、新しく指定された委任 Security Incident Response 管理者アカウントのために AWS Security Incident Response を必ず有効にしてください。

AWS Security Incident Response の組織単位 (OU) によるメンバーシップの管理

AWS Security Incident Response は、個々の組織単位 (OU) のメンバーシップカバレッジをサポートしています。メンバーシップは、特定の OU をカバーするようにいつでも更新できます。子 OU 下にあるアカウントを含め、選択した OU 内のすべてのアカウントがメンバーシップの対象となります。

メンバーシップの関連付けを更新する場合、更新は一度に最大 5 つの OU に適用できます。5 つ以上の OU に変更を加える場合は、5 OU のバッチごとに関連付けの変更を実施し、すべての更新が完了するまでこれを行います。

Console

1. https://console.aws.amazon.com/security-ir/ の Security Incident Response コンソールを開きます

   サインインするには、AWS Organizations 組織の管理アカウントの認証情報を使用します。
2. [メンバーシップを管理] > [アカウント] に移動する
3. [関連付けを更新] をクリックします
4. [Organizational Unit (OU) を選択] を選択する
5. [OU を追加] または [OU を削除] を選択する
6. 更新する OU を最大 5 つ選択します。OU を同時に追加および削除することはできません。

   > **Note**
   >
   > 選択した OU のすべてのアカウントと子 OU が関連付けられます。
7. [関連付けを更新] をクリックします
8. > **Note**
   >
   > 5 つ以上の OU に変更を加える場合は、すべての OU が関連付けられるまでステップ 5 と 6 を繰り返します。

お使いの AWS Organization での OU の変更の詳細については、「Managing organizational units (OUs) with AWS Organizations」を参照してください。

AWS Security Incident Response へのメンバーの追加

AWS Organizations と AWS Security Incident Response メンバーシップには 1 対 1 の関係があります。Organizations または組織単位 (OU) からアカウントが追加 (または削除) されると、これらの変更は AWS Security Incident Response メンバーシップの対象アカウントに反映されます。

メンバーシップにアカウントを追加するには、「Managing accounts in an organization with AWS Organizations」のオプションのいずれかに従います。

また、メンバーシップにいつでも OU を追加できます – 「Managing membership with organizational units (OUs)」を参照してください。

AWS Security Incident Response からのメンバーの削除

メンバーシップからアカウントを削除するには、組織からメンバーアカウントを削除するか、選択した OU からアカウントを移動するか、メンバーシップから OU を削除します。

メンバーシップからアカウントを削除するには、「Removing a member account from an organization」の手順に従います。

OU からアカウントを移動するには、「Moving accounts to an organizational unit (OU) or between the root and OUs with AWS Organizations」の手順に従います。

メンバーシップから OU を削除するには、「Managing membership with organizational units (OUs)」の手順に従ってください。

Amazon EventBridge

Amazon EventBridge を使用すると、AWS Security Incident Response ケースとメンバーシップに関連するイベントに対応、モニタリング、オーケストレーションできます。これらのイベントは、Rules (ファンアウトシナリオの場合は 1 つ以上のターゲット) または Pipes (フィルタリング、エンリッチメント、変換機能を強化したポイントツーポイント統合の場合) を介してルーティングできます。

Security Incident Response とサードパーティーツールの統合を作成したり、生成 AI やその他の AWS ツールを使用してデータを集約して分析したりできます。例えば、Security Incident Response がケースをプロアクティブに作成する場合、EventBridge オートメーションを使用してシステムをトリガーし、ステークホルダーに通知できます。さらに、複数の AWS 環境を管理する場合は、Amazon EventBridge 統合を使用して AWS Security Incident Response メンバーシップをモニタリングし、すべての環境が強力なセキュリティ体制を維持していることを確認できます。

詳細については、「What is Amazon EventBridge?」を確認できます

> **Note**
>
> ITSM 統合を含む Amazon EventBridge と AWS Security Incident Response の統合に関する最新の更新については、「AWS 最新情報」ページの「AWS セキュリティインシデント対応が ITSM 統合をサポートするようになりました」を参照してください。

内容

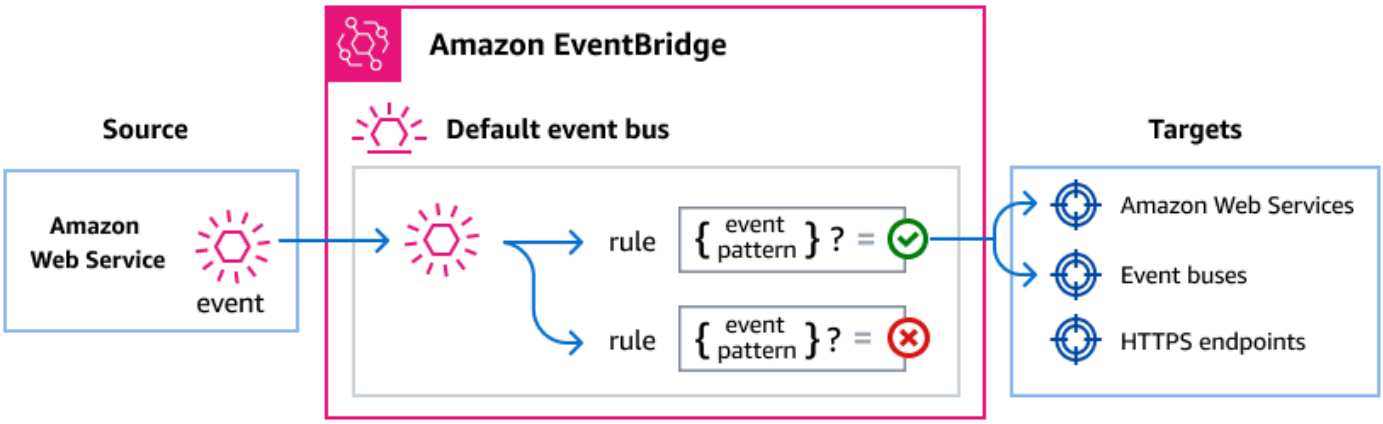
Amazon EventBridge を使用した Security Incident Response イベントの管理

Amazon EventBridge は、イベントを使用してアプリケーションコンポーネント同士を接続するサーバーレスサービスです。これにより、スケーラブルなイベント駆動型アプリケーションを簡単に構築できます。イベント駆動型アーキテクチャとは、イベントの発信と応答によって連携する、疎結合の

ソフトウェアシステムを構築するスタイルです。イベントとは、リソースまたは環境で発生した変更を指します。

処理の流れ

多くの AWS サービスと同様に、Security Incident Response は EventBridge のデフォルトのイベントバスにイベントを生成して送信します。(デフォルトのイベントバスは、AWS アカウントで自動的にプロビジョニングされます)。イベントバスは、イベントを受信して、ゼロ個以上の送信先 (ターゲット) に配信するルーターです。イベントが受信されると、ユーザーがイベントバスに対して指定したルールによって評価されます。各ルールは、イベントがルールのイベントパターンに一致するかどうかをチェックします。一致する場合、イベントバスはそのイベントを指定されたターゲットに送信します。



EventBridge ルールを使用した Security Incident Response イベントの配信

EventBridge のデフォルトイベントバスで Security Incident Response イベントをターゲットに送信させるには、ルールを作成する必要があります。各ルールにはイベントパターンが含まれており、EventBridge はイベントバスで受信した各イベントと照合します。イベントデータが指定したイベントパターンに一致すると、EventBridge は、ルールのターゲットにそのイベントを送信します。

イベントバスルールの詳細な作成方法については、「Amazon EventBridge ユーザーガイド」の「Creating rules that react to events」を参照してください。

Security Incident Response イベントに一致するイベントパターンの作成

各イベントパターンは JSON 形式のオブジェクトで、以下が含まれています。

- イベントを送信するサービスを識別する `source` 属性。Security Incident Response イベントの場合、ソースは `"aws.security-ir"` です。

- (オプション): 照合するイベントタイプの配列を含む `detail-type` 属性。
- (オプション): 照合対象となるその他のイベントデータを含む `detail` 属性。

例えば、以下のイベントパターンは、指定された AWS アカウント のすべての `Case Updated by AWS Security Incident Response Service` イベントと一致します。

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

イベントパターンの記述の詳細については、「EventBridge ユーザーガイド」の「Event patterns」を参照してください。

Security Incident Response イベントの詳細リファレンス

AWS サービスのすべてのイベントには、イベントのソースである AWS サービス、イベントが生成された時刻、イベントが発生したアカウントと地域など、イベントに関するメタデータを含む共通のフィールドセットがあります。これらの一般的なフィールドの定義については、「Amazon EventBridge ユーザーガイド」の「イベント構造リファレンス」を参照してください。

さらに、各イベントには、その特定のイベントに固有のデータを含む `detail` フィールドがあります。以下のリファレンスでは、さまざまな Security Incident Response イベントの詳細フィールドを定義しています。

EventBridge を使用して Security Incident Response イベントの選択と管理を行う場合、以下の点に留意するのが有用です。

- Security Incident Response からのすべてのイベントの `source` フィールドは `"aws.security-ir"` に設定されます。
- `detail-type` フィールドはイベントタイプを指定します。

  例えば、`"Case Updated"`。
- `detail` フィールドには、その特定のイベントに固有のデータが含まれます。

Security Incident Response イベントに一致するようにルールを有効化するイベントパターンの作成方法については、「Amazon EventBridge ユーザーガイド」の「Event patterns」を参照してください。

イベントおよび EventBridge がイベントを処理する方法の詳細については、「Amazon EventBridge ユーザーガイド」の「EventBridge イベント」を参照してください。

共通フィールド: すべての AWS Security Incident Response イベントには、これらの標準 Amazon EventBridge フィールドが含まれます。

- version: EventBridge イベント形式バージョン
- id: イベントの一意の識別子
- detail-type: イベントタイプの人間が読み取れる説明
- source: Security Incident Response イベントの場合は常に「aws.security-ir」
- account: イベントが発生した AWS アカウント ID
- time: イベントが発生したときの ISO 8601 タイムスタンプ
- region: リソースが存在する AWS リージョン
- resources: 影響を受けたリソースの ARN を含む配列

詳細フィールド: `detail` オブジェクトには、Security Incident Response 固有の情報が含まれています

- caseId: ケースの一意の識別子 (ケースイベントのみ)
- membershipId: メンバーシップの一意の識別子 (メンバーシップイベントのみ)
- updatedBy: 更新を実行したユーザー (ケースとコメントの更新イベントのみ)
- createdBy: エンティティを作成したユーザー (ケースとコメントの作成イベントのみ)

アクター値: `updatedBy` および `createdBy` フィールドに含めることができます

- AWS Responder: AWS セキュリティレスポンダーが実行したアクション
- *security-ir.amazonaws.com*: サービスによって自動的に実行されたアクション
- Account ID: お客様によって実行されたアクション (例: "111122223333")

リソース ARN 値: AWS Security Incident Response リソースはこれらの ARN 形式を使用します

- Cases: `arn:aws:security-ir:{region}:{account-id}:case/{case-id}`
- Memberships: `arn:aws:security-ir:{region}:{account-id}:membership/{membership-id}`

ケースイベント

AWS レスポンダーによって作成されたケース

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

サービスによって作成されたケース

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
```

```
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "security-ir.amazonaws.com"
  }
}
```

お客様によって作成されたケース

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

AWS レスポンダーによって更新されたケース

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
```

```
  "account": "111122223333",
  "time": "2023-05-12T01:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "AWS Responder"
  }
}
```

AWS お客様によって更新されたケース

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

AWS Security Incident Response サービスによって更新されたケース

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
```

```
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

クローズされたケース

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Closed",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-15T14:22:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890"
  }
}
```

ケースコメントイベント

AWS レスポンダーによって作成されたケースコメント

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
```

```
  "time": "2023-05-12T04:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

お客様によって作成されたケースコメント

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

AWS Security Incident Response サービスによって作成されたケースコメント

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
```

```
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "security-ir.amazonaws.com"
  }
}
```

お客様によって更新されたケースコメント

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

AWS Security Incident Response サービスによって更新されたケースコメント

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
```

```
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

AWS レスポンダーによって作成されたケースコメント

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "AWS Responder"
  }
}
```

メンバーシップイベント

作成されたメンバーシップ

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Membership Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-04-01T10:00:00Z",
```

```
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

更新されたメンバーシップ

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Updated",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-04-15T16:30:00Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

キャンセルされたメンバーシップ

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Closed",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-06-30T23:59:59Z",
              "region": "us-west-2",
```

```
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

終了したメンバーシップ

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Terminated",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-07-01T00:00:00Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-123456s7890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

AWS Security Incident Response イベントの使用

EventBridge ルールを作成して、これらのイベントを照合し、自動アクションをトリガーできます。ユースケースの例を以下に示します。

すべての AWS Security Incident Response イベントに一致:

```
        {
          "source": ["aws.security-ir"]
        }
```

ケースイベントのみに一致:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Added",
    "Case Comment Updated"
  ]
}
```

AWS レスポンダーによって更新されたケースに一致:

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Case Updated"],
  "detail": {
    "updatedBy": ["AWS Responder"]
  }
}
```

特定のケースのイベントに一致:

```
{
  "source": ["aws.security-ir"],
  "detail": {
    "caseId": ["1234567890"]
  }
}
```

チュートリアル: **Membership Updated** イベントに関する Amazon Simple Notification Service アラートを送信する

このチュートリアルでは、サブスクリプションが `Membership Updated` ステータスに移行したイベントのみをキャプチャする Amazon EventBridge イベントルールを設定します。

前提条件

このチュートリアルでは、メンバーシップに有効なサブスクリプションとアクティブな AWS アカウントがあることを前提としています。

トピック

- チュートリアル: Amazon SNS トピックを作成してサブスクライブする
- チュートリアル: イベントルールを登録する
- チュートリアル: ルールをテストする
- 代替ルール: Security Incident Response Case の更新

チュートリアル: Amazon SNS トピックを作成してサブスクライブする

このチュートリアルでは、新しいイベントルールのイベントターゲットとして使用する Amazon SNS トピックを設定します。

Amazon SNS トピックを作成するには

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. トピック、トピックの作成 の順に選択します。
3. [Type] (タイプ) で、[Standard] (標準) を選択します。
4. 名前として **MembershipUpdated** を入力し、トピックを作成 を選択します。
5. [MembershipUpdated] 画面で、[サブスクリプションの作成] を選択します。
6. [Protocol (プロトコル)] として [Email (E メール)] を選択します。
7. エンドポイント では、現在アクセスできるメールアドレスを入力し、サブスクリプションの作成 を選択します。
8. メールアカウントを確認し、サブスクリプションの確認メールメッセージが届くのを待ちます。確認メールが届いたら、[Confirm subscription] (サブスクリプションの確認) を選択します。

チュートリアル: イベントルールを登録する

次に、`Membership Updated` イベントのみをキャプチャするイベントルールを登録します。

EventBridge ルールを登録するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで [ルール] を選択します。
3. [ルールの作成] を選択します。
4. ルールの名前と説明を入力します。

> **Note**
>
> ルールには同じリージョン内および同じイベントバス上の別のルールと同じ名前を付けることはできません。

5. [イベントバス] で、このルールに関連付けるイベントバスを選択します。このルールをアカウントからのイベントと一致させるには、AWS のデフォルトのイベントバスを選択します。アカウントの AWS サービスがイベントを発行すると、常にアカウントのデフォルトのイベントバスに移動します。

> **Note**
>
> これは、AWS Security Incident Response メンバーシップを作成した AWS Organizations または委任管理者アカウントで設定する必要があります。

6. [ルールタイプ] で、[イベントパターンを持つルール] を選択してください。
7. 次へ を選択します。
8. イベントソース では、[その他] を選択します。
9. イベントパターン では、カスタムパターン (JSON エディター) を選択します。
10. 次のイベントパターンをテキストエリアに貼り付けます。

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Membership Updated"]
}
```

このコードは、サービスメンバーシップが更新または変更されたイベントに一致する EventBridge ルールを定義します。イベントパターンの詳細については、Amazon EventBridge ユーザーガイドのイベントとイベントパターンを参照してください。

11. 次へ をクリックします。
12. [ターゲットタイプ] では、[AWS サービス] を選択します。
13. [ターゲットを選択] には [SNS トピック] を選択し、[トピック] には [MembershipUpdated] を選択します。
14. (オプション) 追加設定では、以下を実行します。

    a. 最大イベント有効期間 に、1 分 (00:01) から 24 時間 (24:00) の間の値を入力します。

    b. 再試行 で、0 ~ 185 の数値を入力します。

    c. デッドレターキュー で、標準 Amazon SQS キューをデッドレターキューとして使用するかどうかを選択します。EventBridge は、このルールに一致するイベントがターゲットに正常に配信されなかった場合に、そのイベントをデッドレターキューに送信します。次のいずれかを行います。

    - デッドレターキューを使用しない場合は、[なし] を選択します。
    - デッドレターキューとして使用する現在の AWS アカウントの Amazon SQS キューを選択 を選択し、ドロップダウンから使用するキューを選択します。
    - 他の AWS アカウントの Amazon SQS キューをデッドレターキューとして選択 を選択し、使用するキューの ARN を入力します。キューにメッセージを送信するための EventBridge 許可を付与するリソースベースのポリシーをそのキューにアタッチする必要があります。詳細については、Amazon EventBridge ユーザーガイドのデッドレターキューへの許可の付与を参照してください。

15. 次へ を選択します。
16. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、Amazon EventBridge ユーザーガイドのAmazon EventBridge のタグを参照してください。
17. 次へをクリックします。
18. ルールの詳細を確認し、ルールの作成 を選択します。

チュートリアル: ルールをテストする

ルールをテストするには、AWS Security Incident Response メンバーシップに更新を送信します。ルールが正しく設定されている場合は、数分以内にイベントテキストが記載されたメールメッセージが届きます。

代替ルール: Security Incident Response Case の更新

すべてのケースの更新をモニタリングするイベントルールを作成するには、以下の変更を加えてこれらのチュートリアルを繰り返します。

1. チュートリアル: Amazon SNS トピックを作成してサブスクライブする では、トピック名として *CaseUpdates* を使用します。
2. チュートリアル: イベントルールを登録する では、JSON エディタで次のパターンを使用します。

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

トラブルシューティング

AWS Security Incident Response 固有のアクション実行に関する問題が発生した場合は、このセクションのトピックを参照してください。

ERROR は、オペレーションの一部またはすべてに障害があることを示すオペレーションのステータスです。または、問題が生じたものの、タスクが完了した場合に警告が表示されます。

内容

問題

正しいコンテキストからリクエストを送信しない。

AWS Security Incident Response API へのすべての呼び出しは、サービス委任管理者またはメンバーシップアカウントの IAM プリンシパルから発信する必要があります。組織の AWS Security Incident Response 委任管理者またはメンバーシップアカウントである AWS アカウント で、正しい IAM プリンシパルから運用されていることを確認します。

エラー

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

AWS 管理者と協力して、AWS Security Incident Response 委任管理者またはメンバーシップアカウントで IAM ロールを引き受けるアクセス許可があることを確認してください。また、ロールにリクエストされたアクションを許可する IAM ポリシーがあることを確認します。詳細については、「AWS Security Incident Response IAM」を参照してください。

ConflictException

リクエストにより不整合状態が発生します。

指定したケース添付ファイル名またはデフォルトのレスポンスチームメンバーが一意であることを確認してください。また、AWS Security Incident Response サービスメンバーシップがまだ設定

されていないことも確認します。https://console.aws.amazon.com/security-ir/ で Security Incident Response コンソールを開き、`Membership Details` に移動します。

InternalServerException

リクエストの処理中に予期しないエラーが発生しました。数分後にもう一度お試しください。問題が解決しない場合は、サポート にケースを提出してください。

ResourceNotFoundException

リクエストが存在しないリソースを参照しています。

リクエストで指定したリソースの 1 つ以上が存在しません。指定したリソース ARN または ID がすべて正しいことを確認してください。AWS Organizations ID、アカウント ID、IAM ロール、メンバーシップ、ケース、対応チームメンバー、ケース、ケースレスポンダー、ケース添付ファイル、ケースコメントが対象です。

ThrottlingException

リクエストのスロットリングにより、リクエストが拒否されました。

指定された期間に IAM プリンシパルがその API 関数に対して行ったリクエストが多すぎます。1 分待ってから、もう一度お試しください。問題が解決しない場合は、エクスポネンシャルバックオフと再試行アルゴリズムの実装を検討してください。

ValidationException

入力が、AWS のサービス で指定された制約を満たしていません。

リクエスト内の 1 つ以上のデータフィールドが検証および/または論理的な組み合わせ要件を満たしていませんでした。すべてのリソース ARN が完了し、「AWS Security Incident Response API リファレンスガイド」のテキスト値がサイズと形式の制約を満たしていることを確認してください。また、値の更新が許可されていることを確認してください。例えば、ケースを AWS サポート対象からセルフマネージドに変更することはできません。

サポート

さらにサポートが必要な場合は、トラブルシューティングのために サポート Center にお問い合わせください。以下の情報をご用意ください。

- 使用した AWS リージョン

- メンバーシップの AWS アカウント ID
- 該当する場合で提出可能な場合には、ソースの内容
- その他問題のトラブルシューティングに役立つと思われる詳細情報

セキュリティ

内容

AWS Security Incident Response でのデータ保護

内容

AWS 責任共有モデルは、AWS Security Incident Response サービスのデータ保護に適用されます。このモデルで説明したように、AWS は、AWS クラウドで提供されるサービスを実行するインフラストラクチャを保護する責任を負います。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクにも責任があります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログ に投稿された「AWS 責任共有モデルおよび GDPR」ブログを参照してください。

データ保護の目的で、AWS セキュリティのベストプラクティスでは、AWS アカウントの認証情報を保護し、AWS IAM Identity Center または Identity and Access Management (IAM) AWS を使用して

個々のユーザーを設定する必要があります。この方法により、それぞれのジョブを遂行するために必要なアクセス許可のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- AWS CloudTrail を使用して API とユーザーアクティビティログを設定します。
- AWS 暗号化ソリューションを AWS のサービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。
- FIPS 140-3 は現在、このサービスではサポートされていません。

E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないでください。これは、コンソール、API、AWS CLI、または AWS SDK によって AWS サポートや他の AWS のサービスを使用する場合も同様です。タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを 強く お勧めします。

データ暗号化

内容

保管中の暗号化

データは、透過的なサーバー側の暗号化を使用して保存時に暗号化されます。これは、機密データの保護における負担と複雑な作業を減らすのに役立ちます。保管時に暗号化することで、セキュリティを重視したアプリケーションを構築して、暗号化のコンプライアンスと規制の要件を満たすことができます。

送信中の暗号化

データは、Transport Layer Security (TLS) で保護されたチャネルを介して AWS Security Incident Response によって排他的に収集およびアクセスされます。

キー管理

AWS Security Incident Response は AWS KMS との統合を実装し、ケースデータと添付データの保管時の暗号化を提供します。

AWS Security Incident Response では、カスタマーマネージドキーはサポートされていません。

ネットワーク間トラフィックのプライバシー

サービスとオンプレミスのクライアントおよびアプリケーションとの間のトラフィック

プライベートネットワークと AWS との間には 2 つの接続オプションがあります:

- AWS Site-to-Site VPN 接続。詳細については、AWS Site-to-Site VPN ユーザーガイド の「AWS Site-to-Site VPN とは」を参照してください。
- Direct Connect 接続。詳細については、Direct Connect ユーザーガイド の「What is Direct Connect? (とは？)」 を参照してください。

ネットワークを介した AWS Security Incident Response へのアクセスは、AWS が発行する API を利用して行われます。クライアントは Transport Layer Security (TLS) 1.2 をサポートしている必要があります。TLS 1.3 をお勧めします。クライアントは、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) などの Perfect Forward Secrecy (PFS) を備えた暗号スイートもサポートする必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。また、リクエストには、IAM プリンシパルに関連付けられたアクセスキー ID およびシークレットアクセスキーによる署名が必要です。または、リクエストへの署名のために一時的にセキュリティ認証情報を生成する AWS Security Token Service (STS) を使用することもできます。

同じリージョン内の AWS リソース間のトラフィック

AWS Security Incident Response の Amazon Virtual Private Cloud (Amazon VPC) エンドポイントは、AWS Security Incident Response のみへの接続を許可する VPC 内の論理エンティティです。Amazon VPC はリクエストを AWS Security Incident Response にルーティングし、レスポンスを VPC にルーティングします。詳細については、Amazon VPC ユーザーガイド の「VPC エンドポイント」を参照してください。VPC エンドポイントからのアクセスのコントロールに使用できるポリシーの例については、「IAM ポリシーを使用して DynamoDB へのアクセスをコントロールします」を参照してください。

> **Note**
>
> Amazon VPC エンドポイントには、AWS Site-to-Site VPN または Direct Connect を使用してアクセスすることはできません。

Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを制御するのに役立つ AWS のサービスです。IAM 管理者は、認証済み (サインイン済み) および AWS Security Incident Response リソースを使用するために承認済み (アクセス許可を持つ) プリンシパルを制御します。IAM は、AWS のサービスで追加料金は発生しません。

内容

対象者

AWS Identity and Access Management (IAM) の用途は、AWS Security Incident Response で行う作業によって異なります。

セキュリティ管理者

これらのユーザーは、AWSSecurityIncidentResponseFullAccess マネージドポリシーを使用して、メンバーシップとケースのリソースへの読み取りおよび書き込みアクセス権を持っていることを確認することをお勧めします。

ケースウォッチャー

これらの個人は、すべてのケースに対して権限のあるアクセス権を持っているわけではなく、明示的にアクセス許可を付与した個々のケースに対して権限のあるアクセス権を持っています。

インシデント対応チームのメンバー

チームのメンバーには、完全なメンバーシップとケースの両方のアクセス権を付与できます。すべての個人に対してサービスメンバーシップに関する権限のあるアクションを付与するのではなく、サービスを通じて作成および管理されるすべてのケースにアクセスできるようにすることをお勧めします。詳細については、「AWS Security Incident Response マネージドポリシー」を参照してください。

アイデンティティによる認証

認証とは、アイデンティティ認証情報を使用して AWS にサインインする方法です。ユーザーは、AWS アカウントのルートユーザーもしくは IAM ユーザーとして、または IAM ロールを引き受けることによって、認証を受ける (AWS にサインインする) 必要があります。

ID ソースから提供された認証情報を使用して、フェデレーティッドアイデンティティとして AWS にサインインできます。AWSフェデレーティッド ID の例としては、IAM Identity Center (IAM Identity Center) ユーザー、貴社のシングルサインオン認証、Google または Facebook の認証情報などがあります。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して AWS にアクセスする場合、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、AWS マネジメントコンソールまたは AWS アクセスポータルにサインインできます。AWS へのサインインの詳細については、「AWS サインインユーザーガイド」の「How to sign in to your AWS account」を参照してください。

プログラムを使用して AWS にアクセスする場合、AWSは Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) を提供し、認証情報を使用してリクエストに暗号で署名します。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに署名する推奨方法の使用については、「IAM ユーザーガイド」の「AWS API リクエストの署名」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、AWS は、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用することをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証 (MFA)」および「IAM ユーザーガイド」の「IAM の AWS 多要素認証」を参照してください。

AWS アカウントのルートユーザー

AWS アカウントを作成する場合は、このアカウントのすべての AWS サービスとリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。このアイデンティティは AWS アカウントルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでのサインインによりアクセスされます。日常的なタスクにルートユーザーを決して使用せず、ルートユーザーの認証情報を保護する手順を実行してください。ルートユーザーのみが実行できるタスクを実行する場合にのみ使用してください。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー資格情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

管理者アクセスを必要とするユーザーを含め、人間のユーザーには ID プロバイダーとのフェデレーションを使用して、一時的な認証情報により、AWS サービスにアクセスするように要求するのがベストプラクティスです。

