AWS セキュリティインシデント対応ユーザーガイド

Version December 1, 2024

AWS セキュリティインシデント対応ユーザーガイド:

Table of Contents

AWS セキュリティインシデント対応とは

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からの復旧に役立つガイダンスを迅速に準備し、対応し、受け取るのに役立ちます。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 セキュリティインシデント対応は、検出結果の優先順位付け、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、影響を受けるリソースを調査する AWS カスタマーインシデント対応チーム (CIRT) にアクセスできます。

> **Note**
>
> 影響を受ける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 セキュリティインシデント対応は、他のAWS 検出および対応サービスと連携し、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 セキュリティインシデント対応では、次の言語とリージョンの設定がサポートされています。

- Language: AWS Security Incident Response は英語で利用できます。
- サポートされている AWS リージョン：

  AWS セキュリティインシデント対応は、 のサブセットで使用できます AWS リージョン。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を行います。

  - 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 (ストックホルム)
- アジアパシフィック (シンガポール)
- アジアパシフィック (ソウル)
- 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)

モニタリングおよび調査機能を有効にすると、 AWS セキュリティインシデント対応はすべてのアクティブな商用の Amazon GuardDuty の検出結果をモニタリングします AWS リージョン。セキュリティのベストプラクティスとして、 では、サポートされているすべての AWS リージョン GuardDuty で を有効にする AWS 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場合でも、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 AWS リージョン 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力バレッジを維持できます。

> **Note**
>
> Amazon は、設定されたリージョンの結果 GuardDuty を報告します。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 およびサードパーティーとの統合によるセキュリティアラートを迅速にレビューし AWS Security Hub、チームが分析する必要のある数を減らします。環境に基づいて抑制ルールを設定し、優先順位付けと調査に必要な優先度の低いアラートを減らします。

インシデント対応の合理化

関連する利害関係者、サードパーティーのサービス、ツールと数分以内にインシデント対応をスケーリングして実行します。

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APIs、 を統合し、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できるように を提供します。

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検証済みツールにアクセスします。

迅速なサポート

AWSのカスタマーインシデント対応チーム (CIRT) に接続して、セキュリティイベントから復旧する方法を調査、封じ込め、ガイダンスを受け取ります。

準備状況と準備状況

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して、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 セキュリティインシデント対応サービスとその仕組みを理解する上で重要です。

Scope： 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関連する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調査。

AWS セキュリティインシデント対応サービスポータル: 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。チケット発行システム、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容易になりました。

コミュニケーション: インシデント対応プロセス中に、 AWS セキュリティインシデント対応チームと顧客の間で進行中の対話と情報共有。

封じ込め、根絶、復旧: 追加の不正なアクティビティ (封じ込め) の防止と、不正なリソースと元の脆弱性 (根絶) の削除、および通常どおりビジネスに戻るためのリソースの復旧。

継続的な改善: AWS セキュリティインシデント対応は、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組み込み、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 セキュリティインシデント対応は up-to-date、進化するセキュリティ課題に対処するための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: セキュリティポリシー、許容可能な使用ポリシー、または標準的なセキュリティプラクティスに違反する、または違反するおそれのあるシステムまたはネットワーク内で観測可能な出現。

インシデント対応チーム: 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。サポート AWS されるケースの場合、これは AWS カスタマーインシデント対応チーム () です CIRT。

インシデント対応ワークフロー: 800-61 NIST 標準に沿った、セキュリティイベントの管理に関連する end-to-end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 セキュリティインシデント対応ツールとサービスにリンクされたロール。

学習した教訓: セキュリティイベントへの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、将来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 セキュリティインシデント対応は、Amazon からのセキュリティアラートを迅速にレビューし GuardDuty、チームが分析する必要がある最も重要なアラートを最優先します。環境の詳細に基づいて抑制ルールを設定し、不要なアラートを防ぎます。

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し、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。

報告とコミュニケーション: 自動通知、通話ブリッジ、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 セキュリティインシデント対応は、 に一元化された単一のダッシュボード AWS Management Console を提供し、すべての AWS セキュリティインシデント対応の取り組みを管理します。

Responder Generated Intelligence: 侵害の指標、戦術、手法、手順、および調査によって AWS CIRT 観察された関連するパターン。

セキュリティイベントの専門知識: 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。特にクラウドの AWS コンテキストで。

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を担当し、お客様はクラウド内のセキュリティを担当します。

脅威インテリジェンス: 進化するセキュリティ脅威を特定して対応するために役立つ、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: セキュリティイベントの初期評価と優先順位付け。適切な対応と次のステップを決定します。

ワークフロー: セキュリティイベントの管理に関連する end-to-end定義された一連のステップとアクティビティ。

開始方法

内容

メンバーシップアカウントを選択する

メンバーシップアカウントは、 AWS 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および履歴セキュリティイベントの作成と管理に使用できるアカウントです。 AWS Security Incident Response のメンバーシップアカウントは、Amazon GuardDuty や などのサービスで有効にしたのと同じアカウントに調整することをお勧めします AWS Security Hub。

を使用して AWS 、セキュリティインシデント対応メンバーシップアカウントを選択するための 2 つのオプションがあります AWS Organizations。Organizations 管理アカウントまたは Organizations 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 セキュリティインシデント対応の管理タスクとケース管理は、委任管理者アカウントにあります。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。

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 セキュリティインシデント対応メンバーシップの中央メンバーシップアカウントになります。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、アクティブおよび解決済みのケースを作成、アクセス、管理する必要があります。

AWS セキュリティインシデント対応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ます。

アクセス許可を追加するには、「特定のステップの IAM ID アクセス許可の追加と削除」を参照してください。

AWS 「セキュリティインシデント対応管理ポリシー」を参照してください。

アクセスIAM許可を確認するには、次の手順に従います。

- IAM ポリシーを確認する： ユーザー、グループ、またはロールにアタッチされている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ます。概要ページで、アタッチされているすべてのポリシーのリストを表示する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。たとえば、ケースにアクセスする必要がある場合は、 を試してくださいListCases。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 を使用するSDK： コマンドラインインターフェイス (CLI) AWS Command Line Interface または AWS SDK任意のプログラミング言語で を使用して、アクセス許可をテストできます。たとえば、 では AWS Command Line Interface、 `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。
- Policy IAM Simulator を使用する： IAM Policy Simulator は、IAMポリシーをテストし、ポリシーがアクセス許可に与える影響を確認できるようにするツールです。

> **Note**
>
> 具体的な手順は、 AWS サービスや実行しようとしているアクションによって異なる場合があります。

メンバーシップの詳細の設定

- AWS リージョン メンバーシップとケースが保存される を選択します。

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

- 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環として、プライマリ連絡先とセカンダリ連絡先を指定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 に関連付ける AWS Organizations

メンバーシップは、リンクされているすべての のカバレッジを付与 AWS アカウント します AWS Organizations。 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。

プロアクティブレスポンスとアラートの優先順位付けワークフローを設定する

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は、有効なセキュリティサービスをモニタリングするために組織内で有効にするオプション機能です。有効にする機能の横にあるトグルを選択します。

オンボーディングの問題が発生した場合は、追加のサポートを受けるAWS Support ケースを作成してください。ID AWS アカウント 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。

プロアクティブレスポンスとアラートの優先順位付け： AWS セキュリティインシデント対応は、Amazon と Security Hub の統合から生成されたアラートをモニタリング GuardDuty および調査します。この機能を使用するには、Amazon を有効にする GuardDuty 必要があります。 AWS セキュリティインシデント対応では、サービスの自動化により優先度の低いアラートをトリアージするため、チームは最も重要な問題に集中できます。 AWS セキュリティインシデント対応と Amazon GuardDuty および との連携の詳細については AWS Security Hub、 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。

この機能により、 AWS Security Incident Response は、組織 AWS リージョン でサポートされているすべてのアカウントとアクティブな の調査結果をモニタリングおよび調査できます。この機能を容易にするために、 AWS Security Incident Response は、 内のすべてのメンバーアカウントにサービスにリンクされたロールを自動的に作成します AWS Organizations。ただし、管理アカウントで

は、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、管理アカウントでサービスにリンクされたロールを作成できません。AWS CloudFormation スタックセットを使用して、管理アカウントでこのロールを手動で作成する必要があります。

封じ込め： セキュリティインシデントが発生した場合、 AWS セキュリティインシデント対応は、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、影響をすばやく軽減するための封じ込めアクションを実行できます。セキュリティインシデント対応では、デフォルトで封じ込め機能は有効になりません。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 セキュリティインシデント対応コンソールのダッシュボードには、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。

を選択してView incident response team、インシデント対応チームメイトの詳細にアクセスします。

アラートのトリアージが有効になっているかどうかを確認するproactive responseには、 を選択します。alert triaging ワークフローを有効にしていない場合は、そのステータスをモニタリングし、有効にProactive Responseすることを選択できます。

ダッシュボードの「My Cases」セクションには、 AWS サポート対象ケースのオープン数とクローズ数、および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、クローズし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利害関係者がいます。メンバーシップの一部として最大 10 人の利害関係者を設定できます。

内部関係者の例には、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、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には、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 (ISV) 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、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権がチームメイトに自動的に付与されることはありません。 AWS セキュリティインシデント対応の 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ます。

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、次のイベントに関する E メール通知を受け取ります。

- ケース (作成、削除、更新)
- コメント (作成、削除、更新)
- 添付ファイル (作成、削除、更新)
- メンバーシップ (作成、更新、キャンセル、再開)

アカウントと の関連付け AWS Organizations

AWS セキュリティインシデント対応を有効にすると、メンバーシップが作成され、 に調整されます AWS Organizations。Organizations 内のすべてのアカウントは、 AWS セキュリティインシデント対応メンバーシップに整合されます。

詳細については、「 による AWS セキュリティインシデント対応アカウントの管理 AWS Organizations」を参照してください。

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 からのセキュリティアラートを確認してトリアージし GuardDuty AWS Security Hub、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 CIRT チームは、トリアージされていない検出結果を調査し、潜在的な問題を迅速に封じ込めるようチームに迅速にエスカレーションし、指示します。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アクセス許可を AWS Security Incident Response に付与できます。

AWS セキュリティインシデント対応は、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 セキュリティインシデント対応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を保護して対応するためのベストプラクティスに従います。

AWS Security Incident Response サービス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、 は AWS CIRT調査します。チームは、 GuardDuty アラートなどのログイベントとサービスデータを収集し、そのデータの優先順位付けと分析、修復と封じ込めのアクティビティの実行、インシデント後のレポートを提供します。

内容

準備

AWS セキュリティインシデント対応チームは、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

AWS セキュリティインシデント対応は、Amazon および 統合からのセキュリティ検出結果をモニタリング、トリアージ GuardDuty 、調査します AWS Security Hub。 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るその他のドクションは次のとおりです。

サポートされている検出ソースの有効化

> **Note**
>
> AWS セキュリティインシデント対応サービスのコストには、サポートされている検出または他の AWS サービスの使用のソースに関連する使用料およびその他のコストと料金は含ま

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

GuardDuty は、 AWS 環境内のデータソースとログを継続的にモニタリング、分析、処理する脅威検出サービスです。 AWS セキュリティインシデント対応を使用するには、 を有効にする GuardDuty 必要はありません。ただし、プロアクティブレスポンスとアラートの優先順位付け機能を使用するには、Amazon を有効にする GuardDuty 必要があります。

組織全体 GuardDuty で 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 GuardDuty で を有効にすることを強くお勧めします AWS リージョン。これにより GuardDuty 、 は、アクティブに使用し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 リージョンとエンドポイント」を参照してください。

を有効にすると、 AWS Security Incident Response GuardDuty は重大な脅威検出データにアクセスでき、 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

Security Hub 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。これらの統合は、 AWS Security Incident Response が他の検出ツールからの結果をモニタリングおよび調査するのに役立ちます。

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

Security Hub 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統合の場合、から統合を購入し AWS Marketplace、統合を設定する必要がある場合があります。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 統合を有効に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は、以下のツールと統合されているときに、結果をモニタリングおよび調査できます AWS Security Hub。

- CrowdStrike - CrowdStrike ファルコン

- レースワーク - レースワーク
- Trend Micro – Cloud One

これらの統合を有効にすることで、 AWS セキュリティインシデント対応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。

結果の分析。

AWS セキュリティインシデント対応の自動化と AWS CIRTサービスチームは、サポートされているツールのすべての結果を分析します。サポート AWS ケースを使用してお客様と通信することで、お客様の環境について学習し始めます。例えば、結果が予想される動作であるか、インシデントにエスカレーションする必要があるかを理解する必要がある場合などです。お客様の環境からさらに詳しく知るため、 サービスと をカスタマイズして通信数を減らします。

イベントのレポート。

AWS セキュリティイベントは、セキュリティインシデント対応サービスポータルから発生させることができます。セキュリティイベント中は待たないことが重要です。 AWS セキュリティインシデント対応では、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の調査、ログの分析、異常なパターンの検索を行います。お客様のパートナーシップと環境の理解により、この分析が加速されます。

通信します。

AWS セキュリティインシデント対応では、イベントチケットを通じてセキュリティ担当者に連絡することで、調査中に最新情報を得ることができます。複数のチームメイトがイベントをサポートできます。すべて、お客様が提供したコンテンツと AWS 更新のイベントチケットを使用します。

通信には、セキュリティアラートの生成時の自動通知、イベント分析中の通信、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継続的な分析、セキュリティイベント中の調査結果の取得などが含まれます。

AWS セキュリティインシデント対応では、2 つの異なるケースタイプを使用してお客様と通信します。アウトバウンド通信 Support ではイベントを通知し、 AWS セキュリティインシデント対応ではお客様がオープンしたケースについて通信します。

AWS サポートケース: サービスは AWS サポートケースを使用してチームと通信します。検出結果が生成される各 AWS アカウント にサポートケースを作成します。このアプローチにより、特定のワークロードを所有する複数のチームとのコミュニケーションが容易になります。これらのチームは、担当分野で発生するイベントについてより多くの知識を持つことになるためです。

AWS セキュリティインシデント対応ケース: 検出結果をセキュリティインシデントにエスカレーションする必要があると判断した場合、 AWS セキュリティインシデント対応ケースを作成します。これにより、重大なセキュリティ問題に適切なレベルの注意と対応がとられます。

これらのコミュニケーションに積極的に関与し、タイムリーな対応を行うことで、 AWS セキュリティインシデント対応サービスが次のことを行うことができます。

- 環境と予想される動作をよりよく理解します。
- 時間の経過とともに誤検出を減らします。
- アラートの精度と関連性を向上させます。
- 真のセキュリティインシデントへの迅速な対応を確保します。
- AWS Security Incident Response サービスの有効性はコラボレーションとともに向上し、より安全で効率的にモニタリングされる AWS 環境につながります。

含む

AWS セキュリティインシデント対応は、 と提携してイベントを含めます。 AWS Security Incident Response のサービスロールを設定して、アラートへの応答としてアカウントで自動および手動アクションを実行できます。また、SSMドキュメントを使用して、お客様自身で、またはサードパーティーの関係と連携して封じ込めを実行することもできます。

封じ込めの重要な部分は、システムのシャットダウン、ネットワークからのリソースの分離、アクセスの無効化、セッションの終了など、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戦略と手順が事前に決定されてい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、潜在的な影響を知らせ、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を補完するガイドを提供します。

AWS セキュリティインシデント対応は、サポート対象の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与える可能性のある時間を短縮します。この機能により、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は次のとおりです。

- EC2 封じ込め： `AWSSupport-ContainEC2Instance`封じ込めの自動化は、EC2インスタンスを元に戻す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、 内外のリソースとの通信を防止しますVPC。

> **Important**
>
> セキュリティグループの変更に伴って既存の追跡対象接続が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「ソースの包含」セクションを参照してください。

- IAM 封じ込め: `AWSSupport-ContainIAMPrincipal`封じ込めの自動化は、 IAM ユーザーまたはロールを元に戻す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 に残しますが IAM、アカウント内のリソースとの通信から分離します。
- S3 コンテナ: `AWSSupport-ContainS3Resource`コンテナオートメーションは、S3 バケットの可逆的なコンテナを実行し、バケットにオブジェクトを残して、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。

> **Important**
>
> AWS Security Incident Response はデフォルトでは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、まず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、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、アカウントごとに、または組織全体で個別に作成できます。

AWS セキュリティインシデント対応では、リスク選好度に適合する主要なイベントタイプごとに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ます。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
- サービス利用不可 (ネットワーク接続、外部当事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 (部分的封じ込めと完全封じ込めなど)
- ソリューションの永続性 (例: 可逆性または非可逆性)

- 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。

AWS セキュリティインシデント対応は、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達成するための段階的なアプローチを推奨します。

- 封じ込め戦略
  - AWS セキュリティインシデント対応はセキュリティイベントの範囲を特定できますか？
    - 「はい」の場合は、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。
    - いいえの場合は、特定されたリソースで次のステップを実行するのと並行して調査します。
  - リソースは分離できますか？
    - 「はい」の場合は、影響を受けるリソースの分離に進みます。
    - いいえの場合は、システム所有者とマネージャーと協力して、問題を抑えるために必要な追加のアクションを決定します。
  - 影響を受ける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？
    - 「はい」の場合は、次のステップに進みます。
    - いいえの場合、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、イベントがそれ以上エスカレートしないようにします。
- 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？
    - 「はい」の場合は、次のステップに進みます。
    - そうでない場合は、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。

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、環境全体に統一された修復を適用することが重要です。

段階的なアプローチを使用して根絶と復旧を行い、修復ステップに優先順位を付けることがベストプラクティスです。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維持する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 CIRT、お客様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フォレンジックの要件はありますか？

復旧

AWS セキュリティインシデント対応は、システムを通常の運用に復元し、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 セキュリティインシデント対応は、システムの復旧に直接役立ちません。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くらいですか？
- 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 セキュリティインシデント対応は、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 セキュリティインシデント対応サービスは、各顧客の主要連絡先に毎月のレポートを E メールで送信します。レポートは、以下で説明するメトリクスを使用して PDF 形式で配信されます。顧客は ごとに 1 つのレポートを受け取ります AWS Organizations。

ケースメトリクス

- 作成されたケース

  - ディメンション名: Type
  - ディメンション値: AWS サポート、自己サポート
  - 単位: 数
  - 説明: 作成されたケースの数。
- ケースのクローズ
  - ディメンション名: Type
  - 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総数の尺度。
- オープンケース
  - ディメンション名: Type
  - ディメンション値: AWS サポート、自己サポート
  - 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

- 受信した結果
  - 単位: 数
  - 説明: トリアージに送信された結果の数。
- アーカイブされた結果
  - 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。
- 検出結果の手動調査
  - 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: 誤検出を引き起こし、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

Cases

AWS セキュリティインシデント対応では、 AWS サポートケースと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 サポートされているケースを作成する

AWS サポートされているケースは、 AWS セキュリティインシデント対応、、APIまたは から作成できます AWS Command Line Interface。 AWS がサポートするケースでは、 AWS カスタマーインシデント対応チーム () からサポートを受けることができますCIRT。

> **Note**
>
> AWS CIRT は 15 分以内にケースに応答します。応答時間は、 からの最初の応答用です AWS CIRT。この期間内に最初のリクエストに応答するために、あらゆる合理的な努力をします。この応答時間は、後続の応答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 Management Consoleにサインインします。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 https://console.aws.amazon.com/security-ir/。
2. ケースの作成を選択する
3. でケースを解決 AWSするを選択する
4. リクエストのタイプを選択する
   a. アクティブ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。
   b. 調査: 調査により、 が AWS CIRTログダイブとインシデント対応調査の二次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のサポートを受けることができます。
5. 開始日の見積もりを、インシデントの最も早い指標の日付に設定します。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する
7. ケースの詳細な説明を入力します。 インシデント対応者がケースを解決するのに役立つ以下の点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か？

d. 既知の影響は何ですか？

e. この場合の緊急性は何ですか？

f. ケースの範囲内にある 1 つ以上の AWS アカウント IDs を追加します。

8. オプションのケースの詳細を追加します。

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. 通知を受け取るケースに、オプションのインシデント対応者を追加します。個人を追加するには、次の操作を行います。

a. E メールアドレスを追加します。

b. オプションの姓名を追加します。

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.ケースにオプションのタグを追加します。

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 サポートされているケースが作成されると、 AWS CIRTとインシデント対応チームにすぐに通知されます。

