AWS テクニカルガイド

AWS セキュリティインシデント対応ガイド

AWS セキュリティインシデント対応ガイド: AWS テクニカルガイド

Table of Contents

AWS セキュリティインシデント対応ガイド

発行日: 2020 年 11 月 23 日 (改訂履歴)

このガイドでは、お客様の AWS クラウド環境におけるセキュリティインシデント対応の基礎について概要を提供します。クラウドセキュリティとインシデント対応の概念に注目し、お客様がセキュリティ問題に対応する際に利用できるクラウドの機能、サービス、メカニズムについて説明します。

このホワイトペーパーは、技術的な役割の従事者を対象としています。読者は、情報セキュリティの一般的な原則に精通しており、現在のオンプレミス環境でのインシデント対応の基本を理解し、クラウドサービスについてある程度詳しいことを前提としています。

はじめに

セキュリティは AWS の最優先事項です。AWS のお客様は、セキュリティを最も重視する組織の要件を満たす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の恩恵を受けることができます。AWS クラウドには、責任共有モデルがあります。AWS はクラウドのセキュリティを管理します。お客様はクラウド内のセキュリティに責任を負います。これは、お客様が実装することを選択したセキュリティのコントロールをお客様が保持することを意味します。セキュリティ目標の達成に役立つ数百ものツールやサービスにアクセスできます。これらの機能を使用して、クラウド内で実行するアプリケーションの目的に合ったセキュリティのベースラインを確立できます。

ベースラインからの逸脱が発生した場合 (設定ミスなどで)、対応して調査する必要があります。適切に対応するには、セキュリティ問題が発生する前に、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、お客様のクラウドチームを準備、教育、トレーニングするために考慮すべき課題を理解する必要があります。どのコントロールと機能を使用できるかを見極め、潜在的な問題の一般的な解決例を確認し、オートメーションを活用して対応を迅速化するために利用できる修復方法を特定することが重要です。

セキュリティインシデント対応は複雑化する場合があるため、以下をお勧めします。まずは、小さく始めて、ランブックを開発します。さらに基本的な機能を活用し、インシデント対応メカニズムの初期ライブラリを作成して、反復しながら改善します。この最初の作業には、法務部門や、セキュリティに関与していないチームも含める必要があります。これにより、インシデント対応 (IR) や選択した方法が企業の目標に及ぼす影響をよりよく理解できます。

トピック

開始する前に

このドキュメントに加えて、セキュリティ、アイデンティティ、コンプライアンスに関するベストプラクティスと AWS クラウド導入フレームワーク (CAF) のセキュリティパースペクティブに関するホワイトペーパーを参照する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署間の調整に役立つガイダンスを提供します。CAF ガイダンスは、クラウドベースの IT システムの実装に関連するいくつかの重点分野に分かれており、これを AWS ではパースペクティブと呼んでいます。セキュリティパースペクティブでは、複数のワークストリームにわたってセキュリティ

プログラムを実装する方法について説明しています。これらのワークストリームの 1 つがインシデント対応に特化しています。本書では、お客様がこのワークストリームで適切なメカニズムを評価して実装するために役立つ AWS の経験について詳しく紹介します。

AWS CAF のセキュリティパースペクティブ

セキュリティパースペクティブには次の 4 つのコンポーネントがあります。

- ディレクティブコントロールは、ガバナンス、リスク、コンプライアンスの各モデルを設定します。このモデル内で環境を運用します。
- 予防コントロールは、ワークロードを保護し、脅威および脆弱性を軽減します。
- 検出コントロールは、AWS でのデプロイの運用を完全に可視化および透明化します。
- 対応コントロールは、セキュリティベースラインからの潜在的な逸脱を修正します。

IR は、通常、対応コントロールコンポーネントに表示されますが、他のコンポーネントにも依存し、これらから影響を受けます。例えば、セキュリティのディレクティブコントロールと予防コントロールは、ベースラインの確立を支援するため、このベースラインからの逸脱をモニタリングして調査できます。このアプローチは、ノイズを除去するだけでなく、防御的なセキュリティ設計にも貢献します。