フェデレーション ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、Identity Center ディレクトリのユーザー、または ID ソースから提供された認証情報を使用して AWS のサービスにアクセスするユーザーです。フェデレーティッド ID が AWS アカウントにアクセスすると、ロールを引き受け、そのロールによって一時的な認証情報が提供されます。

アクセスを一元管理する場合は、AWS IAM Identity Center を使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、すべての AWS アカウントとアプリケーションで使用するために、独自の ID ソースで一連のユーザーとグループに接続して同期することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対する特定の許可を持つ AWS アカウント内のアイデンティティです。パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループ は、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が簡単になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つ、AWS アカウント内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーに関連付けられていません。ロールを切り替えるこ

とで、AWS マネジメントコンソールの IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーテッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。ロールは、クロスアカウントアクセスを許可する主な方法です。ただし、一部の AWS のサービスでは、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス – 一部の AWS のサービスは、AWS の他のサービスの機能を使用します。例えば、サービスで呼び出しを行う場合、そのサービスでは Amazon EC2 でアプリケーションを実行したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロール です。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、IAM ユーザーガイド の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスリンクロール – サービスリンクロールは、AWS のサービスにリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを作成しているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用します。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのアプリケーションで使用できるようにするには、インスタンスに添付されたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、IAM ユーザーガイド の Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、IAM ユーザーガイド の (IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか? を参照してください。

AWS Security Incident Response で IAM を使用する方法

AWS Identity and Access Management IAMは、管理者が AWS リソースへのアクセスを安全にコントロールするために役立つ AWS のサービスです。IAM 管理者は、誰を認証 サインインし、誰に AWS Security Incident Response リソースの使用を許可する アクセス許可を持たせるかを制御します。IAM では、AWS のサービスで追加料金は発生しません。

AWS Security Incident Response で使用できる IAM の機能	
IAM の機能	サービスの調整
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー	はい (グローバル)
ACL	なし
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり

AWS Security Incident Response で使用できる IAM の機能	
サービスロール	いいえ
サービスリンクロール	はい

内容

- AWS Security Incident Response のアイデンティティベースのポリシー
- AWS Security Incident Response 向けのポリシー条件キー
- AWS Security Incident Response のアクセスコントロールリスト (ACL)

AWS Security Incident Response のアイデンティティベースのポリシー

アイデンティティベースのポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイド の IAM ポリシーの作成 を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

内容

- アイデンティティベースのポリシーの例
- ポリシーに関するベストプラクティス
- AWS Security Incident Response コンソールを使用する
- 自分の権限の表示をユーザーに許可する
- リソースベースのポリシー
- ポリシーアクション

アイデンティティベースのポリシーの例

デフォルトでは、 ユーザーおよびロールには、AWS Security Incident Response リソースを作成または変更する権限はありません。また、AWS マネジメントコンソール、AWS コマンドラインインターフェイス (AWS CLI)、または AWS API を使用してタスクを実行することもできません。IAM 管理者は、IAM ポリシーを作成して、リソースで必要なアクションを実行するためのアクセス許可をユーザーに付与できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドの IAM ポリシーの作成 を参照してください。

AWS Security Incident Response が定義するアクションとリソースタイプ (各リソースタイプの ARN の形式など) の詳細については、「サービス認可リファレンス」の「Actions, resources, and condition keys for AWS Security Incident Response」を参照してください。

ポリシーに関するベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが AWS Security Incident Response リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、AWS アカウントに追加料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

AWS マネージドポリシーの使用を開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードへのアクセス許可の付与を開始するには、多くの一般的なユースケースのためにアクセス許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能の AWS マネージドポリシー を参照してください。

最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。

IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。また、AWS CloudFormation などの特定の AWS サービスを介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することも

できます。詳細については、IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer ポリシーの検証 を参照してください。

多要素認証 (MFA) を要求する – AWS アカウントで IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA 保護 API アクセスの設定 を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

AWS Security Incident Response コンソールを使用する

https://console.aws.amazon.com/security-ir/ にアクセスするには、アクセス許可の最小限のセットが必要です。これらの許可により、AWS アカウントの AWS Security Incident Response リソースに関する詳細を一覧表示および表示できるようにする必要があります。最小限必要なアクセス許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) ではコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、コンソールの最小アクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスを許可します。

AWS Security Incident Response Access または ReadOnly AWS マネージドポリシーを添付して、ユーザーとロールがサービスコンソールを使用できるようにします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI もしくは AWS API を使用してプログラム的に、このアクションを完了するための許可が含まれています。

リソースベースのポリシー

AWS Security Incident Response 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、[specify a principal] (プリンシパルを指定する) 必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または AWS のサービスを含めることができます。

詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

ポリシーアクション

AWS Security Incident Response のポリシーアクション

ポリシーアクションのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どの プリンシパル がどの リソース に対してどのような 条件下で アクション を実行できるかということです。

JSON ポリシーの Action 要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない 許可のみのアクション など、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは 依存アクション と呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

AWS Security Incident Response アクションのリストを確認するには、「Service Authorization Reference」の「Actions defined by AWS Security Incident Response」を参照してください。

AWS Security Incident Response のポリシーアクションは、アクションの前に以下のプレフィックスを使用します。

AWS Security Incident Response -identity

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

"Action": ["AWS Security Incident Response -identity:action1", "AWS Security Incident Response -identity:action2"]

Amazon AWS Security Incident Response のポリシーリソース

ポリシーリソースのサポート: あり。管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントには、リソースまたは NotResource 要素のいずれかが含まれている必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可 と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

"Resource": "*"

AWS Security Incident Response 向けのポリシー条件キー

サービス固有のポリシー条件キーへのサポート: なし

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どの プリンシパル がどの リソース に対してどのような 条件下で アクション を実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、AWS は論理 AND 演算を使用してそれらを評価します。単一の条件キーに複数の値を指定する場合、AWS は論理 OR 演算を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS はグローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイド の AWS グローバル条件コンテキストキー を参照してください。

AWS Security Incident Response のアクセスコントロールリスト (ACL)

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

AWS Security Incident Response での属性ベースのアクセス制御 (ABAC)

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。AWS では、属性は タグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール)、および多数の AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを制御するには、AWS:ResourceTag/key-name、AWS:RequestTag/key-name、または AWS:TagKeys の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。ABAC の詳細については、IAM ユーザーガイドのABAC とは? を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、IAM ユーザーガイド の 属性に基づくアクセスコントロール (ABAC) を使用する を参照してください。

AWS Security Incident Response で一時的な認証情報を使用する

一時的な認証情報のサポート: あり

AWS サービスは、一時的な認証情報を使用してサインインしても機能しません。一時的な認証情報を利用できる AWS のサービスを含めた詳細情報については、「IAM ユーザーガイド」の「IAM と連携する AWS サービス」を参照してください。ユーザー名とパスワード以外の方法で AWS マネジメントコンソールにサインインする場合は、一時認証情報を使用していることになります。例えば、会社のシングルサインオン (SSO) リンクを使用して AWS にアクセスすると、そのプロセスは自動的に一時認証情報を作成します。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ロールへの切り替え (コンソール)」を参照してください。

一時的な認証情報は、AWS CLI または AWS API を使用して手動で作成できます。作成後、一時認証情報を使用して AWS にアクセスできるようになります。AWS は、長期的なアクセスキーを使用する代わりに、一時認証情報を動的に生成することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

AWS Security Incident Response の転送アクセスセッション

転送アクセスセッション (FAS) のサポート: あり

IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルとみなされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、AWS サービスを呼び出すプリンシパルの権限を、AWS サービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストは、サービスが、完了するために他の AWS サービスまたはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS Security Incident Response ID とアクセスのトラブルシューティング

次の情報は、AWS Security Incident Response と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- アクションを実行する権限がない
- iam:PassRole を実行する権限がありません
- AWS アカウント以外の人が私の AWS Security Incident Response リソースにアクセスできるようにしたい

アクションを実行する権限がない

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

以下のエラー例は、mateojackson IAM ユーザーがコンソールを使用して架空の my-example-widget リソースに関する詳細情報を表示しようとしているが、架空の AWS Security Incident Response :GetWidget アクセス許可がないという場合に発生します。

User: arn:AWS:iam::123456789012:user/mateojackson is not authorized to perform: AWS Security Incident Response :GetWidget on resource: my-example-widget

この場合、AWS Security Incident Response :GetWidget アクションを使用して my-example-widget リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がない iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して AWS Security Incident Response にロールを渡せるようにする必要があります。

一部の AWS サービスでは、新しいサービスロールまたはサービスリンクロールを作成せずに、既存のロールをサービスに渡すことができます。そのためには、サービスにロールを渡すアクセス許可が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して AWS Security Incident Response でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与されたアクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

User: arn:AWS:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

AWS アカウント以外の人が私の AWS Security Incident Response リソースにアクセスできるようにしたい

他のアカウントのユーザーや組織外のユーザーが、リソースへのアクセスに使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。

詳細については、以下を参照してください。

- Amazon AWS Security Incident Response でこれらの機能がサポートされているかどうかを確認するには、「How AWS Security Incident Response works with IAM」を参照してください。
- 所有している AWS アカウント全体のリソースへのアクセス権を提供する方法については、IAM ユーザーガイドの所有している別の AWS アカウントへのアクセス権を IAM ユーザーに提供を参照してください。
- リソースへのアクセスをサードパーティーの AWS アカウントに提供する方法については、IAM ユーザーガイドの「サードパーティーが所有する AWS アカウントへのアクセスの提供」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイド の 外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可 を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、IAM ユーザーガイド の IAM でのクロスアカウントのリソースへのアクセス を参照してください。

サービスロールの使用

サービスロールのサポート: なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、IAM ユーザーガイド の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

サービスにリンクされたロールの使用

AWS Security Incident Response のサービスにリンクされたロール

内容

- AWS SLR: AWSServiceRoleForSecurityIncidentResponse
- AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage
- AWS Security Incident Response のサービスリンクロールをサポートするリージョン

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、AWS のサービスにリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント内に表示され、サービスによって所有されます。AWS Identity and Access Management 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスリンクロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、AWS Security Incident Response の設定が簡単になります。このサービスリンクロールのアクセス許可は AWS Security Incident Response で定義します。特に定義されている場合を除き、AWS Security Incident Response のみがそのロールを引き受けることができます。定義された権限には、信頼ポリシーと権限ポリシーに含まれており、その権限ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携する AWS のサービス」を参照し、サービスリンクロール列内で はい と表記されたサービスを確認してください。サービスにリンクされたロールに関するサービスのドキュメントを表示するには、「はい」のリンクをクリックします。

AWS SLR: AWSServiceRoleForSecurityIncidentResponse

AWS Security Incident Response は、AWSServiceRoleForSecurityIncidentResponse という名前のサービスにリンクされたロール (SLR) および AWS Security Incident Response ポリシーを使用して、サブスクライブされているアカウントを識別し、ケースを作成し、関連リソースにタグを付けます。

アクセス許可

AWSServiceRoleForSecurityIncidentResponse サービスリンクロールは、次のサービスを信頼してロールを引き受けます。

- `triage.security-ir.amazonaws.com`

このロールには、AWSSecurityIncidentResponseServiceRolePolicy という名前の AWS マネージドポリシーが添付されます。サービスはロールを使用して、次のリソースに対してアクションを実行します。

- AWS Organizations: サービスで使用するメンバーシップアカウントをサービスが検索できるようにします。

- CreateCase: メンバーシップアカウントに代わってサービスがサービスケースを作成できるようにします。
- ListCases: セキュリティ調査の目的で、サービスの AI エージェントがケースを閲覧できるようにします。
- UpdateCase: サービスの AI エージェントがケースのメタデータを更新できるようにします。
- CreateCaseComment: サービスの AI エージェントが結果を症例コメントとして投稿できるようにします。
- ListComments: サービスの AI エージェントが自動調査を実行するために必要なケースコメントを閲覧できるようにします。
- TagResource: サービスの一部として設定されたサービスタグリソースを許可します。

ロールの管理

サービスリンクロールを手動で作成する必要はありません。AWS マネジメントコンソール、AWS CLI、または AWS API で AWS Security Incident Response にオンボードすると、サービスにリンクされたロールが自動的に作成されます。

> **Note**
>
> 委任管理者アカウントを使用してメンバーシップを作成した場合は、AWS Organizations 管理アカウントでサービスにリンクされたロールを手動で作成する必要があります。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は同じ方法でアカウントにロールを再作成できます。サービスにオンボードすると、サービスにリンクされたロールが再度作成されます。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクされたロールのアクセス許可」を参照してください。

AWS SLR: AWSServiceRoleForSecurityIncidentResponse_Triage

AWS Security Incident Response は、AWSServiceRoleForSecurityIncidentResponse_Triage という名前のサービスにリンクされたロール (SLR) および AWS Security Incident Response ポリシーを使用して、セキュリティの脅威について環境を継続的にモニタリングし、セキュリティサービスを調整してアラートノイズを減らし、情報を収集して潜在的なインシデントを調査します。

アクセス許可

AWSServiceRoleForSecurityIncidentResponse_Triage サービスリンクロールは、以下のサービスを信頼してロールを引き受けます。

- `triage.security-ir.amazonaws.com`

このロールには、AWS マネージドポリシー AWSSecurityIncidentResponseTriageServiceRolePolicy が添付されます。サービスはロールを使用して、次のリソースに対してアクションを実行します。

- イベント: Amazon EventBridge マネージドルールの作成をサービスに許可します。このルールは、アカウントからサービスにイベントを配信するために AWS アカウントで必要なインフラストラクチャです。このアクションは、`triage.security-ir.amazonaws.com` によって管理されるすべての AWS リソースで実行されます。
- Amazon GuardDuty: サービスがセキュリティサービスを調整してアラートノイズを減らし、潜在的なインシデントを調査するための情報を収集したり、GuardDuty マルウェアスキャンを開始したりすることが可能になります。
- AWS Security Hub CSPM: サービスが有効化されている標準規格や製品統合の一覧表示、組織メンバーや管理者アカウントの一覧表示、アラートノイズを減らし、潜在的なインシデントを調査するための情報収集を行うことが可能になります。
- AWS Identity and Access Management: サービスが `AWSServiceRoleForAmazonGuardDutyMalwareProtection` サービスにリンクされたロールのロール情報を取得して、GuardDuty MalwareProtection が設定されているかどうかを確認できるようにします。
- AWS Security Incident Response: サービスがケースを作成および更新し、`SecurityIncidentResponseManaged=true` でタグ付けされたリソースに制限されたリソースにタグ付けできるようにします。サービスがメンバーシップ情報 (GetMembership、ListMemberships) を読み取ることを許可します。

ロールの管理

サービスリンクロールを手動で作成する必要はありません。AWS マネジメントコンソール、AWS CLI、または AWS API で AWS Security Incident Response にオンボードすると、サービスにリンクされたロールが自動的に作成されます。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は同じ方法でアカウントにロールを再作成できます。サービスにオンボードすると、サービスにリンクされたロールが再度作成されます。

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクされたロールのアクセス許可」を参照してください。

AWS Security Incident Response のサービスリンクロールをサポートするリージョン

AWS Security Incident Response は、サービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートします。

- 米国東部 (オハイオ)
- 米国西部 (オレゴン)
- 米国東部 (バージニア)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (ミラノ)
- 欧州 (パリ)
- 欧州 (スペイン)
- 欧州 (ストックホルム)
- 欧州 (チューリッヒ)
- アジアパシフィック (香港)
- アジアパシフィック (ハイデラバード)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (メルボルン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)

- カナダ (中部)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)
- 南米 (サンパウロ)
- アフリカ (ケープタウン)

AWS マネージドポリシー

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

ユーザー、グループ、ロールにアクセス許可を追加するには自分でポリシーを作成するよりも、AWS マネージドポリシーを使用する方が簡単です。チームに必要な権限のみを提供する IAM カスタマーマネージドポリシーを作成する には時間と専門知識が必要です。すぐに使用を開始するために、AWS マネージドポリシーを使用できます。これらのポリシーは一般的なユースケースを対象範囲に含めており、AWS アカウントで利用できます。AWS マネージドポリシーの詳細については「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS のサービスは関連する AWS マネージドポリシーを維持および更新します。AWS マネージドポリシーの権限を変更することはできません。サービスでは新しい機能を利用できるようにするために、AWS マネージドポリシーに権限が追加されることがあります。この種類の更新はポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS マネージドポリシーから権限を削除しないため、ポリシーの更新によって既存の権限が破棄されることはありません。

さらに、AWS は複数のサービスにまたがるジョブ機能の特徴に対するマネージドポリシーもサポートしています。例えば、ReadOnlyAccess AWS マネージドポリシーではすべての AWS のサービスおよびリソースへの読み取り専用アクセスを許可します。サービスが新しい機能を起動する場合、AWS は新たなオペレーションとリソース用に、読み取り専用の許可を追加します。ジョブ機能のポリシーの一覧および詳細については、「IAM ユーザーガイド」の「AWS のジョブ機能のマネージドポリシー」を参照してください。

内容

- AWS マネージドポリシー: AWSSecurityIncidentResponseServiceRolePolicy

- AWS マネージドポリシー: AWSSecurityIncidentResponseFullAccess
- AWS マネージドポリシー: AWSSecurityIncidentResponseReadOnlyAccess
- AWS マネージドポリシー: AWSSecurityIncidentResponseCaseFullAccess
- AWS マネージドポリシー: AWSSecurityIncidentResponseTriageServiceRolePolicy
- SLR およびマネージドポリシーに対する AWS Security Incident Response の更新

AWS マネージドポリシー: AWSSecurityIncidentResponseServiceRolePolicy

AWS Security Incident Response は、AWSSecurityIncidentResponseServiceRolePolicy AWS マネージドポリシーを使用します。この AWS マネージドポリシーは、AWSServiceRoleForSecurityIncidentResponse サービスにリンクされたロールに添付されます。このポリシーは、 AWS Security Incident Response がサブスクライブされたアカウントへのアクセス、ケースの作成、ケースの更新、ケースコメントの作成、ケースの一覧表示、ケースコメントの一覧表示、関連リソースのタグ付けを可能にします。

> **Important**
>
> 個人を特定できる情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。AWS Security Incident Response は、タグを使用して管理サービスを提供します。タグは、プライベートデータや機密データに使用することを意図していません

アクセス許可の詳細

サービスは、このポリシーを使用して、次のリソースに対してアクションを実行します。

- AWS Organizations: サービスで使用するメンバーシップアカウントをサービスが検索できるようにします。
- CreateCase: メンバーシップアカウントに代わってサービスがサービスケースを作成できるようにします。
- ListCases: セキュリティ調査の目的で、サービスの AI エージェントがケースを閲覧できるようにします。
- UpdateCase: サービスの AI エージェントがケースのメタデータを更新できるようにします。
- CreateCaseComment: サービスの AI エージェントが結果を症例コメントとして投稿できるようにします。

- ListComments: サービスの AI エージェントが自動調査を実行するために必要なケースコメントを閲覧できるようにします。
- TagResource: サービスの一部として設定されたサービスタグリソースを許可します。

このポリシーに関連付けられているアクセス許可は、AWSSecurityIncidentResponseServiceRolePolicy の AWS マネージドポリシーで確認できます。

AWS マネージドポリシー: AWSSecurityIncidentResponseFullAccess

AWS Security Incident Response は AWSSecurityIncidentResponseAdmin AWS マネージドポリシーを使用します。このポリシーは、サービスリソースへのフルアクセスと、関連する AWS のサービス へのアクセスを付与します。このポリシーを IAM プリンシパルと共に使用して、AWS Security Incident Response のアクセス許可をすばやく追加できます。

> **Important**
>
> 個人を特定できる情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。AWS Security Incident Response は、タグを使用して管理サービスを提供します。タグは、プライベートデータや機密データに使用することを意図していません

アクセス許可の詳細

サービスは、このポリシーを使用して、次のリソースに対してアクションを実行します。

- IAM プリンシパルの読み取り専用アクセス: サービスユーザーに、既存の AWS Security Incident Response リソースに対して読み取り専用アクションを実行する権限を付与します。
- IAM プリンシパル書き込みアクセス: サービスユーザーに AWS Security Incident Response リソースの更新、変更、削除、作成を許可します。

このポリシーに関連付けられているアクセス許可は、AWSSecurityIncidentResponseFullAccess の AWS マネージドポリシーで確認できます。

AWS マネージドポリシー: AWSSecurityIncidentResponseReadOnlyAccess

AWS Security Incident Response は、AWSSecurityIncidentResponseReadOnlyAccess AWS マネージドポリシーを使用します。ポリシーは、サービスケースリソースへの読み取り専用アクセス権を付

与します。このポリシーを IAM プリンシパルと共に使用して、AWS Security Incident Response のアクセス許可をすばやく追加できます。

> **Important**
>
> 個人を特定できる情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。AWS Security Incident Response は、タグを使用して管理サービスを提供します。タグは、プライベートデータや機密データに使用することを意図していません

アクセス許可の詳細

サービスは、このポリシーを使用して、次のリソースに対してアクションを実行します。

- IAM プリンシパルの読み取り専用アクセス: サービスユーザーに、既存の AWS Security Incident Response リソースに対して読み取り専用アクションを実行する権限を付与します。

このポリシーに関連付けられているアクセス許可は、AWSSecurityIncidentResponseReadOnlyAccess の AWS マネージドポリシーで確認できます。

AWS マネージドポリシー: AWSSecurityIncidentResponseCaseFullAccess

AWS Security Incident Response は、AWSSecurityIncidentResponseCaseFullAccess AWS マネージドポリシーを使用します。ポリシーは、サービスケースリソースへのフルアクセス権を付与します。このポリシーを IAM プリンシパルと共に使用して、AWS Security Incident Response のアクセス許可をすばやく追加できます。

> **Important**
>
> 個人を特定できる情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。AWS Security Incident Response は、タグを使用して管理サービスを提供します。タグは、プライベートデータや機密データに使用することを意図していません

アクセス許可の詳細

サービスは、このポリシーを使用して、次のリソースに対してアクションを実行します。

- IAM プリンシパルケースの読み取り専用アクセス: サービスユーザーに、既存の AWS Security Incident Response ケースに対して読み取り専用アクションを実行する権限を付与します。

- IAM プリンシパルケースの書き込みアクセス: サービスユーザーに AWS Security Incident Response ケースの更新、変更、削除、作成を行う権限を付与します。

このポリシーに関連付けられているアクセス許可は、AWSSecurityIncidentResponseCaseFullAccess の AWS マネージドポリシーで確認できます。

AWS マネージドポリシー: AWSSecurityIncidentResponseTriageServiceRolePolicy

AWS Security Incident Response は、AWSSecurityIncidentResponseTriageServiceRolePolicy AWS マネージドポリシーを使用します。この AWS マネージドポリシーは、AWSServiceRoleForSecurityIncidentResponse_Triage サービスにリンクされたロールに添付されます。

このポリシーは AWS Security Incident Response へのアクセスを提供し、セキュリティの脅威について環境を継続的にモニタリングし、セキュリティサービスを調整してアラートノイズを減らし、情報を収集して潜在的なインシデントを調査します。このポリシーを IAM エンティティにアタッチすることはできません。

> **Important**
>
> 個人を特定できる情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。AWS Security Incident Response は、タグを使用して管理サービスを提供します。タグは、プライベートデータや機密データに使用することを意図していません

アクセス許可の詳細

サービスは、このポリシーを使用して、次のリソースに対してアクションを実行します。

- イベント: サービスが Amazon EventBridge マネージドルールを作成できるようにします。このルールは、アカウントからサービスにイベントを配信するために AWS アカウントで必要なインフラストラクチャです。このアクションは、`triage.security-ir.amazonaws.com` によって管理されるすべての AWS リソースで実行されます。
- Amazon GuardDuty: サービスがセキュリティサービスを調整してアラートノイズを減らし、潜在的なインシデントを調査するための情報を収集したり、GuardDuty マルウェアスキャンを開始したりすることが可能になります。

- AWS Security Hub CSPM: サービスが有効化されている標準規格や製品統合の一覧表示、組織メンバーや管理者アカウントの一覧表示、アラートノイズを減らし、潜在的なインシデントを調査するための情報収集を行うことが可能になります。
- AWS Identity and Access Management: サービスが `AWSServiceRoleForAmazonGuardDutyMalwareProtection` サービスにリンクされたロールのロール情報を取得して、GuardDuty MalwareProtection が設定されているかどうかを確認できるようにします。
- AWS Security Incident Response: サービスがケースを作成および更新し、`SecurityIncidentResponseManaged=true` でタグ付けされたリソースに制限されたリソースにタグ付けできるようにします。サービスがメンバーシップ情報 (GetMembership、ListMemberships) を読み取ることを許可します。

このポリシーに関連付けられているアクセス許可は、AWSSecurityIncidentResponseTriageServiceRolePolicy の AWS マネージドポリシーで確認できます。

SLR およびマネージドポリシーに対する AWS Security Incident Response の更新

AWS Security Incident Response SLR およびマネージドポリシーロールに対する更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。

変更	説明	日付
更新済 – AWSSecurityIncidentResponseTriageServiceRolePolicy	このポリシーでは、サービスが `SecurityIncidentResponseManaged=true` でタグ付けされた GuardDuty フィルターを変更したり、ディテクター設定を更新したり、GuardDuty マルウェアスキャンを開始したりできるようになりました。これにより、サービスが Security Hub CSPM の検出結果に自動的に作用するルールを作成および管理し、組織構造を理解できるようになります。	2026 年 3 月 27 日
更新 – AWSSecurityIncidentResponse	このポリシーは現在、以下のリソースに対してアクションを実行します。	2025 年 11 月

変更	説明	日付
ServiceRolePolicy	ListCases: セキュリティ調査の目的で、サービスの AI エージェントがケースを閲覧できるようにします UpdateCase: サービスの AI エージェントがケースのメタデータを更新できるようにします。 CreateCaseComment: サービスの AI エージェントが結果を症例コメントとして投稿できるようにします ListComments: サービスの AI エージェントが自動調査を実行するために必要なケースコメントを閲覧できるようにします	
更新 – AWSSecurityIncidentResponseServiceRolePolicy	ポリシーに、"organizations:DescribeAccount" および "organizations:ListDelegatedAdministrators" 用の 2 つの新しいアクションと新しい条件が含まれるようになりました。 `"Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } }`	2025 年 11 月
SLR を更新し、サービスの使用権限をサポートするアクセス許可を追加しました。	AWSSecurityIncidentResponseTriageServiceRolePolicy が更新され、security-ir:GetMembership、security-ir:ListMemberships、security-ir:UpdateCase、guardduty:ListFilters、guardduty:UpdateFilter、guardduty:DeleteFilter、guardduty:GetAdministratorAccount アクセス許可が追加されました。guardduty:GetAdministratorAccount が、委任アカウントの GuardDuty 自動アーカイブフィルターの管理を容易にするために追加されました。	2025 年 6 月 2 日

変更	説明	日付
新しい SLR – AWSServiceRoleForSecurityIncidentResponse 新しいマネージドポリシー – AWSSecurityIncidentResponseServiceRolePolicy。	メンバーシップを識別するために AWS Organizations アカウントへのサービスアクセスを許可する新しいサービスリンクロールと添付されたポリシー。	2024 年 12 月 1 日
新しい SLR – AWSServiceRoleForSecurityIncidentResponse_Triage 新しいマネージドポリシー – AWSSecurityIncidentResponseTriageServiceRolePolicy	AWS Organizations アカウントへのサービスアクセスを許可し、セキュリティイベントのトリアージを実行できるようにする新しいサービスにリンクされたロールと添付されたポリシー。	2024 年 12 月 1 日
新しいマネージドポリシー – AWSSecurityIncidentResponseFullAccess	AWS Security Incident Response は、サービスの読み取りおよび書き込みアクション用に IAM プリンシパルに添付する新しい SLR を追加しました。	2024 年 12 月 1 日