セルフマネージドケースを作成する

セキュリティ AWS インシデント対応、、APIまたは からセルフマネージド を作成できます AWS Command Line Interface。このタイプのケースは をDOESNOTエンゲージします AWS CIRT。次の例では、 コンソールの使用について説明します。

1. AWS Management Consoleにサインインします。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 https://console.aws.amazon.com/security-ir/。
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指標の日付に設定します。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。タイトルの生成オプションを選択するときは、提案されたように、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 を入力します AWS アカウント IDs。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、アカウントの追加を選択します。
   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入力します。
   a. インシデント対応者がケースを解決するのに役立つ以下の点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か？
      iv. 既知の影響は何ですか？
      v. この場合の緊急性は何ですか？
8. オプションのケースの詳細を追加します。
   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. 通知を受け取るケースに、オプションのインシデント対応者を追加します。個人を追加するには、次の操作を行います。
   a. E メールアドレスを追加します。
   b. オプションの姓名を追加します。
   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. ケースにオプションのタグを追加します。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 生成されたケースへの対応

AWS セキュリティインシデント対応は、アカウントまたはリソースに影響を与える可能性のある対応や認識が必要な場合に、アウトバウンド通知またはケースを作成することがあります。これは、サブスクリプションの一部として有効なプロアクティブレスポンスとアラートの優先順位付けワークフローを有効にした場合にのみ発生します。

これらの通知は Support センターに表示されます。 Support ユーザーガイドには、これらのケースを更新、解決、再開するための情報と詳細な手順が記載されています。

ケースの管理

内容

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ります。

- 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、リクエストされた 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、インシデント対応者がケースの処理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、分析の実行によるデータ駆動型の結論の作成が含まれます。
- 封じ込め、根絶、復旧: このステータスでは、インシデント対応者は、削除のため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。インシデント応答者は、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 インシデント対応者は、影響を受けるアカウント内の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 (複数可) ことに同意を求めます。
- インシデント後のアクティビティ: 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含まれています。現在の焦点は、事業運営を回復し、通常に戻すことです。ケースのリゾルバーがAWSをサポートしている場合は、概要と根本原因の分析が提供されます。
- Closed: 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ケースのステータスを変更します。サポート AWS されるケースでは、ステータスはレスポンダーによって AWS CIRT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がサポートをリクエストできます AWS。このケースのリゾルバーを に変更するには、「Get help from AWS」を選択します AWS。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。既存のケース履歴が利用可能になります AWS CIRT。にヘルプをリクエストすると AWS 、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

ケースに取り組んでいる AWS CIRT応答者は、内部チームにアクションをリクエストできます。

ケースの作成後に表示されるアクション項目は次のとおりです。

- インシデント応答者がケースにアクセスするためのアクセス許可を提供するリクエスト
- ケースに関する詳細情報の提供をリクエストする

顧客アクションが保留中のアクション項目：

- ケースを続行する新しいコメントに対するアクションをリクエストする

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：

- ケースレポートのレビューをリクエストする
- ケースのクローズをリクエストする

ケースを編集する

編集 を選択してケースの詳細を変更します。

AWS 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、次のケースの詳細を変更できます。

- タイトル
- 説明

AWS サポートされているケースのみ：

追加のフィールドは変更できます。

- リクエストタイプ：
  - アクティブ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、 が AWS CIRTログダイブとインシデント対応調査の二次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のサポートを受けることができます。
- 開始日の見積もり: 最初に提供された開始日より前のこのケースのインジケータを受け取った場合は、このフィールドを変更します。説明フィールドに新しく検出されたインジケータ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 CIRT は、ケースを処理するときに、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 CIRT応答者がケースに同時に対応できます。これらは通信ログ内で AWS Responder 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 人の利害関係者を含めることができます。これらの利害関係者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

でケースへのアクセスを提供するには AWS Management Console、アクセスIAM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。

ユーザーまたはロールへのIAMポリシーの追加：

1. アクセスIAM許可ポリシーをコピーします。
2. 経由で IAMで を開きますhttps://console.aws.amazon.com/iam/。
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 セキュリティインシデント対応管理ポリシーを選択します。
8. [Add policy] を選択します。

添付ファイル

インシデント対応者は、セルフマネージドケースの調査で他のインシデント対応者を支援する添付ファイルをケースに追加できます。

> **Note**
>
> AWS 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 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

のコミュニケーションテクノロジーを使用して画面共有を提供する方法で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 になってから 7 日後に削除されますClosed。

[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。

ケースのクローズ

AWS 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「ケースを閉じる」を選択し、任意のステータスでケースを完全にクローズします。ケースは通常、完全にクローズする前に「クローズ準備完了」のステータスに達します。Ready to Close 以外のステータスでケースを途中でクローズした場合、 はこの AWS CIRT AWS サポートされているケースの処理を停止するようリクエストしています。

インシデント対応チームが応答者である場合は、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**
>
> 「Ready to Close」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。

ケースを完全に閉じ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です。誤って閉鎖されないようにするため、ケースを閉鎖することを確認するよう求められます。

AWS CloudFormation スタックセットの使用

> **Important**
>
> AWS Security Incident Response はデフォルトでは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、まず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、 をデプロイすることで、アカウントごとに個別に作成することも AWS CloudFormation StackSets、組織全体で作成することもできます。これにより、必要なロールが作成されます。

サービスマネージド型のアクセス許可を持つスタックセットを作成する具体的な手順を確認できます。

以下は、 ロールAWSSecurityIncidentResponseContainmentとAWSSecurityIncidentResponseContainmentExecutionロールを作成するためのテンプレートスタックセットです。

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for AWS Security Incident Response 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 アクセス CancelMembership 許可を持つロールはAPI、 コンソール、、または からメンバーシップをキャンセルできます AWS Command Line Interface。

> **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。キャンセルは請求サイクルの最後に行われます。その月にキャンセルすると、メンバーシップは月末まで利用可能になります。請求サイクルの最後にメンバーシップが最終的にキャンセルされた時点で`ready to close`終了する`Active`、または終了する予定のリソースまたは調査。

> **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で存続してい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 セキュリティインシデント対応リソースのタグ付け

タグは、ユーザーが割り当てるか、 AWS リソース AWS 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 リソースを特定して整理します。多くの はタグ付け AWS のサービス をサポートしているため、異なるサービスのリソースに同じタグを割り当てて、リソースが関連していることを示すことができます。
- AWS コストを追跡します。ダッシュボードで AWS Billing これらのタグをアクティブ化します。はタグ AWS 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配信します。詳細については、AWS 「 請求ユーザーガイド」の「コスト配分タグを使用する」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の制御」を参照してください。

AWS タグ付けについては、「セキュリティインシデント対応APIリファレンス」を参照してください。

AWS CloudShell を使用して AWS セキュリティインシデント対応を操作する

AWS CloudShell はブラウザベースの事前認証済みシェルで、 から直接起動できます AWS Management Console。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 セキュリティインシデント対応を含む) 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 CloudShell から を起動 AWS Management Consoleすると、コンソールへのサインインに使用した AWS 認証情報が、新しいシェルセッションで自動的に利用可能になります。 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) を使用してセキュリティインシデント対応などの 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

- のIAMアクセス許可の取得 AWS CloudShell
- を使用したセキュリティインシデント対応の操作 AWS CloudShell

のIAMアクセス許可の取得 AWS CloudShell

によって提供されるアクセス管理リソースを使用して AWS Identity and Access Management、管理者は環境の機能にアクセスして AWS CloudShell 使用できるように、IAMユーザーにアクセス許可を付与できます。

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 管理ポリシーを使用することです。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。の次の AWS 管理ポリシーを ID IAM にアタッチ CloudShell できます。

- `AWSCloudShellFullAccess`: すべての機能へのフルアクセス AWS CloudShell で を使用するアクセス許可を付与します。

IAM ユーザーが実行できるアクションの範囲を制限する場合は AWS CloudShell、`AWSCloudShellFullAccess`管理ポリシーをテンプレートとして使用するカスタムポリシーを作成できます。でユーザーが使用できるアクションの制限の詳細については CloudShell、「 AWS CloudShell ユーザーガイド」の「 IAMポリシーによる AWS CloudShell アクセスと使用状況の管理」を参照してください。

> **Note**
>
> IAM ID には、Security Incident Response を呼び出すアクセス許可を付与するポリシーも必要です。

を使用したセキュリティインシデント対応の操作 AWS CloudShell

AWS CloudShell から を起動すると AWS Management Console、コマンドラインインターフェイスを使用してセキュリティインシデント対応の操作をすぐに開始できます。

> **Note**
>
> AWS CLI で を使用する場合 AWS CloudShell、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 とセキュリティインシデント対応の使用

- から AWS Management Console、ナビゲーションバーで使用できる次のオプション CloudShell を選択して を起動できます。
  - CloudShell アイコンを選択します。
  - 検索ボックスに「cloudshell」と入力し始め、オプションを選択します CloudShell。

を使用した AWS セキュリティインシデント対応API呼び出しのログ記録 AWS CloudTrail

AWS Security Incident Response は、ユーザー AWS CloudTrail、ロール、または Security Incident Response の AWS サービスによって実行されたアクションを記録するサービスである と統合されています。 は、Security Incident Response のすべてのAPI呼び出しをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、セキュリティインシデント対応コンソールからの呼び出しと、セキュリティインシデント対応APIオペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、セキュリティインシデント対応の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配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。によって収集された情報を使用して CloudTrail、セキュリティインシデント対応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。

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

のセキュリティインシデント対応情報 CloudTrail

CloudTrail アカウントを作成する AWS アカウント と、 は 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 CloudTrail イベント履歴の他の AWS サービスイベントとともにイベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、「イベント履歴を使用した CloudTrail イベントの表示」を参照してください。

AWS アカウント 過去 90 日間のイベントの継続的な記録については、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。を使用して作成された証跡はすべてマルチリージョン AWS Management Console 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 AWS リージョン 内のすべての でアクティビティをキャプチャするため、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 CloudTrail することで、 から Amazon S3 バケットに継続的な管理イベントのコピーを 1 つ無料で配信できますが、Amazon S3 ストレージ料金が発生します。 CloudTrail 料金の詳細については、AWS CloudTrail 「 料金表」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 では、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、既存のイベントを行ベースのJSON形式で Apache ORC 形式に変換します。 ORC は、データをすばやく取得できるように最適化された列指向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、「 ユーザーガイド」の AWS CloudTrail 「Lake の使用」を参照してください。 AWS CloudTrail

CloudTrail Lake イベントデータストアとクエリにはコストが発生します。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 料金の詳細については、AWS CloudTrail 「 の料金」を参照してください。

すべてのセキュリティインシデント対応アクションは によってログに記録 CloudTrail され、AWS 「セキュリティインシデント対応APIリファレンス」に記載されています。たとえば、、、`UpdateCase`アクションを呼び出す`CreateCase`と`CreateMembership`、 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 root または AWS Identity and Access Management （ IAM) ユーザー認証情報を使用して行われたかどうか。
- 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要素を参照してください。

セキュリティインシデント対応ログファイルエントリについて

証跡は、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できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、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に関する情報が含まれます。 CloudTrail ログファイルはパブリックAPIコール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ています。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA00000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA00000000000000000",
                "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"
}
```

を使用した AWS セキュリティインシデント対応アカウントの管理 AWS Organizations

AWS セキュリティインシデント対応は と統合されています AWS Organizations。組織の AWS Organizations 管理アカウントは、アカウントを AWS セキュリティインシデント対応の委任管理者として指定できます。このアクションにより、信頼されたサービスとして AWS Security Incident Response が有効になります AWS Organizations。これらのアクセス許可の付与方法については、「 を他の AWS サービス AWS Organizations で使用する」を参照してください。

以下のセクションでは、委任セキュリティインシデント対応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

で AWS セキュリティインシデント対応を使用する際の考慮事項と推奨事項 AWS Organizations

以下の考慮事項と推奨事項は、委任されたセキュリティインシデント対応管理者アカウントが AWS セキュリティインシデント対応でどのように動作するかを理解するのに役立ちます。

委任されたセキュリティインシデント対応管理者アカウントはリージョン別です。

> 委任されたセキュリティインシデント対応管理者アカウントとメンバーアカウントは、 を通じて追加する必要があります AWS Organizations。

AWS セキュリティインシデント対応の委任された管理者アカウント。

> 1 つのメンバーアカウントを委任セキュリティインシデント対応管理者アカウントとして指定できます。例えば、 *111122223333*でメンバーアカウントを指定した場合*Europe (Ireland)*、*555555555555*で別のメンバーアカウントを指定することはできません*Canada (Central)*。

他のすべてのリージョンで、委任されたセキュリティインシデント対応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。

組織の管理を委任されたセキュリティインシデント対応管理者アカウントとして設定することはお勧めしません。

組織の管理は、委任されたセキュリティインシデント対応管理者アカウントとすることができます。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されたセキュリティインシデント対応管理者アカウントを削除すると、サブスクリプションが直ちにキャンセルされます。

委任されたセキュリティインシデント対応管理者アカウントを削除すると、 AWS セキュリティインシデント対応は、この委任されたセキュリティインシデント対応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 セキュリティインシデント対応は、これらのすべてのメンバーアカウントで有効になるわけではありません。

の信頼されたアクセスの有効化 AWS Account Management

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、 の各メンバーアカウントに固有の情報とメタデータ (プライマリまたは代替の連絡先の詳細など) を変更できます AWS Organizations。

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、次の手順に従います。

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 (非推奨) としてサインインする必要があります。
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 セキュリティインシデント対応を選択します。
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 セキュリティインシデント対応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、「有効化して確認します」と入力し、「信頼されたアクセスを有効にする」を選択します。

API/CLI

の信頼されたアクセスを有効にするには AWS Account Management

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

- AWS CLI: enable-aws-service-access

  次の例では、呼び出し元のアカウントの組織で AWS Security Incident Response の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。

委任されたセキュリティインシデント対応管理者アカウントを指定するために必要なアクセス許可

委任された管理者を使用して AWS 、セキュリティインシデント対応メンバーシップをセットアップすることを選択できます AWS Organizations。これらのアクセス許可の付与方法については、「 AWS Organizations を他の AWS サービスで使用する」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と管理を行うときに、 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 を信頼することで、手動で有効にする必要がありますsecurity-ir.amazonaws.com。

AWS Organizations マネージャーとして、組織の委任されたセキュリティインシデント対応管理者アカウントを指定する前に、次の AWS セキュリティインシデント対応アクションを実行できることを確認します: `sir:CreateMembership`および `sir:UpdateMembership`。これらのアクションにより、セキュリティインシデント対応を使用して、組織の委任された AWS セキュリティインシデント対応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 アクションを実行できることを確認する必要があります。

これらのアクセス許可を付与するには、アカウントの AWS Identity and Access Management （ IAM) ポリシーに次のステートメントを含めます。

```
{
    "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 管理を委任されたセキュリティインシデント対応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アクションも必要ですCreateServiceLinkedRole。このアクションにより、管理用の AWS セキュリティインシデント対応を初期化できます。ただし、許可の追加に進む前に、「で AWS セキュリティインシデント対応を使用する際の考慮事項と推奨事項 AWS Organizations」を確認してください。

管理を委任されたセキュリティインシデント対応管理者アカウントとして指定し続けるには、次のステートメントをIAMポリシーに追加し、 を組織の管理の AWS アカウント ID *111122223333*に置き換えます。

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

AWS セキュリティインシデント対応の委任管理者の指定

このセクションでは、 AWS セキュリティインシデント対応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、委任されたセキュリティインシデント対応管理者アカウントの運用方法考慮事項とレコメンデーションに関する を必ずお読みください。続行する前に、委任されたセキュリティインシデント対応管理者アカウントを指定するため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、組織の委任セキュリティインシデント対応管理者アカウントを指定します。このステップを実行できるのは管理のみです。

Console

1. 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。 https://console.aws.amazon.com/security-ir/

   サインインするには、 AWS Organizations 組織の管理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、組織の委任セキュリティインシデント対応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