インシデント対応の基礎

組織内のすべての AWS ユーザーは、セキュリティインシデント対応プロセスの基本を理解している必要があり、セキュリティスタッフはセキュリティ問題への対応方法を深く理解している必要があります。クラウドインシデント対応プログラムでは、セキュリティイベントを処理する前に、経験と教育が不可欠です。クラウド内でインシデント対応プログラムを成功させる基礎は、教育、準備、シミュレーション、反復です。

これらの各側面を理解するために、以下の説明を参考にしてください。

- 教育。クラウドテクノロジーとそれを組織でどのように利用するかについて、セキュリティオペレーションおよびインシデント対応スタッフを教育します。
- 準備。クラウド内のインシデントを検出して対応できるように、インシデント対応チームの準備を整えます。この準備のために、検出機能を有効にし、必要なツールやクラウドサービスへの適切なアクセスを確保します。さらに、信頼性の高い一貫した対応を保証するために、手動と自動の両方で必要なランブックを準備します。他のチームと協力して、予想される基本的なオペレーションを確立しておけば、その知識を使って通常のオペレーションからの逸脱を特定できます。

- シミュレーション。クラウド環境内で予期するセキュリティイベントと予期しないセキュリティイベントの両方をシミュレーションし、準備の効果を確認します。
- 反復。シミュレーションの結果を反復することで、対応体制の規模の改善、価値創出に要する時間の短縮、リスクの軽減を行います。

教育

トピック

責任共有

セキュリティとコンプライアンスに対する責任は AWS とお客様の間で共有します。この共有モデルによってお客様の運用上の負担が一部軽減します。AWS が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、サービスを運用する施設の物理的なセキュリティまで、さまざまなコンポーネントの運用、管理、制御を引き受けます。

お客様は、ゲストオペレーティングシステム (アップデートやセキュリティパッチなど) とアプリケーションソフトウェアを管理する責任を負います。また、セキュリティグループ、ネットワークアクセスコントロールリスト、ID とアクセス管理など、AWS が提供するセキュリティコントロールの設定に対しても責任を負います。お客様の責任範囲は、選択したサービス、これらのサービスの IT 環境への統合、該当する法規制によって異なるため、どのサービスを選択するかを注意深く検討する必要があります。図 2 は、Amazon Elastic Compute Cloud (Amazon EC2) などのインフラストラクチャサービスに適用される責任共有モデルの一般例を示しています。ほとんどの責任は、クラウドのセキュリティ (AWS が管理) とクラウド内のセキュリティ (お客様が管理) という 2 つのカテゴリに分かれます。責任は、使用するサービスによって変わります。Amazon S3 や Amazon DynamoDB などの抽象化されたサービスについては、AWS がインフラストラクチャレイヤー、オペレーティングシステム、プラットフォームを運用し、お客様はエンドポイントにアクセスしてデータを保存および取得します。お客様は、データの管理 (暗号化オプションを含む)、アセットの分類、IAM ツールを使用した適切な許可の適用について責任を負います。

ただし、コンテナの追加や、他のサービスによて運用モデルがサービスプロバイダーに移行するに伴って、責任共有モデルは変わります。運用モデルの左側へ向けて、IaaS やデータセンターから PaaS へと移行するに伴って、サービスプロバイダーの責任が増大します。グラフの左側に移行するほど、お客様のクラウド内での責任が減り、運用が容易になります。以下の図を参照し、クラウド内での運用や機能の違いに注意してください。クラウド内での責任共有が変わると、インシデント対応やフォレンジックのオプションも変わります。お客様は、インシデント対応を計画する際に、運用モ

デルで何ができるかについても計画し、選択したモデルで予想されるやり取りを事前に計画する必要があります。これらのトレードオフに備えて計画し、ガバナンスのニーズと適合させることは、インシデント対応の重要なステップです。