変更	説明	日付
新しいマネージドポリシーロール – AWSSecurityIncidentResponseReadOnlyAccess	AWS Security Incident Response は、読み取りアクション用に IAM プリンシパルに添付する新しい SLR を追加しました。	2024 年 12 月 1 日
新しいマネージドポリシーロール – AWSSecurityIncidentResponseCaseFullAccess	AWS Security Incident Response サービスケースの読み取りおよび書き込みアクション用に IAM プリンシパルに添付する新しい SLR を追加しました。	2024 年 12 月 1 日
変更の追跡を開始しました。	AWS Security Incident Response SLR およびマネージドポリシーに対する変更の追跡を開始しました	2024 年 12 月 1 日

インシデントへの対応

セキュリティとコンプライアンスに関して、AWS とお客様の間で責任を共有します。この共有モデルにより、ホストオペレーティングシステムや仮想化レイヤーからサービスが運用されている施設の物理的なセキュリティに至るまで、さまざまなコンポーネントを AWS が運用、管理、制御するため、お客様の運用の負担が軽減されます。お客様は、AWS が提供するセキュリティグループのファイアウォール設定に加えて、ゲストオペレーティングシステム (更新やセキュリティパッチを含む) およびその他の関連アプリケーションソフトウェアを管理し、責任を持って管理する必要があります。詳細については、「AWS 責任共有モデル」を参照してください。

クラウド上で稼働するアプリケーションの目標を満たすセキュリティベースラインを確立することで、対応可能な逸脱を検出できます。セキュリティインシデント対応は複雑なトピックになる可能性があるため、インシデントレスポンスと自分の選択が企業目標に与える影響をよりよく理解できるように、次のリソースを確認することをお勧めします:「AWS Security Best Practices」ホワイトペーパー、および「Security Perspective of the AWS Cloud Adoption Framework」(CAF) ホワイトペーパー。

コンプライアンス検証

サードパーティーの監査者は、複数の AWS コンプライアンスプログラムの一部として AWS のサービスのセキュリティとコンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などが含まれます。

特定のコンプライアンスプログラムの範囲内の AWS サービスのリストについては、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」を参照してください。一般的な情報については、「AWS コンプライアンスプログラム」を参照してください。

サードパーティーの監査報告書は、AWS アーティファクトを使用してダウンロードすることができます。詳細については、「AWS Artifact のレポートのダウンロード」を参照してください。

AWS のサービスの使用時におけるユーザーのコンプライアンス責任は、データの機密性、企業のコンプライアンス目的、適用法と規制に応じて異なります。AWS は、コンプライアンスに役立つ以下のリソースを提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに焦点を当てたベースライン環境を AWS にデプロイするための手順を示します。
- HIPAA のセキュリティとコンプライアンスのアーキテクチャの設計に関するホワイトペーパー – このホワイトペーパーは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。
- AWS コンプライアンスのリソース - お客様の業界および/または場所に適用されるワークブックとガイドのコレクション。
- AWS Config デベロッパーガイドの「Evaluating resources with AWS Config Rules」 – AWS Config は、リソースの設定が社内慣行、業界のガイドライン、および規制にどの程度適合しているかを評価します。
- AWS セキュリティハブ – この AWS サービスは、AWS 内のセキュリティ状態に関する包括的なビューを提供します。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – この AWS サービスは、環境をモニタリングして、疑わしいアクティビティや悪意のあるアクティビティがないか調べることで、AWS アカウント、ワークロード、コンテナ、データに対する潜在的な脅威を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検出要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。

- AWS Audit Manager – この AWS サービスでは、AWS の使用状況を継続的に監査し、リスクの管理方法と、規制や業界標準へのコンプライアンスの管理方法を簡素化できます。

AWS Security Incident Response におけるログ記録とモニタリング

モニタリングは、AWS Security Incident Response および他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な要素です。AWS Security Incident Response は現在、組織と組織内で発生するアクティビティをモニタリングするために、次の AWS サービスをサポートしています。

AWS CloudTrail – CloudTrail を使用すると、AWS Security Incident Response コンソールから API コールをキャプチャできます。例えば、ユーザーが認証すると、CloudTrail はリクエストの IP アドレス、リクエストの実行者、および実行日時などの詳細を記録できます。

Amazon CloudWatch メトリクス – CloudWatch メトリクスでは、監視、報告、およびイベントが発生した場合のほぼリアルタイムでの自動アクションの実行が可能です。例えば、提供されたメトリクスで CloudWatch ダッシュボードを作成して AWS Security Incident Response 使用状況をモニタリングする、または提供されたメトリクスで CloudWatch アラームを作成して、設定されたしきい値の超過を通知することができます。

サービスの名前空間は AWS/Usage/ServiceName です。使用可能なメトリクス名は、ActiveManagedCases と SelfManagedCases です。

「AWS のサービス条件」に従って、AWS Security Incident Response レスポンダーチームは CloudTrail、VPC、DNS、S3 ログデータの履歴にアクセスできます。このデータは、AWS Security Incident Response サービスポータルでケースが開かれている場合、アクティブなセキュリティインシデント中に使用される場合があります。

レジリエンス

AWS のグローバルインフラストラクチャは、AWS リージョンとアベイラビリティーゾーンを中心として構築されています。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、および拡張性が優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

インフラストラクチャセキュリティ

AWS Security Incident Response は、AWS グローバルネットワークセキュリティによって保護されています。AWSセキュリティサービスと AWS がインフラストラクチャを保護する方法については、AWS クラウドセキュリティ を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、セキュリティの柱 - AWS Well-Architected Framework の インフラストラクチャ保護 を参照してください。

AWS の発行済み API コールを使用して、ネットワーク経由で AWS Security Incident Response にアクセスします。クライアントは次をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) で一時的なセキュリティ認証情報を生成して、リクエストに署名することもできます。

設定と脆弱性の分析

サービス格納ロールと関連する CloudFormation スタックセットを管理するのはお客様の責任です。

AWS はゲストオペレーティングシステム (OS) やデータベースへのパッチ適用、ファイアウォール設定、ディザスタリカバリなどの基本的なセキュリティタスクを処理します。これらの手順は適切な第三者によって確認され、証明されています。詳細については、以下の AWS リソースを参照してください。

- 責任共有モデル
- セキュリティ、アイデンティティ、コンプライアンスのベストプラクティス

サービス間の混乱した代理の防止

混乱した代理問題とは、アクションを実行する許可を持たないエンティティが、より高い特権を持つエンティティにそのアクションの実行を強制できるというセキュリティ問題です。AWS では、サービス間でのなりすましによって、混乱した代理問題が発生する場合があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐため、AWS では、アカウントのリソースへのアクセス権が付与されたサービスプリンシパルで、すべてのサービスのデータを保護するために役立つツールを提供しています。

リソースポリシーで AWS:SourceArn および AWS:SourceAccount のグローバル条件コンテキストキーを使用して、Amazon Connect が別のサービスに付与するアクセス許可をそのリソースに制限することをお勧めします。両方のグローバル条件コンテキストキーを同じポリシーステートメントで使用する場合は、AWS:SourceAccount 値と、AWS:SourceArn 値に含まれるアカウントが、同じアカウント ID を使用している必要があります。

混乱した代理問題を回避するための最も効果的な方法は、許可するリソースに正確な Amazon リソースネーム (ARN) を使用することです。リソースの完全な ARN が分からない場合や、複数のリソースを指定する場合は、ARN の不明部分にワイルドカード (*) を使った AWS:SourceArn グローバル条件コンテキストキーを使用します。例えば、arn:AWS:servicename::region-name::your AWS account ID:* です。

混乱した代理問題を防ぐ方法を示すロールの継承ポリシーの例については、「Confused deputy prevention policy」を参照してください。

Service Quotas

AWS Security Incident Response

AWS 全般のリファレンスガイドには、最新の AWS Security Incident Response エンドポイントとクォータが含まれています。

AWS Security Incident Response テクニカルガイド

内容

要約

このガイドでは、お客様の Amazon Web Services (AWS) クラウド環境内のセキュリティインシデントへの対応の基本について説明します。クラウドセキュリティとインシデント対応の概念の概要を示し、セキュリティ問題に対応する顧客が利用できるクラウドの機能、サービス、メカニズムを特定します。

このガイドは、技術的な役割を担う方を対象としており、情報セキュリティの一般的な原則を理解し、現在のオンプレミス環境でのセキュリティインシデント対応の基本的な知識を持ち、クラウドサービスに精通していることを前提としています。

Well-Architected の実現状況の確認

AWS Well-Architected フレームワークは、クラウド内でのシステム構築に伴う意思決定の長所と短所を理解するのに役立ちます。このフレームワークの 6 つの柱により、信頼性、安全性、効率、費用対効果、持続可能性の高いシステムを設計および運用するための、アーキテクチャのベストプラクティスを確認できます。AWS Well-Architected Tool のコンソールで無料で提供されている AWS Well-Architected Tool を使用すると、柱ごとに一連の質問に答えることで、これらのベストプラクティスに照らしてワークロードを評価できます。

クラウドアーキテクチャに関する専門的なガイダンスやベストプラクティス (リファレンスアーキテクチャのデプロイ、図、ホワイトペーパー) については、AWS アーキテクチャセンターを参照してください。

序章

セキュリティは AWS の最優先事項です。AWS のお客様は、最もセキュリティを重視する組織のニーズをサポートするために構築されたデータセンターとネットワークアーキテクチャのメリットが得られます。AWS が使用する責任共有モデルでは、AWS はクラウドのセキュリティを管理し、お客様はクラウド内のセキュリティに責任を負います。つまり、セキュリティ目標の達成に役立つ複数のツールやサービスへのアクセスを含め、セキュリティの実装を完全に制御できます。これらの機能は、AWS クラウドで実行されているアプリケーションのセキュリティベースラインを確立するのに役立ちます。

設定ミスや外部要因の変更など、ベースラインからの逸脱が発生した場合は、対応して調査する必要があります。これを成功させるには、AWS 環境内のセキュリティインシデント対応の基本概念と、セキュリティ問題が発生する前にクラウドチームの準備、教育、トレーニングを行うための要件を理解する必要があります。使用できるコントロールと機能を把握し、潜在的な問題を解決するために現在問題となっている例を確認し、自動化を使用して対応速度と一貫性を向上させる修復方法を特定することが重要です。さらに、これらの要件を満たすためのセキュリティインシデント対応プログラムの構築に関連するコンプライアンス要件や規制要件を理解する必要があります。

セキュリティインシデント対応は複雑な場合があるため、反復的アプローチを実装することをお勧めします。つまり、まずコアセキュリティサービスから開始し、基本的な検出機能と対応機能を構築し、その後プレイブックを作成してインシデント対応メカニズムの初期ライブラリを作成し、これを反復して改善していきます。

[開始する前に]

AWS でのセキュリティイベントのインシデント対応について学習する前に、AWS のセキュリティおよびインシデント対応に関連する標準およびフレームワークを理解しましょう。これらの基礎は、このガイドで説明されている概念とベストプラクティスを理解するのに役立ちます。

AWS のセキュリティ標準とフレームワーク

まず、「セキュリティ、アイデンティティ、コンプライアンスに関するベストプラクティス」、「セキュリティの柱 - AWS Well-Architected フレームワーク」、「Security Perspective of the Overview of the AWS Cloud Adoption Framework (AWS CAF)」ホワイトペーパーを読むことをお勧めします。

AWS CAF は、クラウドに移行する組織の各所での調整をサポートするガイダンスを提供します。AWS CAF ガイダンスは、クラウドベースの IT システムの構築に関連する、パースペクティブと呼ばれるいくつかの重点分野に分かれています。セキュリティパースペクティブは、ワークストリーム全体にセキュリティプログラムを実装する方法について説明するもので、その 1 つがインシデント対応です。本書は、お客様と連携し、効果的かつ効率的なセキュリティインシデント対応プログラムと各種機能の構築を支援してきた当社の経験の成果です。

業界のインシデント対応標準とフレームワーク

このホワイトペーパーは、米国国立標準技術研究所 (NIST) が作成した「コンピュータセキュリティインシデント対応ガイド 800-61 r3」のインシデント対応標準とベストプラクティスに従います。NIST によって導入された概念を読み、理解することは、有益な前提条件です。この NIST ガイドの概念とベストプラクティスは、このホワイトペーパーの AWS テクノロジーに適用されます。ただし、オンプレミスのインシデントシナリオは本書の対象外です。

AWS インシデント対応の概要

まず、クラウドにおけるセキュリティオペレーションとインシデント対応の違いを理解することが重要です。AWS で効果的な対応機能を構築するには、従来のオンプレミス対応からの違いと、インシデント対応プログラムに対するその影響を理解する必要があります。これらの各違いと、AWS インシデント対応の主要な設計原則について、このセクションで詳しく説明します。

AWS におけるインシデント対応の諸側面

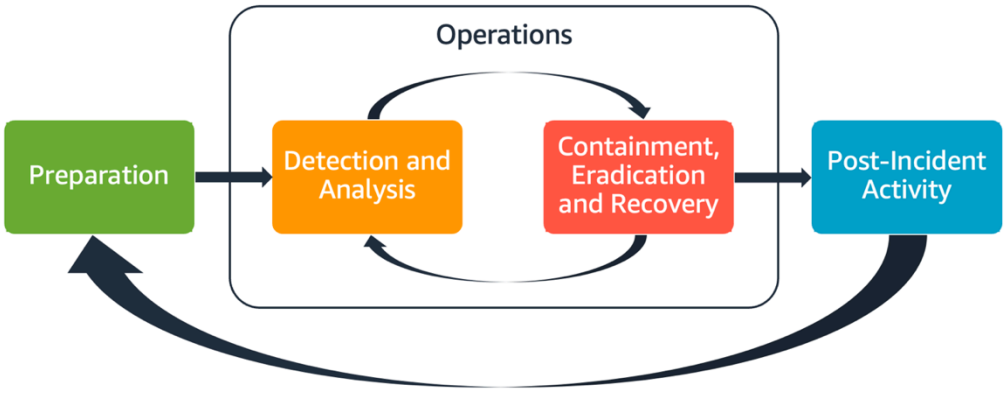
組織内のすべての AWS ユーザーは、セキュリティインシデント対応プロセスの基本を理解している必要があり、セキュリティ担当者はセキュリティ問題への対応方法を理解している必要があります。教育、トレーニング、経験は、クラウドインシデント対応プログラムを成功させるために不可欠であり、起こり得るセキュリティインシデントに対処する前に十分な余裕を持って実施するのが理想的です。クラウドでのインシデント対応プログラムの成功基盤は、準備、オペレーション、インシデント後アクティビティです。

これらの各側面を理解するには、以下の説明を参考にしてください。

- 準備 – 検出制御を有効にし、必要なツールやクラウドサービスへの適切なアクセスを検証することで、インシデント対応チームが AWS 内のインシデントを検出して対応できるように準備します。さらに、信頼性の高い一貫した応答を検証するために、手動と自動の両方で必要なプレイブックを準備します。
- オペレーション – NIST のインシデント対応フェーズ (検出、分析、封じ込め、根絶、復旧) に従って、セキュリティイベントと潜在的なインシデントに対処します。

- インシデント後アクティビティ – セキュリティイベントとシミュレーションの結果を反復することで、対応の有効性を改善し、対応と調査から得られる価値を高め、リスクをさらに軽減します。インシデントから学び、改善活動に対する強いオーナーシップを持つ必要があります。

これらの各側面については、本書で詳しく説明します。下図は、前述の NIST のインシデント対応ライフサイクルに沿った、これらの側面のフローを示しています。ここでの業務には、検出と分析に加えて、封じ込め、根絶、復旧が含まれています。



AWS インシデント対応の諸側面

AWS インシデント対応の原則と設計目標

「NIST SP 800-61 コンピュータセキュリティインシデント対応ガイド」で定義されているインシデント対応の一般的なプロセスとメカニズムは確実ではあるものの、クラウド環境でのセキュリティインシデントへの対応に関連する以下の特定の設計目標についても考慮することをお勧めします。

- 対応目標の確立 – ステークホルダー、法律顧問、組織のリーダーと協力してインシデント対応の目標を決定します。共通の目標には、問題の封じ込めと緩和、影響を受けたリソースの復旧、フォレンジック用のデータの保全、既知の安全な運用への復帰、そして最終的にはインシデントからの学習などがあります。
- クラウドを使用して対応する – イベントとデータが発生するクラウド内に対応パターンを実装します。
- 持っているものと必要なものを知る – ログ、リソース、スナップショット、その他の証拠は、対応専用の一元化されたクラウドアカウントにコピーして保存します。管理ポリシーを適用するタグ、メタデータ、メカニズムを使用します。使用しているサービスを把握し、それらのサービスを調査するための要件を特定する必要があります。環境を理解しやすくするために、タグ付けを使用することもできます。タグ付けについては、本書の「the section called “タグ付け戦略を策定し、実装する”」セクションで後述します。

- 再デプロイメカニズムを使用する – セキュリティの異常が設定ミスに起因する場合は、適切な設定でリソースを再デプロイして差異を取り除くだけで解決できる場合があります。セキュリティ侵害の可能性が見つかった場合は、根本原因に対する適切で検証済みの緩和策が再デプロイに含まれていることを確認します。
- 可能な場合は自動化する – 問題が発生したり、インシデントが繰り返されたりした場合は、一般的なイベントをプログラムで優先順位付けして対応するメカニズムを構築します。自動化が不十分で、特殊かつ複雑、または機密性の高いインシデントには、人手で対応します。
- スケーラブルなソリューションを選択する – 組織のアプローチのスケーラビリティがクラウドコンピューティングと適合しているように努めます。環境全体にスケールできる検出および対応のメカニズムを実装して、検出から対応までの時間を効果的に短縮します。
- プロセスを学び、改善する – プロセス、ツール、人員におけるギャップを積極的に特定し、それらを修正する計画を実施します。シミュレーションは、ギャップを見つけてプロセスを改善する安全な方法です。プロセスを反復的に実行する方法の詳細については、本書の「the section called “インシデント後のアクティビティ”」セクションを参照してください。

これらの設計目標は、インシデント対応と脅威検知の両方を実施する能力について、アーキテクチャの実装を確認することを促すものです。クラウドの実装を計画するときは、インシデントへの対応を検討します。フォレンジックに基づいた対応方法論を使用するのが理想的です。これは、場合によっては、このような対応タスク用に複数の組織、アカウント、ツールを特別に設定することを意味します。これらのツールと機能は、デプロイパイプラインによってインシデント対応担当者が利用できるようにする必要があります。リスクを大きくする可能性があるため、静的な状態のままにしないでください。

クラウドセキュリティインシデントのドメイン

AWS 環境内のセキュリティイベントに効果的に備え、対応するには、クラウドセキュリティインシデントの一般的なタイプを理解する必要があります。セキュリティインシデントが発生する可能性があるのは、サービス、インフラストラクチャ、アプリケーションの 3 つのドメインで、これらはお客様の責任の範囲内にあります。ドメインごとに異なる知識、ツール、対応プロセスが必要です。以下のドメインについて考えてください。

- サービスドメイン – サービスドメイン内のインシデントは、AWS アカウント、AWS Identity and Access Management (IAM) アクセス許可、リソースメタデータ、請求、またはその他の領域に影響する可能性があります。サービスドメインのイベントは、AWS API メカニズムでのみ対応するか、設定またはリソースのアクセス許可に関連する根本原因があり、関連するサービス指向のログ記録がある可能性があるイベントです。

- インフラストラクチャドメイン – インフラストラクチャドメイン内のインシデントには、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス上のプロセスやデータ、仮想プライベートクラウド (VPC) 内の Amazon EC2 インスタンスへのトラフィック、コンテナやその他の将来のサービスといったその他の領域など、データまたはネットワーク関連のアクティビティが含まれます。インフラストラクチャドメインのイベントへの対応には、多くの場合、フォレンジック分析のためのインシデント関連データの取得が含まれます。これには、インスタンスのオペレーティングシステムとのやり取りが含まれる可能性が高く、さまざまなケースで AWS API メカニズムが含まれる場合もあります。インフラストラクチャドメインでは、フォレンジック分析と調査を実行する専用の Amazon EC2 インスタンスなど、ゲストオペレーティングシステム内で AWS API とデジタルフォレンジック/インシデントレスポンス (DFIR) ツールの組み合わせを使用できます。インフラストラクチャドメインのインシデントには、ネットワークパケットキャプチャ、Amazon Elastic Block Store (Amazon EBS) ボリュームのディスクブロック、またはインスタンスから取得した揮発性メモリの分析が含まれる場合があります。
- アプリケーションドメイン – アプリケーションドメイン内のインシデントは、アプリケーションコードや、サービスまたはインフラストラクチャにデプロイされたソフトウェアで発生します。このドメインは、クラウドの脅威の検出と対応プレイブックに含める必要があり、インフラストラクチャドメイン内のインシデントと同様の対応を組み込むことができます。適切で十分に検討されたアプリケーションアーキテクチャでは、自動取得、復旧、デプロイメントを使用して、クラウドツールでこのドメインを管理できます。

これらのドメインでは、AWS アカウント、リソース、またはデータに対して行動を起こすアクターについて検討してください。内部のリスクか外部のリスクかにかかわらず、リスクフレームワークを使用して組織に対する特定のリスクを判断し、それに応じて準備します。さらに、インシデント対応計画の立案や十分に検討されたアーキテクチャの構築に役立つ脅威モデルを開発する必要があります。

AWS でのインシデント対応の主な違い

インシデント対応は、オンプレミスまたはクラウドにおけるサイバーセキュリティ戦略に不可欠な要素です。最小特権や多層防御などのセキュリティ原則は、オンプレミスとクラウドの両方でデータの機密性、完全性、可用性を保護することを目的としています。これらのセキュリティ原則をサポートするいくつかのインシデント対応パターンには、ログ保持、脅威モデリングから派生したアラート選択、プレイブック作成、セキュリティ情報およびイベント管理 (SIEM) の統合が含まれます。お客様がクラウドでこれらのパターンの設計とエンジニアリングを開始するときから違いが生じます。以下は、AWS でのインシデント対応の主な相違点です。

相違点 #1: 責任共有としてのセキュリティ

セキュリティとコンプライアンスの責任は、AWS とお客様の間で共有されます。この共有責任モデルにより、お客様の運用の負担が軽減されます。これは、ホストオペレーティングシステムや仮想化レイヤーからサービスが運用されている施設の物理的なセキュリティに至るまで、さまざまなコンポーネントを AWS が運用、管理、制御するためです。責任共有モデルの詳細については、「責任共有モデル」のドキュメントを参照してください。

クラウドにおける責任共有が変更されると、インシデント対応のオプションも変わります。これらのトレードオフを計画して理解し、ガバナンスのニーズと一致させることは、インシデント対応における重要なステップです。

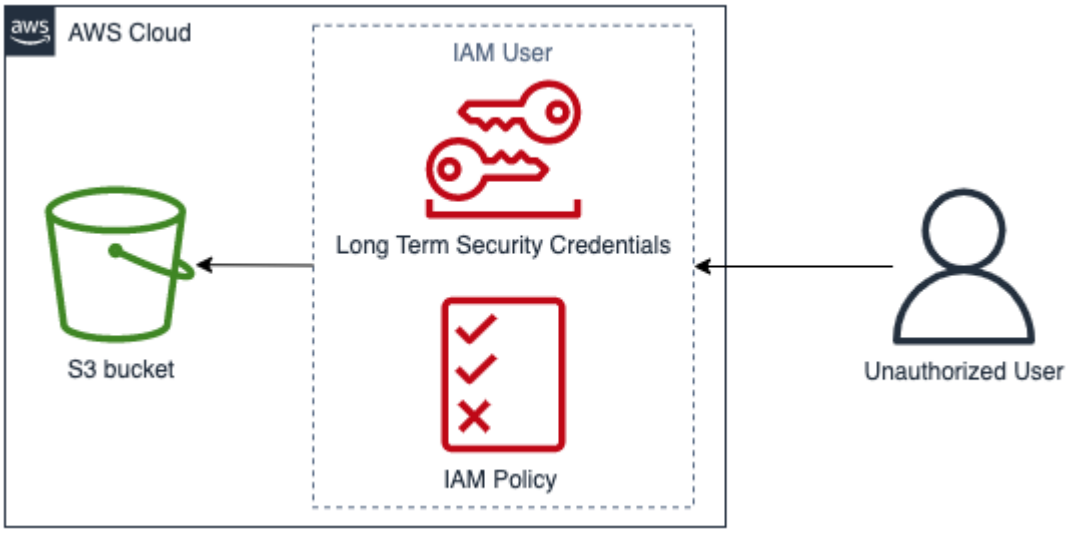
AWS との直接的な関係以外にも、特定の責任モデルにおいて責任を持つ他のエンティティが存在する可能性があります。例えば、オペレーションの一部の側面に責任を持つ内部組織単位があるかもしれません。また、クラウドテクノロジーの一部を開発、管理、運用する他の関係者との関係があるかもしれません。

運用モデルに合った適切なインシデント対応計画と適切なプレイブックを作成し、テストすることは非常に重要です。

相違点 #2: クラウドサービスドメイン

クラウドサービスに存在するセキュリティ上の責任の違いにより、セキュリティインシデントの新しいドメインである「サービスドメイン」が導入されました。これについては、「インシデントドメイン」セクションで前述しました。サービスドメインには、お客様の AWS アカウント、IAM アクセス許可、リソースメタデータ、請求、およびその他の領域が含まれます。このドメインの相違点は、インシデント対応の方法が異なることです。サービスドメイン内の対応は通常、従来のホストベースおよびネットワークベースの対応ではなく、API コールの確認と発行によって行われます。サービスドメインでは、影響を受けるリソースのオペレーティングシステムとはやり取りしません。

次の図は、アーキテクチャのアンチパターンに基づくサービスドメインのセキュリティイベントの例を示しています。このイベントでは、権限のないユーザーが IAM ユーザーの長期的なセキュリティ認証情報を取得します。この IAM ユーザーは、Amazon Simple Storage Service (Amazon S3) バケットからのオブジェクトの取得を許可する IAM ポリシーを保持しています。このセキュリティイベントに対応するには、AWS API を使用して、AWS CloudTrail や Amazon S3 アクセスログなどの AWS ログを分析します。また、AWS API を使用してインシデントを封じ込め、復旧します。



サービスドメインの例

相違点 #3: インフラストラクチャをプロビジョニングするための API

もう 1 つの相違点は、オンデマンドセルフサービスのクラウド特性です。主要施設のお客様は、世界中の多くの地理的場所で利用可能なパブリックエンドポイントとプライベートエンドポイントを介して、RESTful API を使用して AWS クラウド とやり取りします。お客様は、AWS 認証情報を使用してこれらの API にアクセスできます。オンプレミスのアクセスコントロールとは対照的に、これらの認証情報は必ずしもネットワークまたは Microsoft Active Directory ドメインによってバインドされるわけではありません。認証情報は、代わりに AWS アカウント内の IAM プリンシパルに関連付けられます。これらの API エンドポイントは、企業ネットワークの外部からアクセスできます。これは、認証情報が想定されたネットワークまたは地域の外部で使用されているインシデントに対応する際に理解しておくことが重要です。

API ベースである AWS の性質上、セキュリティイベントに対応するための重要なログソースは AWS CloudTrail です。これは AWS アカウントで行われた管理 API コールを追跡し、API コールの送信元の場所に関する情報を見つけることができます。

相違点 #4: クラウドの動的な性質

クラウドは動的であり、リソースをすばやく作成および削除できます。自動スケーリングを使用すると、トラフィックの増加に基づいてリソースをスピンアップおよびスピンダウンできます。存続期間の短いインフラストラクチャとペースの速い変更により、調査対象のリソースがもはや存在しない、または変更されていることがあります。AWS リソースのエフェメラルな性質と、AWS リソースの作成と削除を追跡する方法を理解することが、インシデント分析で重要になります。AWS Config を使用して AWS リソースの設定を評価できます。

相違点 #5: データアクセス

クラウドではデータアクセスも異なります。セキュリティ調査に必要なデータを収集するためにサーバーに接続することはできません。データは、有線および API コールを介して収集されます。この変化に備えるために、API でデータ収集を実行する方法を練習して理解し、効果的な収集とアクセスのための適切なストレージがあることを検証する必要があります。