- 組織の管理の AWS アカウント の認証情報 CreateMembership を使用して を実行します。
  - または、 AWS Command Line Interface を使用してこれを行うことができます。次の AWS CLI コマンドは、委任されたセキュリティインシデント対応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次のとおりです。

```
{
  "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 AWS されたセキュリティインシデント対応管理者アカウントでセキュリティインシデント対応が有効になっていない場合、何も実行できません。まだ有効にしていない場合は、新しく指定された委任 AWS されたセキュリティインシデント対応管理者アカウントでセキュリティインシデント対応を有効にしてください。

AWS セキュリティインシデント対応へのメンバーの追加

AWS Organizations と AWS セキュリティインシデント対応メンバーシップには 1 対 1 の関係があります。Organizations からアカウントが追加 (または削除) されると、これは AWS セキュリティインシデント対応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、 を使用して組織内のアカウントを管理する AWS Organizationsオプションのいずれかに従います。

AWS セキュリティインシデント対応からメンバーを削除する

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手順に従います。

トラブルシューティング

AWS セキュリティインシデント対応に固有のアクションの実行に関連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、一部またはすべてのオペレーションで障害を示すオペレーションのステータスです。または、問題が発生してもタスクは完了すると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ていない。

AWS Security Incident Response 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APIsされる必要があります。組織の AWS セキュリティインシデント対応の委任された管理者またはメンバーシップアカウント AWS アカウント である の正しいIAMプリンシパルから運用し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 セキュリティインシデント対応の委任された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 「セキュリティインシデント対応IAM」を参照してください。

ConflictException

リクエストにより、整合性のない状態が発生します。

指定したケースアタッチメント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設定

されていないことを確認します。で https://console.aws.amazon.com/security-ir/セキュリティインシデント対応コンソールを開き、 に移動しますMembership Details。

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。数分後にもう一度試してください。問題が解決しない場合は、 にケースを提出してください Support。

ResourceNotFoundException

リクエストは、存在しないリソースを参照します。

リクエストで指定された 1 つ以上のリソースが存在しません。指定されたリソースARNsまたは がすべてIDs正しいことを確認してください。これは AWS Organizations IDs、アカウント IDs、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、ケースアタッチメント、ケースコメントに適用されます。

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。

指定した期間にプリンIAM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、もう一度試してください。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 で指定された制約を満たしていません AWS のサービス。

リクエスト内の 1 つ以上のデータフィールドが検証要件や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ARNsが完了し、AWS 「 セキュリティインシデント対応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ます。例えば、ケースを AWS サポートされている からセルフマネージドに変更することはできません。

Support

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目的で Support センターにお問い合わせください。次の情報を入手できます。

- AWS リージョン 使用した

- 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 セキュリティインシデント対応におけるデータ保護

内容

責任 AWS 共有モデルは、セキュリティインシデント対応サービスのデータ保護 AWS に適用されます。 https://aws.amazon.com/compliance/shared-responsibility-model/このモデルで説明されているように、 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があります。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 サービスのセキュリティ設定および管理タスクについても責任を負います。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FAQ」を参照してください。欧州におけるデータ保護の詳細については、 AWS セキュリティブログの AWS 責任共有モデルとGDPRブログ投稿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、アカウント認証情報を保護し AWS 、Identity Center または AWS Identity and Access Management () を使用して AWS IAM個々のユーザーを設定する必要がありますIAM。これにより、各ユーザーには職務を果たすために必要なアクセス許可のみが付与されます。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。1TLS.2 が必要で、1.3 TLS をお勧めします。
- API とユーザーアクティビティのログ記録をセットアップします AWS CloudTrail。
- AWS 暗号化ソリューションと、 AWS サービス内のすべてのデフォルトのセキュリティコントロールを使用します。
- FIPS 140-3 は現在、 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機密情報や機密情報をタグや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入れないでください。これは、コンソール、、または を使用して AWS サポートまたは他の AWS サービスを使用する場合も同様ですAPI AWS CLI AWS SDKs。名前に使用されるタグまたは自由形式のテキストフィールドに入力したデータは、請求ログまたは診断ログに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を 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

AWS Security Incident Response によって収集およびアクセスされるデータは、Transport Layer Security (TLS) で保護されたチャネルを経由する場合のみです。

キー管理

AWS Security Incident Response は、 との統合を実装 AWS KMS して、ケースデータとアタッチメントデータの保管時の暗号化を提供します。

AWS セキュリティインシデント対応は、カスタマーマネージドキーをサポートしていません。

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 の間には 2 つの接続オプションがあります AWS。

- 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。
- AWS Direct Connect 接続。詳細については、「AWS Direct Connect ユーザーガイド」の「AWS Direct Connectとは」を参照してください。

ネットワーク経由で AWS のセキュリティインシデント対応へのアクセスは、 AWS 公開された を通じて行われますAPIs。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。1.3 TLS をお勧めします。クライアントは、エフェメラル Diffie-Hellman (PFS) や楕円曲線 Diffie-Hellman Ephemeral () など、Perfect Forward Secrecy (DHE) を使用する暗号スイートもサポートする必要がありますECDHE。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、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 セキュリティインシデント対応用の Amazon Virtual Private Cloud (Amazon VPC) エンドポイントは、 AWS セキュリティインシデント対応への接続のみVPCを許可する 内の論理エンティティです。Amazon は、リクエストを AWS セキュリティインシデント対応にVPCルーティングし、レスポンスを にルーティングしますVPC。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を制御するため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 へのアクセスを制御する」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 経由でアクセスすることはできません AWS Direct Connect。

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 サービスです。 IAM管理者は、 AWS Security Incident Response リソースを使用するための認証された (サインインした) プリンシパルと認可された (アクセス許可を持つ) プリンシパルを制御します。 IAMは、追加料金なしで使用できる AWS サービスです。

内容

- アイデンティティを使用した認証
- AWS セキュリティインシデント対応と の連携方法 IAM

対象者

AWS Identity and Access Management （ IAM) の使用方法は、 AWS セキュリティインシデント対応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管理ポリシーを使用して、メンバーシップおよびケースリソースへの読み取りおよび書き込みアクセス権があ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

これらの個人には、すべてのケースに対する権限があるわけではなく、明示的なアクセス許可を付与する個々のケースに対する権限があります。

インシデント対応チームメンバー

チームのメンバーには、メンバーシップとケースの両方へのフルアクセスを付与できます。すべての個人がサービスメンバーシップに対して権限のあるアクションを持つのではなく、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 「セキュリティインシデント対応管理ポリシー」を参照してください。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。 AWS アカウントのルートユーザーとして、 IAM ユーザーとして、または IAMロールを引き受けることで、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAMIdentity Center (IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーテッドアイデンティティ としてサインインする場合、管理者は以前に IAM ロールを使用して ID フェデレーションを設定しています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーの種類に応じて、 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。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 AWS 「アカウントにサインインする方法」を参照してください。AWS

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS 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。推奨される方法を使用してリクエストに署名する方法の詳細については、「 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。

使用する認証方法にかかわらず、追加のセキュリティ情報の提供が必要になる場合があります。たとえば、 では、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 AWS 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」およびIAM「 ユーザーガイド」の「 での多要素認証 (MFA) の使用 AWS」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ときは、アカウント内のすべての AWS サービスとリソースへの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 ID は AWS accountroot ユーザーと呼ばれ、アカウントの作成に使用した 8 つのアドレスとパスワードでサインインすることでアクセスできます。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の実行にのみ使用します。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む人間のユーザーに、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を使用して AWS サービスにアクセスすることを要求することをお勧めします。

フェデレーティッドアイデンティティは、エンタープライズユーザーディレクトリ、ウェブアイデンティティプロバイダー、 AWS Directory Service、Identity Center ディレクトリ、または ID ソースを通じて提供された認証情報を使用して AWS 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アイデンティティがアカウントにアクセスする AWS と、ロールを引き受け、ロールは一時的な認証情報を提供します。

一元的なアクセス管理を行うには、 IAM Identity Center を使用する AWS 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ことも、すべての AWS アカウントとアプリケーションで使用できるように、独自の ID ソース内のユーザーとグループのセットに接続して同期することもできます。Identity Center の詳細については、IAMIAM「 Identity Center ユーザーガイド」の「Identity Center とは」を参照してください。AWS IAM

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたはアプリケーションに対して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。パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧めします。IAM ユーザーとの長期的な認証情報を必要とする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ユーザーのコレクション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容易になります。例えば、 という名前のグループを作成しIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

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 (ロールではなく) IAM ユーザーを作成するタイミングを参照してください。

IAM の 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。IAM ロールを切り替え

ることで、 AWS マネジメントコンソールで ロールを一時的に引き受けることができます。https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.htmlロールを引き受けるには、 または AWS APIオペレーションを AWS CLI呼び出すか、カスタム を使用しますURL。ロールの使用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 ロールと一時認証情報は、次の状況で役立ちます。

- フェデレーティッドユーザーアクセス – フェデレーティッドアイデンティティにアクセス許可を割り当てるには、ロールを作成し、そのロールのアクセス許可を定義します。フェデレーティッド 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ロールの詳細については、「 IAMユーザーガイド」の「サードパーティー ID プロバイダーのロールの作成」を参照してください。 IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス許可セットを のロールに関連付けますIAM。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「アクセス許可セット」を参照してください。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に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、別のアカウントのユーザー (信頼されたプリンシパル) がアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の AWS 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) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスの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「 でのクロスアカウントリソースアクセスIAM」を参照してください。
- クロスサービスアクセス — 一部の AWS サービスは、他の AWS 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と、そのサービスが Amazon でアプリケーションを実行EC2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 - サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける 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 – サービスにリンクされたロールは、 サービスにリンクされた AWS サービスロールの一種です。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは AWS アカウントに表示さ

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。

- Amazon で実行されているアプリケーション EC2– IAMロールを使用して、EC2インスタンスで実行され、 または AWS API リクエストを行う AWS CLIアプリケーションの一時的な認証情報を管理できます。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、インスタンスにアタッチ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認証情報を取得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ロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与する」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「いつ (ユーザーではなく) IAMロールを作成するか」を参照してください。

AWS セキュリティインシデント対応と の連携方法 IAM

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制御するのに役立つ AWS サービスです。 IAM管理者は、誰を認証 (サインイン) し、誰に Security Incident Response リソースの使用 AWS を承認する (アクセス許可を付与する) かを制御します。IAMは、追加料金なしで使用できる AWS サービスです。

IAM AWS Security Incident Response で使用できる の機能	
IAM 機能	サービスの調整
アイデンティティベースポリシー	はい
リソースベースのポリシー	いいえ
ポリシーアクション	はい
ポリシーリソース	あり
ポリシー条件キー	はい (グローバル)
ACLs	いいえ
ABAC (ポリシー内のタグ)	あり

IAM AWS Security Incident Response で使用できる の機能	
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	いいえ
サービスリンクロール	あり

内容

AWS セキュリティインシデント対応のため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、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アクセス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 の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、またアクションが許可または拒否され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は、「 IAMユーザーガイド」の「 IAMJSON ポリシー要素リファレンス」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

デフォルトでは、ユーザーとロールには、 AWS セキュリティインシデント対応リソースを作成または変更するアクセス許可はありません。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 を使用してタスクを実行することはできません AWS API。IAM 管理者は、必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するIAMポリシーを作成できます。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。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSON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。

各リソースタイプの の形式など、セキュリティインシデント対応で AWS 定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」のARNs AWS 「セキュリティインシデント対応のアクション、リソース、および条件キー」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では、 AWS アカウントのコスト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 管理ポリシーを開始し、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にアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理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、アクセス許可をさらに減らす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「AWS ジョブ機能の管理ポリシー」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アクセス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 を使用してアクセス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 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 を使用して送信するように指定できますSSL。条件を使用して、サービスアクションが などの特定の AWS サービスを介して使用される場合に、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 AWS CloudFormation。詳細については、「 IAMユーザーガイド」のIAMJSON「ポリシー要素: 条件」を参照してください。

IAM Access Analyzer を使用してIAMポリシーを検証し、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。 IAMAccess Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。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。

多要素認証を要求する (MFA) – AWS アカウントでIAMユーザーまたはルートユーザーを必要とするシナリオがある場合は、セキュリティを強化MFAするために をオンにします。API オペレーションが呼び出されるMFAタイミングを要求するには、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「 で保護された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 セキュリティインシデント対応コンソールの使用

アクセスするには https://console.aws.amazon.com/security-ir/、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 AWS アカウント内の AWS セキュリティインシデント対応リソースの詳細を一覧表示および表示できます。最小限必要な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) に対してコンソールが意図したとおりに機能しません。

または のみを AWS CLI呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません AWS API。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 セキュリティインシデント対応アクセスまたは ReadOnly AWS 管理ポリシーをアタッチして、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 ID にアタッチされたインラインおよび管理ポリシーの表示を IAM ユーザーに許可するポリシーを作成する方法を示します。このポリシーには、 コンソールで、または または を使用して AWS CLIプログラムでこのアクションを実行するアクセス許可が含まれています AWS API。

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "ViewOwnUserInfo",
"Effect": "Allow",
"Action": [
"iam:GetUserPolicy",
"iam:ListGroupsForUser",
"iam:ListAttachedUserPolicies",
"iam:ListUserPolicies",
"iam:GetUser"
],
"Resource": ["arn:AWS:iam::*:user/${AWS:username}"]
},
{
"Sid": "NavigateInConsole",
"Effect": "Allow",
"Action": [
"iam:GetGroupPolicy",
"iam:GetPolicyVersion",
"iam:GetPolicy",
"iam:ListAttachedGroupPolicies",
"iam:ListGroupPolicies",
"iam:ListPolicyVersions",
"iam:ListPolicies",
"iam:ListUsers"
],
"Resource": "*"
}
]
}
```

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、リソースにアタッチするJSONポリシードキュメントです。リソースベースポリシーの例としては、IAMロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。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「 でのクロスアカウントリソースアクセスIAM」を参照してください。

AWS セキュリティインシデント対応のポリシーアクション

サポートポリシーアクション: はい

管理者はポリシーを使用して AWS JSON、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。

JSON ポリシーのアクション要素は、ポリシーで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を記述します。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オペレーションがないアクセス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 セキュリティインシデント対応アクションのリストを確認するには、「サービス認可リファレンス」の AWS 「セキュリティインシデント対応で定義されるアクション」を参照してください。

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

AWS セキュリティインシデント対応 - ID

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。

「アクション」: [AWS 「セキュリティインシデント対応 -identity:action1」、AWS 「セキュリティインシデント対応 -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： はい 管理者はポリシーを使用して AWS JSON、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。

リソース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 要素を含める必要があります。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": "*"

セキュリティインシデント対応の AWS ポリシー条件キー

サービス固有のポリシー条件キーをサポート： なし

管理者はポリシーを使用して AWS JSON、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。

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になる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。

ステートメントで複数の Condition 要素を指定するか、単一の Condition 要素で複数のキーを指定すると、 は論理ANDオペレーションを使用してそれら AWS を評価します。1 つの条件キーに複数の値を指定すると、 は論理 OR オペレーションを使用して条件 AWS 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。たとえば、IAM ユーザー名でタグ付けされている場合のみ、リソースにアクセスする IAM ユーザーアクセス許可を付与できます。詳細については、IAMユーザーガイドの「 IAMポリシーエレメント: 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 セキュリティインシデント対応のアクセスコントロールリスト (ACLs)

をサポートACLs： なし

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。 ACLsは、ポリシードキュメント形式を使用しませんが、リソースベースのJSONポリシーと似ています。

AWS Security Incident Response による属性ベースのアクセスコントロール (ABAC)

サポート ABAC (ポリシー内のタグ): はい

属性ベースのアクセスコントロール (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。では AWS、これらの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、 の最初のステップですABAC。次に、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する場合に、オペレーションを許可するABACポリシーを設計します。ABAC は、急速に成長している環境で役立ち、ポリシー管理が面倒な状況に役立ちます。

タグに基づいてアクセスを制御するには、 : ResourceTag/key-name、 AWS : AWS RequestTag/key-name、または AWS : TagKeys condition キーを使用して、ポリシーの条件要素にタグ情報を指定します。サービスがすべてのリソースタイプで 3 つの条件キーをすべてサポートしている場合、その値はサービスではいです。サービスが一部のリソースタイプでのみ 3 つの条件キーをすべてサポートしている場合、値は部分的です。 の詳細についてはABAC、「 IAMユーザーガイド」の「 ABACとは」を参照してください。をセットアップする手順を含むチュートリアルを表示するにはABAC、「 ユーザーガイド」の「属性ベースの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。 IAM

Amazon AWS Security Incident Response による一時的な認証情報

一時的な認証情報のサポート: あり

AWS 一時的な認証情報を使用してサインインすると、 サービスは機能しません。一時的な認証情報を使用する AWS サービスなどの詳細については、「 IAMユーザーガイド」のAWS 「 と連携するサービスIAM」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、一時的な認証情報を使用しています。たとえば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。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、 CLIまたは AWS を使用して手動で作成できます AWS API。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。 AWS では、長期的なアクセスキーを使用する代わりに、一時的な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、「」の「一時的なセキュリティ認証情報IAM」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をサポート (FAS): はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用すると、別のサービスで別のアクションを開始するアクションを実行できます。 FASは、 AWS サービスを呼び出すプリンシパルのアクセス許可を、リクエスト元の AWS サービスと組み合わせて使用してダウンストリームサービスにリクエストを行います。 FAS リクエストは、他の AWS サービスまたはリソースとのやり取りを必要とするリクエストをサービスが受信した場合にのみ行われます。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 セキュリティインシデント対応のアイデンティティとアクセスのトラブルシューティング

次の情報は、セキュリティインシデント対応と の使用 AWS 時に発生する可能性がある一般的な問題の診断と修正に役立ちますIAM。

トピック

- アクションの実行を承認されていない
- iam を実行する権限がありません。PassRole
- AWS アカウント以外のユーザーに AWS Security Incident Response リソースへのアクセスを許可したい

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。

次の例のエラーは、mateojackson IAMユーザーが コンソールを使用して架空の my-example-widget リソースの詳細を表示しようとしているが、架 AWS 空の Security Incident Response :GetWidget permissions がない場合に発生します。

ユーザー: arn:AWS:iam::123456789012:user/mateojackson は、以下を実行する権限がありません：AWS セキュリティインシデント対応 :GetWidgeton resource: my-example-widget

この場合、mateojackson ユーザーのポリシーを更新して、 AWS セキュリティインシデント対応 :GetWidget action を使用してリソースへのアクセス my-example-widgetを許可する必要があります。

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

iam を実行する権限がありません：PassRole iam:PassRole action 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 にロールを渡すことができ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にリンクされたロールを作成する代わりに、既存のロールをその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権限が必要です。

次の例のエラーは、marymajor という名前の IAMユーザーがコンソールを使用して Security Incident Response で AWS 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権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

ユーザー: arn:AWS:iam::123456789012:user/marymajor には、次の操作を実行する権限がありません: iam:PassRole

この場合、Mary のポリシーを更新して iam:PassRole action を実行できるようにする必要があります。サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

AWS アカウント以外のユーザーに AWS Security Incident Response リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするため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 がこれらの機能をサポートしているかどうかを確認するには、 AWS 「セキュリティインシデント対応が と連携する方法」を参照してくださいIAM。
- 所有しているアカウント間で AWS リソースへの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「所有している別の AWS アカウントの IAM ユーザーへのアクセスを提供する」を参照してください。

- サードパーティー AWS アカウントに リソースへの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「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を提供する」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でのロールとリソースベースのポリシーの使用の違いについては、「 IAMユーザーガイド」の「 でのクロスアカウントリソースアクセスIAM」を参照してください。

サービスロールの使用

サービスロールをサポート： いいえ

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、削除できます。詳細については、「 IAMユーザーガイド」の「 AWS 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 のサービスにリンクされたロールでサポートされているリージョン

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、 サービスにリンクされた AWS サービスロールの一種です。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。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。

サービスにリンクされた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。 AWS Security Incident

Response は、サービスにリンクされたロールのアクセス許可を定義します。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。定義されるアクセス権限には、信頼ポリシーやアクセス権限ポリシーなどがあり、そのアクセス権限ポリシーをその他の 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の詳細については、AWS 「 と連携する のサービスIAM」を参照し、「サービスにリンクされたロール」列で「はい」があるサービスを探してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[Yes] (はい) リンクを選択します。

AWS SLR: AWSServiceRoleForSecurityIncidentResponse

AWS セキュリティインシデント対応は、 AWS という名前のサービスにリンクされたロール (SLR) AWSServiceRoleForSecurityIncidentResponse を使用して、サブスクライブされた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 サービスにリンクされたロールは、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`

このロールにアタッチされているのは、 AWSSecurityIncidentResponseServiceRolePolicyという名前の AWS 管理ポリシーです。このサービスは、 ロールを使用して、次のリソースでアクションを実行します。

- AWS Organizations： サービスで使用するためにメンバーシップアカウントを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ケースを作成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

サービスにリンクされたロールを手動で作成する必要はありません。 AWS Management Console、、 AWS CLIまたは の AWS Security Incident Response にオンボードすると AWS API、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、サービスにリンクされたロールを AWS Organizations 管理アカウントで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。

IAM エンティティ (ユーザー、グループ、ロールなど) がサービスにリンクされたロールを作成、編集、削除できるようにするには、アクセス権限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「サービスに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 セキュリティインシデント対応は、 AWS という AWSServiceRoleForSecurityIncidentResponse_Triage 名前のサービスにリンクされたロール (SLR) を使用して、セキュリティ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、潜在的なインシデントを調査するための情報を収集します。

アクセス許可

AWSServiceRoleForSecurityIncidentResponse_Triage サービスにリンクされたロールは、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、 AWS AWSSecurityIncidentResponseTriageServiceRolePolicyマネージドポリシーがアタッチされます。このサービスは、 ロールを使用して、次のリソースで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、 AWS アカウントから サービスにイベントを配信するために必要なインフラストラクチャです。このアクションは、 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triage.security-ir.amazonaws.com。
- 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できるようにします。このアクションは任意の AWS リソースで実行されます。

- AWS Security Hub： 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できるようにします。このアクションは任意の AWS リソースで実行されます。

ロールの管理

サービスにリンクされたロールを手動で作成する必要はありません。 AWS Management Console、、 AWS CLIまたは の AWS Security Incident Response にオンボードすると AWS API、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。

IAM エンティティ (ユーザー、グループ、ロールなど) がサービスにリンクされたロールを作成、編集、削除できるようにするには、アクセス権限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「サービスに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 のサービスにリンクされたロールでサポートされているリージョン

AWS Security Incident Response は、サービスが利用可能な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 (ストックホルム)
- アジアパシフィック (シンガポール)
- アジアパシフィック (ソウル)
- 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)

AWS 管理ポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールに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 管理ポリシーを使用する方が簡単です。必要なアクセス許可のみをチームに付与するように IAM カスタマー管理ポリシーを作成するには、時間と専門知識が必要です。すぐに開始するには、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としており、 AWS アカウントで利用できます。 AWS 管理ポリシーの詳細については、「 IAMユーザーガイド」の「 AWS 管理ポリシー」を参照してください。

AWS サービスは、関連する AWS 管理ポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。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 管理ポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が損なわれることはありません。

さらに、 は、複数の サービスにまたがる職務機能の マネージドポリシー AWS をサポートしています。たとえば、 ReadOnlyAccess AWS 管理ポリシーは、すべての AWS サービスとリソースへの読み取り専用アクセスを提供します。サービスが新機能を起動すると、 は新しいオペレーションとリソースに読み取り専用アクセス許可 AWS を追加します。職務機能ポリシーのリストと説明については、IAM「 ユーザーガイド」のAWS 「職務機能用の 管理ポリシー」を参照してください。

内容

AWS 管理ポリシー： AWSSecurityIncidentResponseServiceRolePolicy

AWS セキュリティインシデント対応では、 AWSSecurityIncidentResponseServiceRolePolicy AWS マネージドポリシーを使用します。この AWS 管理ポリシーは、AWSServiceRoleForSecurityIncidentResponseサービスにリンクされたロールにアタッチされます。このポリシーは、 AWS Security Incident Response がサブスクライブし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るためのアクセスを提供します。

> **Important**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに保存しないでください。AWS セキュリティインシデント対応では、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または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

このサービスは、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ためにメンバーシップアカウントを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ケースを作成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たアクセス許可は、 の AWSSecurityIncidentResponseServiceRolePolicy AWS 管理ポリシーで表示できます。

AWS 管理ポリシー： AWSSecurityIncidentResponseFullAccess

AWS セキュリティインシデント対応では、 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 へのアクセスを許可します AWS のサービス。このポリシーをIAMプリンシパルとともに使用して、 AWS セキュリティインシデント対応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) やその他の機密情報や機密情報をタグに保存しないでください。AWS セキュリティインシデント対応では、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または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