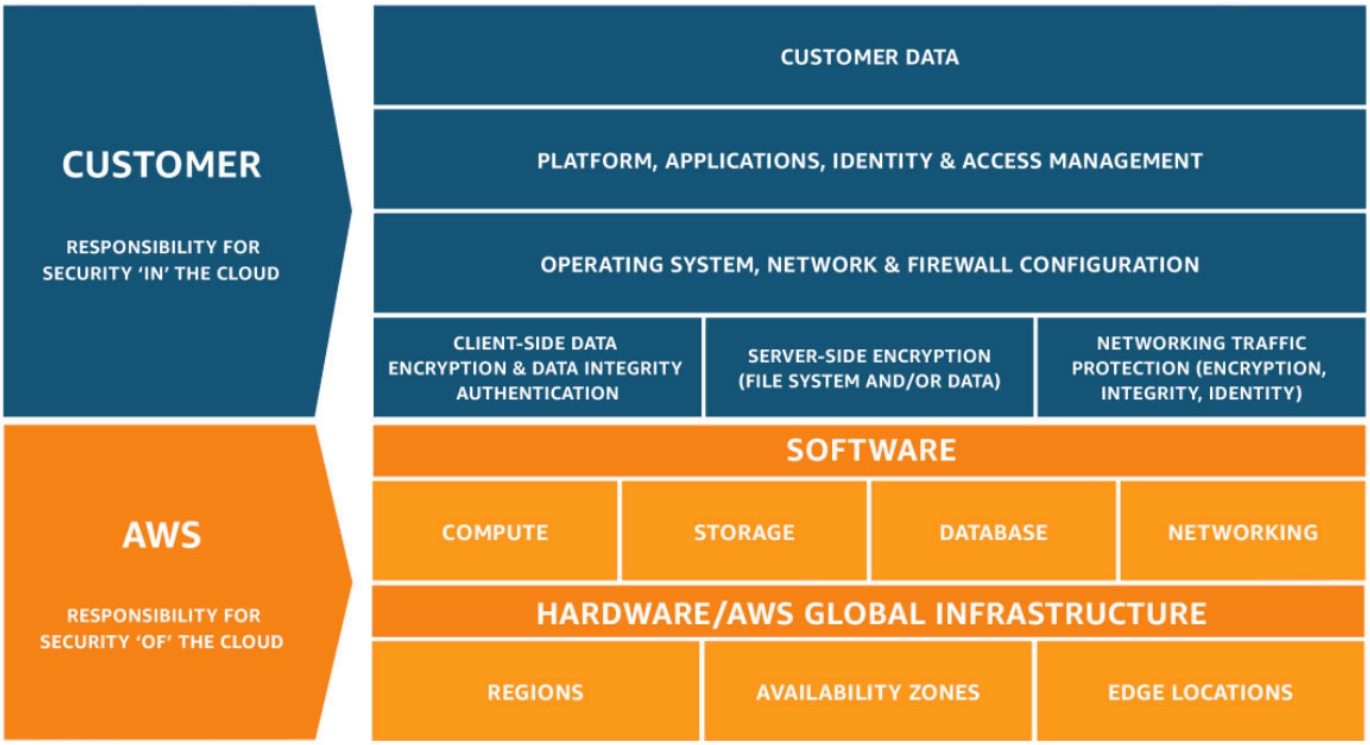

図 1: 責任共有モデル

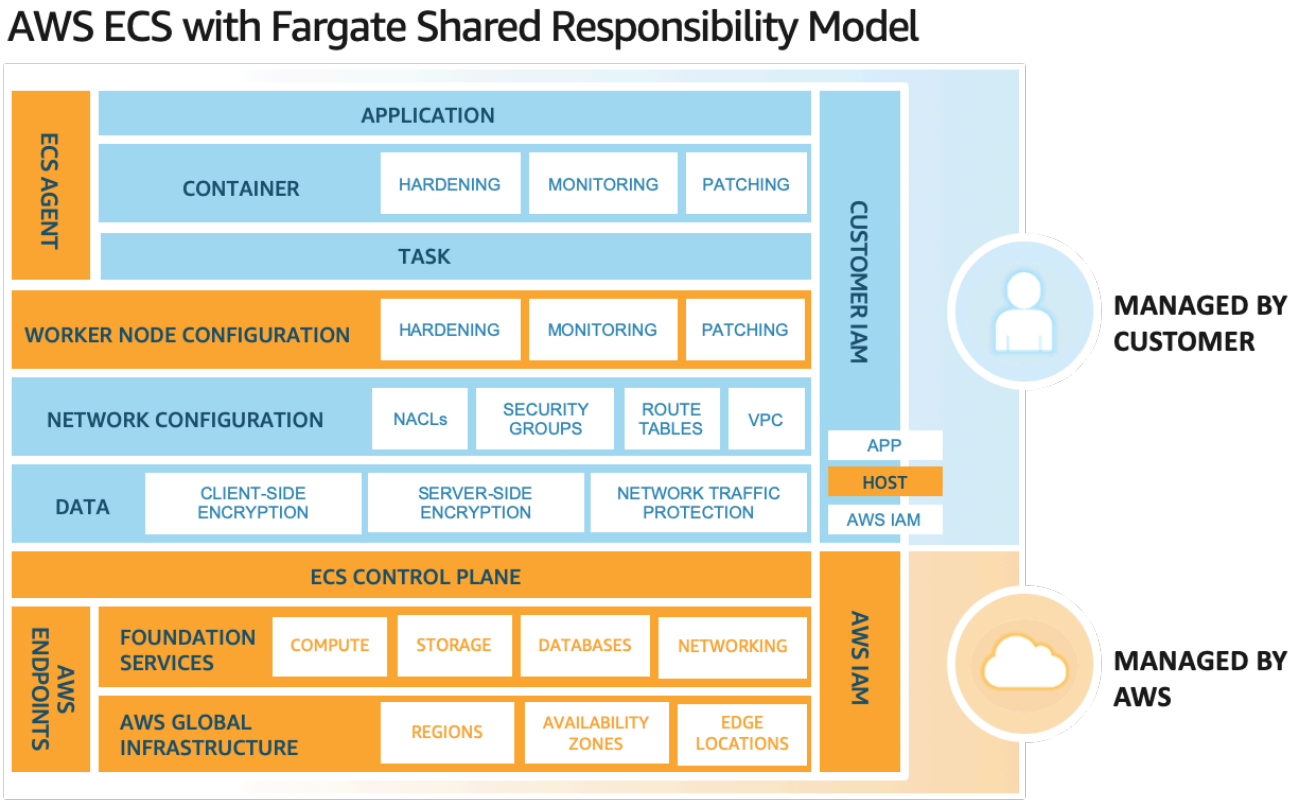

図 2: Amazon Elastic Container Service (Amazon ECS) および AWS Fargate タイプの責任共有モデル

お客様と AWS との直接的な関係に加えて、お客様の特定の責任モデルで他のエンティティが責任を分担している場合があります。例えば、社内の組織単位が一部の業務を担当している場合があります。また、パートナーや他のサードパーティーがクラウドテクノロジーの一部を開発、管理、運用している場合があります。

運用モデルに合った適切なインシデント対応とフォレンジックのランブックを作成することが非常に重要です。成功するかどうかは、選択した運用モデルに合わせて、どのような種類のツールを作成または購入する必要があるかを理解しているかどうかにかかっています。利用可能なツールをよく理解するほど、エンタープライズのガバナンスリスクとコンプライアンス (GRC) モデルのニーズを満たす準備が整います。

クラウド内でのインシデント対応

クラウドレスポンスの設計目標

インシデント対応の一般的なプロセスやメカニズム (NIST SP 800-61 コンピュータセキュリティインシデント対応ガイドなどで定義) は依然として正しいものですが、特にクラウド環境でのセキュリティインシデント対応に関連した以下の設計目標を検討することをお勧めします。