相違点 #6: 自動化の重要性

お客様がクラウド導入のメリットを完全に実感するには、運用戦略に自動化を採用する必要があります。Infrastructure as Code (IaC) は、AWS サービスがコードを使用してデプロイ、設定、再設定、破棄される、効率に優れた自動化環境のパターンの 1 つであり、AWS CloudFormation またはサードパーティーソリューションなどのネイティブ IaC サービスによって促進されます。これにより、インシデント対応の実装で、特に証拠を処理するときに人為的なミスを回避するために望ましい高度な自動化が実現します。自動化はオンプレミスで使用されますが、AWS クラウドではよりシンプルで不可欠です。

これらの相違点に対処する

これらの相違点に対処するには、次のセクションで説明するステップに従って、人員、プロセス、テクノロジー全体でインシデント対応プログラムが適切に準備されていることを確認します。

準備

インシデントへの準備は、タイムリーかつ効果的なインシデント対応にとって重要です。準備は次の 3 つの分野にわたって行われます。

- 人員 – セキュリティインシデントに備えて人員を準備するには、インシデント対応に関連するステークホルダーを特定し、インシデント対応とクラウド技術に関するトレーニングを行う必要があります。
- プロセス – セキュリティインシデントに備えてプロセスを準備するには、アーキテクチャの文書化、徹底的なインシデント対応計画の策定、セキュリティイベントへの一貫した対応のためのプレイブックの作成が必要です。
- テクノロジー – セキュリティインシデントに備えてテクノロジーを準備するには、アクセスの設定、必要なログの集約と監視、効果的なアラートメカニズムの実装、対応と調査機能の開発が必要です。

これらの各分野は、効果的なインシデント対応にとって等しく重要です。3 つすべてが揃わなければ、インシデント対応プログラムは完全でも効果的でもありません。インシデントに備えるには、人員、プロセス、テクノロジーを緊密に連携して準備する必要があります。

People

セキュリティイベントに対応するには、セキュリティイベントへの対応をサポートするステークホルダーを特定する必要があります。さらに、効果的な対応のためには、AWS テクノロジーと AWS 環境に関するトレーニングを受講させることが重要です。

役割と責任を定義する:

セキュリティイベントに対処するためには、組織横断的な規律と行動力が必要です。組織内には、人事 (HR)、経営陣、法務部など、インシデント発生時に責任、説明責任、相談、情報提供の役割を持つ担当者が多くいるはずです。これらの役割と責任、および第三者が関与する必要があるかどうかを検討してください。多くの地域には、義務や禁止事項を規定する現地の法律があることに注意してください。セキュリティ対応計画のために責任、説明責任、相談、情報提供 (RACI) チャートを作成するのはマニュアル的に思われるかもしれませんが、作成することで、迅速かつ直接的なコミュニケーションが可能になり、イベントのさまざまな段階のリーダーシップを明確に説明できます。

インシデントが発生した場合、影響の測定に役立つ情報や背景を提供できる対象分野のエキスパート (SME) である、影響を受けるアプリケーションやリソースの所有者/開発者を巻き込むことが重要です。インシデント対応について開発者やアプリケーション所有者の専門知識に頼る際は、事前にやり取りを行い、関係を構築してください。アプリケーション所有者や SME (クラウド管理者やエンジニアなど) は、不慣れまたは複雑な環境、対応者がアクセスできない状況下で対応することが必要な場合もあります。

最後に、信頼できる関係性は、さらなる専門知識や価値のある調査を提供できるため、調査や対応に関与する可能性があります。自分のチームにこれらのスキルがない場合は、外部の人材に支援を依頼するということも検討できます。

インシデント対応スタッフをトレーニングする

組織が使用するテクノロジーのトレーニングをインシデント対応スタッフに受けさせることは、セキュリティイベントに適切に対応するために不可欠です。スタッフが基盤となるテクノロジーを理解していない場合、対応が長引くおそれがあります。従来のインシデント対応の概念に加えて、AWS サービスとその AWS 環境を理解することも重要です。オンライントレーニングやクラスルームトレーニングなど、インシデントスタッフをトレーニングするための仕組みは従来から多数あります。また、トレーニングの仕組みとして、ゲームデーやシミュレーションの実行も検討する必要があり

ます。シミュレーションの実行方法の詳細については、本書の「the section called “定期的にシミュレーションを実行する”」セクションを参照してください。

AWS クラウドのテクノロジーを理解する

依存関係を減らし、対応時間を短縮するには、セキュリティチームと対応者に対してクラウドサービスに関する教育を実施し、組織が使用する特定のクラウド環境で実践的な練習を行う機会が設けられていることを確認してください。インシデント対応者が効果的に機能するためには、AWS の基礎、IAM、AWS Organizations、AWS のロギングおよびモニタリングサービス、AWS セキュリティサービスを理解することが重要です。

AWS は、AWS のセキュリティおよびモニタリングサービスに関する実践的な経験を積むことができるオンラインセキュリティワークショップ (AWS セキュリティワークショップを参照) を提供します。AWSはまた、デジタルトレーニング、クラスルームトレーニング、AWS トレーニングパートナー、認定を通じて、さまざまなトレーニングオプションと学習パスも提供します。詳細については、「AWS のトレーニングと認定」を参照してください。

AWS は、複数のペルソナと重点分野をサポートする無料のトレーニングおよびサブスクリプションベースのトレーニングの両方を提供します。詳細については、AWS Skillbuilder を参照してください。

AWS 環境を理解する

AWS サービス、そのユースケース、およびそれらが相互にどのように統合されるかを理解することに加えて、組織の AWS 環境が実際にどのように設計され、どのような運用プロセスが実施されているかを理解することも同様に重要です。多くの場合、このような内部知識は文書化されておらず、少数のドメインエキスパートのみが把握しているため、依存関係が生まれ、イノベーションが妨げられ、対応時間が遅くなります。

これらの依存関係を回避し、対応時間を短縮するには、セキュリティアナリストが AWS 環境に関する内部知識を文書化し、アクセス可能にし、理解する必要があります。クラウドフットプリント全体を理解するには、関連するセキュリティ関係者とクラウド管理者間のコラボレーションが必要です。インシデント対応の準備プロセスには、アーキテクチャ図の文書化と一元化が含まれます。これについては、このホワイトペーパーの後半にある「the section called “アーキテクチャ図の文書化と一元化”」で説明します。ただし、人員の観点からは、アナリストが AWS 環境に関連する図や運用プロセスにアクセスして理解できることが重要です。

AWS 対応チームとサポートを理解する

サポート

サポート は、AWS ソリューションの成功とオペレーションの正常性をサポートするツールと専門知識にアクセスできる一連のプランを用意しています。AWS 環境の計画、導入、最適化に役立つテクニカルサポートや、より多くのリソースが必要な場合は、AWS ユースケースに最適なサポートプランを選択できます。

AWS リソースに影響する問題に関してサポートを得るための連絡窓口として、AWS マネジメントコンソール (サインインが必要) のサポートセンターを検討します。サポート へのアクセスは IAM によって制御されます。AWS サポートの機能を利用する方法については、「Getting started with サポート」を参照してください。

さらに、不正使用を報告する必要がある場合は、AWS Trust and Safety チームにお問い合わせください。

セキュリティインシデント対応エンジニア

セキュリティインシデント対応エンジニアは、AWS 責任共有モデルのお客様側のセキュリティイベントが発生したときにお客様にサポートを提供する、常時対応の専門のグローバル AWS チームです。

セキュリティインシデント対応エンジニアは、ユーザーをサポートする際に、AWS で発生しているセキュリティイベントのトリアージと復旧を支援します。AWS サービスログを使用して根本原因の分析を支援し、復旧のための推奨事項を提示します。また、将来のセキュリティイベントを回避するのに役立つセキュリティに関する推奨事項やベストプラクティスを提供します。

AWS のお客様は、AWS サポートケースを通じてセキュリティインシデント対応エンジニアを関与させることができます。

- すべてのお客様:
  1. アカウントと請求
  2. サービス: アカウント
  3. カテゴリ: セキュリティ
  4. 重要度: 一般的な質問

- デベロッパー向け サポートプランをご利用のお客様:

1. アカウントと請求
2. サービス: アカウント
3. カテゴリ: セキュリティ
4. 重要度: 重要な質問

- ビジネス向け サポートプランをご利用のお客様:
  1. アカウントと請求
  2. サービス: アカウント
  3. カテゴリ: セキュリティ
  4. 重要度: ビジネスに影響を与える緊急の質問

- エンタープライズ向け サポートプランをご利用のお客様:
  1. アカウントと請求
  2. サービス: アカウント
  3. カテゴリ: セキュリティ
  4. 重要度: 重大なビジネスリスクに関する質問

- AWS Security Incident Response サブスクリプションをご利用のお客様: https://console.aws.amazon.com/security-ir/ でセキュリティインシデント対応コンソールを開きます。

DDoS 対応のサポート

AWS の AWS Shield は、AWS で実行されているウェブアプリケーションを保護するマネージド型分散型サービス拒否 (DDoS) 保護サービスを提供します。AWS Shield は、アプリケーションのダウンタイムとレイテンシーを最小限に抑えることができる常時オンの検出機能と自動インライン緩和を提供するため、サポートに問い合わせることなく DDoS 保護のメリットを享受できます。AWS Shield には、Shield Standard と Shield Advanced の 2 つのティアがあります。両者の違いに関する詳細は、「Shield の特徴」を参照してください。

AWS Managed Services (AMS)

AWS Managed Services (AMS) は AWS インフラストラクチャ管理を継続的に提供するため、お客様はアプリケーションに集中できます。AMS は、ベストプラクティスを実行してインフラストラクチャを管理することで、運用のオーバーヘッドとリスクを減らします。AMS は、変更リクエスト、モニタリング、パッチ管理、セキュリティ、バックアップサービスなどの一般的なアクティビティを

自動化し、インフラストラクチャをプロビジョニング、実行、サポートする、ライフサイクル全般にわたるサービスを提供します。

AMS は、一連のセキュリティ検出コントロールの展開に責任を持ち、毎日第一線でアラートに対応します。アラートが発生すると、AMS は標準的な自動プレイブックと手動プレイブックに従って、一貫した対応が行われていることを確認します。これらのプレイブックはオンボーディング中に AMS の顧客に共有されるため、顧客は AMS と対応策を練り、調整することができます。

プロセス

インシデント対応のプロセスを熟考し、明確に定義することは、インシデント対応プログラムを成功させ、拡張性を持たせるための鍵となります。セキュリティイベントが発生した場合、明確な手順とワークフローがあれば、タイムリーに対応できます。既にインシデント対応プロセスがある場合もあります。現在の状態にかかわらず、インシデント対応プロセスを定期的に更新、反復、テストすることが重要です。

インシデント対応計画を作成してテストする

インシデント対応のために最初に作成する文書は、インシデント対応計画です。インシデント対応計画は、インシデント対応プログラムと戦略の基礎となるように設計されています。インシデント対応計画は、通常は以下のセクションを含む概要文書です。

- インシデント対応チームの概要 – インシデント対応チームの目標と機能の概要が記されている
- 役割と責任 – インシデントに対応する利害関係者が一覧表示され、インシデント発生時のそれぞれの役割が詳しく記されている
- コミュニケーションプラン – 連絡先とインシデント発生時の連絡方法が記されている

  インシデント関連の通信のバックアップ方法としては、帯域外通信を確保することがベストプラクティスです。安全な帯域外通信チャネルを提供するアプリケーションの例は AWS Wickr です。
- インシデント対応の各段階と取るべき措置 – インシデント対応の各段階 (検出、分析、根絶、封じ込め、復旧など) を一覧にし、各段階で取るべき措置を大まかに記している
- インシデントの深刻度と優先順位の決定 – インシデントの深刻度の分類方法、インシデントの優先付け方法、深刻度の定義がエスカレーション手順にどう影響するか、を詳しく説明している

これらのセクションは、さまざまな規模や業界の企業で共通していますが、各組織のインシデント対応計画は異なります。組織に最適なインシデント対応計画を立てる必要があります。

アーキテクチャ図の文書化と一元化

セキュリティイベントに迅速かつ正確に対応するには、システムとネットワークがどのように設計されているかを理解する必要があります。これらの内部パターンを理解することは、インシデント対応だけでなく、そのパターンがベストプラクティスに従って設計されているというアプリケーション間の一貫性を検証する上でも重要です。また、この文書が最新であり、新しいアーキテクチャパターンに従って定期的に更新されていることを確認する必要があります。次のような項目を詳述する文書と内部リポジトリを作成する必要があります。

- AWS アカウント構造 - 以下を把握しておく必要があります。
  - AWS アカウントはいくつ存在するか?
  - それらの AWS アカウントはどのように整理されているか?
  - AWS アカウントのビジネスオーナーは誰か?
  - サービスコントロールポリシー (SCP) を使用しているか？ 使用している場合、SCP を使用してどのような組織的なガードレールが実装されているか?
  - 使用できるリージョンとサービスを制限しているか?
  - ビジネスユニットと環境 (dev/test/prod) にどのような違いがあるか?
- AWS サービスパターン
  - どの AWS サービスを使用しているか?
  - 最も広く使用されている AWS サービスは何か?
- アーキテクチャパターン
  - どのクラウドアーキテクチャを使用しているか?
- AWS 認証パターン
  - デベロッパーは通常、AWS をどのように認証しているか?
  - IAM ロールまたはユーザー (またはその両方) を使用しているか? AWS の認証は ID プロバイダー (IdP) に接続されているか?
  - IAM ロールまたはユーザーを従業員またはシステムにどのように対応付けているか?
  - 権限がなくなった人のアクセス権をどのように取り消しているか?
- AWS 認可パターン
  - 開発者はどのような IAM ポリシーを使用しているか?
  - リソースベースのポリシーを使用しているか?
- ログ記録とモニタリング
  - 使用しているログ記録のソースと保存場所は?

  - AWS CloudTrail ログを集計しているか? 集計している場合、どこに保存しているか?
  - CloudTrail ログをどのようにクエリしているか?
  - Amazon GuardDuty が有効になっているか?
  - GuardDuty の検出結果 (コンソール、チケットシステム、SIEM など) にどのようにアクセスしているか?
  - 検出結果またはイベントは SIEM に集約されているか?
  - チケットは自動的に作成されるか?
  - 調査用にログを分析するためにどのようなツールが用意されているか?
- ネットワークトポロジ
  - ネットワーク上のデバイス、エンドポイント、および接続は、物理的または論理的にどのように配置されているか?
  - ネットワークは AWS とどのように接続されているか?
  - ネットワークトラフィックは環境間でどのようにフィルタリングされているか?
- 外部インフラストラクチャ
  - 外部向けアプリケーションはどのようにデプロイされているか?
  - パブリックアクセス可能な AWS リソースは何か?
  - 外部向けインフラストラクチャが含まれている AWS アカウントは?
  - どのような DDoS または外部フィルタリングが使用されているか?

内部のテクニカルな図およびプロセスを文書化すると、インシデント対応アナリストが業務を容易に行えるようになり、セキュリティイベントに対応するための制度上の知識を迅速に取得できます。内部のテクニカルプロセスの詳細な文書化は、セキュリティ調査を簡素化するだけでなく、プロセスの合理化と評価も調整します。

インシデント対応プレイブックを作成する

インシデント対応プロセスを準備する上で重要なのは、プレイブックを作成することです。インシデント対応プレイブックには、セキュリティイベントが発生したときに従うべき一連の規範的なガイダンスと手順が記載されています。明確な体制と手順があると、対応が簡単になり、人為的ミスの可能性が低くなります。

プレイブックの作成対象

プレイブックは、次のようなインシデントシナリオ向けに作成する必要があります。

- 予想されるインシデント – プレイブックは、予測されるインシデントに合わせて作成する必要があります。これには、サービス拒否 (DoS)、ランサムウェア、認証情報の漏えいなどの脅威が含まれます。
- 既知のセキュリティ上の検出結果またはアラート – プレイブックは、既知のセキュリティ上の検出結果とアラート (GuardDuty の検出結果など) に基づいて作成する必要があります。GuardDuty の検出結果を受け取っても、どうすればよいかわからないといったことがあるかもしれません。そこで、GuardDuty の検出結果を誤って処理したり無視したりすることがないように、GuardDuty で検出される可能性のある問題ごとにプレイブックを作成しておきます。修正に関する詳細とガイダンスについては、GuardDuty のドキュメントで確認できます。なお、GuardDuty はデフォルトでは有効になっておらず、コストがかかりますので注意してください。GuardDuty の詳細については、「付録 A: クラウド機能定義 - the section called “可視性とアラート”」を参照してください。

プレイブックに含める内容

プレイブックには、起こりうるセキュリティインシデントを適切に調査して対応するために、セキュリティアナリストが実行すべき技術的な手順を記載する必要があります。

プレイブックに記載すべき項目には次のようなものがあります。

- プレイブックの概要 – このプレイブックがどのようなリスクやインシデントシナリオに対応しているか。このプレイブックの目的は何か。
- 前提条件 – このインシデントシナリオには、どのようなログおよび検出メカニズムが必要か。どのような通知が想定されるか。
- ステークホルダー情報 – 関係者とその連絡先情報。各利害関係者の責任は何か。
- 対応ステップ – インシデント対応の各フェーズで、どのような戦術的措置を講じるべきか。アナリストはどのようなクエリを実行すべきか。望ましい結果を得るためにどのようなコードを実行すべきか。
  - 検知 – インシデントはどのように検出されるか。
  - 分析 – 影響範囲はどのように特定されるか。
  - 封じ込め – 影響範囲を限定するために、インシデントをどのように隔離するか。
  - 根絶 – どのようにして脅威を環境から取り除くか。
  - 復旧 – 影響を受けたシステムやリソースをどのようにして本番環境に戻すか。
- 期待される結果 – クエリとコードが実行された後、プレイブックで想定される結果はどのようなものか。

各プレイブックの情報の一貫性を検証するには、プレイブックテンプレートを作成して他のセキュリティプレイブックで使用すると便利です。ステークホルダー情報など、以前にリストアップした項目の一部は、複数のプレイブック間で共有できます。この場合、その情報を一元化した文書を作成し、プレイブックで参照してから、そのプレイブックで明示的な違いを列挙することができます。これにより、すべてのプレイブックで同じ情報を逐一更新する必要がなくなります。テンプレートを作成し、プレイブックで共通の情報または共有されている情報を特定することで、プレイブックの作成を簡素化し、スピードアップできます。最後に、プレイブックは時間の経過に伴って進化する可能性があります。ステップの一貫性を確認しておくことは、自動化の要件となります。

サンプルプレイブック

いくつかのサンプルプレイブックを付録 B の「the section called “プレイブックリソース”」に用意しています。ここでの例は、どのようなプレイブックを作成するか、どのような内容をプレイブックに含めるかの手引きとして使用できます。とはいえ、重要なのはビジネスに最も関連のあるリスクを組み込んだプレイブックを作成することです。プレイブック内のステップとワークフローに、あなたの会社のテクノロジーとプロセスが含まれていることを確認する必要があります。

定期的にシミュレーションを実行する

組織は時間の経過に伴って成長し、進化しますが、それは脅威の状況も同様です。このため、インシデント対応機能を継続的に見直すことが重要です。この評価を行う方法の 1 つとして、シミュレーションがあります。シミュレーションでは、脅威アクターの戦術、手法、手順 (TTP) を模倣するように設計された現実のセキュリティイベントシナリオを使用します。これにより、組織は実際に発生する可能性のある模擬サイバーイベントに対応することで、インシデント対応能力を訓練し、評価できます。

シミュレーションには、次のようなさまざまな利点があります。

- サイバー脅威への準備状況を検証し、インシデント対応者の信頼度を高めます。
- ツールとワークフローの精度と効率性をテストします。
- インシデント対応計画に沿うように、コミュニケーションとエスカレーションの方法を改良します。
- あまり一般的でないベクトルに対応する機会を提供します。

シミュレーションのタイプ

シミュレーションには主に 3 つのタイプがあります。

- 机上演習 – 机上でのシミュレーションは、インシデントに対応するさまざまな利害関係者が参加して役割や責任を実践し、確立されたコミュニケーションツールやプレイブックを活用する、完全にディスカッションベースのセッションです。演習は、通常はバーチャル会場、実際の施設、またはそれらの組み合わせが可能で、丸 1 日かけて進行します。ディスカッションベースのため、机上演習ではプロセス、人材、コラボレーションに焦点を当てます。テクノロジーは議論に不可欠ですが、インシデント対応ツールやスクリプトを実際に使用することは、一般的に机上演習には含まれません。
- パープルチーム演習 – パープルチーム演習は、インシデント対応者 (ブルーチーム) と模擬の脅威アクター (レッドチーム) のコラボレーションレベルを高めるものです。ブルーチームはセキュリティオペレーションセンター (SOC) のメンバーで構成されますが、実際のサイバーイベントに関与する他の利害関係者が参加することもあります。レッドチームは通常、攻撃的なセキュリティのトレーニングを受けたペンテストチームまたは主な利害関係者で構成されています。レッドチームは、シナリオが正確で実現可能なものになるように、演習のファシリテーターと協力して作業します。パープルチーム演習では、インシデント対応の取り組みを支援する検出メカニズム、ツール、標準運用手順 (SOP) に重点が置かれます。
- レッドチーム演習 – レッドチーム演習では、攻撃側 (レッドチーム) は、あらかじめ決められた範囲から、ある目的または一連の目的を達成するためのシミュレーションを行います。防御側 (ブルーチーム) は、演習の範囲と期間について必ずしも知っているとは限らないため、実際のインシデントにどのように対応するか、より現実的に評価できます。レッドチーム演習では侵入テストになる可能性があります。そのため慎重に行い、コントロールを実施して、演習によって環境に実害を与えないことを確認してください。

> **Note**
>
> AWS では、お客様は、パープルチーム演習またはレッドチーム演習を行う前に、ペネトレーションテストのウェブサイトで利用可能なペネトレーションテストのポリシーを確認する必要があります。

表 1 は、これらのタイプのシミュレーションの主な違いをまとめたものです。定義は一般に緩やかな定義と見なされ、組織のニーズに合わせてカスタマイズできることに注意してください。

表 1 – シミュレーションのタイプ

	机上演習	パープルチーム演習	レッドチーム演習
まとめ	1 つの特定のセキュリティインシデントシナリオに焦点を当てた、紙ベースの演習。概要または技術的な内容とすることができ、紙の資料を使用して実行されます。	机上演習と比較してより現実的なタイプです。パープルチーム演習の間、ファシリテーターは参加者と協力して演習の工ンゲージメントを高め、必要に応じてトレーニングを提供します。	一般的に、より高度なタイプのシミュレーションです。通常は隠密性が高く、参加者が演習のすべての詳細を把握しない場合があります。
必要なリソース	必要な技術リソースは限定的	さまざまなステークホルダーが必要、高度な技術リソースが必要	さまざまなステークホルダーが必要、高度な技術リソースが必要
複雑さ	低	中	高

定期的にサイバーシミュレーションを実施することを検討してください。演習は、タイプごとにそれぞれのメリットを参加者と組織全体にもたらします。それほど複雑ではないタイプのシミュレーション (机上演習など) から始めて、より複雑なシミュレーションタイプ (レッドチーム演習) に進むこともできます。セキュリティの成熟度、リソース、目標とする成果に基づいてシミュレーションタイプを選択する必要があります。お客様によっては、複雑さやコスト面から、レッドチーム演習を選択しない場合があります。

演習ライフサイクル

選択したシミュレーションタイプにかかわらず、シミュレーションは通常、以下のような手順に従います。

1. 演習の中核要素の定義 – シミュレーションのシナリオと目的を定義します。いずれも、リーダーの承認が必要です。
2. 主な利害関係者の特定 – 少なくとも、演習には演習のファシリテーターと参加者が必要です。シナリオによっては、追加で法務、コミュニケーション、経営幹部などの利害関係者が関与する場合があります。

3. シナリオの構築とテスト – 特定の要素が実現不可能な場合は、シナリオの構築中に再定義が必要なこともあります。このステージのアウトプットとして、シナリオの最終版が完成することが期待されます。
4. シミュレーションの進行 – シミュレーションのタイプによって、使用する進行内容 (紙ベースのシナリオと技術的に高度なシミュレーションシナリオの比較) が決まります。ファシリテーターは、演習進行の戦略を目的に合わせて調整し、最大の効果が得られるように、できるだけすべての参加者に演習に参加してもらう必要があります。
5. アフターアクションレビュー (AAR) の作成 – うまくいった部分、改善の余地がある部分、潜在的なギャップを特定します。AAR では、シミュレーションの有効性だけでなく、シミュレートされたイベントに対するチームの反応も測定して、今後のシミュレーションの進捗を経時的に追跡できるようにする必要があります。

テクノロジー

セキュリティインシデントの前に適切なテクノロジーを開発し、実装すると、インシデント対応スタッフは適切なタイミングで調査し、範囲を理解し、アクションを実行できるようになります。

AWS アカウント構造を開発する

AWS Organizations では、AWS リソースの拡大とスケールに合わせて、AWS 環境を一元的に管理および運用できます。AWS 組織は、AWS アカウントを統合し、1つの単位として管理できるようにするものです。組織単位 (OU) を使用すると、アカウントをまとめてグループ化し、単一の単位として管理できます。

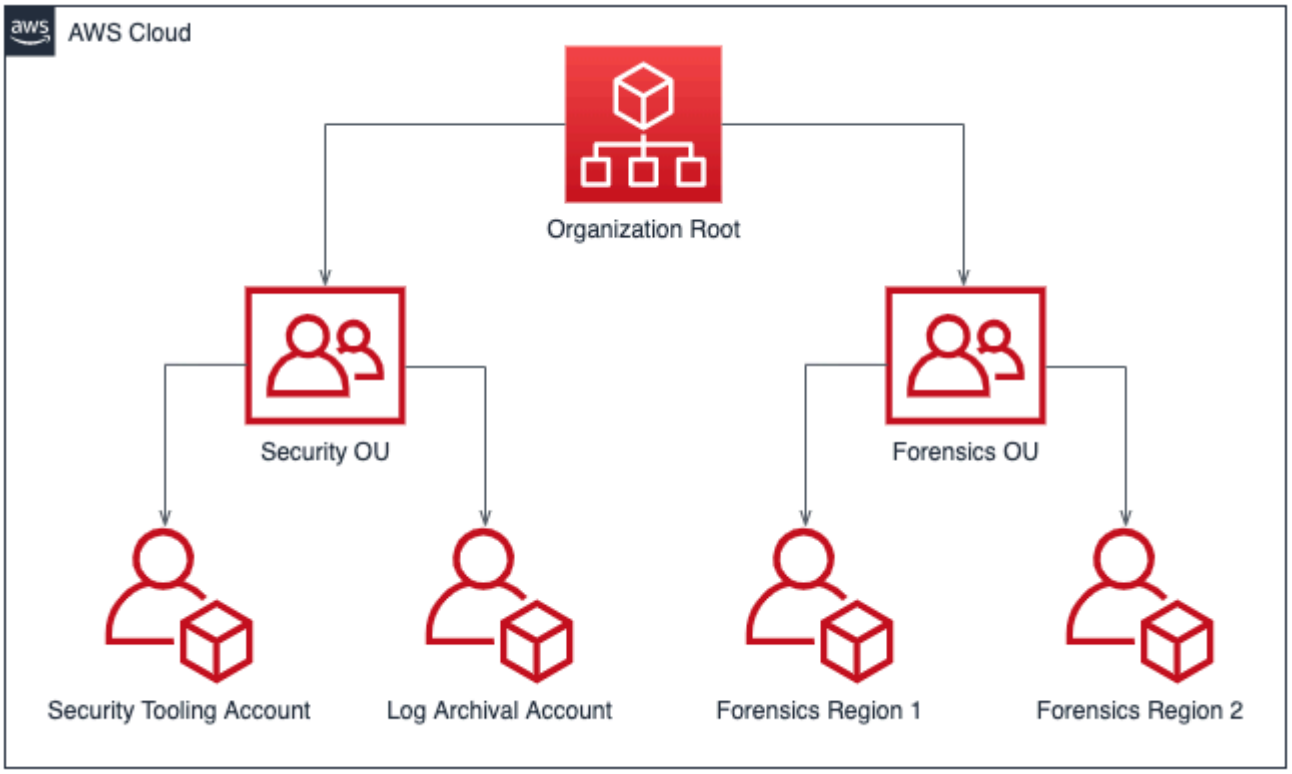
インシデント対応には、セキュリティ OU およびフォレンジック OU を含むインシデント対応の機能をサポートする AWS アカウント構造があると便利です。セキュリティ OU 内には、次のアカウントが必要です。