このサービスは、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： AWS サービスユーザーに Security Incident Response リソースの更新、変更、削除、および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たアクセス許可は、 の AWSSecurityIncidentResponseFullAccess AWS 管理ポリシーで表示できます。

AWS 管理ポリシー： AWSSecurityIncidentResponseReadOnlyAccess

AWS セキュリティインシデント対応では、 AWSSecurityIncidentResponseReadOnlyAccess AWS マネージドポリシーを使用します。このポリシーは、サービスケースリソースへの読み取り専用アクセスを許可します。このポリシーをIAMプリンシパルとともに使用して、 AWS セキュリティインシデント対応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) やその他の機密情報や機密情報をタグに保存しないでください。AWS セキュリティインシデント対応では、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または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

このサービスは、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たアクセス許可は、 の AWSSecurityIncidentResponseReadOnlyAccess AWS 管理ポリシーで表示できます。

AWS 管理ポリシー： AWSSecurityIncidentResponseCaseFullAccess

AWS セキュリティインシデント対応では、 AWSSecurityIncidentResponseCaseFullAccess AWS マネージドポリシーを使用します。このポリシーは、サービスケースリソースへのフルアクセスを許可します。このポリシーをIAMプリンシパルとともに使用して、 AWS セキュリティインシデント対応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) やその他の機密情報や機密情報をタグに保存しないでください。AWS セキュリティインシデント対応では、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または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

このサービスは、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 セキュリティインシデント対応ケースを更新、変更、削除、および作成する機能を付与します。

このポリシーに関連付けられたアクセス許可は、 の AWSSecurityIncidentResponseCaseFullAccess AWS 管理ポリシーで表示できます。

AWS 管理ポリシー： AWSSecurityIncidentResponseTriageServiceRolePolicy

AWS セキュリティインシデント対応では、 AWSSecurityIncidentResponseTriageServiceRolePolicy AWS マネージドポリシーを使用します。この AWS 管理ポリシーは、AWSServiceRoleForSecurityIncidentResponse_Triage サービスにリンクされたロールにアタッチされます。

このポリシーは、 AWS 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、潜在的なインシデントを調査するための情報を収集す

るためのセキュリティインシデント対応へのアクセスを提供します。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) やその他の機密情報や機密情報をタグに保存しないでください。AWS セキュリティインシデント対応では、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または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

このサービスは、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、 AWS アカウントから サービスにイベントを配信するために必要なインフラストラクチャです。このアクションは、 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triage.security-ir.amazonaws.com。
- 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できるようにします。このアクションは任意の AWS リソースで実行されます。
- AWS Security Hub： 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できるようにします。このアクションは任意の AWS リソースで実行されます。

このポリシーに関連付けられたアクセス許可は、 の AWSSecurityIncidentResponseTriageServiceRolePolicy AWS 管理ポリシーで表示できます。

AWS SLRsおよび マネージドポリシーに対するセキュリティインシデント対応の更新

このサービスがこれらの変更の追跡を開始した以降の、 AWS セキュリティインシデント対応SLRsと管理ポリシーのロールの更新に関する詳細を表示します。

変更	説明	日付
新規 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アタッチされたポリシー。	2024 年 12 月 1 日
新規 SLR – AWSServiceRoleForSecurityIncidentResponse_Triage 新しい マネージドポリシー – AWSSecurityIncidentResponseTriageServiceRolePolicy	新しいサービスリンクロールとアタッチされたポリシーにより、 AWS Organizations アカウントへのサービスアクセスが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なります。	2024 年 12 月 1 日
新しい 管理ポリシー – AWSSecurityIncidentResponseFullAccess	AWS セキュリティインシデント対応は、サービスの読み取りおよび書き込みアクションのためにIAMプリンシパルにSLRアタッチする新しい を追加します。	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 セキュリティインシデント対応は、読み取りアクションのためにIAMプリンシパルにアタッチSLRする新しい を追加します。	2024 年 12 月 1 日
新しい マネージドポリシーロール – AWSSecurityIncidentResponseCaseFullAccess	AWS セキュリティインシデント対応は、サービスケースの読み取りおよび書き込みアクションのためにIAMプリンシパルにアタッチSLRする新しい を追加します。	2024 年 12 月 1 日
変更の追跡を開始しました。	AWS セキュリティインシデント対応SLRsと 管理ポリシーの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は、 AWS とお客様の間の責任共有です。この共有モデルは、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まで、コンポーネントを AWS 運用、管理、制御する際のお客様の運用上の負担を軽減するのに役立ちます。お客様は、ゲストオペレーティングシステム (更新プログラムやセキュリティパッチを含む) 、その他の関連するアプリケーションソフトウェア、および AWS 提供されたセキュリティグループファイアウォールの設定について、責任と管理を引き受けます。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、インシデント対応と選択が企業の目標に与える影響をよりよく理解できるように、AWS 「セキュリティのベストプラクティス」ホワイトペーパーとAWS 「 クラウド導入フレームワークのセキュリティパースペクティブ (CAF) 」ホワイトペーパーを確認することをお勧めします。

コンプライアンス検証

サードパーティーの AWS 監査者は、複数の コンプライアンスプログラムの一環として サービスのセキュリティと AWS コンプライアンスを評価します。これには、SOC、PCI、FedRAMP、 HIPAA などが含まれます。

AWS セキュリティインシデント対応は、前述のプログラムへの準拠について評価されていません。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、AWS「コンプライアンスプログラムによる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。

AWS Artifact を使用してサードパーティーの監査レポートをダウンロードできます。詳細については、AWS「アーティファクトでのレポートのダウンロード」を参照してください。

AWS サービスを使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性、貴社のコンプライアンス目的、および該当する l AWS と規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- 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重点を置いたベースライン環境をデプロイする手順を示します AWS。
- HIPAA セキュリティとコンプライアンス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では、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 コンプライアンスリソース – 業界や場所ごとに適用されるワークブックやガイドのコレクション。
- 「Config デベロッパーガイド – AWS Config」の「Config ルールによるリソースの評価」では、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS AWS
- AWS Security Hub – この AWS サービスは、セキュリティ状態を包括的に表示します AWS。Security Hub 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、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環境を監視することで、 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。 PCI GuardDuty は、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知要件を満たすことでDSS、 などのさまざまなコンプライアンス要件に対応するのに役立ちます。

- AWS Audit Manager – この AWS サービスは、 AWS 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準拠を簡素化するのに役立ちます。

AWS セキュリティインシデント対応でのログ記録とモニタリング

モニタリングは、 AWS セキュリティインシデント対応およびその他の 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部分です。 AWS セキュリティインシデント対応は現在、組織とその内部で発生するアクティビティをモニタリングするために以下の 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 セキュリティインシデント対応コンソールからAPI通話をキャプチャできます。たとえば、ユーザーが認証されると、 はリクエストの IP アドレス、リクエスト者、リクエスト日時などの詳細を記録 CloudTrail できます。

Amazon CloudWatch メトリクス – CloudWatch メトリクスを使用すると、イベントが発生した場合にほぼリアルタイムでモニタリング、レポート、自動アクションを実行できます。例えば、提供されたメトリクスに CloudWatch ダッシュボードを作成して AWS セキュリティインシデント対応の使用状況をモニタリングしたり、提供されたメトリクスに CloudWatch アラームを作成して、設定されたしきい値を超過したときに通知したりできます。

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

AWS サービス条件に従って、 AWS セキュリティインシデント対応の応答者は CloudTrail、、VPC、DNSおよび S3 ログデータの履歴にアクセスできます。このデータは、Security Incident Response サービスポータルで AWS ケースが開いているときに、アクティブなセキュリティインシデント中に利用される場合があります。

耐障害性

AWS 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に構築されています。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が高く、フォールトトレラントで、スケーラブルです。

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 セキュリティインシデント対応は、 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 がインフラストラクチャ AWS 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」の「インフラストラクチャの保護」を参照してください。 AWS

AWS が公開したAPI呼び出しを使用して、ネットワーク経由で AWS Security Incident Response にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS) 。1TLS.2 が必要で、1.3 TLS をお勧めします。
- DHE (エフェメラル Diffie-HellmanPFS) や (エリプティックカーブエフェメラル Diffie-Hellman) など、完全な前方秘匿性 ECDHE () を持つ暗号スイート。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の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) を使用して一時的なセキュリティ認証情報を生成し、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

サービスコンテナロールと関連する AWS 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

混乱した代理問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。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。これを防ぐために、 は、アカウント内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を持つすべての サービスのデータを保護するのに役立つツール AWS を提供します。

リソースポリシーで AWS：SourceArn および AWS：SourceAccount 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使用する場合、同じポリシーステートメントで使用する場合、 AWS：SourceAccount value と AWS：SourceArn value のアカウントは同じアカウント ID を使用する必要があります。

混乱した代理問題から保護する最も効果的な方法は、許可するリソースの正確な Amazon リソースネーム (ARN) を使用することです。リソースARNの完全版がわからない場合、または複数のリソースを指定する場合は、 の不明な部分にワイルドカード (*) が付いた AWS：SourceArn global context 条件キーを使用しますARN。たとえば、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、「混乱した代理防止ポリシー」を参照してください。

Service Quotas

AWS セキュリティインシデント対応

次の表に、お客様のアカウントAWS のセキュリティインシデント対応リソースのクォータを示します AWS。一部のクォータは、サービスマネージャーの承認により、以下に記載されているクォータよりも引き上げられる場合があります。特記されていない場合、これらのクォータはリージョンごとに存在します。

	名前	デフォルト	引き上げ可能	コメント
1	AWS サポートされているアクティブなケース	10	はい (最大 50)	サポートをリクエストするアクティブなケースの数 AWS CIRT。
2	アクティブなセルフマネージドケース	50	はい (最大 100)	プラットフォームを使用するアクティブなケースのうち、サポートされていないケースの数 AWS CIRT。
3	24 時間以内に作成されたサービスサポートケース	10	いいえ	24 時間のローリングウィンドウで作成された からサポートをリクエストするために AWS CIRT 作成されたケースの数。
4	デフォルトのインシデント対応チームのエン	10	いいえ	デフォルトのインシデント対応チームのエン

	名前	デフォルト	引き上げ可能	コメント
	ティティの最大数			ティティの最大数。
5	ケースの追加メンバーの最大数	30	いいえ	ケースに関連付けられているエンティティの最大数。これは、最初はデフォルトのインシデント対応チームのエンティティが入力されます。
6	ケースアタッチメントの最大数	50	はい (最大 100)	ケースにアタッチできるファイルの最大数。
7	ケースコメントの最大サイズ	1,000	いいえ	ケースコメントの最大文字数。
8	ケースアタッチメントファイル名の最大サイズ	255	いいえ	ファイル名の最大文字数。

AWS セキュリティインシデント対応テクニカルガイド

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礎の概要を説明します。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、技術担当者を対象としており、情報セキュリティの一般的な原則に精通していること、現在のオンプレミス環境におけるセキュリティインシデント対応の基本的な知識があること、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 コンソールで無料で利用できる を使用すると、

柱ごとに一連の質問に答えることでAWS Well-Architected Tool、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確認できます。

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 の最優先事項です AWS。 AWS お客様は、最もセキュリティの影響を受けやすい組織のニーズに対応できるよう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からメリットを得られます。 には責任共有モデル AWS があります。 はクラウドのセキュリティ AWS 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など、セキュリティ実装を完全に制御できます。これらの機能は、 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 AWS クラウド。

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のトピックの例を確認し、自動化を使用して応答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と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、反復的なアプローチを実装することをお勧めします。コアセキュリティサービスから始めて、基本的な検出と対応機能を構築し、反復と改善を行うインシデント対応メカニズムの初期ライブラリを作成するためのプレイブックを作成します。

[開始する前に]

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を開始する前に AWS、 AWS セキュリティとインシデント対応に関連する標準とフレームワークを理解してください。これらの基盤は、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 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、コンプライアンスの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」、AWS 「 クラウド導入フレームワークの概要 (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さまざまな部分間の調整をサポートするガイダンスを提供します。この 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視点と呼ばれるいくつかの重点分野に分かれています。セキュリティの観点では、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を説明します。その 1 つはインシデント対応です。このドキュメントは、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機能の構築を支援するために、お客様と連携した経験の成果です。

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 () によって作成された「コンピュータセキュリティインシデント処理ガイド SP 800-61 r2」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、有用な前提条件NIST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、このガイドの対象外です。

AWS インシデント対応の概要

まず、クラウドでのセキュリティオペレーションとインシデント対応がどのように異なるかを理解することが重要です。で効果的な対応機能を構築するには AWS、従来のオンプレミス対応からの逸脱と、インシデント対応プログラムへの影響を理解する必要があります。これらの違いのそれぞれと、インシデント対応の主要な AWS 設計原則については、このセクションで詳しく説明します。

AWS インシデント対応の側面

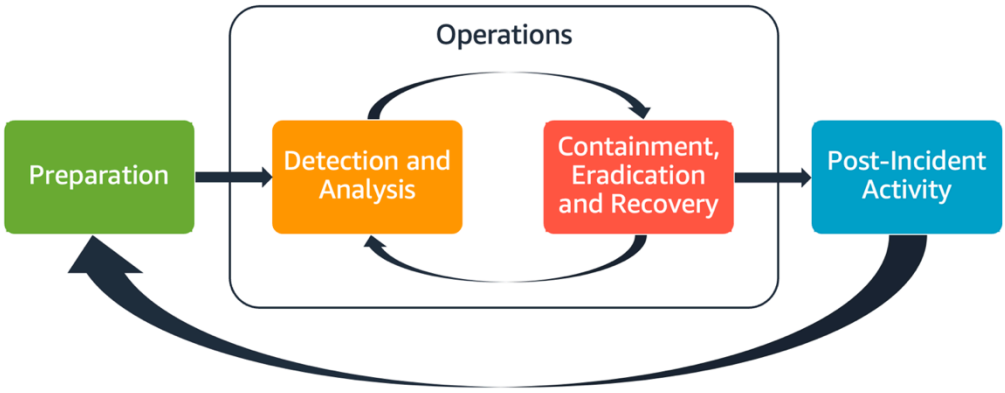
組織内のすべての AWS ユーザーは、セキュリティインシデント対応プロセスの基本を理解し、セキュリティ担当者はセキュリティ問題への対応方法を理解する必要があります。教育、トレーニング、経験は、クラウドインシデント対応プログラムを成功させるために不可欠であり、起こり得るセキュリティインシデントに対処する前に十分な余裕を持って実施するのが理想的です。クラウドでのインシデント対応プログラムを成功させるための基盤は、準備、運用、インシデント後のアクティビティです。

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 — 検出コントロールを有効にし、必要なツールとクラウドサービスへの適切なアクセスを検証 AWS することで、インシデント対応チームが 内のインシデントを検出して対応できるよう準備します。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。
- 運用 — インシデント対応の フェーズの後に、セキュリティイベントと潜在的なインシデントを運用NISTします。検出、分析、封じ込め、根絶、復旧です。

- インシデント後のアクティビティ — セキュリティイベントとシミュレーションの結果を繰り返して、対応の有効性を向上させ、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、このガイドで詳しく説明しています。次の図は、前述のNIST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が、封じ込め、根絶、復旧による検出と分析を含むオペレーションが含まれています。



AWS インシデント対応の側面

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処理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正常ですが、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特定の設計目標も考慮することをお勧めします。

- 対応目標の策定 — ステークホルダー、法律顧問、組織のリーダーと協力して、インシデントに対応する目標を決定します。一般的な目標には、問題の抑制と軽減、影響を受けるリソースの復旧、フォレンジック用のデータの保存、既知の安全な運用への復帰、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応答する – イベントとデータが発生するクラウド内に応答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、その他の証拠をコピーして、対応専用の一元化されたクラウドアカウントに保存することで保存します。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。使用するサービスを理解し、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、the section called “タグ付け戦略を策定し、実装する”「」セクションのこのドキュメントで後述します。

- 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可能性がある場合、適切な設定でリソースを再デプロイすることで差異を取り除くのと同じくらい簡単な修復になる可能性があります。侵害の可能性が特定された場合は、再デプロイに根本原因の正常な緩和策と検証済みの緩和策が含まれていることを確認します。
- 可能な場合は自動化 — 問題が発生したりインシデントが繰り返されたりしたら、一般的なイベントにプログラムでトリアージして対応するためのメカニズムを構築します。自動化が不十分な一意、複雑、または機密性の高いインシデントには、人間の対応を使用します。
- スケーラブルなソリューションを選択する – クラウドコンピューティングに対する組織のアプローチのスケーラビリティに合わせて努めます。検出と応答の間の時間を効果的に短縮するために、環境全体にスケールする検出と応答のメカニズムを実装します。
- プロセスについて学び、改善する – プロセス、ツール、または人材のギャップを積極的に特定し、それらを修正する計画を立てます。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ための安全な方法です。プロセスの反復処理方法の詳細については、このドキュメントの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。クラウド実装を計画する際は、インシデントへの対応を検討してください。理想的には、フォレンジックな対応方法論を採用することをお勧めします。場合によっては、これらの応答タスク用に複数の組織、アカウント、ツールが特別にセットアップされている可能性があります。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ドメイン

AWS 環境のセキュリティイベントを効果的に準備して対応するには、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 つのドメインがお客様の責任内に存在します。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。以下のドメインを検討してください。

- 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。サービスドメインイベントは、 メカニズムのみで AWS API応答するか、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内の Amazon EC2インスタンスへのトラフィック (VPC) 、コンテナやその他の将来のサービスなどの他の領域などの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イベントへの対応には、多くの場合、フォレンジック分析用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メカニズムが含まれる AWS API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 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 AWS APIs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またはサービスや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のものと同様のレスポンスを組み込むことができます。適切で慎重に設計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する可能性のあるアクターを検討してください。内部的か外部的かにかかわらず、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決定し、それに応じて準備します。さらに、インシデント対応の計画や慎重に検討したアーキテクチャ構築に役立つ脅威モデルを開発する必要があります。

でのインシデント対応の主な違い AWS

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の不可欠な部分です。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、プレイブック開発、セキュリティ情報とイベント管理 (SIEM) 統合などに適しています。この違いは、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したときに始まります。以下は、 でのインシデント対応の主な違いです AWS。

違い #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 とその顧客の間で共有されます。この責任共有モデルは、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まで、コンポーネントを AWS 運用、管理、制御するため、お客様の運用上の負担の一部を軽減します。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。

クラウドでの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。

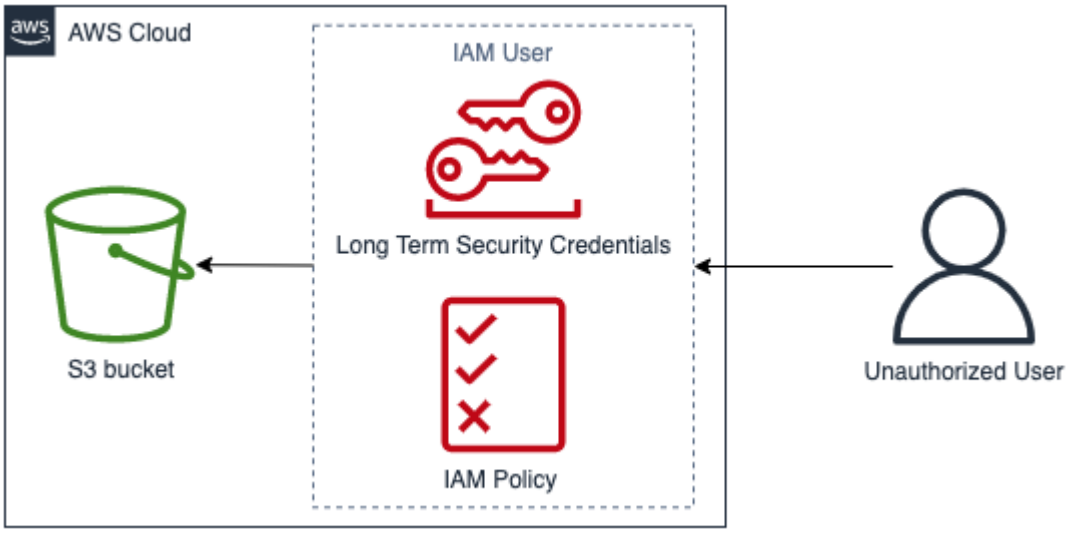
直接的な関係に加えて AWS、特定の責任モデルで責任を持つ他のエンティティが存在する可能性があります。例えば、オペレーションの一部の側面を担当する内部組織単位があるとします。また、クラウドテクノロジーの一部を開発、管理、または運用する他の関係者との関係がある場合もあります。