- 対応目標を定める - ステークホルダー、法律顧問、組織のリーダーと協力してインシデント対応の目標を定めます。一般的な目標としては、問題の抑制と軽減、影響を受けたリソースの復旧、フォレンジック用のデータの保持、アトリビューションなどがあります。
- クラウドを使用して対応する - イベントとデータが発生する対応パターンを実装します。
- 持っているものと必要なものを知る - ログ、スナップショット、その他の証拠を一元化されたセキュリティクラウドアカウントにコピーして保持します。タグ、メタデータ、メカニズムを使用して保持ポリシーを適用します。例えば、Linux dd コマンドまたは Windows の同等コマンドを使用して、調査目的でデータの完全なコピーを作成することを選択できます。
- 再デプロイのメカニズムを使用する - セキュリティの異常が設定ミスに起因する場合は、設定ミスを修正してリソースを再デプロイするだけで解決できる場合があります。可能であれば、対応メカニズムを安全に繰り返して実行したり、未知の状態に対して実行したりできるようにします。
- 可能な場合は自動化する - 問題やインシデントが繰り返し発生する場合は、プログラムによって一般的な状況の順序をトリアージ方式で決めて対応するメカニズムを構築します。インシデントが独特で、新しく、機密性の高いものである場合は、手動で対応します。
- スケーラブルなソリューションを選択する - 組織のアプローチをクラウドコンピューティングに合わせてスケールし、検出から対応までの時間を短縮します。
- プロセスを確認して改善する - プロセス、ツール、または人材のギャップを見つけて、修正を計画します。シミュレーションは、ギャップを見つけてプロセスを改善する安全な方法です。