- ログアーカイブ – ログアーカイブ用 AWS アカウントでログを集約します。
- セキュリティツール – セキュリティサービスをセキュリティツール用の AWS に一元化します。このアカウントは、セキュリティサービスの委任管理者として機能します。

フォレンジック OU 内では、お客様のビジネスモデルと運用モデルに最適なフォレンジックアカウントに応じて、フォレンジック用に 1 つのアカウントを実装するか、事業を展開するリージョンごとにアカウントを実装できます。リージョンごとのアカウントアプローチの例として、米国東部 (バージニア北部) (us-east-1) と米国西部 (オレゴン) (us-west-2) でのみ運用する場合、フォレンジック OU には 2 つのアカウントがあります (1 つは us-east-1 用、もう 1 つは us-west-2 用)。新しいア

カウントのプロビジョニングには時間がかかるため、インシデントのかなり前にフォレンジックアカウントを作成して実装し、対応担当者が効果的に対応できるように準備しておくことが重要です。

次の図は、リージョンごとのフォレンジックアカウントを持つフォレンジック OU を含むアカウント構造の例を示しています。



インシデント対応のためのリージョンごとのアカウント構造

タグ付け戦略を策定し、実装する

AWS リソースを取り巻くビジネスユースケースやかかわりのある内部関係者についての背景情報の入手は難しい場合があります。これを達成する方法の 1 つとして、タグを使用して、ユーザー定義のキーと値で構成されるメタデータを AWS リソースに割り当てる方法があります。タグを作成して、目的、所有者、環境、処理されるデータの種類など、任意の基準でリソースを分類できます。

一貫したタグ付け戦略があると、AWS リソースに関する背景情報をすばやく特定、識別できるため、応答時間を短縮することができます。タグは、対応の自動化を開始するためのメカニズムとしても機能します。タグ付けする内容の詳細については、「AWS リソースのタグ付けに関するドキュメント」を参照してください。まず、組織全体に導入するタグを定義する必要があります。その後、このタグ付け戦略を導入し、適用します。導入と適用の詳細については、AWS のブログ「Implement AWS resource tagging strategy using AWS Tag Policies and Service Control Policies (SCPs)」を参照してください。

AWS アカウントの連絡先情報を更新する

AWS アカウントごとに、正確で最新の連絡先情報を指定して、セキュリティ、請求、運用などのトピックについて、適切な関係者が AWS からの重要な通知を受け取るようにすることが重要です。AWS アカウントごとに、セキュリティ、請求、運用に関する主要な連絡先と代替連絡先を指定できます。これらの連絡先の違いについては、「AWS アカウント管理リファレンスガイド」を参照してください。

代替連絡先の管理の詳細については、「代替連絡先の追加、変更、または削除に関する AWS ドキュメント」を参照してください。請求、運用、セキュリティ関連の問題をチームで管理する場合は、E メール配信リストを使用することをお勧めします。1 人の従業員への依存は不在時や退職時に業務が滞る原因となる場合がありますが、E メール配信リストによってそれが解消されます。また、ルートアカウントのパスワードリセットと多要素認証 (MFA) リセットから守るために、電話番号を含む E メールとアカウントの連絡先情報が十分に保護されていることを確認する必要があります。

AWS Organizations を使用しているお客様の場合、組織管理者は、各 AWS アカウントの認証情報を必要とせずに、管理アカウントまたは委任された管理者アカウントを使用して、メンバーアカウントの代替連絡先を一元管理できます。また、新しく作成されたアカウントに正確な連絡先情報があることも確認する必要があります。ブログ記事「Automatically update alternate contacts for newly created AWS アカウント」を参照してください。

AWS アカウントへのアクセス権を準備する

インシデントの間、インシデント対応チームはインシデントに関連する環境とリソースにアクセスできる必要があります。イベントが発生する前に、チームに職務を実行するための適切なアクセス権があることを確認しておきましょう。そのためには、チームメンバーが必要とするアクセスレベル (どのような対策を講じる可能性があるかなど) を把握し、最小特権アクセスを事前にプロビジョニングしておく必要があります。

このアクセス権を実装およびプロビジョニングするには、AWS アカウント戦略とクラウドアイデンティティ戦略を特定し、組織のクラウドアーキテクトと話し合い、どのような認証および認可方法が設定されているのかを理解する必要があります。これらの認証情報は特権的であるため、実装の一環として、承認フローを使用するか、保管庫や金庫から認証情報を取得することを検討する必要があります。実装後、イベントが発生する前にチームメンバーのアクセス権を文書化およびテストし、遅延なく対応できることを確認する必要があります。

最後に、セキュリティインシデントへの対応に特化して作成されたユーザーには、十分なアクセス権を提供するために特権が付与されることがよくあります。そのため、これらの認証情報についてはその使用を制限および監視し、日常業務に使用しないようにする必要があります。

脅威の状況を理解する

脅威モデルを作成する

脅威モデルを作成することで、組織は、権限のないユーザーに先立って脅威と緩和策を特定できます。脅威モデリングには多くの戦略とアプローチがあります。ブログ記事「脅威モデリングのアプローチ方法」を参照してください。インシデント対応において、脅威モデルは、脅威アクターがインシデント中に使用した可能性のある攻撃ベクトルを特定するのに役立ちます。適切なタイミングで対応するには、何から守っているのかを理解することが不可欠です。脅威モデリングに AWS Partner を活用することもできます。AWS パートナーを検索するには、AWS Partner Networkを使用します。

サイバー脅威インテリジェンスを統合して使用する

サイバー脅威インテリジェンスは、脅威アクターの意図、機会、能力に関するデータと分析です。脅威インテリジェンスを取得し、利用することは、インシデントを早期に検出し、脅威アクターの行動をよりよく理解するのに役立ちます。サイバー脅威インテリジェンスには、IP アドレスやマルウェアのファイルハッシュなどの静的インジケータが含まれます。また、動作パターンやインテントなどの概要情報も含まれます。脅威インテリジェンスは、多数のサイバーセキュリティベンダーやオープンソースリポジトリから収集できます。

AWS 環境に脅威インテリジェンスを統合し、最大限に活用するには、既存の機能を使用して独自の脅威インテリジェンスリストを統合できます。Amazon GuardDuty は、AWS 内部およびサードパーティーの脅威インテリジェンスソースを使用します。DNS ファイアウォールや AWS WAF ルールなどの他の AWS サービスも、AWS の高度な脅威インテリジェンスグループから情報を受け取ります。一部の GuardDuty の検出結果は MITRE ATT&CK Framework にマッピングされ、攻撃者の戦術と手法に関する実際の観測情報として提供されます。

分析とアラート発行のための口グを選択して設定する

セキュリティ調査中、インシデントの全容とタイムラインを記録して理解するために、関連口グを確認できる必要があります。口グはまた、関心のある特定のアクションが発生したことを示すアラート生成にも必須です。クエリと取得のメカニズムとアラートを選択、有効化、保存、セットアップし、アラート発行を設定することが非常に重要となります。これらの各アクションについて、このセクションで確認します。詳細については、AWS ブログ記事「Logging strategies for security incident response」を参照してください。

ログソースを選択して有効にする

セキュリティ調査の前に、関連するログを取得し、過去にさかのぼって AWS アカウントでアクティビティを再構築する必要があります。AWS アカウントのワークロードに関連するログソースを選択して有効にします。

AWS CloudTrail は、AWS のサービスアクティビティをキャプチャする AWS アカウントに対して API コールをトラッキングするログサービスです。これはデフォルトで有効になっており、管理イベントは 90 日間保持され、AWS マネジメントコンソール、AWS CLI、AWS SDK のいずれかを使用して CloudTrail イベント履歴から検索することが可能です。データイベントをより長く保持し、確認できるようにするには、CloudTrail 証跡を作成して、これを Amazon S3 バケットと CloudWatch ロググループ (任意) に関連付ける必要があります。あるいは、CloudTrail Lake を作成する方法もあります。この方法では、CloudTrail ログを最長 7 年間保持でき、SQL ベースのクエリ機能を利用できます。

AWS では、VPC を使用しているお客様には、VPC フローログと Amazon Route 53 Resolver のクエリログをそれぞれ使用してネットワークトラフィックと DNS ログを有効にし、それらを Amazon S3 バケットまたは CloudWatch ロググループにストリーミングすることを推奨しています。VPC、サブネット、またはネットワークインターフェイスの VPC フローログを作成できます。VPC フローログについては、コストを削減するためにどこでどのようにフローログを有効にするかを選択できます。

AWS CloudTrail ログ、VPC フローログ、Route 53 Resolver のクエリログは、AWS でのセキュリティ調査をサポートする三大基本ログです。

AWS のサービスは、Elastic Load Balancing ログ、AWS WAF ログ、AWS Config レコーダーログ、Amazon GuardDuty の検出結果、Amazon Elastic Kubernetes Service (Amazon EKS) 監査ログ、Amazon EC2 インスタンスのオペレーティングシステムとアプリケーションログなど、三大基本ログではキャプチャされないログを生成できます。ログ記録とモニタリングのオプションの完全なリストについては、「the section called “付録 A: クラウド機能の定義”」を参照してください。

ログストレージを選ぶ

どのログストレージを選ぶかは、使用しているクエリツール、保持機能、使いやすさ、コストなどが関わってきます。AWS サービスログを有効にするときは、ストレージ施設を指定します。通常は Amazon S3 バケットまたは CloudWatch ロググループです。

Amazon S3 バケットは、ライフサイクルポリシーがオプションで備わっている、費用対効果に優れ、耐久性の高いストレージを提供します。Amazon S3 バケットに保存されているログは、Amazon Athena などのサービスを使ってネイティブにクエリすることができます。CloudWatch

ロググループは、CloudWatch Logs Insights により、耐久性の高いストレージとビルトインクエリ施設を提供します。

適切なログ保持を特定する

S3 バケットまたは CloudWatch ロググループを使ってログを保存するときは、各ログソースに対して適切なライフサイクルを選び、ストレージと取得コストを最適化する必要があります。顧客のログは通常 3 か月 ~ 12 か月間はすぐにクエリでき、最長 7 年間保持されます。可用性と保持の選択は、セキュリティ要件と、法令、規制、およびビジネス上の義務の組み合わせに合わせるべきです。

ログのクエリメカニズムを選択して実装する

AWS でログのクエリに使用できる主なサービスとして、CloudWatch ロググループに保存されているデータ用の CloudWatch Logs Insights と、Amazon S3 に保存されているデータ用の Amazon Athena と Amazon OpenSearch Service があります。また、セキュリティ情報とイベント管理 (SIEM) など、サードパーティーのクエリツールを使用することもできます。

ログクエリツールを選択するためのプロセスは、セキュリティオペレーションの人材、プロセス、およびテクノロジー側面を考慮する必要があります。オペレーション、ビジネス、セキュリティの要件を満たし、長期的にアクセスとメンテナンスが可能なツールを選択します。ログクエリツールは、スキャンするログの数がツールの制限内に収まっている場合、動作が最適であることに注意してください。コストや技術的な制約から、お客様が複数のクエリツールを所有することも珍しくありません。例えば、過去 90 日間のデータにはサードパーティーの SIEM ツールを使用し、SIEM のログインジェストコストが原因で 90 日以前のデータをクエリする際は Athena を使用するとった場合です。どのような実装であっても、必要なツールの数を最小限に抑えることで、特にセキュリティイベントの調査時に、運用効率が最大となるアプローチであることを確認してください。

アラートにログを使用する

AWS は、Amazon GuardDuty、、AWS Security Hub CSPM、、および AWS Config などのセキュリティサービスを通じてアラートをネイティブに提供します。また、これらのサービスの対象外となるセキュリティアラートや、自分の環境に関連する特定なアラートについては、カスタムアラート生成エンジンを使用することもできます。これらのアラートと検出の構築については、本書の「the section called “検出”」セクションで説明します。

フォレンジック機能を開発する

セキュリティインシデントが発生する前に、セキュリティイベントの調査を支援するフォレンジック機能の整備を検討します。NIST の「インシデント対応にフォレンジック手法を統合するためのガイド」にこのようなガイダンスが記載されています。

AWS でのフォレンジック

AWS には、従来のオンプレミスフォレンジックの概念が適用されます。ブログ記事「Forensic investigation environment strategies in the AWS クラウド」には、フォレンジックの専門知識を AWS に移行するための重要な情報が記載されています。

フォレンジックのための環境と AWS アカウント構造が整ったら、次の 4 つのフェーズにわたってフォレンジックに適した方法論を効果的に実行するために必要なテクノロジーを定義することができます。

- 収集 – AWS CloudTrail、AWS Config、VPC フローログ、ホストレベルのログなどの関連 AWS ログを収集します。AWS リソースのスナップショット、バックアップ、メモリダンプを収集します。
- 調査 – 関連する情報を抽出して評価することにより、収集されたデータを検証します。
- 分析 – 収集したデータを分析してインシデントを解明し、そこから結論を導き出します。
- レポート – 分析フェーズから得られた情報を報告します。

バックアップとスナップショットをキャプチャする

主要なシステムとデータベースのバックアップをセットアップすることは、セキュリティインシデントからの回復とフォレンジックのために重要です。バックアップを作成しておけば、システムを以前の安全な状態に復元できます。AWS では、さまざまなリソースのスナップショットを作成できます。スナップショットでは、こうしたリソースのポイントインタイムバックアップを作成できます。バックアップや復旧をサポートできる AWS のサービスは数多くあります。これらのサービスと、バックアップとリカバリのアプローチの詳細については、「バックアップとリカバリの規範ガイダンス」を参照してください。詳細については、ブログ記事「Use backups to recover from security incidents」を参照してください。

特にランサムウェアのような状況では、バックアップをしっかりと保護することが重要です。バックアップの保護に関するガイダンスについては、「Top 10 security best practices for securing backups in AWS」を参照してください。バックアップの保護に加えて、バックアップと復元のプロセスを定期的にテストして、導入しているテクノロジーとプロセスが想定どおりに機能することを確認する必要があります。

AWS でフォレンジックを自動化する

セキュリティイベント中、インシデント対応チームは、イベント前後の期間の証拠を、正確性を維持しながら迅速に収集して分析できなければなりません。インシデント対応チームにとって、クラウド

環境内の関連する証拠を手作業で収集することは困難であり、時間もかかります。多数のインスタンスやアカウントが対象となる場合は特にそうです。さらに、手作業による収集では人為的ミスが起こりやすくなります。このような理由から、お客様はフォレンジックの自動化を開発し、実装する必要があります。

AWS では、付録「the section called “フォレンジックリソース”」にまとめられているフォレンジックの自動化リソースを多数提供しています。これらのリソースは、当社が開発し、お客様が実装したフォレンジックパターンの例です。手始めに参考にするリファレンスアーキテクチャとしては有効かもしれませんが、環境、要件、ツール、フォレンジックプロセスに基に変更するか、新しいフォレンジック自動化パターンを作成することを検討してください。

準備項目の概要

タイムリーで効果的なインシデント対応には、セキュリティイベントに対応するための入念な準備が不可欠です。インシデント対応の準備には、人員、プロセス、テクノロジーが関わります。準備を進める上で、これら 3 つのドメインはすべて等しく重要です。3 つのドメインすべてに関して、インシデント対応プログラムを準備し、進化させる必要があります。

表 2 は、このセクションで詳述する準備項目をまとめたものです。

表 2 – インシデント対応準備項目

ドメイン	準備項目	アクション項目
人員	役割と責任を定義します。	• 関連するインシデント対応ステークホルダーを特定します。 • インシデントの責任、説明責任、情報提供、相談 (RACI) チャートを作成します。
人員	AWS に関してインシデント対応スタッフをトレーニングします。	• AWS の基礎についてインシデント対応ステークホルダーをトレーニングします。 • AWS のセキュリティサービスおよびモニタリングサービスについてインシデント

ドメイン	準備項目	アクション項目
		対応ステークホルダーをトレーニングします。 • AWS 環境とその設計方法についてインシデント対応ステークホルダーをトレーニングします。
人員	AWS サポートオプションを理解します。	• AWS サポート、セキュリティインシデント対応エンジニア、DDoS 対応チーム (DRT)、および AMS の違いを理解します。 • 必要に応じて、セキュリティイベントの発生中にセキュリティインシデント対応エンジニアに問い合わせるためのトリアージとエスカレーションパスを理解します。
プロセス	インシデント対応計画を作成します。	• インシデント対応プログラムと戦略を定義する概要文書を作成します。 • RACI、コミュニケーション計画、インシデント定義、およびインシデント対応のフェーズをインシデント対応計画に記載します。

ドメイン	準備項目	アクション項目
プロセス	アーキテクチャ図を文書化し、一元化します。	• アカウント構造、サービス使用状況、IAM パターン、およびその他の AWS 設定のコア機能全体について、AWS 環境の設定を詳しく文書化します。 • クラウドアーキテクチャのアーキテクチャ図を作成します。
プロセス	独自のインシデント対応プレイブックを作成します。	• プレイブックの構造用テンプレートを作成します。 • 予想されるセキュリティイベントのプレイブックを作成します。 • GuardDuty の検出結果など、既知のセキュリティアラートのプレイブックを作成します。
プロセス	定期的なシミュレーションを実行します。	• インシデントシミュレーションを定期的に実行する頻度を設定します。 • 得られた結果と教訓を活用して、インシデント対応プログラムを反復的に実行します。

ドメイン	準備項目	アクション項目
テクノロジー	AWS アカウント構造を作成します。	• アカウント構造で、ワークロードを AWS アカウントごとに分離する方法を計画します。 • セキュリティツールとログアーカイブアカウントを使用してセキュリティ OU を作成します。 • 運用するリージョンごとにフォレンジックアカウントを使用してフォレンジック OU を作成します。
テクノロジー	対応者が検出結果の所有者とコンテキストを特定するのに役立つタグ付け戦略を開発し、実装します。	• タグ付け戦略と、AWS リソースに関連付けるタグの計画を立てます。 • タグ付け戦略を実装して適用します。
テクノロジー	AWS アカウントの連絡先情報を更新します。	• AWS アカウントに連絡先情報がリストされていることを確認します。 • 連絡先情報のメール配信リストを作成して、単一障害点を排除します。 • AWS アカウント情報に関連付けられているメールアカウントを保護します。

ドメイン	準備項目	アクション項目
テクノロジー	AWS アカウントへのアクセス権を準備します。	• インシデントに対応するために、インシデント対応者がどのようなアクセス権を必要とするかを定義します。 • アクセス権を実装、テスト、監視します。
テクノロジー	脅威の状況を理解します。	• 環境とアプリケーションの脅威モデルを開発します。 • サイバー脅威インテリジェンスを統合し、利用します。
テクノロジー	ログを選択し、設定します。	• 調査のためのログを特定し、有効にします。 • ログストレージを選択します。 • ログの保持を特定して実装します。 • ログとアーティファクトを取得およびクエリするためのメカニズムを開発します。 • ログを使用してアラートを設定します。

ドメイン	準備項目	アクション項目
テクノロジー	フォレンジック機能を開発します。	• フォレンジック収集に必要なアーティファクトを特定します。 • 主要なシステムのバックアップをキャプチャして保護します。 • 特定されたログとアーティファクトを分析するメカニズムを定義します。 • フォレンジック分析の自動化を実装します。

インシデント対応の準備には、反復的なアプローチが推奨されます。これらの準備項目をすべて一晩で行うことはできません。小さく始めて、時間の経過に伴ってインシデント対応能力を継続的に改善するように計画を立てる必要があります。

オペレーション

インシデント対応の実施では、オペレーションが中核となります。ここで、セキュリティインシデントへの対応と修復が行われます。オペレーションには、検出、分析、封じ込み、根絶、復旧 の 5 つのフェーズが含まれます。これらのフェーズと目標の説明を表 3 に記載しています。

表 3 – オペレーションフェーズ

[Phase] (フェーズ)	目標
検出	潜在的なセキュリティイベントを特定します。
分析	セキュリティイベントがインシデントかどうかを判断し、インシデントの範囲を評価します。
封じ込め	セキュリティイベントの範囲を最小限に抑え、制限します。

[Phase] (フェーズ)	目標
根絶	セキュリティイベントに関連する不正なリソースやアーティファクトを削除します。セキュリティインシデントの原因となった緩和策を実装します。
復旧	システムを既知の安全な状態に復元し、これらのシステムを監視して脅威が再発しないことを確認します。

これらのフェーズは、効果的かつ堅牢な方法で対応するために、セキュリティインシデントに対応して運用する際の指針となるはずです。実際に実行するアクションは、インシデントによって異なります。例えば、ランサムウェアが関係するインシデントは、パブリック Amazon S3 バケットに関連するインシデントとは異なる対応手順を踏む必要があります。さらに、これらのフェーズは必ずしも連続して発生するわけではありません。封じ込みおよび根絶後は、分析に戻って対策が効果的だったかどうかを把握する必要があるかもしれません。

検出

アラートは、検出フェーズの主要コンポーネントです。対象の AWS アカウントの脅威アクティビティに基づいて、インシデント対応プロセスの開始通知を生成します。

精度の高いアラートの生成は難しく、インシデントが発生したか、進行中か、または将来発生するかを常に確実に判断できるわけではありません。いくつかの理由を次に示します。

- 検出メカニズムは、ベースラインからの逸脱、既知のパターン、内部または外部エンティティからの通知に基づいています。
- それぞれがセキュリティインシデントの手段とアクターであるテクノロジーと人員の予測不可能な性質が原因で、ベースラインは時間の経過に伴って変化します。不正なパターンは、脅威アクターの新しいまたは変更された戦術、技術、手順 (TTP) を通じて発生します。
- 人員、テクノロジー、プロセスへの変更は、インシデント対応プロセスにすぐには組み込まれません。調査の進行中に発見されるものもあります。

アラートのソース

アラートを定義するには、次のソースの使用を検討してください。

- 検出結果 – Amazon GuardDuty、AWS Security Hub CSPM、Amazon Macie、Amazon Inspector、AWS Config、IAM Access Analyzer、Network Access Analyzer などの AWS サービスでは、アラートの作成に使用できる検出結果が生成されます。
- ログ – Amazon S3 バケットと CloudWatch ロググループに保存されている AWS サービス、インフラストラクチャ、アプリケーションログを解析し、相関させることでアラートを生成できます。
- 請求アクティビティ – 請求アクティビティの突然の変更は、セキュリティイベントを示している可能性があります。これは「AWS の予想請求額をモニターリングする請求アラームの作成」ドキュメントに従ってモニタリングします。
- サイバー脅威インテリジェンス – サードパーティーのサイバー脅威インテリジェンスフィードをサブスクライブする場合、その情報を他のログおよびモニタリングツールと関連付けて、イベントの潜在的な指標を特定できます。
- パートナーツール – AWS Partner Network (APN) のパートナーは、セキュリティ目標の達成に役立つ最上位の製品を提供しています。インシデント対応では、エンドポイントの検出と対応 (EDR) または SIEM を使用するパートナー製品は、インシデント対応目標をサポートします。詳細については、「Security Partner Solutions」と「Security Solutions in the AWS Marketplace」を参照してください。
- AWS の信頼と安全 – 不正または悪意のあるアクティビティを特定した場合、サポート からお客様に連絡することがあります。
- 1 回限りの問い合わせ – お客様、開発者、または組織内の他のスタッフが異常に気付く可能性があるため、セキュリティチームへの連絡方法を周知させ、適切に公開することが重要です。一般的な選択肢には、チケットシステム、連絡先メールアドレス、ウェブフォームなどがあります。一般ユーザーと連携する組織の場合、一般向けのセキュリティに関する問い合わせ手段が必要になる場合もあります。

調査中に使用できるクラウド機能の詳細については、本書の「the section called “付録 A: クラウド機能の定義”」を参照してください。

セキュリティコントロールエンジニアリングの一環としての検出

検出メカニズムは、セキュリティコントロールの開発に欠かせないものです。ディレクティブコントロールと予防的コントロールを定義したら、関連する検出コントロールと対応コントロールを構築する必要があります。例えば、ある組織が AWS アカウントのルートユーザーに関連するディレクティブコントロールを確立したとします。このコントロールは、具体的な、明確に定義されたアクティビティにのみ使用する必要があります。これを、AWS 組織のサービスコントロールポリシー (SCP) を使用して実装された予防的コントロールに関連付けます。ルートユーザーのアクティビティが予想ベースラインを超えた場合、EventBridge ルールと SNS トピックを使用して実装された検出コント

ロールが、セキュリティオペレーションセンター (SOC) に警告します。対応コントロールが、SOC に適切なプレイブックを選択させ、分析を実行させ、インシデントの解決まで作業に当たらせます。

セキュリティコントロールは、AWS で実行されているワークロードの脅威モデリングによって定義するのが最も適切です。検出コントロールの重要度は、特定のワークロードに対するビジネスインパクト分析 (BIA) を確認して設定されます。検出コントロールによって生成されたアラートは、そのままの状態で処理されるものではなく、初期の重要度に基づいて分析中に調整されます。アラートの初期の重要度は優先順位付けに役立ちますが、実際の重要度はアラートが発生した文脈によって決まります。例えば、ある組織が、ワークロードの一部である EC2 インスタンスに使用される検出コントロールのコンポーネントとして Amazon GuardDuty を使用しているとします。検出結果 `Impact:EC2/SuspiciousDomainRequest.Reputation` が生成され、ワークロード内のリストされた Amazon EC2 インスタンスが悪意が疑われるドメイン名をクエリしていることが通知されました。このアラートはデフォルトでは重要度が低く設定されていましたが、分析フェーズが進むにつれて、不正なアクターによって数百もの `p4d.24xlarge` タイプの EC2 インスタンスがデプロイされ、組織の運用コストが大幅に増加していることが判明しました。この時点で、インシデント対応チームは、このアラートの重要度を高に調整し、緊急性を高め、さらなるアクションを迅速に行うことを決定します。GuardDuty の検出結果の重要度は変更できないことに注意してください。

検出コントロールの実装

検出コントロールは、特定のイベントに対してアラートをどのように利用するかを決定するのに役立つため、検出コントロールの実装方法を理解することが重要です。技術上、検出コントロールには主に 2 つの実装方法があります。

- 動作検出は、一般的に機械学習 (ML) または人工知能 (AI) と呼ばれる数学モデルに依存します。検出は推論によって行われるため、アラートは必ずしも実際のイベントを反映しているとは限りません。
- ルールベースの検出は決定論的で、お客様はアラートの対象となるアクティビティの正確で確実なパラメータを設定できます。

侵入検知システム (IDS) などの検出システムの最新の実装には、通常、両方のメカニズムが使用されます。以下に、GuardDuty を使用したルールベースの検出と動作検出の例を示します。

- 検出結果 `Exfiltration:IAMUser/AnomalousBehavior` が生成されると、「アカウント内で異常な API リクエストが観察されました」という通知が表示されます。さらに詳しく見ると、「ML モデルはアカウント内のすべての API リクエストを評価し、攻撃者が使用する手法に関連付けられる異常なイベントを識別しました」と表示されます。これは、この検出結果が動作的な性質であることを示しています。