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てテストすることは非常に重要です。

違い #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、お客様のアカウント AWS 、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。このドメインは、インシデント対応の対応方法によって異なります。サービスドメイン内のレスポンスは、通常、従来のホストベースおよびネットワークベースのレスポンスではなく、API通話を確認して発行すること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やり取りすることはありません。

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。この場合、権限のないユーザーは 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。IAM ユーザーには、Amazon Simple Storage Service (Amazon S3) バケットからオブジェクトを取得することを許可する IAMポリシーがあります。このセキュリティイベントに対応するには、 AWS APIsを使用して、 AWS CloudTrailや Amazon S3 アクセス AWS ログなどのログを分析します。また、 を使用して AWS APIsインシデントを封じ込め、インシデントから復旧します。



サービスドメインの例

違い #3: APIs インフラストラクチャのプロビジョニング

もう 1 つの違いは、オンデマンドセルフサービスの クラウド特性です。主な施設であるお客様は、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RESTfulAPIを介して AWS クラウド を使用して とやり取りします。顧客は認証情報APIsを使用してこれらにアクセスできます AWS 。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工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、認証情報が予想されるネットワークまたは地域外で使用されるインシデントにいつ対応するかを理解することが重要です。

APIベースの性質上 AWS、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 です。これは、 AWS アカウントで行われた管理API呼び出しを追跡し AWS CloudTrail、API呼び出しのソースの場所に関する情報を見つけることができます。

違い #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高速な変更により、調査対象のリソースが存在しないか、変更されている可能性があります。 AWS リソースの一時的な性質と、 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は、インシデント分析にとって重要です。を使用してAWS Config、 AWS リソースの設定履歴を追跡できます。

違い #5: データアクセス

データアクセスはクラウドでも異なります。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、電話とAPI通話を介して収集されます。このシフトに備えAPIsるために、 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に適切なストレージを検証する必要があります。

違い #6: 自動化の重要性

クラウド導入のメリットをお客様が十分に実感するには、運用戦略で自動化を採用する必要があります。Infrastructure as Code (IaC) は、 AWS CloudFormationやサードパーティーソリューションなどのネイティブ IaC サービスによって容易になるコードを使用して、 AWS のサービスをデプロイ、設定、再設定、および破棄する、非常に効率的な自動化環境のパターンです。これにより、インシデント対応の実装が高度に自動化されます。これは、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ことです。自動化はオンプレミスで使用されますが、 ではよりシンプルで不可欠です AWS クラウド。

これらの違いへの対応

これらの違いに対処するには、次のセクションで説明するステップに従って、人、プロセス、テクノロジーにわたるインシデント対応プログラムの準備が整っ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。

- 人材 — セキュリティインシデントに備えるには、インシデント対応に関連する利害関係者を特定し、インシデント対応とクラウドテクノロジーについてトレーニングする必要があります。
- プロセス – セキュリティインシデントに対するプロセスの準備には、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作成、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含まれます。
- 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モニタリング、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。

人員

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けることが重要です。

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。多くの地域では、すべきこととすべきでないこと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について、責任、説明責任、相談、情報 (RACI) のグラフを構築することは、機関にとっては当たり前のように思えるかもしれませんが、そう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にわたるリーダーシップを明確に概説できます。

インシデントの発生時には、影響を受けるアプリケーションやリソースの所有者/開発者を含むことが重要です。これらは、影響の測定に役立つ情報とコンテキストを提供できる対象分野のエキスパート (SMEs) であるためです。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。クラウド管理者やエンジニアなどのアプリケーション所有者や はSMEs、環境が不慣れな場合や複雑である場合、または応答者がアクセスできない場合に、対応する必要がある場合があります。

最後に、信頼関係は、追加の専門知識や貴重な調査を提供できるため、調査や対応に関与してい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

インシデント対応スタッフに、組織が使用するテクノロジーをトレーニングすることは、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、対応が長くなる可能性があります。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従来のメカニズムは多数あります。トレーニングのメカニズムとして、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、このドキュメントのthe section called “定期的な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 テクノロジーを理解する

依存関係を減らし、応答時間を短縮するには、セキュリティチームと応答者がクラウドサービスについて教育され、組織が使用する特定のクラウド環境を実践する機会があることを確認してください。インシデント応答者を効果的に機能させるには、 AWS 基盤、IAM AWS Organizations、 AWS ログ記録と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、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 AWS 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) を提供しています。 AWS また、 は、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ラーニングパスを提供しています。詳細については、AWS 「トレーニングと認定」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にしか理解されないため、依存関係が生まれ、イノベーションが妨げられ、応答時間が遅くなります。

これらの依存関係を回避し、応答時間を短縮するには、 AWS 環境に関する社内知識をセキュリティアナリストが文書化し、アクセスし、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ためのプロセスの準備の一環として、このホワイトペーパーのthe section called “アーキテクチャ図の文書化と一元化”後半にあるアーキテクチャ図の文書化と一元化が含まれます。ただし、人の観点からは、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

Support

Support は、 AWS ソリューションの成功と運用の健全性をサポートするツールと専門知識へのアクセスを提供するさまざまなプランを提供します。 AWS 環境の計画、デプロイ、最適化に役立つテクニカルサポートとその他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のサポートを受けるには、 のサポートセンター AWS Management Console （ サインインが必要) を連絡の中心として検討してください。へのアクセス Support は

によって制御されますIAM。 AWS サポート機能へのアクセスの詳細については、「 の開始方法 Support」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 Tust and Safety チームに連絡してください。

AWS 顧客インシデント対応チーム (CIRT)

AWS カスタマーインシデント対応チーム (CIRT) は、AWS 責任共有モデルの顧客側でアクティブなセキュリティイベント中に顧客にサポートを提供する、特化された常時利用可能なグローバル AWS チームです。

が AWS CIRTサポートすると、アクティブなセキュリティイベントのトリアージと復旧に関するサポートが提供されます AWS。これらは、 AWS サービスログを使用して根本原因の分析を支援し、復旧に関する推奨事項を提供します。また、今後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の推奨事項とベストプラクティスも提供します。

AWS のお客様は、 AWS CIRT AWS サポートケースを通じて をエンゲージできます。

- 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 Support 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 Support 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: 緊急のビジネスに影響を与える質問

- エンタープライズ Support 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 セキュリティインシデント対応サブスクリプションをご利用のお客様: 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。 https://console.aws.amazon.com/security-ir/

DDoS レスポンスのサポート

AWS はAWS Shield、 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の分散サービス拒否 (DDoS) 保護サービスを提供します AWS。 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ための常時オンの検出と自動インライン緩和 AWS Shield を提供するため、DDoS保護のメリットを享受 Support する必要はありません。Shield Standard と AWS Shield Shield Advanced の 2 つの階層があります。これら 2 つの階層の違いについては、Shield 機能のドキュメント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を継続的に管理するため、アプリケーションに集中できます。インフラストラクチャを維持するためのベストプラクティスを実装することで、 AMSは運用上のオーバーヘッドとリスクを軽減します。 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AMS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、サポートするためのライフサイクル全体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をデプロイする責任を担い、アラートに毎日対応します。アラートが開始されると、 は、自動化されたプレイブックと手動プレイブックの標準セットAMSに従って、一貫したレスポンスを検証します。これらのプレイブックはオンボーディング中にAMS顧客と共有されるため、顧客は と対応を開発および調整できますAMS。

プロセス

完全で明確に定義されたインシデント対応プロセスを開発することは、成功したスケーラブルなインシデント対応プログラムにとって重要です。セキュリティイベントが発生すると、明確なステップとワークフローがタイムリーに対応するのに役立ちます。既存のインシデント対応プロセスが既に存在

している可能性があります。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の策定とテスト

インシデント対応のために最初に作成するドキュメントは、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、通常以下のセクションを含む高レベルのドキュメントです。

- 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
- 役割と責任 — インシデント対応の利害関係者を一覧表示し、インシデント発生時の役割を詳述します。
- コミュニケーション計画 – 連絡先情報とインシデント発生時のコミュニケーション方法の詳細

  インシデントコミュニケーションのバックアップとしてコミュニケーションを取る out-of-bandことがベストプラクティスです。安全な out-of-band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フェーズと実行するアクション – インシデント対応のフェーズを列挙します。例えば、検出、分析、根絶、封じ込め、復旧など、これらのフェーズ内で実行する高レベルのアクションが含まれます。
- インシデントの重大度と優先順位付けの定義 – インシデントの重大度を分類する方法、インシデントの優先順位付け方法、重大度の定義がエスカレーション手順にどのように影響するかの詳細

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作成する必要があります。

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、ベストプラクティスに従ってパターンが設計されている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、このドキュメントが最新であり、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ドキュメント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 - 以下を知る必要があります。
  - AWS アカウントはいくつありますか？

  - これらの AWS アカウントはどのように整理されていますか？
  - AWS アカウントの事業所有者は誰ですか？
  - サービスコントロールポリシー (SCPs) を使用していますか？ その場合、 を使用してどのような組織ガードレールを実装しますかSCPs？
  - 使用できるリージョンとサービスを制限していますか？
  - ビジネスユニットと環境 (dev/test/prod) にはどのような違いがありますか？
- AWS サービスパターン
  - どの AWS サービスを使用していますか？
  - 最も広く使用されている AWS サービスは何ですか？
- 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ますか？
- AWS 認証パターン
  - デベロッパーは通常、どのように認証しますか AWS？
  - IAM ロールまたはユーザー (またはその両方) を使用していますか？ への認証は ID プロバイダー (IdP) AWS に接続されていますか？
  - IAM ロールまたはユーザーを従業員またはシステムにマッピングする方法
  - 誰かが認可されなくなった場合、アクセスはどのように取り消されますか？
- 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ますか？
  - リソースベースのポリシーを使用していますか？
- ログ記録とモニタリング
  - どのログ記録ソースを使用し、どこに保存されていますか？
  - AWS CloudTrail ログを集約していますか？ その場合は、どこに保存されますか？
  - CloudTrail ログをクエリする方法
  - Amazon GuardDuty が有効になっていますか？
  - GuardDuty 検出結果 (コンソール、チケットシステム、 などSIEM) には、どのようにアクセスしますか？
  - 検出結果またはイベントは に集約されていますかSIEM？
  - チケットは自動的に作成されますか？
  - 調査の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ますか？
- 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ますか？
  - ネットワークは とどのように接続されますか AWS？
  - 環境間でネットワークトラフィックをフィルタリングする方法
- 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ますか？
  - パブリックにアクセス可能な AWS リソース
  - 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
  - どのようなDDoSフィルタリングや外部フィルタリングがありますか？

内部の技術図とプロセスを文書化すると、インシデント対応アナリストのジョブが容易になり、セキュリティイベントに対応するための組織的な知識をすばやく得ることができます。内部の技術プロセスの詳細なドキュメントは、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に合わせて調整します。

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 – 予想されるインシデントのプレイブックを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検出結果またはアラート – プレイブックは、検出結果などの既知のセキュリティ GuardDuty 検出結果とアラート用に作成する必要があります。 GuardDuty 「さて、どうなるか」という結果が表示され、 GuardDuty 結果の誤った処理や結果の無視を防ぐには、潜在的なGuardDuty結果ごとにプレイブックを作成します。一部の修復の詳細とガイダンスは、 GuardDuty ドキュメントに記載されています。 GuardDuty はデフォルトで有効になっておらず、コストが発生することに注意してください。の詳細については GuardDuty 、「付録 A: クラウド機能の定義 - 」を参照してくださいthe section called “可視性とアラート”。

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 – このプレイブックはどのようなリスクまたはインシデントシナリオに対処していますか？ 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と検出メカニズムが必要ですか？ 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。
- 対応手順 – インシデント対応のフェーズ全体で、どのような戦術的手順を実行すべきですか？ 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。
  - 検出 — インシデントはどのように検出されますか？
  - 分析 — 影響範囲はどのように決定されますか？
  - 封じ込め — インシデントを隔離して範囲を制限するにはどうすればよいですか？
  - Eradicate – 脅威を環境からどのように排除しますか？
  - 復旧 — 影響を受けるシステムまたはリソースを本番環境に戻すにはどうすればよいですか？
- 期待される成果 — クエリとコードが実行された後、プレイブックの期待される成果は何ですか？

各プレイブックの一貫した情報を検証するには、他のセキュリティプレイブックで使用するプレイブックテンプレートを作成すると便利です。ステークホルダー情報など、以前にリストされた項目の一部は、複数のプレイブック間で共有できます。その場合は、その情報の一元化されたドキュメントを作成し、プレイブックで参照して、プレイブックの明示的な違いを列挙できます。これにより、個々のプレイブックで同じ情報を更新する必要がなくなります。テンプレートを作成し、プレイブックの共通または共有情報を特定することで、プレイブックの開発を簡素化し、高速化できます。最後に、プレイブックは時間の経過とともに進化する可能性があります。ステップが一貫していることを確認したら、自動化の要件を形成します。

サンプルプレイブック

サンプルプレイブックは、 の付録 B にありますthe section called “プレイブックリソース”。ここでの例を使用して、作成するプレイブックとプレイブックに含める内容を確認できます。ただし、ビジネスに最も関連性の高いリスクを組み込むプレイブックを作成することが重要です。プレイブック

内のステップとワークフローに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。

定期的なシミュレーションを実行する

脅威の状況と同様に、組織は時間の経過とともに成長し、進化します。このため、インシデント対応機能を継続的に確認することが重要です。シミュレーションは、この評価の実行に使用できる 1 つの方法です。シミュレーションでは、脅威アクターの戦術、手法、手順 (TTPs) を模倣するように設計された実際のセキュリティイベントシナリオを使用し、組織はこれらの模擬サイバーイベントに実際に発生する可能性があるときに対応することで、インシデント対応能力を実践して評価できます。

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 – シミュレーションへの机上アプローチは、厳密には、さまざまなインシデント対応関係者が役割と責任を実践し、確立されたコミュニケーションツールとプレイブックを使用するためのディスカッションベースのセッションです。演習の円滑化は、通常、仮想会場、物理的な会場、または組み合わせで 1 日で行うことができます。ディスカッションベースの性質のため、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の不可欠な部分ですが、インシデント対応ツールやスクリプトの実際の使用は、通常、机上演習の一部ではありません。
- 紫色のチームの演習 – 紫色のチームの演習では、インシデント対応者 (ブルーチーム) とシミュレートされた脅威アクター (赤チーム) の間のコラボレーションのレベルが向上します。Blue Team は通常、 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を含めることもできます。Red Team は通常、攻撃的なセキュリティのトレーニングを受けた侵入テストチームまたは主要な利害関係者で構成されています。Red Team は、シナリオを設計する際に演習のファシリテーターと協力して、シナリオが正確で実行可能になるようにします。Purple Team の演習では、インシデント対応の取り組みをサポートする検出メカニズム、ツール、標準運用手順 (SOPs) に重点を置いています。

- Red Team の演習 – Red Team の演習では、違反 (Red Team) がシミュレーションを実施して、事前に定義されたスコープから特定の目標または一連の目標を達成します。防御者 (ブルーチーム) は、必ずしも演習の範囲と期間を知っているわけではありません。これにより、実際のインシデントにどのように対応するかについてより現実的な評価が得られます。Red Team の演習は侵入テストになる可能性があるため、演習によって環境に実際に害が及ばないことを確認するためのコントロールを実装する必要があります。

> **Note**
>
> AWS では、お客様は、Purple Team または Red Team の演習を行う前に、Penetration Testing 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。定義は一般的にルーズな定義と見なされ、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	紫色のチーム演習	Red Team の演習
概要	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、ペーパー駆動型の演習。これらは高レベルでも技術的でもよく、一連の紙の注入によって駆動されます。	机上演習よりもリアルな提供。Purple Team の演習では、ファシリテーターは参加者と協力して演習のエ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、より高度なシミュレーションサービスです。通常、高いレベルの秘密性があり、参加者は演習の詳細をすべて知らない可能性があります。
必要なリソース	必要な技術リソースの制限	さまざまなステークホルダーが必要で、高レベルの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で、高レベルの技術リソースが必要
複雑さ	低	Medium	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。各演習タイプは、参加者と組織全体に固有の利点をもたらすことができるため、より複雑なシミュレーションタイプ (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 (Red Team 演習) に進むことを選択できます。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。一部のお客様は、複雑さとコストのために Red Team の演習を実行しない場合があります。

演習のライフサイクル

選択したシミュレーションのタイプにかかわらず、シミュレーションは通常、以下のステップに従います。

1. 主要な演習要素を定義する — シミュレーションシナリオとシミュレーションの目的を定義します。いずれも、リーダーの承認が必要です。
2. 主要な利害関係者を特定する — 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 — 特定の要素が実行可能でない場合は、シナリオの構築中にシナリオを再定義する必要がある場合があります。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円滑化 – シミュレーションのタイプによって、使用する円滑化が決まります (高度な技術的でシミュレートされたシナリオと比較した、紙ベースのシナリオ) 。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ポートを作成する (AAR) – うまくいった分野、改善を利用できる分野、潜在的なギャップを特定します。は、シミュレーションの有効性と、シミュレートされたイベントに対するチームの反応を測定し、今後のシミュレーションで進行状況を経時的に追跡できるようにAAR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て実装すると、インシデント対応スタッフが調査し、範囲を理解し、タイムリーにアクションを実行できるようになります。

AWS アカウント構造の開発

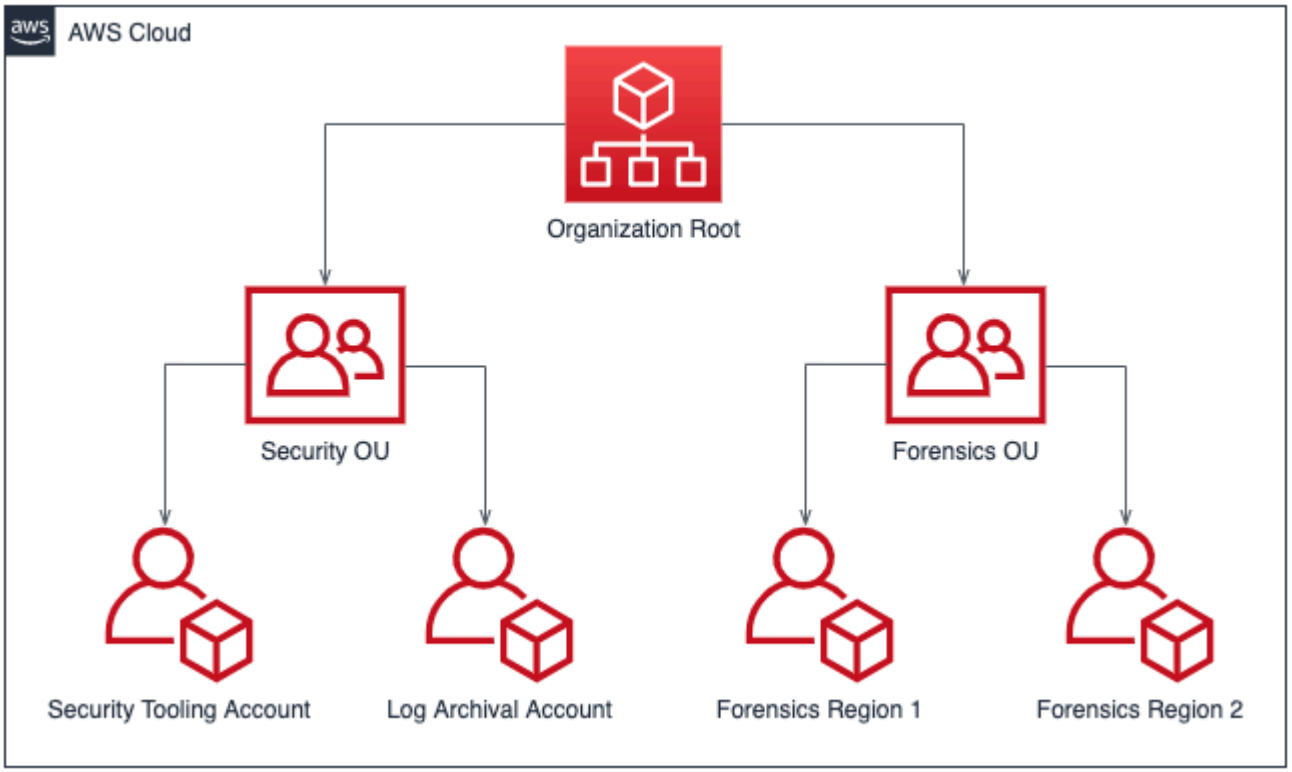
AWS Organizations は、 AWS リソースの拡大とスケーリングに応じて AWS 環境を一元管理します。 AWS 組織は AWS アカウントを統合し、1 つのユニットとして管理できるようにします。組織単位 (OUs) を使用してアカウントをグループ化し、1 つの単位として管理できます。