- 検出結果 `Impact:S3/MaliciousIPCaller` について、GuardDuty は CloudTrail の Amazon S3 サービスからの API コールを分析し、`SourceIPAddress`のログ要素を、脅威インテリジェンスフィードを含むパブリック IP アドレスのテーブルと比較しています。エントリに直接一致するものが見つかると、検出結果が生成されます。

脅威モデル内のすべてのアクティビティに対してルールベースのアラートを実装することができない場合もあるため、動作アラートとルールベースのアラートの両方を実装することをお勧めします。

人員ベースの検出

これまではテクノロジーベースの検出について説明してきました。もう 1 つの重要な検出の情報源は、お客様の組織内外の人々です。内部の人間は従業員または請負業者として定義でき、外部の人間はセキュリティ研究者、法執行機関、ニュース、ソーシャルメディアなどのエンティティです。

テクノロジーベースの検出は体系的に設定できますが、人員ベースの検出には、メール、チケット、郵便、ニュース投稿、電話、対面でのやり取りなど、さまざまな形式があります。テクノロジーベースの検出の通知はほぼリアルタイムで配信されることが予想されますが、人員ベースの検出の場合、時間軸についての期待はされません。セキュリティへの多層防御アプローチでは、セキュリティ文化が人員ベースの検出メカニズムを組み込み、それを促進して強化することが不可欠です。

概要

検出では、ルールベースと動作主導のアラートを組み合わせることが重要です。さらに、社内外のスタッフがセキュリティ上の問題に関するチケットを送信できるメカニズムを用意する必要があります。人はセキュリティイベントの最も価値ある情報源の 1 つとなる可能性があるため、懸念を工スカレーションするプロセスを設けることが重要です。検出コントロールの構築を開始するには、環境の脅威モデルを使用する必要があります。脅威モデルは、環境に最も関連性の高い脅威に基づいてアラートを作成することに役立ちます。最後に、MITRE ATT&CK などのフレームワークを使用して、脅威アクターの戦術、技術、手順 (TTP) を理解できます。MITRE ATT&CK フレームワークは、さまざまな検出メカニズム間の共通言語として使用するのに役立ちます。

分析

ログ、クエリ機能、脅威インテリジェンスは、分析フェーズで必要とされるサポートコンポーネントの一部です。検出に使用されるログと同じものが分析にも多数使用され、クエリツールのオンボーディングと設定が必要になります。

アラートの影響の検証、範囲の特定、評価を行う

分析フェーズでは、アラートの検証、範囲の定義、考えられる侵害の影響評価を目的として、包括的なログ分析が実行されます。

- アラートの検証は、分析フェーズのエントリポイントです。インシデント対応者は、さまざまな情報源のログエントリを調べ、影響を受けるワークロードの所有者と直接やり取りします。
- 次のステップは範囲の特定です。関係者が誤検出の可能性が低いと判断した後に、関連するすべてのリソースのインベントリが作成され、アラートの重要度が調整されます。
- 最後に、インパクト分析で、実際のビジネスの中断について詳しく調べます。

影響を受けるワークロードのコンポーネントが特定されると、範囲の特定結果を関連するワークロードの目標復旧時点 (RPO) と目標復旧時間 (RTO) と相関させ、アラートの重要度を調整して、リソースの割り当てと次に発生するすべてのアクティビティが開始されます。すべてのインシデントが、ビジネスプロセスをサポートするワークロードの運用を直接的に中断するわけではありません。機密データの開示、知的財産の盗難、またはリソースのハイジャック (暗号通貨マイニングなど) といったインシデントは、ビジネスプロセスをすぐに停止または弱体化させることはできませんが、後で被害が生じる可能性があります。

セキュリティログと検出結果を強化する

脅威インテリジェンスと組織の背景情報による強化

分析の過程で、アラートのコンテキスト化を高めるため、対象の観察結果を強化する必要があります。「準備」セクションで説明したように、サイバー脅威インテリジェンスの統合と活用は、セキュリティに関する検出結果をより詳細に理解するのに役立ちます。脅威インテリジェンスサービスは、パブリック IP アドレス、ドメイン名、およびファイルハッシュに評価を割り当て、オーナーシップを帰属させるために使用されます。これらのツールには有料サービスと無料サービスがあります。

ログクエリツールとして Amazon Athena を採用しているお客様は、AWS Glue ジョブを利用して脅威インテリジェンス情報をテーブルとして読み込むことができます。脅威インテリジェンステーブルを SQL クエリで使用して、IP アドレスやドメイン名などのログ要素を関連付けることで、分析対象のデータの詳細なビューを提供できます。

AWS は脅威インテリジェンスをお客様に直接提供しませんが、Amazon GuardDuty などのサービスは脅威インテリジェンスを活用して強化や検出結果の生成を行います。独自の脅威インテリジェンスに基づいて、カスタム脅威リストを GuardDuty にアップロードすることもできます。

自動化による強化

自動化は AWS クラウドのガバナンスに欠かせません。これは、インシデント対応ライフサイクルのさまざまなフェーズで使用できます。

検出フェーズでは、ルールベースの自動化により、ログ内の脅威モデルから目的のパターンが照合され、通知の送信などの適切なアクションが実行されます。分析フェーズでは、検出メカニズムを活用して、イベントのコンテキスト化のためにログをクエリして検察結果を強化できるエンジンにアラート本文を転送できます。

アラート本文は、その基本的な形式において、リソースと ID で構成されます。例えば、アラート本文の ID またはリソースがアラートの発生時に実行した AWS API アクティビティを CloudTrail にクエリする自動化を実装すると、特定された API アクティビティの `eventSource`、`SourceIPAddress`、`eventName`、および `userAgent` などの追加のインサイトを提供できます。これらのクエリを自動的に実行することで、対応者は優先順位付けの時間を節約し、より多くのコンテキストを取得して、より適切な情報に基づいた意思決定を行うことができます。

自動化を使用してセキュリティの検出結果を強化し、分析を簡素化する方法の例については、ブログ記事「How to enrich AWS Security Hub findings with account metadata」を参照してください。

フォレンジック証拠の収集と分析を行う

フォレンジックとは、本書の「the section called “準備”」セクションで説明されているように、インシデント対応中にアーティファクトを収集して分析するプロセスです。AWS では、ネットワークトラフィックのパケットキャプチャ、オペレーティングシステムのメモリダンプなどのインフラストラクチャドメインリソース、および AWS CloudTrail ログなどのサービスドメインリソースに適用されます。

フォレンジックプロセスには、次の基本的な特性があります。

- 一貫性 — 文書化された手順から逸脱することなく正確に従います。
- 再現可能 – 同じアーティファクトに対して処理を繰り返すと、まったく同じ結果が生成されます。
- 慣習的 – 公開され、広く採用されています。

インシデント対応中に収集されたアーティファクトの管理の連鎖を維持することが重要です。アーティファクトを読み取り専用リポジトリに保存するだけでなく、この収集を自動化し、記録を自動生成させると便利です。整合性を維持するために、分析は収集されたアーティファクトの正確なレプリカに対してのみ実行する必要があります。

関連するアーティファクトを収集する

これらの特性を念頭に置き、関連するアラートおよびインパクトと範囲の評価に基づいて、さらなる調査と分析に関連するデータを収集する必要があります。サービス/コントロールプレーンログ (CloudTrail、Amazon S3 データイベント、VPC フローログ)、データ (Amazon S3 メタデータとオブジェクト)、およびリソース (データベース、Amazon EC2 インスタンス) など、調査に関連する可能性のあるさまざまなタイプとデータソースがあります。

サービス/コントロールプレーンログは、ローカル分析用に収集することも、ネイティブ AWS サービス (該当する場合) を使用して直接クエリすることもできます。データ (メタデータを含む) を直接クエリして関連情報を取得したり、ソースオブジェクトを取得したりできます。例えば、AWS CLI を使用して Amazon S3 バケットとオブジェクトメタデータを取得し、ソースオブジェクトを直接取得します。リソースは、リソースタイプおよび目的の分析方法と一致する方法で収集する必要があります。例えば、データベースを実行しているシステムのコピー/スナップショットを作成したり、データベース自体のコピー/スナップショットを作成したり、調査に関連するデータベースから特定のデータとログをクエリおよび抽出したりすることで、データベースを収集できます。

Amazon EC2 インスタンスの場合、分析と調査のために大量のデータを取得および保存するため、収集する必要があるデータセットと、実行する必要がある収集順序が決まっています。

具体的には、レスポンスが Amazon EC2 インスタンスから大量のデータを取得して保持する順序は次のとおりです。

1. インスタンスメタデータの取得 – 調査およびデータクエリに関連するインスタンスメタデータを取得します (インスタンス ID、タイプ、IP アドレス、VPC/サブネット ID、リージョン、Amazon マシンイメージ (AMI) ID、アタッチされたセキュリティグループ、起動時間)。
2. インスタンス保護とタグの有効化 – 終了保護、シャットダウン動作を停止に設定 (終了するように設定されている場合)、アタッチされた EBS ボリュームの終了時の削除属性の無効化、および視覚的な表示と対応の自動化での使用の両方に適切なタグの適用 (例えば、名前 `Status` と値 `Quarantine` を持つタグを適用すると、データのフォレンジック取得が実行され、インスタンスが分離される) などのインスタンス保護を有効にします。
3. ディスクの取得 (EBS スナップショット) – アタッチされた EBS ボリュームの EBS スナップショットを取得します。各スナップショットには、(スナップショットを作成した瞬間からの) データを新しい EBS ボリュームに復元するために必要な情報が含まれます。インスタンスストアボリュームを使用している場合は、ライブレスポンス/アーティファクト収集を実行するための手順を参照してください。
4. メモリの取得 – EBS スナップショットは Amazon EBS ボリュームに書き込まれたデータのみをキャプチャするため、アプリケーションまたは OS によってメモリに保存またはキャッシュされ

たデータは除外される可能性があります。システムから利用可能なデータを取得するためには、適切なサードパーティーのオープンソースまたは市販のツールを使用してシステムメモリのイメージを取得する必要があります。

5. (オプション) ライブレスポンス/アーティファクト収集の実行 – ディスクまたはメモリを別途取得できない場合、または有効なビジネス上の理由または運用上の理由がある場合にのみ、システムのライブレスポンスを通じてターゲットデータ収集 (ディスク/メモリ/ログ) を実行します。これを行うと、重要なシステムデータとアーティファクトが変更されます。
6. インスタンスの使用停止 – Auto Scaling グループからインスタンスをデタッチし、ロードバランサーからインスタンスを登録解除し、構築済みのインスタンスプロファイルを最小限のアクセス許可またはアクセス許可なしによって調整または適用します。
7. インスタンスの分離または封じ込め – インスタンスとの現在の接続を終了し、将来の接続を防止することで、インスタンスが環境内の他のシステムやリソースから効果的に分離されていることを確認します。詳細については、本書の「the section called “封じ込み”」セクションを参照してください。
8. 対応者の選択 – 状況と目標に基づいて、次のいずれかを選択します。
   - システムを使用停止してシャットダウンします (推奨)。

     利用可能な証拠を取得したら、システムをシャットダウンして、インスタンスによる環境への将来的な影響に対抗する最も効果的な緩和策を検証します。
   - モニタリング用に実装された分離環境内で、インスタンスの実行を継続します。

     標準アプローチとしては推奨されませんが、インスタンスの継続的な観察に値する状況であれば (例えば、インスタンスの包括的な調査と分析を実行するために追加のデータや指標が必要な場合など)、インスタンスをシャットダウンし、その AMI を作成し、インスタンスをフォレンジック専用アカウント内のサンドボックス環境で再起動することを検討してください。サンドボックス環境は完全に分離されるように事前に実装されており、インスタンスのほぼ継続的なモニタリングを容易にするように設定されています (例: VPC フローログまたは VPC トラフィックミラーリング)。

> **Note**
>
> 利用可能な揮発性 (および価値ある) データをキャプチャするには、ライブレスポンスアクティビティやシステムの分離またはシャットダウンの前にメモリをキャプチャすることが重要です。

説明文を作成する

分析と調査中に、実行したアクション、実施した分析、特定された情報を文書化して、後続のフェーズ、および最終的には最終レポートで使用します。これらの説明文は簡潔かつ正確でなければならず、インシデントを効果的に理解し、正確なタイムラインを維持するための関連情報が含まれていることを確認する必要があります。コアインシデント対応チーム以外の人々を関与させる場合にも役立ちます。以下がその例です。

> 2022 年 3 月 15 日に、機密データの公開を避けたければ暗号通貨で支払えと要求する身代金要求書が営業マーケティング部門宛に届きました。SOC は、営業マーケティング部門に属する Amazon RDS データベースが 2022 年 2 月 20 日にパブリックアクセス可能だったと判断しました。SOC が RDS アクセスログをクエリした結果、ウェブ開発者の 1 人である Major Mary に属する認証情報 *mm03434* により、IP アドレス 198.51.100.23 が 2022 年 2 月 20 日に使用されたと判断しました。SOC は VPC フローログにクエリを実行し、同日 (タイムスタンプ 2022-02-20T15:50+00Z) に同じ IP アドレスに約 256MB のデータが送信されたと判断しました。SOC は、オープンソースの脅威インテリジェンスを通じて、認証情報がパブリックリポジトリ *https[:]//example[.]com/majormary/rds-utils* でプレーンテキストで利用可能な状況だと判断しました。

封じ込み

インシデント対応に関連する封じ込めの定義の 1 つは、セキュリティイベントの処理中に、セキュリティイベントの範囲を最小限に抑え、環境内での不正使用の影響を封じ込める戦略を処理または実装することです。

封じ込め戦略は多くの要因に依存し、封じ込め戦術の適用、タイミング、目的に関して、組織ごとに異なるものになる可能性があります。「NIST SP 800-61 コンピュータセキュリティインシデント処理ガイド」では、適切な封じ込め戦略を決定するためのいくつかの基準について概説しています。これには、以下が含まれます。

- リソースへの潜在的な損害および盗難
- 証拠保全の必要性
- サービスの可用性 (ネットワーク接続、外部の関係者に提供されるサービス)
- 戦略の実装に必要な時間とリソース
- 戦略の有効性 (部分的または完全な封じ込め)

- ソリューションの期間 (4 時間で削除する緊急回避策、2 週間で削除する一時的な回避策、永続的な解決策)

ただし、AWS のサービスについては、基本的な封じ込めステップを次の 3 つのカテゴリに絞り込むことができます。

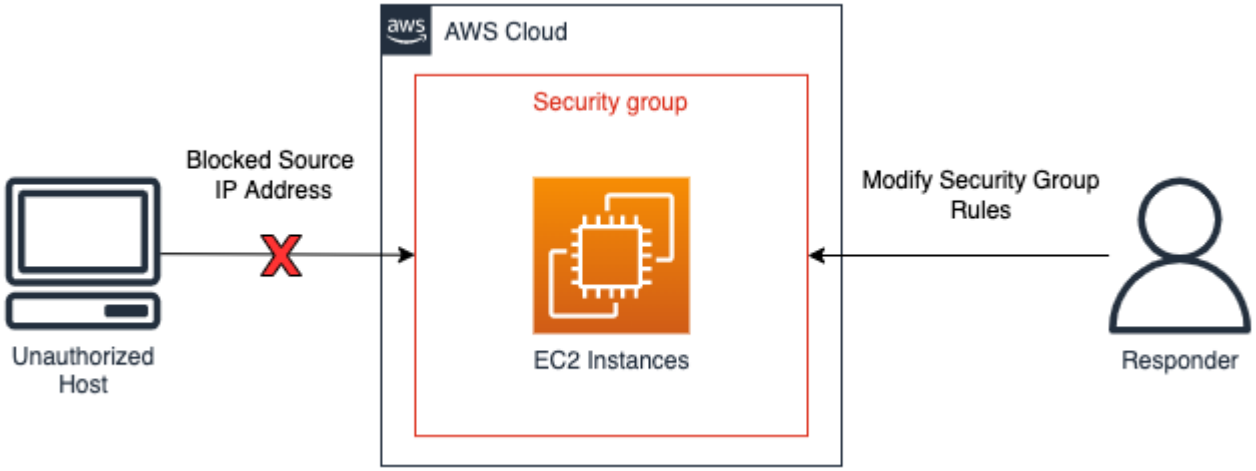
- ソースの封じ込め — フィルタリングとルーティングを使用して、特定のソースからのアクセスを防止します。
- 手法とアクセス権の封じ込め – アクセス権を削除して、影響を受けるリソースへの不正アクセスを防止します。
- 送信先の封じ込め — フィルタリングとルーティングを使用して、ターゲットリソースへのアクセスを防止します。

ソースの封じ込め

ソースの封じ込めとは、特定のソース IP アドレスまたはネットワーク範囲からリソースにアクセスされることを防ぐために、環境内でフィルタリングまたはルーティングを使用および適用することです。AWS サービスを使用したソースの封じ込めの例を以下に示します。

- セキュリティグループ – 分離セキュリティグループを作成して Amazon EC2 インスタンスに適用するか、既存のセキュリティグループからルールを削除すると、Amazon EC2 インスタンスまたは AWS リソースへの不正なトラフィックを封じ込めることができます。セキュリティグループを変更しても、既存の追跡対象の接続はシャットダウンされないことに注意してください。実際は将来のトラフィックのみが新しいセキュリティグループによってブロックされます (追跡対象の接続と追跡対象でない接続の詳細については、このインシデント対応プレイブックと「セキュリティグループの接続の追跡」を参照してください)。
- ポリシー – Amazon S3 バケットポリシーは、IP アドレス、ネットワーク範囲、または VPC エンドポイントからのトラフィックをブロックまたは許可するように設定できます。ポリシーにより、疑わしいアドレスと Amazon S3 バケットへのアクセスをブロックすることができます。バケットポリシーの詳細については、「Adding a bucket policy using the Amazon S3 console」を参照してください。
- AWS WAF – ウェブアクセスコントロールリスト (ウェブ ACL) は、リソースが応答するウェブリクエストをきめ細かく制御するために AWS WAF で設定できます。AWS WAF で設定された IP セットに IP アドレスまたはネットワーク範囲を追加し、ブロックなどの一致条件を IP セットに適用できます。これにより、発信元トラフィックの IP アドレスまたはネットワーク範囲が IP セットルールで設定されたものと一致する場合、リソースへのウェブリクエストがブロックされます。

ソースの封じ込めの例を次の図に示します。インシデント対応アナリストが Amazon EC2 インスタンスのセキュリティグループを変更して、新しい接続を特定の IP アドレスのみに制限します。セキュリティグループの箇条書きで説明したように、セキュリティグループを変更しても、既存の追跡対象の接続はシャットダウンされません。



ソース封じ込めの例

> **Note**
>
> セキュリティグループとネットワーク ACL では、Amazon Route 53 へのトラフィックはフィルタリングされません。EC2 インスタンスを封じ込める場合、外部ホストとの通信を防ぐには、DNS 通信も明示的にブロックしてください。

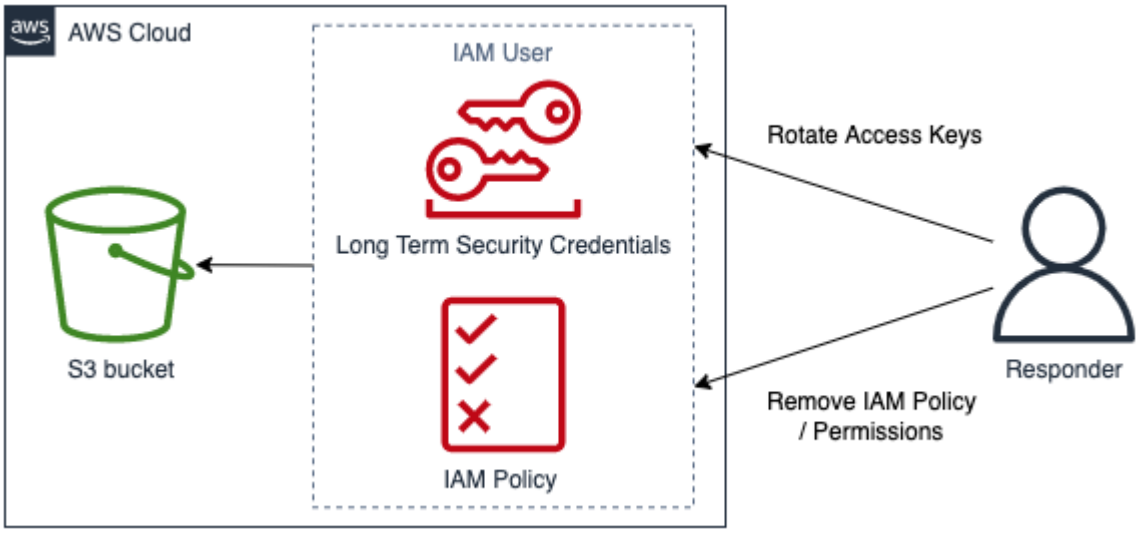
手法とアクセス権の封じ込め

リソースへのアクセス権を持つ役割と IAM プリンシパルを制限することで、リソースの不正使用を防止します。これには、リソースにアクセスできる IAM プリンシパルのアクセス許可の制限や、一時的なセキュリティ認証情報の取り消しも含まれます。AWS サービスを使用した手法とアクセス権の封じ込めの例を以下に示します。

- アクセス許可の制限 – IAM プリンシパルに割り当てられたアクセス許可は、最小特権の原則に従う必要があります。ただし、セキュリティイベントの発生中に、特定の IAM プリンシパルからターゲットリソースへのアクセスをさらに制限することが必要になる場合があります。この場合、封じ込め対象の IAM プリンシパルからアクセス許可を削除することで、リソースへのアクセスを制限できます。これは IAM サービスで行われ、AWS マネジメントコンソール、AWS CLI または AWS SDK を使用して適用できます。

- キーの取り消し – IAM アクセスキーは、IAM プリンシパルがリソースにアクセスまたは管理するために使用されます。これらは、AWS CLI または AWS API へのプログラムによるリクエストに署名し、プレフィックス AKIA で始まる長期的な静的認証情報です (詳細については、「IAM 識別子」の「一意の ID プレフィックスを理解する」セクションを参照してください)。IAM アクセスキーが侵害された IAM プリンシパルのアクセス権を封じ込めるには、アクセスキーを非アクティブ化または削除できます。次の点に留意することが重要です。
  - アクセスキーを非アクティブ化した後、再アクティブ化できます。
  - アクセスキーは一度削除すると復元できません。
  - IAM プリンシパルは、いつでも最大 2 つのアクセスキーを持つことができます。
  - アクセスキーを使用するユーザーまたはアプリケーションは、キーが非アクティブ化または削除されるとアクセス権を失います。
- 一時的なセキュリティ認証情報の取り消し – 一時的なセキュリティ認証情報は、AWS リソースへのアクセスを制御するために組織で使用でき、プレフィックス ASIA で始まります (詳細については、「IAM 識別子」の「一意の ID プレフィックスを理解する」セクションを参照してください)。一時的な認証情報は通常、IAM ロールによって使用され、有効期間があるため、ローテーションを行ったり明示的に取り消したりする必要はありません。一時的なセキュリティ認証情報の有効期限が切れる前に、一時的なセキュリティ認証情報が関与するセキュリティイベントが発生した場合は、既存の一時的なセキュリティ認証情報の有効なアクセス許可を変更する必要がある場合があります。これは、AWS マネジメントコンソール内の IAM サービスを使用して完了できます。一時的なセキュリティ認証情報は、(IAM ロールではなく) IAM ユーザーにも発行できますが、本書の執筆時点では、AWS マネジメントコンソール内の IAM ユーザーの一時的なセキュリティ認証情報を取り消すオプションはありません。権限のないユーザーが一時的なセキュリティ認証情報を作成し、ユーザーの IAM アクセスキーが侵害されたセキュリティイベントでは、次の 2 つの方法を使用して一時的なセキュリティ認証情報を取り消すことができます。
  - セキュリティトークンの発行時間に基づいてアクセス権を禁止するインラインポリシーを IAM ユーザーにアタッチします (詳細については、「一時的なセキュリティ認証情報のアクセス権限を無効にする」の「特定の時間より前に発行した一時的なセキュリティ認証情報のアクセスを拒否する」セクションを参照してください)。
  - 侵害されたアクセスキーを所有する IAM ユーザーを削除します。必要に応じてユーザーを再作成します。
- AWS WAF - 権限のないユーザーが使用する特定の手法には、SQL インジェクションやクロスサイトスクリプティング (XSS) を含むリクエストなど、一般的な悪意のあるトラフィックパターンが含まれます。 AWS WAF は、AWS WAF 組み込みルールステートメントを使用して、これらの手法を使用するトラフィックを照合して拒否するように設定できます。

手法とアクセス権の封じ込めの例を次の図に示します。インシデント対応者がアクセスキーをローテーションするか、IAM ポリシーを削除して、IAM ユーザーが Amazon S3 バケットにアクセスできないようにします。



手法とアクセス権の封じ込めの例

送信先の封じ込め

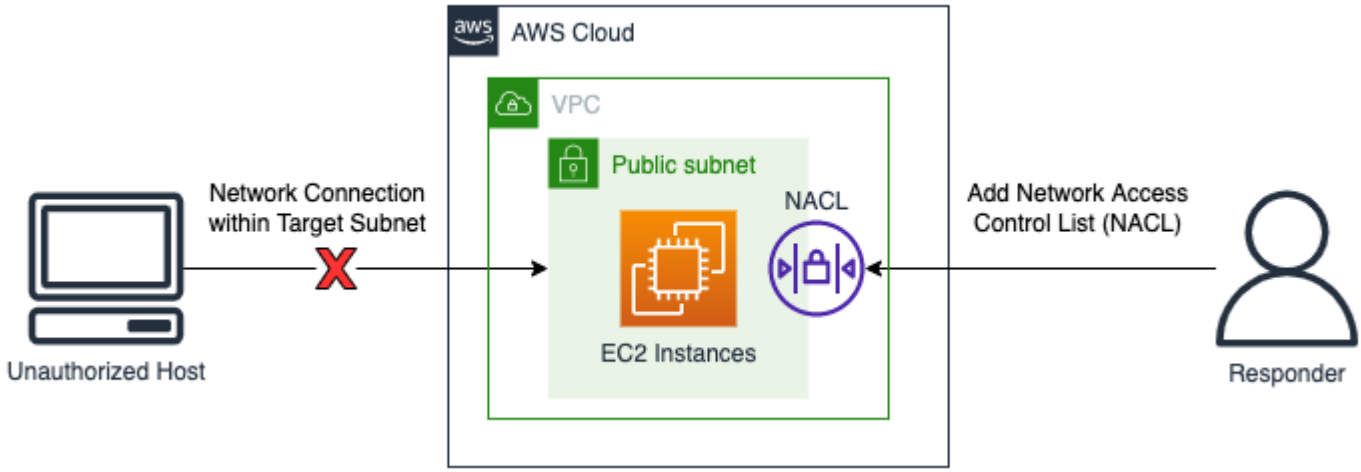
送信先の封じ込めは、ターゲットのホストまたはリソースへのアクセスを防ぐために、環境内でフィルタリングまたはルーティングを行うことです。場合によっては、送信先の封じ込めは、正当なリソースが可用性を保つためレプリケートされていることを確認するために回復力の形式を取る場合もありまれます。そのため、分離と封じ込めのためにリソースをこうした形式の回復力からデタッチする必要があります。AWS サービスを使用した送信先の封じ込めの例は次のとおりです。

- ネットワーク ACL – AWS リソースが含まれるサブネットで設定されたネットワーク ACL には、拒否ルールを追加できます。これらの拒否ルールは、特定の AWS リソースへのアクセスを防ぐために適用できます。ただし、ネットワークアクセスコントロールリスト (ネットワーク ACL) を適用すると、承認なしでアクセスされるリソースだけでなく、サブネット上のすべてのリソースに影響します。ネットワーク ACL 内にリストされているルールはトップダウン順序で処理されるため、既存のネットワーク ACL の最初のルールは、ターゲットリソースとサブネットへの不正なトラフィックを拒否するように設定する必要があります。または、インバウンドトラフィックとアウトバウンドトラフィックの両方に対して単一の拒否ルールを使用するまったく新しいネットワーク ACL を作成し、ターゲットリソースを含むサブネットに関連付けることで、新しいネットワーク ACL を使用したサブネットへのアクセスを防ぐこともできます。
- シャットダウン — リソースを完全にシャットダウンすると、不正使用の影響を封じ込める効果があります。リソースをシャットダウンすると、ビジネスで必要な正当なアクセスが妨げられ、揮発