インシデント対応には、セキュリティ OU とフォレンジック OU を含むインシデント対応の機能をサポートする AWS アカウント構造を持つと便利です。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 AWS アカウントにログを集約します。
- 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 AWS アカウントに集中させます。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については、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) でのみ運用している場合、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 用です。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

ビジネスユースケースおよび AWS リソースに関連する内部ステークホルダーに関するコンテキスト情報を取得するのは難しい場合があります。これを行う 1 つの方法はタグの形式で、 AWS リソースにメタデータを割り当て、ユーザー定義のキーと値で構成されます。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を持つことで、 AWS リソースに関するコンテキスト情報をすばやく特定して識別できるため、応答時間を短縮できます。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。タグ付けする対象の詳細については、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。実装と適用の詳細については、 AWS ブログAWS 「タグポリシーとサービスコントロールポリシーを使用した AWS リソースタグ付け戦略の実装 (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、正確な連絡先情報を用意して、 up-to-dateセキュリティ、請求、オペレーションなどのトピック AWS に関する重要な通知を適切な利害関係者が から受け取ることが重要で

す。 AWS アカウントごとに、セキュリティ、請求、運用に関する主要連絡先と代替連絡先があります。これらの問い合わせの違いは、AWS 「 アカウント管理リファレンスガイド」に記載されています。

代替連絡先の管理の詳細については、AWS 代替連絡先の追加、変更、削除に関するドキュメントを参照してください。チームが請求、運用、セキュリティ関連の問題を管理する場合は、E メール配布リストを使用するのがベストプラクティスです。E メール配信リストは、1 人の人物への依存関係を削除します。これにより、不在や退職時に障害が発生する可能性があります。また、電話番号を含む E メールとアカウントの連絡先情報が、ルートアカウントのパスワードのリセットや多要素認証 (MFA) のリセットから保護するために十分に保護されていることを確認する必要があります。

を使用するお客様の場合 AWS Organizations、組織管理者は、各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 AWS 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が正確な連絡先情報を持っていることも確認する必要があります。「新しく作成された AWS アカウント ブログ記事の代替連絡先を自動的に更新する」を参照してください。

へのアクセスを準備する AWS アカウント

インシデント中、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、チームが職務を実行するための適切なアクセス権を持っていることを確認します。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 (たとえば、どのようなアクションを実行する可能性があるか) を把握し、最小特権アクセスを事前にプロビジョニングする必要があります。

このアクセスを実装してプロビジョニングするには、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て組織のクラウドアーキテクトと話し合い AWS 、設定されている認証方法と認可方法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、ボールトまたは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を文書化してテストし、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に対応するために特別に作成されたユーザーは、十分なアクセス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。したがって、これらの認証情報の使用を制限し、モニタリングし、日常のアクティビティには使用しないようにします。

脅威の状況を理解する

脅威モデルを開発する

脅威モデルを開発することで、組織は、権限のないユーザーが脅威と緩和策を特定できるようになる前に特定できます。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。「脅威モデリングのアプローチ方法」ブログ記事を参照してください。インシデント対応の場合、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。タイムリーに対応するためには、防御対象を理解することが不可欠です。脅威モデリング AWS Partner に を使用することもできます。パートナーを検索する AWS には、 を使用しますAWS Partner Network。

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、能力のデータと分析です。脅威インテリジェンスを取得して使用すると、インシデントを早期に検出し、脅威アクターの動作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高レベルの情報も含まれています。多く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脅威インテリジェンスを収集できます。

AWS 環境の脅威インテリジェンスを統合して最大化するには、いくつかの out-of-the-box機能を使用し、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高度な脅威インテリジェンスグループから情報を取得します。一部の GuardDuty 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を提供します。

分析とアラート発行のためのロ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、関連ログを確認できる必要があります。ログはまた、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は、このセクションで確認します。詳細については、「セキュリティインシデント対応のログ記録戦略 AWS 」ブログ記事を参照してください。

ログソースの選択と有効化

セキュリティ調査の前に、関連するログをキャプチャして、 AWS アカウントのアクティビティを遡及的に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、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行われたAPI呼び出しを追跡するログ記録 AWS サービスです。デフォルトでは、、 AWS Management Console、 AWS CLIまたは を使用して CloudTrail、 のイベント履歴機能を通じて取得できる管理イベントの 90 日間の保持で有効になっています AWS SDK。データイベントの保持と可視性を長くするには、 CloudTrail Trail を作成し、Amazon S3 バケット、およびオプションで CloudWatch ロググループに関連付ける必要があります。または、最大 7 年間 CloudTrail ログを保持し、 SQLベースのクエリ機能を提供する CloudTrail Lake を作成することもできます。

AWS を使用するお客様は、それぞれVPCフローDNSログと Amazon Route 53 リゾルバークエリログを使用してネットワークトラフィックとログVPCを有効にし、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お勧めします。、サブネットVPC、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 フローログでは、コストを削減するためにフローログを有効にする方法と場所を選択できます。

AWS CloudTrail ログ、VPCフローログ、および Route 53 リゾルバークエリログは、セキュリティ調査をサポートする基本的なログ記録のトリフェクタです AWS。

AWS サービスでは、Elastic Load Balancing ログ、 AWS WAF ログ、 AWS Config 順序ログ、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、基本的なログ記録トリフェタによって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オプションの完全なリストthe section called “付録 A: クラウド機能の定義”については、「」を参照してください。

ログストレージの選択

ログストレージの選択は、一般的に、使用するクエリツール、保持機能、知識、コストに関連しています。 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、オプションのライフサイクルポリシーを使用して、費用対効果の高い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用してネイティブにクエリできます。 CloudWatch ロググループは、CloudWatch Logs Insights を通じて耐久性の高いストレージと組み込みクエリ機能を提供します。

適切なログ保持を特定する

S3 バケットまたは CloudWatch ロググループを使用してログを保存する場合は、ログソースごとに適切なライフサイクルを確立して、ストレージと取得のコストを最適化する必要があります。お客様

は通常、クエリに 3～12 か月のログを簡単に利用でき、保持期間は最大 7 年です。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

では AWS、ログのクエリに使用できる主なサービスは、ログ CloudWatch グループに保存されているデータの CloudWatch Logs Insights と、Amazon S3 に保存されているデータの Amazon Athena と Amazon OpenSearch Service です。 Amazon S3 セキュリティ情報やイベント管理 () などの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SIEM。

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。運用、ビジネス、セキュリティの要件を満たし、長期的にアクセス可能で保守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により、顧客が複数のクエリツールを持つことは珍しくありません。たとえば、お客様は、 のログ取り込みコストのため、サードパーティーを使用して過去 90 日間のデータに対してクエリSIEMを実行し、Athena を使用して 90 日を超えるクエリを実行する場合がありますSIEM。実装に関係なく、特にセキュリティイベントの調査中に、運用効率を最大化するために必要なツールの数を最小限に抑えるアプローチであることを確認します。

アラートにログを使用する

AWS は、Amazon、、 GuardDuty AWS Security Hub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 AWS Config。また、カスタムアラート生成エンジンは、これらのサービスでカバーされていないセキュリティアラートや、環境に関連する特定のアラートにも使用できます。これらのアラートと検出の構築については、このドキュメントの「」というセクションthe section called “検出”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。フォレンジック手法をインシデント対応に統合するためのガイドNISTには、このようなガイダンスが記載されています。

のフォレンジック AWS

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 AWS。ブログ記事のフォレンジック調査環境戦略 AWS クラウドには、フォレンジックの専門知識の移行を開始するための重要な情報が記載されています AWS。

フォレンジック用に環境と AWS アカウント構造を設定したら、次の 4 つのフェーズでフォレンジックサウンドの手法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必要があります。

- 収集 — AWS CloudTrail、、VPCフロー AWS ログ AWS Config、ホストレベルのログなどの関連ログを収集します。影響を受ける 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 — 関連情報を抽出して評価することで収集されたデータを調べます。
- 分析 — インシデントを理解し、そこから結論を引き出すために収集されたデータを分析します。
- レポート — 分析フェーズの結果に関する情報を表示します。

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。では AWS、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。スナップショットは、 point-in-timeこれらのリソースのバックアップを提供します。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、「バックアップを使用してセキュリティインシデントから復旧する」ブログ記事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、ブログ記事の「バックアップを保護するためのセキュリティのベストプラクティスのトップ 10 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。

でのフォレンジックの自動化 AWS

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正確性を維持しながら、証拠を迅速に収集して分析できる必要があります。インシデント対応チームがクラウド環境、特に多数のインスタンスやアカウントで関連する証拠を手動で収集するのは、困難で時間がかかります。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て実装する必要があります。

AWS はフォレンジック用のオートメーションリソースを多数提供しています。これらは、 の付録に統合されていますthe section called “フォレンジックリソース”。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

セキュリティイベントに対応するための徹底的な準備は、タイムリーで効果的なインシデント対応に不可欠です。インシデント対応の準備には、人、プロセス、テクノロジーが含まれます。これらの 3 つのドメインはすべて、準備に等しく重要です。インシデント対応プログラムを 3 つのドメインすべてにわたって準備し、進化させる必要があります。

表 2 は、このセクションで説明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
人物	役割と責任を定義します。	• 関連するインシデント対応のステークホルダーを特定します。 • インシデントの責任者、説明責任者、通知先、相談先 (RACI) チャートを作成します。
人物	インシデント対応スタッフをトレーニングします AWS。	• AWS 基盤に関するインシデント対応のステークホルダーをトレーニングします。 • AWS セキュリティおよびモニタリングサービスについてインシデント対応のステークホルダーをトレーニングします。 • インシデント対応のステークホルダーを AWS 環境と設計方法についてトレーニングします。

ドメイン	準備項目	アクション項目
人物	AWS サポートオプションについて説明します。	• AWS サポート、カスタマーインシデント対応チーム (CIRT) 、対応DDoSチーム (DRT) 、 の違いを理解しますAMS。 • 必要に応じて、アクティブなセキュリティイベント CIRT中に に到達するためのトリアージとエスカレーションのパスを理解します。
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高レベルのドキュメントを作成します。 • RACI、コミュニケーション計画、インシデント定義、インシデント対応計画へのインシデント対応のフェーズを含めます。
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、サービスの使用法、IAMパターン、その他の主要機能全体にわたる AWS 環境の設定に関する詳細を AWS 構成に文書化します。 • 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。

ドメイン	準備項目	アクション項目
プロセス	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の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 検出結果などの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	通常の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開発します。 • 学んだ成果と教訓を使用して、インシデント対応プログラムを反復処理します。
テクノロジー	AWS アカウント構造を開発します。	• ワークロードをアカウントでどのように分離するかについて、 AWS アカウント構造を計画します。 • 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。

ドメイン	準備項目	アクション項目
テクノロジー	応答者が検出結果の所有権とコンテキストを特定できるようにするタグ付け戦略を策定して実装します。	• タグ付けの戦略と、リソースに関連付けるタグを計画します AWS 。 • 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 E メール配信リストを作成して、単一障害点を削除します。 • アカウント情報に関連付けられている E メール AWS アカウントを保護します。
テクノロジー	AWS アカウントへのアクセスを準備します。	• インシデントへの対応に必要なアクセスインシデント応答者を定義します。 • アクセスを実装、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て使用します。

ドメイン	準備項目	アクション項目
テクノロジー	ログを選択して設定します。	• 調査のログを特定して有効にします。 • ログストレージを選択します。 • ログ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してクエリするメカニズムを開発します。 • アラートには ログを使用します。
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。 • キー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。これらの準備項目はすべて夜間に行うことはできません。小規模から始めて、時間の経過とともにインシデント対応能力を継続的に改善する計画を作成する必要があります。

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は、表 3 に記載されています。

表 3 – 運用フェーズ

[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であるかどうかを判断し、インシデントの範囲を評価します。
コンテナ	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。
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モニタリングして、脅威が戻ら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。対象となる AWS アカウントのアクティビティに基づいてインシデント対応プロセスを開始する通知を生成します。

アラートの精度は困難です。インシデントが発生したのか、進行中なのか、または将来発生するのかを、常に完全な確実性で判断できるとは限りません。いくつかの理由があります。

- 検出メカニズムは、ベースライン偏差、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。

- テクノロジーと人材の予測不可能な性質、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ため、ベースラインは時間の経過とともに変化します。不正なパターンは、新規または変更された脅威アクターの戦術、手法、手順 () によって発生しますTTPs。
- 人、テクノロジー、プロセスに対する変更は、すぐにインシデント対応プロセスに組み込まれるわけではありません。調査の進行中に検出されるものもあります。

アラートソース

アラートを定義するには、次のソースの使用を検討する必要があります。

- 検出結果 – Amazon GuardDuty、、AWS Security HubAmazon Macie、Amazon Inspector、AWS Config、IAMAccess 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、およびアプリケーション CloudWatch ログを解析し、関連付けてアラートを生成できます。
- 請求アクティビティ y — 請求アクティビティが突然変化した場合は、セキュリティイベントを示している可能性があります。「請求アラームの作成」のドキュメントに従って、これを監視する予想 AWS 請求額を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と、その情報を他のログ記録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 – (APN) の AWS Partner Network 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。インシデント対応の場合、エンドポイントの検出と対応 (EDR) または を備えたパートナー製品はSIEM、インシデント対応目標のサポートに役立ちます。詳細については、「」の「 セキュリティパートナーソリューションとセキュリティソリューション」を参照してください。 AWS Marketplace
- のAWS 信頼と安全性 — 虐待的または悪意のあるアクティビティを特定した場合、お客様に連絡 Support する可能性があります。
- 1 回限りのコンタクト — 組織内の顧客、開発者、またはその他のスタッフで、何か変わったことに気付く可能性があるため、セキュリティチームに連絡する方法はよく知られており、広く公開されていることが重要です。一般的な選択肢には、チケット発行システム、連絡先の E メールアドレス、ウェブフォームなどがあります。組織が一般ユーザーと連携する場合は、一般向けセキュリティ問い合わせメカニズムが必要になる場合もあります。

調査に使用できるクラウド機能の詳細については、このドキュメントthe section called “付録 A: クラウド機能の定義”の「」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不可欠な要素です。ディレクティブコントロールと予防的コントロールが定義されると、関連する検出コントロールとレスポンシブコントロールを構築する必要があります。例えば、組織は 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ます。これは、明確に定義された特定のアクティビティにのみ使用する必要があります。 AWS 組織のサービスコントロールポリシー () 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SCP。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 トピックで実装された検出コントロールは、セキュリティオペレーションセンター () に警告しますSOC。レスポンシブコントロールには、適切なプレイブックSOCの選択、分析の実行、インシデントが解決されるまでの作業が含まれます。

セキュリティコントロールは、 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最もよく定義されます AWS。検出コントロールの重要性は、特定のワークロードのビジネス影響分析 (BIA) を確認することで設定されます。検出コントロールによって生成されたアラートは、入力時に処理されず、初期重要度に基づいて分析中に調整されます。初期重要度セットは優先順位付けに役立ちます。アラートが発生したコンテキストによって、その真の重要度が決まります。例えば、組織は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 GuardDuty として Amazon を使用します。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、悪意があると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す。このアラートはデフォルトで重要度が低く設定され、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のタイプのEC2インスタンス`p4d.24xlarge`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と判断されました。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く調整し、緊急性を高め、さらなるアクションを迅速化することを決定します。 GuardDuty 結果の重要度は変更できないことに注意してください。

Detective コントロールの実装

検出コントロールは、アラートが特定のイベントにどのように使用され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。技術的検出コントロールには主に 2 つの実装があります。

- 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す。顧客は、アラートの対象となるアクティビティの正確なパラメータを設定できます。これは確実です。

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付属しています。以下は、 を使用したルールベースおよび動作検出の例です GuardDuty。

- 結果`Exfiltration:IAMUser/AnomalousBehavior`が生成されると、「アカウントで異常なAPIリクエストが観察された」ことが通知されます。ドキュメントを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する異常なイベントを識別します」と示されています。これは、この検出結果が動作上の性質があることを示しています。
- 検出結果 について`Impact:S3/MaliciousIPCaller`、 GuardDuty は の Amazon S3 サービスからのAPI呼び出しを分析し CloudTrail、`SourceIPAddress`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ます。エントリに直接一致するものが見つかると、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は必ずしも可能ではないため、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。

人ベースの検出

これまで、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 つの重要な検出ソースは、顧客の組織内外の人物です。インサイダーは従業員または請負業者として定義でき、アウトサイダーはセキュリティ調査員、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、人ベースの検出には、E メール、チケット、メール、ニュース投稿、電話、対面によるやり取りなど、さまざまな形式があります。テクノロジーベースの検出通知はほぼリアルタイムで配信されることが期待できますが、人ベースの検出にはタイムライン上の期待はありません。セキュリティ文化は、セキュリティに対する多層防御アプローチのために、人ベースの検出メカニズムを組み込み、促進し、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駆動型のアラートを組み合わせることが重要です。さらに、セキュリティ上の問題に関するチケットを社内外から送信するメカニズムが必要です。人間はセキュリティイベントの最も貴重な情報源の 1 つになる可能性があるため、懸念をエスカレーションするプロセスを用意することが重要です。環境の脅威モデルを使用して、検出の構築を開始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のに役立ちます。最

後に、MITREATT&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、手法、手順 () を理解できますTTPs。MITRE ATT&CK フレームワークは、さまざまな検出メカニズムで共通言語としてを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、分析フェーズに必要なサポートコンポーネントの一部です。検出に使用されるのと同じログの多くは分析にも使用され、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。

アラートの影響を検証、範囲指定、評価する

分析フェーズでは、アラートの検証、範囲の定義、侵害の可能性の影響の評価を目的として、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。インシデント応答者は、さまざまなソースからのログエントリを探し、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、関係者が誤検出の可能性が低いと判断した場合に、関連するすべてのリソースがインベントリ化され、アラートの重要度が調整される場合です。
- 最後に、影響分析では、実際のビジネスの中断について詳しく説明します。

影響を受けるワークロードコンポーネントが特定されると、スコープ結果は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と相関し、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を開始できます。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) などのインシデントは、ビジネスプロセスをすぐに停止または低下させることはできませんが、後で結果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の強化

脅威インテリジェンスと組織コンテキストによる強化

分析の過程で、対象オブザーバビリティはアラートのコンテキスト化を強化するために強化を必要とします。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を統合して活用すると、セキュリティ上の検出結果の詳細を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と属性の所有権を割り当てるために使用されます。これらのツールは有料サービスとして利用でき、料金はかかりません。

Amazon Athena をログクエリツールとして採用しているお客様は、 Glue ジョブを活用して AWS 脅威インテリジェンス情報をテーブルとしてロードできます。脅威インテリジェンステーブルは、IP アドレスやドメイン名などのログ要素を関連付けるSQLクエリで使用でき、分析対象のデータを詳細に表示できます。

AWS は脅威インテリジェンスを顧客に直接提供しませんが、Amazon などのサービスは脅威インテリジェンスを利用して強化や結果の生成 GuardDuty を行います。独自の脅威インテリジェンス GuardDuty に基づいて、カスタム脅威リストを 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 ガバナンスの不可欠な部分です。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がログ内の脅威モデルから関心のあるパターンを照合し、通知の送信などの適切なアクションを実行します。分析フェーズでは、検出メカニズムを活用し、ログをクエリしてオブザーバビリティを強化してイベントのコンテキスト化を可能にす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、その基本的な形式で、リソースとアイデンティティで構成されます。例えば、アラート本文のアイデンティティまたはリソースがアラート発生時に実行したアクティビティ CloudTrail を AWS APIクエリする自動化を実装し、特定されたAPIアクティビティ`userAgent`の`eventSource`、、`eventNameSourceIPAddress`、 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で実行することで、応答者はトリアージ中の時間を節約し、追加のコンテキストを取得して、十分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、「アカウントメタデータで AWS Security Hub の検出結果を強化する方法」ブログ記事を参照してください。

フォレンジック証拠の収集と分析

フォレンジックは、このドキュメントの 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および分析するプロセスです。では AWS、ネットワークトラフィック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 — 文書化された正確なステップに従い、逸脱はありません。

- 繰り返し可能 – 同じアーティファクトに対して繰り返した場合、まったく同じ結果が生成されます。
- カスタム - 公開されており、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保管チェーンを維持することが重要です。オートメーションを使用し、このコレクションの自動ドキュメントを生成すると、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ことに加えて役立ちます。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いて、関連するアラートと影響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 (、Amazon S3 データイベントCloudTrail、VPCフローログ) 、データ (Amazon S3 メタデータとオブジェクト) 、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。

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。たとえば、 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、リソースタイプと意図した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、データベース自体copy/snapshot of the system running the database, creating a copy/snapshot全体の 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最大量のデータを取得して保持するために収集する必要がある特定のデータセットと、実行する必要がある収集の特定の順序があります。

具体的には、レスポンスが Amazon EC2インスタンスから最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. インスタンスの保護とタグを有効にする – 終了保護、停止するシャットダウン動作の設定 (終了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、および視覚的な表現と可能な応答オートメーションでの使用の両方に適切なタグの適用 (たとえば、 の名

前Statusと値を持つタグを適用する場合Quarantine、データのフォレンジック取得を実行してインスタンスを分離する) 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、(スナップショットが作成された時点から) 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ています。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/アーティファクトコレクションを実行するステップ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ているデータを除外する可能性があるため、システムから利用可能なデータを取得するために、適切なサードパーティーのオープンソースまたは商用ツールを使用してシステムメモリ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または運用上の理由がある場合にのみ、システムでライブレスポンスを通じてターゲットデータ収集 (disk/memory/logs) を実行します。これにより、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. インスタンスの廃止 – 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、アクセス許可が最小限またはまったくない事前構築済みインスタンスプロファイルを調整または適用します。
7. インスタンスを分離または格納する – インスタンスを現在および将来の接続を終了して防止することで、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、このドキュメントのthe section called “封じ込み”「」セクションを参照してください。
8. 応答者の選択 – 状況と目標に基づいて、次のいずれかを選択します。
   - システムを廃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の影響の可能性に対して最も効果的な緩和策を検証します。
   - モニタリング用に計測された隔離された環境でインスタンスの実行を続行します。

     標準アプローチとしては推奨されませんが、 状況がインスタンスの継続的な監視を必要とする場合 (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することを検討してください。 インスタンスAMIの を作成する 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ために、完全に分離され、インストルメンテーションで設定されているサンドボックス環境内の専用フォレンジックアカウントでインスタンスを再起動する (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 (および貴重な) 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または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不可欠です。

説明文を作成する

分析と調査中に、実行されたアクション、実行された分析、特定された情報を文書化して、後続のフェーズと最終的に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ある必要があり、インシデントの効果的な理解を検証し、正確なタイムラインを維持するために、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。また、コアインシデント対応チーム以外のユーザーを関与させる場合にも役立ちます。以下がその例です。

> マーケティング部門と営業部門が、機密データの公開を避けるために、暗号通貨での支払いを要求する身代金明細書を 2022 年 3 月 15 日に受け取りました。は、マーケティングおよび販売に属する Amazon RDS データベースが 2022 年 2 月 20 日にパブリックにアクセス可能であったSOCと判断しました。SOC クエリされたRDSアクセスログにより、IP アドレス 198.51.100.23 が 2022 年 2 月 20 日にウェブデベロッパーの 1 人であるメジャーメアリー*mm03434*に属する認証情報で使用されたと判断されました。SOC クエリされたVPCフローログと は、約 256MB のデータが同じ日付 (タイムスタンプ 2022-02-20T15:50+00Z) に同じ IP アドレスに出力されたと判断しました。オープンソースの脅威インテリジェンスによって、認証情報がパブリックリポジトリ のプレーンテキストで現在利用可能であるSOCと判断された *https[:]//example[.]com/majormary/rds-utils*。

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含む戦略のプロセスまたは実装です。

封じ込め戦略はさまざまな要因に依存し、封じ込めの戦術、タイミング、目的の適用に関して組織ごとに異なる場合があります。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と盗難
- 証拠の保存が必要
- サービスの可用性 (ネットワーク接続、外部当事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 (緊急回避策は 4 時間で削除、一時的な回避策は 2 週間で削除、永続的なソリューション)

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。
- 技術とアクセスの封じ込め — 影響を受けるリソースへの不正アクセスを防ぐために、アクセスを削除します。
- 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。

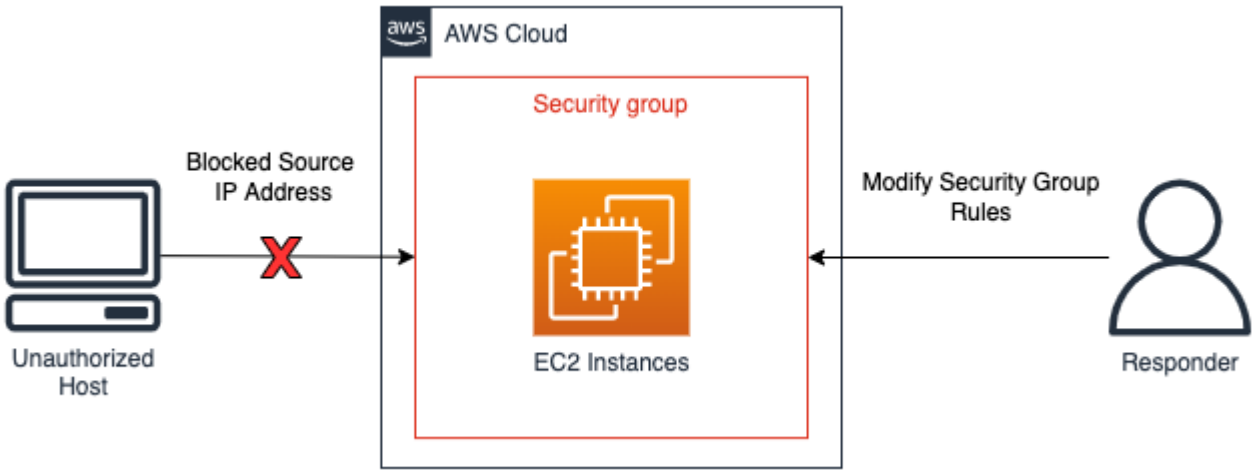
ソースの封じ込め

ソースの封じ込めとは、特定の送信元 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できないように、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と適用です。 AWS サービスを使用したソース封じ込めの例は、ここで強調表示されています。

- 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のに役立ちます。セキュリティグループの変更に伴って既存の追跡対象接続が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によって効果的にブロックされます (追跡対象接続と追跡対象外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。ポリシーは、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機能を作成します。バケットポリシーの詳細については、Amazon S3コンソールを使用したバケットポリシーの追加」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 ACLs) 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 AWS WAF するように で設定できます。IP アドレスまたはネットワーク範囲を に設定されている IP セットに追加し AWS WAF、 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、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されているように、セキュリティグループが変更されても、既存の追跡対象接続はシャットダウンされません。



ソース格納の例

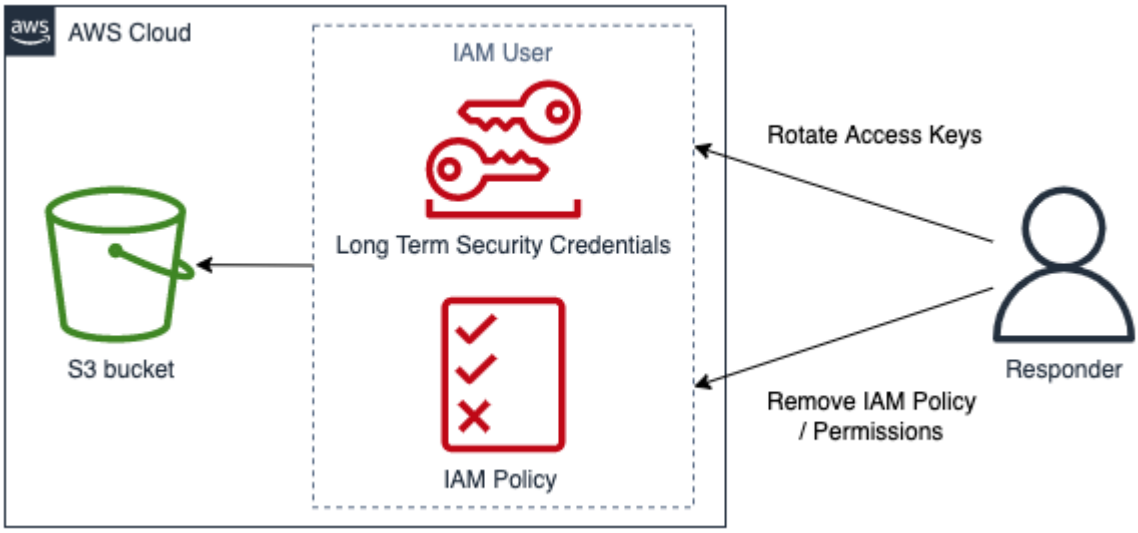
テクニックとアクセスの封じ込め

リソースにアクセスできる関数と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が含まれます。また、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テクニックとアクセス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、アクティブなセキュリティイベント中に、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必要がある場合があります。この場合、含まれるプリンIAM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含めることができます。これは IAMサービスで行われ、 AWS Management Console、 AWS CLI、または を使用して適用できます AWS SDK。

- キーの取り消し – IAM アクセスキーは、プリンIAM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、 プレフィックスで始まる長期的な静的認証情報です AKIA (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)。アクセスキーが侵害された IAMプリンシパルのIAMアクセスを含めるには、アクセスキーを非アクティブ化または削除できます。次の点に注意してください。
  - アクセスキーは、非アクティブ化された後に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できなくなります。
- 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、組織によってリソースへのアクセス AWS を制御し、 プレフィックスで始めるために使用できます ASIA (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、有効期間が限られているため、ローテーションまたは明示的に取り消す必要はありません。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を含む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、 内の IAMサービスを使用して AWS Management Console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、この執筆時点では、 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 AWS Management Console。一時的なセキュリティ認証情報を作成した権限のないユーザーによってユーザーのIAMアクセスキーが侵害されたセキュリティイベントの場合、次の 2 つの方法で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問題時間に基づいてアクセス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許可を無効にする」の「特定の時間前に発行された一時的なセキュリティ認証情報へのアクセスを拒否する」セクションを参照してください)。 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_control-access_disable-perms.html
  - 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 () 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XSS。 AWS WAF AWS WAF は、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一致および拒否するように設定できます。

技術とアクセスの封じ込めの例を次の図に示します。インシデント応答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。



テクニックとアクセスの封じ込めの例

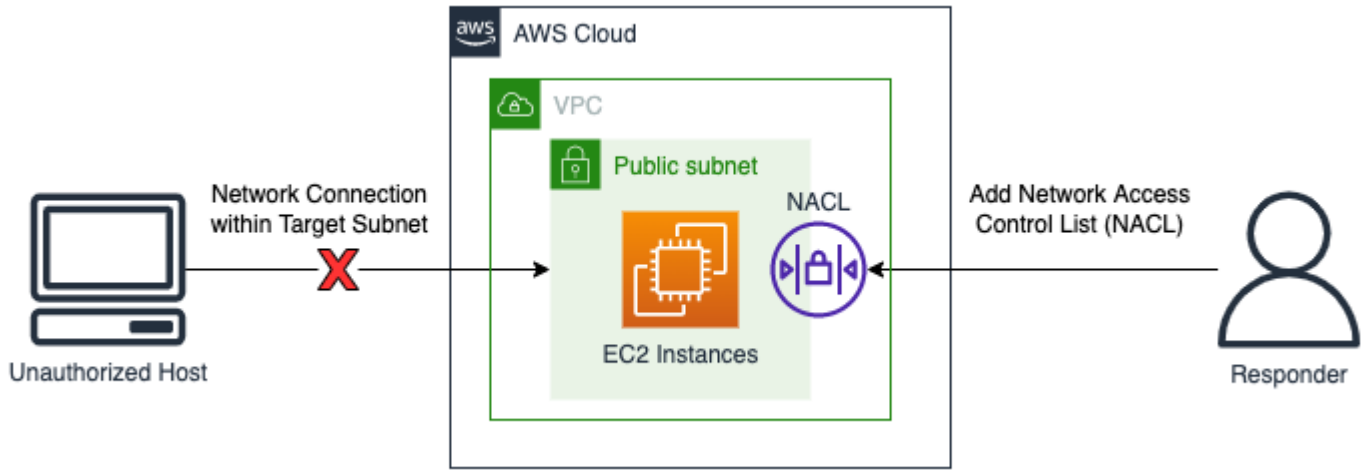
送信先コンテナ

送信先コンテナは、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するアプリケーションです。場合によっては、送信先の封じ込めには、正当なリソースが可用性のためにレプリケートされていることを確認するための回復力の形式も含まれます。分離と封じ込めのために、これらの形式の回復力からリソースを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コンテナの例を次に示します。

- ネットワーク ACLs – AWS リソースを含むサブネットに設定されているネットワーク ACLs (ネットワーク ACLs) に拒否ルールを追加することができます。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。ネットワーク内にリストされているルールACLはトップダウンの順序で処理されるため、既存のネットワークの最初のルールは、対象の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ACL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してまったく新しいネットワークを作成し、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 を使用してサブネットにアクセスできないACLようにすることもできますACL。

- 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、不正使用の影響を抑えるのに効果的です。リソースをシャットダウンすると、ビジネスニーズに対する正当なアクセスが妨げられ、変動するフォレンジックデータの取得も妨げられるため、これは意図的な決定であり、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 VPCs – 分離を使用すると、正当なトラフィック (ウイルス対策 (AV)、インターネットへのアクセスを必要とするEDRソリューション、外部マネジメントコンソールなど) へのアクセスを提供しながら、リソースを効果的に封じ込めVPCsることができます。分離VPCsは、有効な IP アドレスとポートを許可するようにセキュリティイベントの前に事前設定でき、アクティブなセキュリティイベントVPC中にターゲットリソースをすぐにこの分離に移動してリソースを格納できます。同時に、インシデント対応の後続のフェーズで、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は、使用VPCする前に新しい分離でシャットダウンして再起動する必要があるVPCことです。既存のEC2インスタンスを別のVPCアベイラビリティーゾーン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、「Amazon EC2インスタンスを別のサブネット、アベイラビリティーゾーン、または に移動する方法」で説明されているステップに従いますVPC。
- Auto Scaling グループとロードバランサー – AWS Auto Scaling グループとロードバランサーにアタッチされたリソースは、送信先の格納手順の一部として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 Management Console、、 AWS CLI、およびを使用して実行できます AWS SDK。

宛先の封じ込めの例を次の図に示し、インシデント対応アナリストが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、ACLサブネットにネットワークを追加します。



送信先コンテナの例

概要

封じ込めはインシデント対応プロセスの 1 ステップであり、手動または自動で行うことができます。全体的な封じ込め戦略は、組織のセキュリティポリシーとビジネスニーズに合致し、根絶と復旧の前に悪影響ができるだけ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連して、アカウントを既知の安全な状態に戻すために不審なリソースや不正なリソースを削除することです。根絶戦略は、組織のビジネス要件に応じて、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、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、および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発見された場合 (新しいマルウェアの侵入など)、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、これは、利用可能な口グまたは CloudWatch Logs や Amazon などの自動ツールで検出および分析されたイベントによってさらに絞り込むことができます GuardDuty。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実行すべき修復を決定する基礎となる必要があります。

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決定することです。これは、使用可能な口グデータソース、リソース、および自動ツールの分析によって実現されます。

- アカウントの ID IAM 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アクセスや変更を特定します。
- 不正なリソースまたはIAMユーザーの作成を特定します。
- 不正な変更がある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、リソースが削除されたり復元されたりした場合にビジネスへの影響を判断する必要があります。たとえば、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、影響を受けたサーバー

を削除するAMI前に、検証済みの安全なバックアップからリソースを復元するか、クリーン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。

ビジネスインパクト分析を終了したら、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引き続き実行する機能を削除します。
- 不正である可能性のあるIAMユーザー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。

- マルウェアを攻撃する場合、 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 には、マルウェアの分析や削除のためのネイティブツールはありません。ただし、Amazon の GuardDuty Malware モジュールを使用している場合はEBS、提供された検出結果に対してレコメンデーションが利用できる場合があります。

特定された影響を受けるリソースを根絶したら、 はアカウントのセキュリティレビューを実行する AWS ことをお勧めします。これは、 AWS Config ルール、Prowler や などのオープンソースソリューション ScoutSuite、または他のベンダーを通じて実行できます。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 1 ステップであり、インシデントや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。全体的な戦略は、組織のセキュリティポリシーやビジネスニーズに沿ったものであり、不適切なリソースや設定が削除されると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、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、少なくとも以下を判断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、次の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のシステムの復元。
  - システムに復元する前に、バックアップが評価され、メンテナンスが存在しないことを確認し、セキュリティイベントの回復を防ぎます。

    バックアップメカニズムが適切に動作し、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ために、ディザスタリカバリテストの一環としてバックアップを定期的に評価する必要があります。
  - 可能であれば、根本原因分析の一部として識別された最初のイベントタイムスタンプより前のからのバックアップを使用します。
- オートメーション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 AWS 。
- 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。

  これを行うときは、細心の注意が必要です。復旧するファイルが安全で、インシデントの影響を受けないことが確実に確認されている必要があります。
- パッチのインストール。
- パスワードの変更。
  - これには、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、プリンシIAM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。

- ネットワーク境界セキュリティ (ファイアウォールルールセット、境界ルーターアクセスコントロールリスト) の強化。

リソースが復旧したら、学んだ教訓をキャプチャし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。

つまり、既知の安全なオペレーションへの復帰を容易にする復旧プロセスを実装することが不可欠です。復旧には長い時間がかかる場合があり、ビジネスへの影響と再感染のリスクのバランスをとるために、封じ込め戦略との密接な連携が必要です。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	テクニックと方法論
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であるかどうかを判断し、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 • Automation
コンテナ	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 • テクニックとアクセスの封じ込め • 送信先コンテナ

[Phase] (フェーズ)	目標	テクニックと方法論
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 • 不正なリソースの削除 • マルウェアの削除 • セキュリティスキャン
復旧	システムを既知の正常な状態に復元し、これらのシステムをモニタリングして、脅威が戻ら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 • ゼロから再構築されたシステム • 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、潜在的なセキュリティインシデントを効果的に検出、対応、調査し、潜在的な脆弱性を減らし、対応までの時間を短縮し、安全な運用に戻る能力を向上させるために、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実装すると、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、同じミス、露出、設定ミスの繰り返しを回避し、セキュリティ体制を改善するだけでなく、予防可能な状況で失われ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
- 改善を効果的に追跡して実装するにはどうすればよいですか？

これらの大まかな結果に加えて、適切な質問をして、プロセスから最大の価値 (実用的な改善につながる情報) を引き出すことが重要です。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。
  - 既存のツールにより、インシデントの効果的な調査 (検索/分析) が可能になりましたか？
- 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 を実装してテストmonitoring/preventative controls/processするスケジュールはどのくらいですか？

このリストはすべてを網羅しているわけではありません。組織やビジネスのニーズを特定し、インシデントから最も効果的に学習し、セキュリティ体制を継続的に改善するために分析する方法を特定するための出発点となる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、インシデント対応能力を効果的に測定、評価、改善するために必要です。メトリクスがないと、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リファレンスはありません。インシデント対応に共通するメトリクスがいくつかあり、運用上の優秀性の実現に向けた期待とリファレンスを確立したいと考えている組織にとって、良い出発点となります。

検出の平均時間

検出の平均時間は、セキュリティインシデントの可能性を発見するのにかかる平均時間です。具体的には、最初の侵害の指標が出現してから、最初の識別またはアラートが発生するまでの時間です。

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 環境内に残らないことを確認する上で重要です。

平均検出時間が長くなるほど、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の、追加の、またはより効果的なアラートとメカニズムを構築する必要性が高くなります。平均検出時間が短いほど、検出とアラートのメカニズムが機能しやすくなります。