性のフォレンジックデータの取得も妨げられます。そのため、これは目的を持って決定する必要があり、組織のセキュリティポリシーに照らして判断する必要があります。

- 分離 VPC – 分離 VPC を使用すると、正当なトラフィック (インターネットや外部マネジメントコンソールへのアクセスを必要とするウイルス対策 (AV) や EDR ソリューションなど) へのアクセス権を提供しながら、リソースを効果的に封じ込めることができます。分離 VPC は、セキュリティイベントに先立って、有効な IP アドレスとポートを許可するように事前設定できます。セキュリティイベントが発生するとターゲットリソースはすぐにこの分離 VPC に移動してリソースを封じ込めると同時に、インシデント対応の後続フェーズでターゲットリソースが正当なトラフィックを送受信できるようにします。分離 VPC を使用する上で重要な点は、EC2 インスタンスなどのリソースを使用する前に新しい分離 VPC でシャットダウンおよび再起動する必要があることです。既存の EC2 インスタンスを別の VPC または別のアベイラビリティーゾーンに移動することはできません。これを行うには、「How do I move my Amazon EC2 instance to another subnet, Availability Zone, or VPC?」で説明されているステップに従います。
- 送信先の封じ込め手順の一部として、Auto Scaling グループとロードバランサー – Auto Scaling グループとロードバランサーにアタッチされた AWS リソースをデタッチおよび登録解除する必要があります。AWS リソースのデタッチと登録解除は、AWS マネジメントコンソール、AWS CLI、および AWS SDK を使用して実行できます。

送信先の封じ込めの例を次の図で示します。インシデント対応アナリストは、不正なホストからのネットワーク接続リクエストをブロックするために、ネットワーク ACL をサブネットに追加します。



送信先の封じ込めの例

概要

封じ込めはインシデント対応プロセスのステップの 1 つであり、手動または自動で行うことができます。封じ込め戦略全体を組織のセキュリティポリシーとビジネスニーズに一致させ、根絶と復旧の前に、悪影響が可能な限り効率的に軽減されていることを確認する必要があります。

根絶

根絶とは、セキュリティインシデント対応に関して、アカウントを既知の安全な状態に戻すために、疑わしいリソースや不正なリソースを排除することです。根絶戦略は、組織のビジネス要件に依存する複数の要因によって異なります。

「NIST SP 800-61 コンピュータセキュリティインシデント処理ガイド」には、次に示すような根絶のためのいくつかのステップが記載されています。

1. 悪用されたすべての脆弱性を特定して軽減します。
2. マルウェア、不適切なマテリアル、その他のコンポーネントを削除します。
3. 影響を受けるホストがさらに検出された場合 (新しいマルウェアへの感染など)、検出と分析の手順を繰り返して、影響を受ける他のすべてのホストを特定し、インシデントを封じ込めて根絶します。

AWS リソースの場合、CloudWatch Logs や Amazon GuardDuty などの利用可能な口グや自動ツールを通じて検出および分析されたイベントを通じて、この手順をさらに洗練させることができます。これらのイベントは、環境を既知の安全な状態に適切に復元するためにどのような修復を実行するかを判断する基礎となります。

根絶の最初のステップは、AWS アカウント内で影響を受けたリソースを特定することです。これは、使用可能な口グデータソース、リソース、自動ツールの分析によって実現されます。

- アカウントの IAM ID によって実行された不正なアクションを特定します。
- アカウントへの不正なアクセスまたは変更を特定します。
- 不正なリソースまたは IAM ユーザーの作成を特定します。
- 不正な変更が行われたシステムまたはリソースを特定します。

リソースのリストを特定したら、それぞれを評価して、リソースが削除または復元された場合のビジネスへの影響を判断する必要があります。例えば、ウェブサーバーがビジネスアプリケーションをホストしていて、それを削除するとダウンタイムが発生する場合は、影響を受けるサーバーを削除する

前に、検証済みの安全なバックアップからリソースを復旧するか、クリーンな AMI からシステムを再起動することを検討する必要があります。

ビジネスへの影響分析を終了したら、ログ分析のイベントを使用して、アカウントに移動し、次のような適切な修復を実行する必要があります。

- キーのローテーションまたは削除 - このステップでは、アクターがアカウント内でアクティビティを実行し続けることができないようにします。
- 不正な疑いのある IAM ユーザ認証情報をローテーションします。
- 認識されないリソースまたは許可されていないリソースを削除します。

> **Important**
>
> 調査のためにリソースを保持する必要がある場合は、それらのリソースのバックアップを取ることを検討してください。例えば、規制、コンプライアンス、または法的理由で Amazon EC2 インスタンスを保持する必要がある場合は、インスタンスを削除する前に Amazon EBS スナップショットを作成します。

- マルウェアの感染については、AWS Partnerまたは他のベンダーに連絡する必要がある場合があります。AWS は、マルウェアの分析や削除のためのネイティブツールを提供していません。ただし、Amazon EBS に GuardDuty Malware モジュールを使用している場合は、提供された検出結果に対する推奨事項が利用できる場合があります。

特定した影響を受けるリソースを根絶したら、AWS でアカウントのセキュリティレビューを実行することをお勧めします。これは、AWS Config ルールを使用する、Prowler や ScoutSuite などのオープンソースソリューションを使用する、または他のベンダーを通じて行うことができます。また、残余リスクを評価するために、パブリック (インターネット) 向けリソースに対して脆弱性スキャンを実行することも検討する必要があります。

根絶はインシデント対応プロセスのステップの 1 つであり、インシデントと影響を受けるリソースに応じて手動または自動で行うことができます。戦略全体を組織のセキュリティポリシーとビジネスニーズに一致させ、不適切なリソースや設定を削除した場合に悪影響が軽減されることを確認する必要があります。

復旧

復旧とは、システムを既知の安全な状態に復元し、復元前にバックアップが安全であるかまたはインシデントの影響を受けていないことを検証し、復元後にシステムが適切に動作していることを検証し、セキュリティイベントに関連する脆弱性に対処するプロセスです。

復旧の順序は、組織の要件によって異なります。復旧プロセスの一環として、ビジネスへの影響分析を実行して、少なくとも以下を決定する必要があります。

- ビジネスまたは依存関係の優先順位
- 復元プラン
- 認証と認可

「NIST SP 800-61 コンピュータセキュリティインシデント処理ガイド」には、次に示すような、システムを復旧するためのいくつかのステップが記載されています。

- クリーンバックアップからシステムを復元します。
  - バックアップがシステムへの復元前に評価されていることを確認し、感染がないことを確認し、セキュリティイベントの再発を防止します。

    バックアップは、ディザスタリカバリテストの一環として定期的に評価して、バックアップメカニズムが適切に動作していること、データの整合性が復旧ポイントの目的を満たしていることを確認する必要があります。
  - 可能であれば、根本原因分析の一環として特定された最初のイベントのタイムスタンプより前のバックアップを使用します。
- 自動化を使用した信頼できるソースからの再デプロイなど、システムをゼロから再構築します (場合によっては新しい AWS アカウントで)。
- 侵害されたファイルをクリーンバージョンに置き換えます。

  これを行う際には、細心の注意が必要です。復旧するファイルの安全性が既知であり、インシデントの影響を受けていないことを確認する必要があります。
- パッチをインストールします。
- パスワードを変更します。
  - 悪用された可能性のある IAM プリンシパルのパスワードが含まれます。
  - 可能であれば、最小特権戦略の一環として、IAM プリンシパルとフェデレーションのロールを使用することをお勧めします。

- ネットワーク境界のセキュリティを強化します (ファイアウォールルールセット、境界ルーターのアクセスコントロールリスト)。

リソースを復旧したら、学んだ教訓を取り入れてインシデント対応ポリシー、手順、ガイドを更新することが重要です。

要約すると、既知の安全な運用への復帰を容易にする復旧プロセスを実装することが欠かせません。復旧には時間がかかる場合があり、封じ込め戦略と密接に連携してビジネスへの影響と再感染のリスクのバランスを取ることが必要です。復旧手順には、リソースとサービス、IAM プリンシパルを復元し、アカウントのセキュリティレビューを実行して残余リスクを評価する手順を含める必要があります。

結論

各運用フェーズには、固有の目標、手法、方法論、戦略があります。表 4 は、これらのフェーズと、このセクションで説明する手法と方法論の一部をまとめたものです。

表 4 – 運用フェーズ: 目標、手法、方法論

[Phase] (フェーズ)	目標	手法と方法論
検出	潜在的なセキュリティイベントを特定します。	• 検出のためのセキュリティコントロール • 動作とルールベースの検出 • 人員ベースの検出
分析	セキュリティイベントがインシデントかどうかを判断し、インシデントの範囲を評価します。	• アラートの検証と範囲設定 • ログをクエリする • 脅威インテリジェンス • オートメーション
封じ込め	セキュリティイベントの影響を最小限に抑え、制限します。	• ソースの封じ込め • 手法とアクセス権の封じ込め • 送信先の封じ込め

[Phase] (フェーズ)	目標	手法と方法論
根絶	セキュリティイベントに関連する不正なリソースやアーティファクトを削除します。	• 侵害された、または不正な認証情報のローテーションまたは削除 • 許可されていないリソースの削除 • マルウェアの削除 • セキュリティスキャン
復旧	システムを既知の安全な状態に復元し、これらのシステムを監視して脅威が再発しないことを確認します。	• バックアップからのシステム復元 • システムのゼロからの再構築 • 侵害されたファイルをクリーンバージョンに置き換える

インシデント後のアクティビティ

脅威の状況は絶えず変化しているため、環境を効果的に保護するためには、組織の能力も同様に動的なものにすることが重要です。継続的な改善の鍵は、インシデントとシミュレーションの結果を反復することで、想定されるセキュリティインシデントを効果的に検出、対応、調査する能力を向上させることです。これにより、想定される脆弱性や、対応までの時間を短縮し、安全なオペレーションに復帰することができます。以下のメカニズムは、組織がどのような状況でも効果的に対応するための最新の能力と知識を十分に備えていることを確認するのに役立ちます。

インシデントから学ぶためのフレームワークを確立する

教訓フレームワークと方法論を導入することは、インシデント対応能力の向上だけでなく、インシデントの再発防止にも役立ちます。各インシデントから学ぶことで、同じ失敗、露出、設定ミスの繰り返しを防ぐことができ、セキュリティ体制が強化されるだけでなく、予防できたはずの状況に無駄にする時間を最小限に抑えることができます。

以下の点を大まかに確立して達成する教訓フレームワークを実装することが重要です。

- 事後検証会を実施するタイミング

- 事後検証会を通して行うこと
- 事後検証会の実施方法
- そのプロセスに関わる人物、またかかわり方
- 改善の余地がある領域の特定方法
- 改善事項を効果的に追跡、実装する方法

これらの大局的な成果とは別に、プロセスから最大の価値 (実行可能な改善につながる情報) を引き出すためには、適切な質問を行うことが重要です。教訓についての議論を進めるうえで役立つ質問には次のようなものがあります。

- どのようなインシデントでしたか。
- インシデントが最初に特定されたのはいつでしたか。
- どのようにして特定されましたか。
- どのシステムからアクティビティについてのアラートが発行されましたか。
- どのようなシステム、サービス、データが関与しましたか。
- 具体的に何が起きましたか。
- 何がうまくいきましたか。
- 何がうまくいきませんでしたか。
- インシデントに対応できなかった、またはスケールに失敗したのはどのプロセスまたは手順ですか。
- 次の領域で改善できることは何でしょうか。
  - 人員
    - 連絡する必要があった担当者に実際に連絡がつきましたか。また、連絡先リストの情報は最新のものでしたか。
    - インシデントに効果的に対応して調査するために必要なトレーニングや能力を欠いていましたか。
    - 適切なリソースは用意されていましたか。
  - プロセス
    - 対応はプロセスと手順に従って進められましたか。
    - この (タイプの) インシデントについて、プロセスと手順が文書化され、利用可能になっていましたか。
    - 必要なプロセスや手順が欠けていましたか。

    - 対応担当者は、問題に対応するために必要な情報にタイムリーにアクセスできましたか。
  - テクノロジー
    - 既存のアラートシステムは、アクティビティを効果的に特定してアラートを出しましたか。
    - この (タイプの) インシデントに備えて、既存のアラートを改善する、または新しいアラートを作成する必要がありますか。
    - 既存のツールでインシデントを効果的に調査 (検索/分析) できましたか。
- この (タイプの) インシデントをより早く特定するにはどうすればよいでしょうか。
- この (タイプの) インシデントの再発を防ぐにはどうすればよいでしょうか。
- 改善計画の所有者は誰ですか。また、その実施状況をどのように検証しますか。
- 追加のモニタリング/予防的統制/プロセスを導入し、テストするまでのスケジュールはどのようになっていますか。

このリストはすべてを網羅しているわけではなく、インシデントから最も効果的に学び、セキュリティ体制の継続的な改善に向けて、組織とビジネスのニーズを見極め、その分析方法を特定するための出発点として活用いただくことを目的としています。最も重要なのは、事後検証会を標準的なインシデント対応プロセスと文書化の一部として取り入れ、想定されるものとして関係者全員にも定着させることです。

成功のメトリクスを確立する

メトリクスは、インシデント対応機能を効果的に測定、評価、改善するために必要です。メトリクスがなければ、組織のパフォーマンスを正確に測定したり、特定したりするための基準が存在しないことになります。インシデント対応には共通するいくつかのメトリクスがあり、オペレーショナルエクセレンスの実現に向けて取り組むための期待と基準を確立しようとしている組織に適した開始点となります。

検出までの平均時間

検出までの平均時間は、潜在的なセキュリティインシデントを検出するまでの平均時間です。具体的には、最初の侵害インジケータの発生から最初の特定またはアラートまでの時間です。

このメトリクスを使用して、検出およびアラートシステムのパフォーマンスを追跡できます。効果的な検出とアラートのメカニズムは、潜在的なセキュリティインシデントが環境内にいつまでも残らないようにする上で重要です。

検出までの平均時間が長いほど、潜在的なセキュリティインシデントを特定して検出するために、追加またはより効果的なアラートおよびメカニズムを構築する必要性が高くなります。検出までの平均時間が短いほど、検出とアラートのメカニズムがより良好に機能しています。

認識までの平均時間

認識までの平均時間は、潜在的なセキュリティインシデントを認識して優先順位を付けるのにかかる平均時間です。具体的には、アラートの生成から、SOC のメンバーまたはインシデント対応スタッフがアラートを特定し、処理の優先順位を付けるまでの時間です。

このメトリクスを使用して、チームがどの程度適切にアラートを処理し、優先順位を付けているかを追跡できます。チームがアラートを効果的に特定し、優先順位を付けることができない場合、対応は遅れ、効果的でなくなります。

認識までの平均時間が長いほど、潜在的なセキュリティインシデントを迅速に認識して対応の優先順位を付けるため、チームに適切なリソースとトレーニングの両方が用意されていることを確認する必要性が高くなります。認識までの平均時間が短いほど、チームはセキュリティアラートに適切に対応でき、効果的に準備して優先順位を付けられることがわかります。

対応までの平均時間

対応までの平均時間は、潜在的なセキュリティインシデントに対する最初の対応を開始するまでの平均時間です。具体的には、最初のアラートまたは潜在的なセキュリティインシデントの検出から、最初に実行された対応アクションまでの時間です。認識までの平均時間に似ていますが、認識までの平均時間が状況の単純な認識または確認であるのに対して、このメトリクスは具体的な対応アクション (例: システムデータの取得、システムの封じ込めなど) を測定するものです。

このメトリクスを使用して、セキュリティインシデントに対応するための準備状況を追跡できます。前述のように、準備は効果的な対応のための鍵となります。本書の「the section called “準備”」セクションを参照してください。

対応までの平均時間が長いほど、対応プロセスを効果的に文書化して活用できるように、チームが対応方法に関する適切なトレーニングを受けていることを確認する必要性が高くなります。対応までの平均時間が短いほど、チームは特定されたアラートに対する適切な対応を特定し、安全な運用への復帰を開始するために必要な対応アクションをより適切に実行できます。

封じ込めまでの平均時間

封じ込めまでの平均時間は、潜在的なセキュリティインシデントを封じ込めるのにかかる平均時間です。具体的には、最初のアラートまたは潜在的なセキュリティインシデントの検出から、対応アク

ションが完了し、攻撃者や侵害されたシステムによってそれ以上被害が広まることを効果的に防止するまでの時間です。

このメトリクスを使用して、チームが潜在的なセキュリティインシデントをどの程度軽減または封じ込めることができるかを追跡できます。潜在的なセキュリティインシデントを迅速かつ効果的に封じ込めることができないと、影響や範囲が広がり、さらなる侵害を受ける可能性が高まります。

封じ込めまでの平均時間が長いほど、発生しているセキュリティインシデントを迅速かつ効果的に軽減して封じ込めるために、知識と能力の両方を構築する必要性が高まります。封じ込めまでの平均時間が短いほど、ビジネスへの影響、範囲、リスクを軽減するために、チームは特定された脅威を軽減および封じ込めるために必要な対策をより深く理解し、採用できる状態にあります。

復旧までの平均時間

復旧までの平均時間は、潜在的なセキュリティインシデントから安全な運用を完全に回復するまでの平均時間です。具体的には、最初のアラートまたは潜在的なセキュリティインシデントの検出から、インシデントの影響のない正常かつ安全な運用状態に戻るまでの時間です。

このメトリクスを使用して、セキュリティインシデント後にチームがシステム、アカウント、環境を安全な運用にどの程度効果的に戻しているかを追跡できます。迅速かつ効果的に安全な運用に戻ることができないと、セキュリティに影響を与えるだけでなく、ビジネスとその運用への影響とコストも増大する可能性があります。

復旧までの平均時間が長いほど、セキュリティインシデントが運用やビジネスに与える影響を最小限に抑えるために、チームや環境で適切なメカニズム (クリーンシステムを安全に再デプロイするためのフェイルオーバープロセスや CI/CD パイプラインなど) を備える必要性が高くなります。復旧までの平均時間が短いほど、チームはより効果的にセキュリティインシデントが運用とビジネスに与える影響を最小限に抑えることができます。

攻撃者のドウェル時間

攻撃者のドウェル時間は、権限のないユーザーがシステムまたは環境にアクセス可能な時間を平均したものです。この時間枠は攻撃者がシステムまたは環境へのアクセス権を最初に取得した瞬間 (最初のアラートまたは検出よりも前であると考えられる) から始まることを除き、封じ込めまでの平均時間に似ています。

このメトリクスを使用して、環境に影響を与えるために攻撃者や脅威が使える時間、アクセス権、機会を削減するために多数のシステムとメカニズムがどの程度うまく連携しているかを追跡できます。攻撃者のドウェル時間を短縮することは、チームやビジネスにとって最優先事項です。

攻撃者のドウェル時間が長いほど、インシデント対応プロセスのどの部分を改善する必要があるかを特定し、チームが環境内の脅威や攻撃の影響と範囲を最小限に抑える能力を確保する必要性が増します。攻撃者のドウェル時間が短いほど、チームは脅威や攻撃者が環境内で使える時間と機会を最小限に減らし、最終的に運用やビジネスへのリスクと影響を軽減できます。

メトリクスのまとめ

インシデント対応のメトリクスを確立し、追跡することで、インシデント対応能力を効果的に測定、評価、改善できます。これを実現するためのいくつかの一般的なインシデント対応メトリクスについて、このセクションで説明しました。表 5 は、これらのメトリクスをまとめたものです。

表 5 – インシデント対応メトリクス

メトリクス	説明
検出までの平均時間	潜在的なセキュリティインシデントを発見するまでの平均時間
認識までの平均時間	潜在的なセキュリティインシデントを認識 (および優先順位付け) するまでの平均時間
対応までの平均時間	潜在的なセキュリティインシデントに対する最初の対応を開始するまでの平均時間
封じ込めまでの平均時間	潜在的なセキュリティインシデントを封じ込めるまでの平均時間
復旧までの平均時間	潜在的なセキュリティインシデントから安全な運用を完全に回復するまでの平均時間
攻撃者のドウェル時間	攻撃者がシステムまたは環境にアクセスできる平均時間

侵害インジケータ (IOC) を使用する

侵害のインジケータ (IOC) とは、ネットワーク、システム、または環境内で観察され、悪意のあるアクティビティまたはセキュリティインシデントを (高い信頼性レベルで) 特定できるアーティファクトです。IOC は、IP アドレス、ドメイン、TCP フラグやペイロードなどのネットワークレベルのアーティファクト、実行可能ファイルなどのシステムレベルまたはホストレベルのアーティファク

ト、ファイル名とハッシュ、ログファイルエントリ、レジストリエントリなど、さまざまな形式で存在します。また、システム上の特定の項目またはアーティファクトの存在 (特定のファイルまたは一連のファイルおよびレジストリ項目)、特定の順序で実行されるアクション (特定の IP からシステムにログインし、その後に特定の異常なコマンドを実行する)、または特定の脅威、攻撃、攻撃者の方法論を示す可能性のあるネットワークアクティビティ (特定のドメインとの間の異常なインバウンドトラフィックまたはアウトバウンドトラフィック) など、複数の項目またはアクティビティが組み合わさる場合もあります。

インシデント対応プログラムを反復的に改善するには、検出とアラートを継続的に構築して改善し、調査の速度と有効性を向上させるメカニズムとして、IOC を収集、管理、利用するフレームワークを実装する必要があります。まず、IOC の収集と管理をインシデント対応プロセスの分析と調査フェーズに組み込むことから開始できます。IOC をプロセスの標準部分としてプロアクティブに識別、収集、保存することで、(より包括的な脅威インテリジェンスプログラムの一環として) データのリポジトリを構築できます。このリポジトリを使用することで、既存の検出とアラートの改善、追加の検出とアラートの構築、アーティファクトの発生場所と発生日時の特定、一致する IOC が関与していた過去の調査の実施方法に関するドキュメントの構築と参照などを行うことができます。

継続的な教育とトレーニング

教育とトレーニングはどちらも進化し続ける継続的な取り組みであり、意図的に遂行して維持する必要があります。チームがテクノロジーの進化と脅威の状況に見合った認識、知識、能力を維持していることを確認するための多種多様なメカニズムが存在します。

1 つのメカニズムは、チームの目標と運用の標準的な部分として継続的な教育を採用することです。準備セクションで説明したように、インシデント対応スタッフとステークホルダーは、AWS 内のインシデントの検出、対応、調査について効果的にトレーニングを受ける必要があります。しかし、教育は「1 回限り」の取り組みではありません。教育は継続的に遂行されなければなりません。これにより、対応の有効性と効率を向上させるために活用できる最新の技術的進歩、更新、改善についてだけでなく、調査と分析を改善するために活用できるデータの追加や更新についてもチームが認識していることを確認できます。

もう 1 つのメカニズムは、ビジネスの特定の成果に焦点を当てたシミュレーションを定期的に (四半期ごとなど) 実行することです。本書の「the section called “定期的にシミュレーションを実行する”」セクションを参照してください。

最初のテーブルトップ演習を実行することは、改善のための最初のベースラインを生成できる優れた方法ですが、改善を続け、運用の現在の状態を最新かつ正確に反映し続けるためには、継続的なテストが鍵となります。最新かつ最も重要なセキュリティ状況と、最も重要な対応能力または最新の対応

能力をテストし、学習した教訓を教育、運用、プロセス/手順に組み込むことで、対応プロセスとプログラムを全体として継続的に改善できることが検証されます。

結論

クラウドジャーニーを続ける上で、AWS 環境の基本的なセキュリティインシデント対応の概念を考慮することが重要になります。利用可能なコントロール、クラウド機能、修復オプションを組み合わせて、クラウド環境のセキュリティを向上させることができます。また、最初は小さく始めて、反復的に実行しながら対応速度を向上させる自動化機能を採用することで、セキュリティイベントの発生に備えることもできます。

寄稿者

本書の現在および過去の寄稿者は次のとおりです。

- Amazon Web Services、Senior Security Solutions Architect、Anna McAbee
- Amazon Web Services、Senior Security Consultant、Freddy Kasprzykowski
- Amazon Web Services、Senior Security Engineer、Jason Hurst
- Amazon Web Services、Principal Security Consultant、Pat Gaw
- Amazon Web Services、Security Solutions Architecture、Senior Manager、Josh Du Lac
- Amazon Web Services、Principal Security Engineer、Paco Hope
- Amazon Web Services、Senior Security Engineer、Ryan Tick
- Amazon Web Services、Senior Security Engineer、Steve de Vera

付録 A: クラウド機能の定義

AWS では、200 を超えるクラウドサービスと数千の機能を提供しています。これらの多くは検出、予防、対応のネイティブ機能備えているほか、カスタムセキュリティソリューションの構築に使用できるものもあります。このセクションでは、クラウドでのインシデント対応に最も関連性の高いサービスのサブセットについて説明します。

トピック

- オートメーション
- 安全なストレージ
- 将来のセキュリティ機能とカスタムセキュリティ機能

ログ記録とイベント

AWS CloudTrail – AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、およびリスク監査などを可能にするサービスです。CloudTrail を使用すると、AWS サービス全体のアクションに関連するアカウントアクティビティをログに記録し、継続的にモニタリングし、保持できます。CloudTrail は、AWS マネジメントコンソール、AWS SDK、コマンドラインツール、およびその他の AWS サービスを通じて実行されたアクションなどの AWS アカウントアクティビティのイベント履歴を提供します。このイベント履歴により、セキュリティ分析、リソースの変更追跡、トラブルシューティングが簡素化されます。CloudTrail は次の 2 種類の AWS API アクションをログに記録します。

- CloudTrail 管理イベント (コントロールプレーンオペレーションとも呼ばれる) は、AWS アカウントのリソースで実行される管理オペレーションを示します。これには、Amazon S3 バケットの作成やログ記録の設定などのアクションが含まれます。
- CloudTrail データイベント (データプレーンオペレーションとも呼ばれる) は、AWS アカウントのリソース上またはリソース内で実行したリソースオペレーションを示します。これらの操作は、多くの場合、高ボリュームのアクティビティです。これには、Amazon S3 オブジェクトレベルの API アクティビティ (例: `GetObject`、`DeleteObject`、`PutObject` API オペレーション) や Lambda 関数の呼び出しアクティビティなどのアクションが含まれます。

AWS Config – AWS Config は、お客様が AWS リソースの設定の査定、監査、評価を行えるようにするサービスです。AWS Config は、AWS リソース設定を継続的に監視および記録し、記録された設定を、必要な設定に照らして自動的に評価することができます。AWS Config を使用すると、手動または自動での AWS リソース間の設定や関連性の変更を確認し、詳細なリソース設定履歴を調べ、お客様のガイドラインで指定された設定に対して、全体的なコンプライアンスを判断できます。これにより、コンプライアンス監査、セキュリティ分析、変更管理、運用上のトラブルシューティングを簡素化できます。

Amazon EventBridge – Amazon EventBridge は、AWS リソースの変更を記述したシステムイベントのストリームをほぼリアルタイムに配信するか、または API コールが AWS CloudTrail によって公開されたときに配信します。すぐに設定できる簡単なルールを使用して、ルールに一致したイベントを 1 つ以上のターゲット関数またはストリームに振り分けることができます。オペレーションの変更が発生すると、EventBridge はその変更を認識します。EventBridge は、これらのオペレーションの変

更に応答し、必要に応じて、応答メッセージを環境に送り、機能をアクティブ化し、変更を行い、状態情報を収集することによって、修正アクションを実行します。Amazon GuardDuty などの一部のセキュリティサービスは、EventBridge イベントの形式で出力を生成します。多くのセキュリティサービスは、出力を Amazon S3 に送信するオプションも提供しています。