確認までの平均時間

承認までの平均時間は、セキュリティインシデントの可能性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、アラートの生成と、 SOCまたはインシデント対応スタッフのメンバーとの間の時間であり、処理するアラートを識別して優先順位を付けます。

このメトリクスを使用して、チームがアラートをどの程度処理し、優先順位付けし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て優先順位を付けることができない場合、対応が遅れ、効果がありません。

平均確認時間が高いほど、対応のために考えられるセキュリティインシデントを迅速に確認して優先順位を付けるために、チームが適切なリソースを提供し、トレーニングされていることを検証する必要性が高くなります。承認までの平均時間が短いほど、チームがセキュリティアラートにうまく対応でき、効果的に準備ができ、優先順位を付けることができることを示します。

平均応答時間

平均応答時間は、セキュリティインシデントの可能性に対する最初の応答を開始す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、対応のために実行された最初のアクションまでの時間です。これは平均確認時間に似ていますが、状況の単純な認識または確認と比較して、特定の応答アクション (システムデータの取得、システムを含むなど) の測定です。

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鍵です。このドキュメントの the section called “準備”セクションを参照してください。

平均応答時間が長いほど、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。平均応答時間が短いほど、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、安全な運用に戻るための必要な対応アクションを実行しやすくなります。

含める平均時間

封じ込める平均時間は、セキュリティインシデントの可能性を封じ込めるのにかかる平均時間です。具体的には、セキュリティインシデントの可能性を最初に警告または検出してから、攻撃者または侵害されたシステムがさらなる害を行うことを効果的に防ぐ対応アクションが完了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。セキュリティインシデントの可能性を迅速かつ効果的に封じ込められないと、影響、範囲、およびさらなる侵害の可能性にさらされます。

封じ込める平均時間が長いほど、経験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くなります。封じ込める平均時間が短いほど、チームはビジネスへの影響、範囲、リスクを軽減するために特定された脅威を軽減し、封じ込めるために必要な対策を理解し、採用しやすくなります。

平均復旧時間

平均復旧時間は、セキュリティインシデントから安全なオペレーションを完全に返す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が発見されてから、そのインシデントの影響を受けることなく、通常かつ安全に事業が再開されるまでの時間です。

このメトリクスを使用して、セキュリティインシデントの発生後に、チームがシステム、アカウント、環境を安全な運用に戻すうえでの効率性を追跡できます。安全なオペレーションに迅速かつ効果的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、ビジネスとそのオペレーションへの影響と費用も増大する可能性があります。

平均復旧時間が長くなるほど、運用やビジネスに対するセキュリティインシデントの影響を最小限に抑えるための適切なメカニズム (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) をチームや環境に備える必要性が増します。平均復旧時間が短いほど、チームが運用やビジネスに対するセキュリティインシデントの影響を最小限に抑えるうえでより効果的になります。

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できる平均時間です。これは、攻撃者がシステムまたは環境へのアクセスを取得した最初の時点から始まる期間を除いて、平均保存期間に似ています。最初のアラートまたは検出より前である可能性があります。

このメトリクスを使用して、攻撃者や脅威が環境に影響を与える時間、アクセス、機会を減らすために、連携しているシステムとメカニズムの数を追跡できます。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くなるほど、インシデント対応プロセスのどの部分を改善して、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ことができるかを特定する必要性が高くなります。攻撃者のドウェル時間が短いほど、チームは環境内で脅威や攻撃者が持つ時間と機会を最小限に抑えることができ、最終的に運用やビジネスへのリスクと影響が軽減されます。

メトリクスの概要

インシデント対応のメトリクスを確立および追跡することで、インシデント対応機能を効果的に測定、評価、改善できます。これを実現するには、このセクションで強調表示されている一般的なインシデント対応メトリクスが多数あります。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
検出の平均時間	セキュリティインシデントの可能性を発見するのにかかる平均時間
確認までの平均時間	セキュリティインシデントの可能性を認識 (および優先順位付け) するのにかかる平均時間
平均応答時間	セキュリティインシデントの可能性に対する最初の対応を開始するのにかかる平均時間
含める平均時間	セキュリティインシデントの可能性を封じ込めるのにかかる平均時間
平均復旧時間	潜在的なセキュリティインシデントから安全なオペレーションを完全に返すのにかかる平均時間
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

侵害の指標を使用する (IOCs)

侵害のインジケータ (IOC) は、悪意のあるアクティビティやセキュリティインシデントを (高いレベルの信頼度で) 識別できるネットワーク、システム、または環境で観察されるアーティファクトです。 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、ファイル名やハッシュ、ログファイルエントリ、レジストリエントリなどのシステムまたはホストレベルのアーティファクトなど、さまざまな形式で存在IOCsできます。また、システム上の特定の項目やアーティファクト (特定のファイルまたは一連のファイルやレジストリ項目) の存在、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が実行される) 、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で送受信される異常なトラフィック) など、項目やアクティビティの組み合わせである場合もあります。

インシデント対応プログラムを反復的に改善する際には、検出とアラートを継続的に構築して改善し、調査のスピードと有効性を向上させるメカニズムIOCsとして、収集、管理、活用するフレームワークを実装する必要があります。まず、 の収集と管理IOCs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ができます。プロセスの標準部分IOCsとして事前に特定、収集、保存することで、データのリポジトリを (より包括的な脅威インテリジェンスプログラムの一部として) 構築できます。このリポジトリは、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出現場所と出現日時の特定、 のマッチングを含む調査の過去の実施状況に関するドキュメントの作成と参照IOCsなどに使用できます。

継続的な教育とトレーニング

教育とトレーニングは進化し続けており、意図的に取り組み、維持する必要があります。チームがテクノロジーの進化状況や脅威の状況に見合った意識、知識、能力を維持していることを検証するには、さまざまなメカニズムがあります。

1 つのメカニズムは、継続的な教育をチームの目標と運用の標準として採用することです。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利害関係者は、内部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されている必要があります AWS。ただし、教育は「1 回限り」の労力ではありません。対応の有効性と効率性を向上させるために活用できる最新の技術の進歩、更新、改善、調査と分析の改善に活用できるデータの追加や更新について、チームが認識していることを確認するために、教育を継続的に進める必要があります。

もう 1 つのメカニズムは、シミュレーションが定期的に (四半期ごとなど) 実行され、ビジネスの特定の成果に焦点を当てていることを確認することです。このドキュメントの the section called “定期的な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。

最初の机上演習を実行することは、改善のための初期ベースラインを生成する優れた方法ですが、継続的なテストは、継続的な改善と、運用の現在の状態と up-to-date正確な反映を維持する上で重要です。最新かつ最も重要なセキュリティ状況と、対応のために最も重要な機能や最新の機能に対してテストし、教訓を教育、運用、プロセス/手順に組み込んで、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を確認できます。

結論

クラウドジャーニーを続ける際には、 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です。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、応答速度を向上させる自動化

機能の導入時に小規模から始めて反復処理できるため、セキュリティイベントが発生したときの準備が整います。

寄稿者

このドキュメントの現在および過去の寄稿者には以下が含まれます。

- Amazon Web Services McAbee、Senior Security Solutions Architect、Anna
- Amazon Web Services、Senior Security Consultant、Freddy Kasprzykowski
- Amazon Web Services、シニアセキュリティエンジニア、Jason Hurst
- Amazon Web Services、Principal Security Consultant、Jonathon Poling
- Amazon Web Services、セキュリティソリューションアーキテクチャ、シニアマネージャー、Josh Du Lac
- Amazon Web Services、Principal Security Engineer、Paco Hope
- Amazon Web Services、シニアセキュリティエンジニア、Ryan Tick
- Amazon Web Services、シニアセキュリティエンジニア、Steve de Vera

付録 A: クラウド機能の定義

AWS 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、ネイティブの検出、予防、応答機能を提供し、その他を使用してカスタムセキュリティソリューションを設計できます。このセクションには、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が含まれています。

トピック

および イベントの口グ記録

AWS CloudTrail – AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にする AWS CloudTrail サービス。を使用すると CloudTrail、 AWS のサービス間のアクショ

ンに関連するアカウントアクティビティを口グに記録し、継続的にモニタリングし、保持できます。 CloudTrail は、 AWS Management Console、、コマンドラインツール、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 AWS SDKs、 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、リソース変更の追跡、および troubleshooting. CloudTrail logs の 2 つの異なるタイプの AWS APIアクションが簡素化されます。

- 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ます) は、アカウントの AWS 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 バケットの作成や口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ます) は、アカウントの AWS リソース上またはリソース内で実行される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 (、`DeleteObject`、 `PutObject`APIオペレーションなど) や Lambda `GetObject`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 リソースの設定を評価、監査、評価できるようにするサービスです。 AWS Config は AWS 、リソースの設定を継続的にモニタリングおよび記録し、記録した設定を目的の設定と照らし合わせて評価を自動化できます。を使用すると AWS Config、お客様は AWS リソース間の設定や関係の変更を手動または自動で確認し、詳細なリソース設定履歴を確認し、お客様のガイドラインで指定されている設定に対する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、運用トラブルシューティングが簡素化されます。

Amazon EventBridge – Amazon EventBridge は、 AWS リソースの変更、または によってAPI呼び出しが発行されたタイミングを記述するシステムイベントのほぼリアルタイムのストリームを提供します AWS CloudTrail。すばやく設定できる簡単なルールを使用すると、イベントを照合して 1 つ以上のターゲット関数または streams にルーティングできます。 EventBridge は、運用上の変更が発生したときにその変更を認識します。 は、これらの運用上の変更に応答し、必要に応じて、応答するメッセージを送信し、関数をアクティブ化し、変更を行い、状態情報を収集することで、修正措置を講じる EventBridge ことができます。Amazon などの一部のセキュリティサービスは、 EventBridge イベント形式で出力 GuardDutyを生成します。多くのセキュリティサービスでは、出力を Amazon S3 に送信するオプションも用意されています。

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 ログとは別のログです。アクセスログレコードはベストエフォートベースで配信さ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 Amazon CloudWatch Logs を使用して、Logs CloudWatch 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、およびその他のソースから発信されるログファイルをモニタリング、保存、およびアクセスできます。 CloudWatch ログは 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。その後、お客様は ログから関連する CloudWatch ログデータを取得できます。

Amazon VPC Flow Logs – VPCフローログを使用すると、 のネットワークインターフェイスとの間で送受信される IP トラフィックに関する情報をキャプチャできますVPCs。フローログを有効にすると、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、過度に制限された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モニタリング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。フローVPCログ記録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します。

AWS WAF ログ — 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 AWS WAF 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、サードパーティー製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) 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VPC。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 に存在してDNSクエリを実行するVPCと、この機能によってログに記録されます。これにより、アプリケーションの動作を詳しく調べて理解することができます。

その他の AWS ログ – 新しいログ記録およびモニタリング機能を持つお客様向けに、 AWS サービス機能を継続的にリリースします。各 AWS サービスで使用できる機能については、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 Hub – AWS Security Hub AWS アカウント全体の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 は、Amazon、Amazon Inspector、Amazon Macie GuardDuty、 AWS Partner ソリューションなどの AWS のサービスからの結果を集約、整理、優先順位付けします。結果は、実用的なグラフとテーブルを含む統合ダッシュ

ボードに視覚的に要約されます。また、組織が従う AWS 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、悪意のある動作や不正な動作を継続的にモニタリングし、アカウント AWS や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。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の侵害、または悪意のある人物による偵察の可能性を示す異常なAPI呼び出しや不正なデプロイの可能性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およびワークロード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疑わしい不正行為者を特定します。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 イベント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、アラートが実行可能になり、既存のイベント管理およびワークフローシステムに統合が簡単になります。

GuardDuty には、特定の サービスによる脅威をモニタリングするための 2 つのアドオンも用意されています。Amazon GuardDuty for Amazon S3 Protection と Amazon GuardDuty for Amazon EKS Protection です。Amazon S3 保護により、 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て、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ます。Kubernetes 保護により GuardDuty 、 は Amazon 内の Kubernetes クラスターの疑わしいアクティビティや潜在的な侵害を検出できますEKS。

Amazon Macie – Amazon Macie は AI を活用したセキュリティサービスであり、 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、データ損失を防ぐのに役立ちます AWS。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、このデータが保存されている場所と組織内でどのように使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したときに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、 によって記録された関連リソースの設定変更に対して評価されます AWS Config。ダッシュボードのリソースの設定に対してルールを評価した結果を確認できます。 AWS Config ルールを使用すると、設定の観点から全体的なコンプライアンスとリスクのステータスを評価し、時間の経過に伴うコンプライアンスの傾向を表示し、リソースがルールに準拠していない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。 は、

AWS 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 Trusted Advisor を提供します。 CloudWatch イベント統合を含むすべての Trusted Advisor チェックセットは、ビジネス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、 リソースと実行するアプリケーションのモニタリングサービス AWS クラウド です AWS。 CloudWatch を使用して、メトリクスの収集と追跡、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 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、アプリケーションとサービスによって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ログファイルをモニタリングできます。Amazon を使用すると CloudWatch 、リソースの使用率、アプリケーションのパフォーマンス、運用状態をシステム全体で可視化できます。これらのインサイトを使用して、それに応じて対応し、アプリケーションをスムーズに実行し続けることができます。

Amazon Inspector – Amazon Inspector は、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のに役立つ自動化されたセキュリティ評価サービスです AWS。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。評価を実行すると、Amazon Inspector は重要度のレベルによって優先順位が付けられたセキュリティ検出結果の詳細なリストを生成します。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 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API。

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フローログなどの複数のデータソースからの何兆ものイベントを分析し CloudTrail GuardDuty、リソース、ユーザー、およびそれらの間のインタラクションを経時的に統合したインタラクティブなビューを自動的に作成します。この統合ビューを使用すると、すべての詳細とコンテキストを 1 か所で視覚化して、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ドリルダウンして、根本原因をすばやく特定できます。

Automation

AWS Lambda – AWS Lambda は、イベントに応じてコードを実行し、基盤となるコンピューティングリソースを自動的に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、カスタムロジックで他の AWS サービスを拡張したり、 AWS 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サービスを作成したりできます。Lambda は、高可用性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、サーバーとオペレーティングシステムのメンテナンス、容量のプロビジョニン

グと自動スケーリング、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 ビジュアル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簡単に調整できます。Step Functions には、アプリケーションのコンポーネントを一連のステップとして配置および視覚化するためのグラフィカルコンソールが用意されています。これにより、複数ステップのアプリケーションを簡単に構築して実行できます。Step Functions は、各ステップを自動的に開始して追跡し、エラーが発生したときに再試行するため、アプリケーションは想定どおりに順番に実行されます。

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、より迅速に革新できます。 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 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オーケストレーションにも使用できますECS。

AWS Systems Manager – AWS Systems Manager インフラストラクチャの可視性と制御を提供します AWS。Systems Manager には、複数の AWS サービスからの運用データを表示できる統一されたユーザーインターフェイスが用意されており、 AWS リソース全体の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の運用データを表示し、リソースのグループを操作できます。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、どこからでも任意の量のデータを保存および取得するために構築されたオブジェクトストレージです。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にデータを管理するために使用する方法を柔軟に利用できます。Amazon S3 には query-in-place、Amazon S3 に保管中のデータに対して強力な分析を直接実行できる機能が用意されています。Amazon S3 は、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、およびその他の AWS サービスの最大のコミュニティの 1 つから統合され、高度にサポートされているクラウドストレージサービスです。

Amazon S3 Glacier – Amazon S3 Glacier は、データのアーカイブと長期バックアップのための、安全で耐久性があり、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% の耐久性を実現するように設計されており、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。S3 Glacier には query-in-place、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る機能が用意されています。コストを低く抑えながら、さまざまな取り出しニーズに適した状態を維持するために、S3 Glacier には、数分から数時間までのアーカイブへのアクセスに 3 つのオプションが用意されています。

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網羅的なリストではありません。 AWS は継続的に新機能を追加しています。詳細については、「 および AWS クラウドセキュリティの最新情報 AWS」ページを確認することをお勧めします。がネイティブクラウドサービスとして AWS 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。

Amazon や AWS CloudTrail Amazon Macie など GuardDuty、アカウント内でセキュリティサービスの基本セットを有効にすることをお勧めしますが、最終的にはこれらの機能を拡張してログアセットから追加の価値を引き出すことをお勧めします。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、利用可能なパートナーツールは多数あります。ログを検索するために独自のクエリを記述することもできます。 AWS が提供するマネージドサービスが多数あるため、これはこれまで以上に簡単になりました。Amazon Athena、Amazon OpenSearch Service、Amazon、Amazon Machine Learning、 QuickSightAmazon など、このホワイトペーパーの範囲外の調査に役立つ多くの追加 AWS サービスがありますEMR。 Amazon Machine Learning

付録 B: AWS インシデントレスポンスリソース

AWS は、インシデント対応機能の開発を支援するリソースを公開します。ほとんどのコード例と手順は、外部 GitHub パブリックリポジトリにあります AWS 。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例です。
- 独自のインシデント対応プレイブックを作成する - このワークショップは、インシデント対応プレイブックの作成に慣れるのに役立つように設計されています AWS。

- インシデント対応プレイブックのサンプル - AWS 顧客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。
- Jupyter プレイブックと CloudTrail Lake を使用して AWS インシデント対応ランブックを構築する - このワークショップでは、Jupyter ノートブックと CloudTrail Lake を使用して、環境 AWS のインシデント対応プレイブックを構築する方法について説明します。

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、調査、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。自動化ステップの運用、アーティファクトの保存、フォレンジック環境の作成を行うためのアカウントの分離を提供します。
- Amazon 用自動フォレンジックオーケストレーター EC2 – 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。
- でフォレンジックディスク収集を自動化する方法 AWS – 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、分析のためにディスクの証拠をキャプチャする自動化ワークフローをセットアップする方法について詳しく説明します。ソリューションをデプロイするための AWS CloudFormation テンプレートも含まれています。

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ており、(b) 通知なしに変更される可能性がある現在の AWS 製品提供および慣行を表し、(c) AWS およびその関連会社、サプライヤー、または許諾者からのいかなる約束または保証も作成しません。 AWS 製品またはサービスは、明示または黙示を問わず、いかなる種類の保証、表明、または条件もなしに、現状のままで提供されます。お客様 AWS に対する の責任および責任は AWS 契約によって管理され、本書は AWS とお客様との間の契約の一部でも変更ものでもありません。

ドキュメント履歴

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からの更新。	stackset テンプレートに https://docs.aws.amazon.com/security-ir/latest/userguide/setupmonitoring-and-investigation-workflows.html を更新しました。 エントリ triage.security-ir.com を triage.security-ir.amazonaws.com に修正しました。 on AWSSupport. https://docs.aws.amazon.com/security-ir/latest/userguide/containhtml の -ContainEC2Reversible の追跡された接続ノートを追加しました。 https://docs.aws.amazon.com/security-ir/latest/userguide/managing関連アカウント.html のリンク切れを修正しました。 メンバーシップアカウントの定義が at https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html に追加されました。 管理アカウントの https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/	2024 年 12 月 20 日

変更	説明	日付
	using-service-linked-roles.html に明確化ノート AWS Organizations を追加しました。	

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からの更新。	テキスト AWS AWS 内の重複した複数の を削除しました。 https://docs.aws.amazon.com/security-ir/latest/userguide/sir_tagging.html and https://docs.aws.amazon.com/security-ir/latest/userguide/servicename-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。Replaced AWSSupport-ContainEC2Reversible を Contain AWSSupportに置き換えましたEC2Instance。C AWSSupportontainIAMReversible を AWSSupportC に置き換えましたontainIAMPrincipal。Replaced AWSSupport-ContainS3Reversible with AWSSupport-ContainS3Resource。 https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/issues.html のフォーマットを更新 サポートチケットCIRTで に連絡するように顧客に指示す	2024 年 12 月 10 日

変更	説明	日付
	る場合、 https://docs.aws.amazon.com/security-ir/latest/userguide/understand-response-teams-and-support.html はサポートフォームで選択するためのオプションを提供するようになりました。 Events を削除 CloudWatch し、 EventBridge on https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html に置き換えました。 文法は on https://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html を更新します。 公開日を https://docs.aws.amazon.com/security-ir/latest/userguide/securityincident-response-guide.html から削除し、この表の更新に置き換えました。	
更新: AWS 管理ポリシーとサービスにリンクされたロール。	管理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 でのサービス起動の初期サービスドキュメント	2024 年 12 月 1 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。