Amazon S3 アクセスログ – 機密情報が Amazon S3 バケットに保存されている場合、お客様は Amazon S3 アクセスログを有効にして、そのデータに対するすべてのアップロード、ダウンロード、変更を記録できます。このログは、バケット自体への変更 (アクセスポリシーやライフサイクルポリシーの変更など) を記録する CloudTrail ログとは別に追加されます。アクセスログレコードの配信は、ベストエフォートベースで行われることに注意してください。ログ記録用に適切にバケットを設定した場合、そのバケットへのほとんどのリクエストについてログレコードが配信されます。サーバーログの完全性や適時性は保証されません。

Amazon CloudWatch Logs – お客様は、CloudWatch Logs エージェントを使用して Amazon EC2 インスタンスで実行されているオペレーティングシステム、アプリケーション、その他のソースから発信されたログファイルを、Amazon CloudWatch Logs を使用して監視、保存、およびアクセスできます。CloudWatch Logs は、AWS CloudTrail、Route 53 DNS クエリ、VPC フローログ、Lambda 関数などの送信先になります。関連するログデータは CloudWatch Logs から取得することができます。

Amazon VPC フローログ – VPC フローログを使用すると、VPC のネットワークインターフェイスとの間で行き来する IP トラフィックに関する情報をキャプチャすることができます。フローログを有効にした後で、Amazon CloudWatch Logs と Amazon S3 にストリーミングできます。VPC フローログは、特定のトラフィックがインスタンスに到達しない理由のトラブルシューティング、過度に制限の厳しいセキュリティグループルールの診断、EC2 インスタンスへのトラフィックを監視するためのセキュリティツールとしての使用など、さまざまなタスクでお客様を支援します。VPC フローログの最新バージョンを使用して、最も堅牢なフィールドを取得できます。

AWS WAF ログ – AWS WAF は、サービスによって検査されたすべてのウェブリクエストの完全なログ記録をサポートします。お客様は、これらを Amazon S3 に保存して、コンプライアンスと監査の要件を満たすだけでなく、デバッグとフォレンジックも実行できます。これらのログは、開始されたルールとブロックされたウェブリクエストの根本原因をお客様が判断するのに役立ちます。ログは、サードパーティーの SIEM およびログ分析ツールと統合できます。

Route 53 Resolver クエリログ – Route 53 Resolver クエリログを使用すると、Amazon Virtual Private Cloud (Amazon VPC) 内のリソースによって行われたすべての DNS クエリをログに記録できます。Amazon EC2 インスタンス、AWS Lambda 関数、またはコンテナのいずれであっても、Amazon VPC 内から DNS クエリを行うと、この機能がそれをログに記録します。これにより、アプリケーションの動作を調べて理解を深めることができます。

その他の AWS ログ – AWS は、お客様向けにサービス機能を継続的にリリースし、新しいログ記録およびモニタリング機能を提供しています。各 AWS サービスで使用できる機能の詳細については、公開ドキュメントを参照してください。

可視性とアラート

AWS Security Incident Response – AWS Security Incident Response は、自動化された機能と専門家のサポートを組み合わせることで、組織がライフサイクル全体を通じてセキュリティイベントを処理するのに役立つ包括的なサービスです。このサービスは、自動モニタリングと調査機能を活用して、セキュリティを注意深く監視しながら組織のリソースを解放します。また、セキュリティイベントが発生した場合、ステークホルダー間の迅速なコミュニケーションと調整を容易にし、応答時間が短縮されます。このサービスは、セキュリティイベントの準備とシミュレーション、アクティブなインシデントへの対応、インシデント後の報告と分析の合理化など、複数のユースケースをサポートしているため、組織はあらゆる段階でセキュリティ上の課題に対応する十分な準備が整います。

AWS Security Hub CSPM – AWS Security Hub CSPM は、AWS アカウント全体で優先度の高いセキュリティアラートとコンプライアンスステータスを包括的に把握できます。Security Hub CSPM は、Amazon GuardDuty、Amazon Inspector、Amazon Macie、AWS Partner ソリューションなど、さまざまな AWS サービスからの脅威検出結果を集約し、整理して優先順位を付けます。検出結果は、実用的なグラフとテーブルを含む統合ダッシュボードで視覚的に要約されます。また、組織が準拠する AWS のベストプラクティスと業界標準に基づいて、自動化されたコンプライアンスチェックを使用して環境を継続的にモニタリングすることもできます。

Amazon GuardDuty – Amazon GuardDuty は、悪意ある動作や不正な挙動を継続的にモニタリングし、お客様の AWS アカウントとワークロードの保護を支援するマネージド脅威検出サービスです。異常な API コール、不正なデプロイの可能性 (Amazon EC2 インスタンス、Amazon S3 バケットのアカウントやリソースが侵害された可能性を示す)、悪意のある人物による偵察などのアクティビティをモニタリングします。

GuardDuty は、機械学習を使用してアカウントとワークロードのアクティビティの異常を検出し、統合された脅威インテリジェンスフィードを通じて悪意が疑われる人物を特定します。潜在的な脅威が検出されると、サービスは GuardDuty コンソールと CloudWatch Events に詳細なセキュリティアラートを送信します。これにより、アラートに対して行動を起こすことが可能になり、既存のイベント管理およびワークフローシステムに簡単に統合できます。

GuardDuty には、Amazon S3 Protection 用の Amazon GuardDuty と Amazon EKS Protection 用の Amazon GuardDuty の 2 つの脅威モニタリング用アドオンも用意されています。Amazon S3 Protection により、GuardDuty はオブジェクトレベルの API オペレーションをモニタリングし、Amazon S3 バケット内のデータの潜在的なセキュリティリスクを特定できるようになりま

す。Kubernetes Protection により、GuardDuty は、Amazon EKS 内の Kubernetes クラスターの疑わしいアクティビティと侵害の可能性を検出できます。

Amazon Macie – Amazon Macie は AI を活用したセキュリティサービスであり、AWS に保存されている機密データを自動的に検出、分類、保護することで、データ損失を防ぐことに役立ちます。Macie は機械学習 (ML) を使用して、個人を特定できる情報 (PII) や知的財産などの機密データを認識し、ビジネス価値を割り当て、このデータが組織のどこに保存され、どのように利用されているかを可視化します。Amazon Macie は、データアクセスアクティビティの異常を継続的にモニタリングし、不正アクセスや不注意によるデータ漏洩のリスクを検出すると、アラートを送信します。

AWS Config ルール – AWS Config ルールは、リソースの優先設定を表し、AWS Config によって記録される関連リソースの設定変更に対して評価されます。リソースの設定に対するルールの評価結果は、ダッシュボードで確認できます。AWS Config ルールを使用すると、全体的なコンプライアンスとリスクのステータスを設定の観点から評価し、時間の経過に伴うコンプライアンスの傾向を確認し、リソースがルールに準拠しなくなる原因となった設定変更を見つけることができます。

AWS Trusted Advisor – AWS Trusted Advisor は、AWS 環境を最適化することでコストを削減し、パフォーマンスを向上させ、セキュリティを向上させるのに役立つオンラインリソースです。Trusted Advisor は、AWS のベストプラクティスに従ってリソースをプロビジョニングするのに役立つリアルタイムのガイダンスを提供します。CloudWatch Events の統合を含むすべての Trusted Advisor チェックは、ビジネスサポートプランおよびエンタープライズサポートプランのお客様が利用できます。

Amazon CloudWatch – Amazon CloudWatch は、AWS クラウドのリソースと、AWS で実行されるアプリケーションをモニタリングするサービスです。CloudWatch を使用して、メトリクスの収集とトラッキング、ログファイルの収集とモニタリング、アラームの設定、AWS リソースの変更への自動対応を行うことができます。CloudWatch では、Amazon EC2 インスタンス、Amazon DynamoDB テーブル、Amazon RDS DB インスタンスなどの AWS リソース、およびアプリケーションやサービスに生成されたカスタムメトリクス、アプリケーションが生成するあらゆるログファイルをモニタリングできます。Amazon CloudWatch を使用して、リソースの使用率、アプリケーションのパフォーマンス、運用の状況をシステム全体で把握できます。これらの洞察を使用して適宜対応し、アプリケーションのスムーズな動作を維持できます。

Amazon Inspector – Amazon Inspector は、AWS にデプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるための、自動化されたセキュリティ評価サービスです。Amazon Inspector では、自動的にアプリケーションを評価し、脆弱性やベストプラクティスからの逸脱がないかどうかを確認できます。評価を実行した後、Amazon Inspector は、重要度のレベルごとに優先順位が付けられたセキュリティ結果の詳細なリストを作成します。これらの検出結果は、直接確認す

ることも、Amazon Inspector コンソールまたは API から入手できる詳細な評価レポートの一部として確認することもできます。

Amazon Detective – Amazon Detective は、AWS リソースからログデータを自動的に収集し、機械学習、統計分析、グラフ理論を使用して、より迅速かつ効率的なセキュリティ調査を実施できるリンクされたデータセットを構築するセキュリティサービスです。Detective は、VPC フローログ、CloudTrail、GuardDuty などの複数のデータソースの何兆ものイベントを分析し、リソース、ユーザー、およびそれらの間の時間の経過に伴うインタラクションを統合したインタラクティブビューを自動的に作成します。この統合されたビューを使用して、すべての詳細とコンテキストを 1 か所で可視化して、検出結果の根本的な理由を特定し、関連する過去のアクティビティを掘り下げ、根本原因をすばやく特定できます。

オートメーション

AWS Lambda – AWS Lambda はイベント発生時にお客様のコードを実行し、基盤となるコンピューティングリソースをお客様に代わって自動で管理する、サーバーレスコンピューティングサービスです。Lambda を使用して、AWS の他のサービスをカスタムロジックで拡張したり、AWS のスケール、パフォーマンス、セキュリティで動作する独自のバックエンドを作成したりすることができます。Lambda は可用性の高いコンピューティングインフラストラクチャでコードを実行し、コンピューティングリソースの管理を実行します。これにはサーバーおよびオペレーティングシステムの管理、容量のプロビジョニングおよびオートスケーリング、コードとセキュリティパッチのデプロイ、コードのモニタリングとログ記録などが含まれます。必要なのはコードを提供することだけです。

AWS Step Functions – AWS Step Functions により、視覚的なワークフローを使用して分散アプリケーションとマイクロサービスのコンポーネントを容易に調整できるようになります。Step Functions には、アプリケーションのコンポーネントを整理し、一連のステップとして可視化できるグラフィカルコンソールがあります。これにより、複数のステップが必要なアプリケーションを簡単に構築して実行できます。Step Functions では、各ステップが自動的に開始および追跡され、エラーが発生した場合は再試行されるため、アプリケーションが意図したとおりの順序で実行されます。

また、Step Functions では各ステップの状態がログに記録されるため、問題が発生した場合は、問題を簡単に診断およびデバッグできます。コードを記述せずにステップを変更および追加できるため、アプリケーションを進化させ、イノベーションを高速化できます。AWS Step Functionsは AWS Serverless の一部であり、サーバーレスアプリケーションの AWS Lambda 関数を簡単にオーケストレーションできます。Step Functions は、Amazon EC2 や Amazon ECS などのコンピューティングリソースを使用したマイクロサービスのオーケストレーションにも使用できます。

AWS Systems Manager – AWS Systems Manager は、AWS 上のインフラストラクチャを可視化し、制御するためのサービスです。Systems Manager を使用すると、統合ユーザーインターフェイスで複数の AWS サービスの運用データを確認でき、AWS リソース全体に関わる運用タスクを自動化できます。Systems Manager を使用すると、アプリケーションごとにリソースをグループ化し、モニタリングとトラブルシューティングのために運用データを確認し、リソースのグループに対して対応できます。Systems Manager は、インスタンスを定義された状態に保ち、アプリケーションの更新やシェルスクリプトの実行などのオンデマンドの変更を実行し、その他の自動化タスクやパッチ適用タスクを実行できます。

安全なストレージ

Amazon Simple Storage Service – Amazon S3 はオブジェクトストレージであり、任意の場所の任意の量のデータを保存および取得するように構築されています。99.999999999% の耐久性を実現するように設計されており、あらゆる業界のマーケットリーダーが使用する数百万ものアプリケーションのデータを保存します。Amazon S3 は包括的なセキュリティを提供し、規制要件を満たすように設計されています。これにより、コストの最適化、アクセスコントロール、コンプライアンスのためのデータの管理に使用する方法に柔軟性がもたらされます。Amazon S3 が提供する query-in-place 機能により、Amazon S3 に保存されているデータに対して強力な分析を直接実行できます。Amazon S3 は広くサポートされているクラウドストレージサービスであり、サードパーティーソリューション、システムインテグレーターパートナー、その他の AWS サービスの最大のコミュニティの 1 つと統合されています。

Amazon Glacier – Amazon Glacier は、データのアーカイブと長期バックアップ用の、安全で耐久性が高く、非常に低コストのクラウドストレージサービスです。99.999999999% の耐久性を実現し、包括的なセキュリティを提供し、規制要件を満たすように設計されています。Amazon Glacier が提供する query-in-place 機能により、保管中のアーカイブデータに対して強力な分析を直接実行できます。コストを抑えながらさまざまな取り出しニーズに対応できるように、Amazon Glacier では、アーカイブへのアクセスに数分から数時間まで 3 つのオプションを用意しています。

将来のセキュリティ機能とカスタムセキュリティ機能

前述のサービスと機能はすべてを網羅しているわけではありません。AWS では新機能が継続的に追加されます。詳細については、「AWS の最新情報」ページおよび「AWS クラウドセキュリティ」ページを確認することをお勧めします。AWS がネイティブクラウドサービスとして提供するセキュリティサービスに加えて、AWS サービス上に独自の機能を構築することに関心があるかもしれません。

AWS CloudTrail、Amazon GuardDuty、Amazon Macie など、セキュリティサービスの基本セットをアカウントで有効にすることをお勧めしますが、最終的に、これらの機能を拡張してログアセットか

らさらなる価値を引き出すことができます。APN セキュリティコンピテンシープログラムに記載されているツールなど、多数の利用可能なパートナーツールがあります。また、独自のクエリを作成してログを検索することもできます。AWS が提供する多数のマネージドサービスにより、今まで以上に簡単に実行できます。Amazon Athena、Amazon OpenSearch Service、Amazon Quick、Amazon Machine Learning、Amazon EMR など、調査に役立つ追加の AWS サービスで、本ホワイトペーパーに記載されていないものも多数存在します。

付録 B: AWS インシデント対応リソース

AWS では、インシデント対応能力の育成を支援するリソースを公開しています。ほとんどのコード例と手順は、AWS 外部の GitHub パブリックリポジトリにあります。以下は、インシデント対応の実行方法の例を示すリソースです。

プレイブックリソース

- インシデント対応プレイブックのフレームワーク - AWS サービスを使用する際の潜在的な攻撃シナリオに備えて、お客様がセキュリティプレイブックを作成、開発、統合するためのフレームワークのサンプル。
- インシデント対応プレイブックのサンプル - AWS のお客様が直面する一般的なシナリオを カバーするプレイブック。
- AWS は、5 つの公開ワークショップのリリースを発表しました。

フォレンジックリソース

- 自動インシデント対応とフォレンジックフレームワーク – このフレームワークとソリューションは、封じ込め、取得、検査、分析のフェーズで構成される標準のデジタルフォレンジックプロセスを提供します。AWS Λ 関数を活用して、自動化された反復可能な方法でインシデント対応プロセスをトリガーします。自動化ステップを運用し、アーティファクトを保存し、フォレンジック環境を作成するためにアカウントの分離を行います。
- Amazon EC2 用自動フォレンジックオーケストレーター – この実装ガイドは、潜在的なセキュリティ問題が検出された場合に、フォレンジック分析のために EC2 インスタンスおよびアタッチされたボリュームからデータをキャプチャして調査するためのセルフサービスソリューションを提供します。ソリューションをデプロイするための AWS CloudFormation テンプレートがあります。
- AWS でフォレンジックディスク収集を自動化する方法 – この AWS ブログでは、潜在的なセキュリティインシデントの範囲と影響を判断するために、ディスク証拠をキャプチャして分析を行う

自動化ワークフローを設定する方法について説明します。ソリューションをデプロイするための AWS CloudFormation テンプレートもあります。

注意

お客様は、本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。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明しており、これらは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上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または黙示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は AWS 契約によって規定されます。本書は、AWS とお客様との間で締結されるいかなる契約の一部でもなく、その内容を修正するものでもありません。

© 2024 Amazon Web Services, Inc. or its affiliates. All rights reserved.

ドキュメント履歴

次の表は、2026 年 1 月 1 日以降に行われた AWS Security Incident Response ドキュメントへの重要な追加項目をまとめたものです。このドキュメントの更新に関する通知については、RSS フィードにサブスクライブできます。

変更	説明	日付
AWS Security Incident Response Triage サービスロールポリシーのポリシーの説明を更新する	AWS Security Incident Response Triage サービスロールポリシーのポリシーの説明を更新して、サービスがサービスの調整を改善し、潜在的なインシデントを調査するための情報を収集できるようにする変更を反映します。	2026 年 3 月 27 日
メタデータを送信	AWS サポート ケースを通してメタデータを送信する手順を追加しました。	2026 年 3 月 27 日
封じ込め設定を送信	AWS サポート ケースを通して封じ込め設定を送信する手順を追加しました。	2026 年 3 月 27 日
封じ込め StackSet テンプレート	封じ込め StackSet CloudFormation テンプレートを更新しました。	2026 年 3 月 27 日
委任管理者アカウントに関する AWS リージョン 考慮事項を明確にする	初期設定時に 1 つの AWS リージョン で委任された AWS Security Incident Response 管理者アカウントを指定しますが、このサービスはサポートされているすべての AWS リージョン にわ	2026 年 3 月 20 日

	たって組織全体をカバーします。	
封じ込めアクションの設定を定義する	封じ込めアクションの設定セクションを、現在のオプションに合わせて更新しました。	2026 年 3 月 19 日
プロアクティブレスポンスとアラートのトリアージ	プロアクティブレスポンスとアラートのトリアージワークフローがオプションであるという参照箇所を削除しました。	2026 年 3 月 3 日
対応タイムライン	対応タイムラインを更新して、ケースの受付確認に 15 分の SLO、ケースがクローズされる前のお客様の応答に 5 営業日を指定しました。	2026 年 2 月 24 日
コミュニケーションのベストプラクティス	ケースのクローズタイムラインを更新して、重要な情報リクエストに対するお客様の応答に 5 営業日を指定しました。	2026 年 2 月 24 日
「AWS CloudShell を使用して Security Incident Response とやり取りする」に AWS CLI リファレンスを追加しました。	「AWS Security Incident Response 向けの AWS Command Line Interface リファレンス」のリンクを追加しました。	2026 年 2 月 24 日
RACI マトリックス	RACI マトリックスの「CIRT 封じ込めアクションの承認」を「封じ込めアクションの承認」に更新しました。	2026 年 2 月 13 日

封じ込め設定	封じ込め設定オプションを「封じ込めアクションなし」、「承認後に封じ込め」、「自動封じ込め」から「承認が必要」、「確認されたリソースを封じ込める」、「疑わしいリソースを封じ込める」に更新し、説明を改訂しました。	2026 年 2 月 13 日
Security Incident Response のデプロイ後	「AWS Security Incident Response: New Integrations and OU-Level Subscription」デモへのリンクを追加しました。	2026 年 2 月 4 日
モニタリングと調査	このページの概要とサブセクションに改訂された内容を追加しました。	2026 年 2 月 4 日
検出と分析	このページの概要とサブセクションに改訂された内容を追加しました。	2026 年 2 月 4 日
封じ込め	このページに改訂されたコンテンツを追加しました。	2026 年 2 月 4 日
AI 調査エージェント	このページに「顧客データの使用」免責事項を追加しました。免責事項:「AI 調査エージェント」は、モデルトレーニングに顧客データを使用せず、また、サードパーティーと顧客データを共有しません。	2026 年 2 月 4 日

変更	説明	日付
メンバーシップをキャンセルする	解除操作を行うと、会員資格およびサービスが課金サイクルの終了時ではなく、直ちに終了する旨を明示するように「会員資格解除ページ」を更新しました。	2025 年 11 月 20 日
AWS マネージポリシー	サービスが提供するアクションの一覧に、ケースの更新、ケースコメントの作成、ケースの一覧表示、ケースコメントの一覧表示を追加しました。	2025 年 11 月 19 日
サービスにリンクされたロールの使用	サービスが提供するアクションの一覧に、ケースの更新、ケースコメントの作成、ケースの一覧表示、ケースコメントの一覧表示を追加しました。	2025 年 11 月 19 日
通信設定	新機能ドキュメントの「コミュニケーション設定」セクションを作成および更新しました。	2025 年 11 月 12 日
オンボーディングガイドの追加と更新	以下のセクションを含むオンボーディングガイドの追加を作成および更新しました 「セキュリティインシデント対応を有効にする」セクションを追加しました。 「セキュリティインシデント対応エンジニアが脅威封じ込	2025 年 11 月 12 日

変更	説明	日付
	めアクションを実行することを承認する」セクションを追加しました。 「セキュリティインシデント対応のデプロイ後」セクションを追加しました。 インシデント対応チームの更新 セクションを追加しました。 GuardDuty の結果と抑制ルール セクションを追加しました。 Amazon EventBridge セクションを追加しました。 統合と外部ツールワークフロー セクションを追加しました。 外部ツールワークフロー セクションを追加しました。 付録 A: 連絡先 セクションを追加しました。	

変更	説明	日付
コンプライアンスと請求言語の更新	AWS Security Incident Response がフレームワークの対象ではないというステートメントが削除され、更新されました。AWSSecurity Incident Response が HITRUST で対象となりました。今後さらに増える予定です。 可視性とコントロール が更新され、AWS Security Incident Response を追加されました。 メンバーシップのキャンセル を更新し、サービスの請求期間を明確にしました。 AWS Security Incident Response の使用を開始するための一般的なタスクに関する追加のコンテキストを提供する動画を「開始方法」に追加しました。	2025 年 8 月 15 日

変更	説明	日付
更新 – AWSSecurityIncidentResponseServiceRolePolicy	ポリシーに、"organizations:DescribeAccount" および "organizations:ListDelegatedAdministrators" 用の 2 つの新しいアクションと新しい条件が含まれるようになりました。 `"Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } }`	TBD
機能の更新: 特定の組織単位 (OU) またはお使いの AWS Organization 全体にサブスクライブする	ユーザーインターフェイスのヘルプパネルが更新され、特定の組織単位 (OU) またはお使いの AWS Organization 全体にサブスクライブするための更新が反映されました。 新しいページ「Managing membership with organizational units (OUs)」の作成 新しい OU 管理機能を反映するように AWS Organizations に関連するページが更新されました。	2025 年 8 月 7 日

変更	説明	日付
サービスクォータを更新	Service Quotas ページを更新し、「AWS 全般のリファレンスガイド」の「AWS Security Incident Response endpoints and quotas」を参照できるようにしました。	2025 年 8 月 7 日
ユーザーフィードバックの更新	AWS Security Incident Response ケースにサービスのハイパーリンクを追加しました。 「セキュリティ技術ガイド」で「コンピュータセキュリティインシデント対応ガイド SP 800-61 r3」を反映するように更新	2025 年 8 月 7 日
Amazon EventBridge の AWS Security Incident Response との統合に関するページを追加しました。	Amazon EventBridge が AWS Security Incident Response でどのように統合されるかを説明する新しいコンテンツセクション。	2025 年 6 月 26 日

変更	説明	日付
SLR を更新し、サービスの使用権限をサポートするアクセス許可を追加しました。	AWSSecurityIncidentResponseTriageServiceRolePolicy が更新され、security-ir:GetMembership、security-ir:ListMemberships、security-ir:UpdateCase、guardduty:ListFilters、guardduty:UpdateFilter、guardduty:DeleteFilter、guardduty:GetAdministratorAccount アクセス許可が追加されました。guardduty:GetAdministratorAccount が、委任アカウントの GuardDuty 自動アーカイブフィルターの管理を容易にするために追加されました。	2025 年 6 月 2 日
リソースの更新。	https://docs.aws.amazon.com/security-ir/latest/userguide/appendix-b-incident-response-resources.html#playbook-resources を更新し、お客様が利用できるアクティブなワークショップを反映しました。	2025 年 5 月 23 日
サービスは日本語をサポートしています。	サポートされている設定を更新して、日本現地時間での日本語サポートを明記しました。英語はグローバルにサポートされています。	2025 年 5 月 13 日

変更	説明	日付
コンテンツの更新とお客様のフィードバック。	セットアップの一部として委任管理者アカウントを使用する場合の追加タスクを反映するために、https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html に注記を追加しました。 サービス生成ケースを使用する際のカスタマーエクスペリエンスと「検出と分析」を更新しました。 アカウントのキャンセルの詳細を更新し、メンバーシップをキャンセル した場合の請求への影響をより明確にしました。	2025 年 5 月 9 日
新たにサポートされる 3 つのリージョンを追加しました。	https://docs.aws.amazon.com/security-ir/latest/userguide/supported-configs.html に 3 つの新しいリージョンを追加しました。ムンバイ、パリ、サンパウロ。	2025 年 5 月 7 日

変更	説明	日付
更新: ドキュメントに関するお客様のコメントに基づく更新。	複数ページのスペルエラーと文法エラーが修正されました。 security-ir をサービスプレフィックスとして正確に反映するように https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/organizations_permissions.html を更新しました。 Route53 と DNS に関する注記を https://docs.aws.amazon.com/security-ir/latest/userguide/source-containment.html に追加しました。	2025 年 2 月 7 日

変更	説明	日付
更新: ドキュメントに関するお客様のコメントに基づく更新。	https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html を stackset テンプレートに更新しました。 エントリ triage.security-ir.com を triage.security-ir.amazonaws.com に修正しました https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html で AWSSupport-ContainEC2Reversible の追跡される接続に関する注記を追加しました。 https://docs.aws.amazon.com/security-ir/latest/userguide/managing-associated-accounts.html のリンク切れを修正しました。 https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html にメンバーシップアカウントの定義を追加しました。 AWS Organizations 管理アカウントに関する補足の注記を https://docs.aws.amazon.com/en_us/security-ir/latest/u	2024 年 12 月 20 日

変更	説明	日付
	serguide/using-service-linked-roles.html に追加しました。	

変更	説明	日付
更新: ドキュメントに関するお客様のコメントに基づく更新。	テキスト内の複数の重複した AWS AWS を削除しました。 https://docs.aws.amazon.com/security-ir/latest/userguide/sir_tagging.html および https://docs.aws.amazon.com/security-ir/latest/userguide/service-name-info-in-cloudtrail.html のリンク切れを修正しました。 https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html の更新。最初の段落から > を削除しました。AWSSupport-ContainEC2Reversible を AWSSupport-ContainEC2Instance に置き換えました。AWSSupport-ContainIAMReversible を AWSSupport-ContainIAMPrincipal に置き換えました。AWSSupport-ContainS3Reversible を AWSSupport-ContainS3Resource に置き換えました。 https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/issues.html のフォーマットを更新しました サポートチケットを使用してセキュリティインシデント対応に連絡するようお客	2024 年 12 月 10 日

変更	説明	日付
	様に指示する際に使用できるよう、https://docs.aws.amazon.com/security-ir/latest/userguide/understand-response-teams-and-support.html に、サポートフォームで選択するオプションを記載しました。 https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html の CloudWatch Events を削除し、EventBridge に置き換えました。 https://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html での文法の更新。 https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide.html から公開日を削除し、この表の更新に置き換えました。	
更新: AWS マネージドポリシーとサービスにリンクされたロール。	マネージドポリシーとサービスにリンクされたロールの更新。	2024 年 12 月 1 日
サービスの起動	re:Invent 2024 でのサービス開始に関連する初期サービスドキュメント	2024 年 12 月 1 日