NIST の設計目標に従って、アーキテクチャがインシデント対応と脅威検出の両方を実行できることを確認します。クラウドの実装を計画する場合、インシデントやフォレンジックイベントへの対応を考慮します。これは、これらの対応を専門に担当する複数の組織、アカウント、ツールを設定することを意味する場合があります。これらのツールや機能は、デプロイパイプラインを通じてインシデント対応の担当者に利用してもらいます。静的に設定しないでください。静的にするとリスクが大きくなります。

クラウドセキュリティインシデント

トピック

インシデントドメイン

お客様の責任内で、セキュリティインシデントが発生し得るドメインとして、サービス、インフラストラクチャ、アプリケーションの 3 つがあります。これらのドメイン間の違いは、対応時に使用するツールに関係してきます。各ドメインについて検討します。

- サービスドメイン - サービスドメインのインシデントは、お客様の AWS アカウント、IAM 許可、リソースメタデータ、請求、その他の領域に影響を与えます。サービスドメインのイベントは、AWS API メカニズムのみを使用して対応するイベントです。または、根本原因が設定やリソースのアクセス許可に関連していて、関連するサービス指向のログが記録されるイベントです。
- 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のインシデントには、データまたはネットワークに関連したアクティビティが含まれます。例えば、VPC 内の Amazon EC2 インスタンスへのトラフィック、Amazon EC2 インスタンス上のプロセスとデータ、その他の領域 (コンテナや他の将来のサービスなど) です。インフラストラクチャドメインのイベント対応には、多くの場合、フォレンジック用のインシデント関連データの検索、復元、または取得が伴います。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場合があり、AWS API メカニズムが関与する場合もあります。
- アプリケーションドメイン – アプリケーションドメインのインシデントは、アプリケーションコードで発生するか、サービスやインフラストラクチャにデプロイしたソフトウェアで発生します。このドメインは、クラウドの脅威の検出および対応ランブックに含める必要があります。このドメインの対応は、インフラストラクチャドメインの対応と似ている面があります。よく考えられた適切なアプリケーションアーキテクチャでは、自動化されたフォレンジック、復旧、および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、アカウント、リソース、またはデータを損なう可能性があるアクターを考慮する必要があります。組織の内外を問わず、リスクフレームワークを使用して組織への具体的なリスクを判断し、それに応じて準備します。

サービスドメインでは、AWS API のみを使用して目標の達成に取り組みます。例えば、Amazon S3 バケットからのデータ漏えいインシデントを処理するには、API コールを通じてバケットのポリシー

を取得し、S3 アクセスログを分析します。場合により、AWS CloudTrail ログを確認します。この例では、データフォレンジックツールやネットワークトラフィック分析ツールが調査に必要になる可能性はほぼありません。

インフラストラクチャドメインでは、IR 業務のために準備した Amazon EC2 インスタンスなど、ワークステーションのオペレーティングシステム内で使い慣れたデジタルフォレンジック/インシデント対応 (DFIR) ソフトウェアを AWS API と組み合わせて使用できます。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のキャプチャ、Amazon Elastic Block Store (Amazon EBS) ボリューム上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必要になる場合があります。

クラウドセキュリティイベントの指標

多くのセキュリティイベントは、インシデントに該当しなくても、慎重を期して調査した方がよい場合があります。AWS クラウド環境でセキュリティ関連のイベントを検出するには、以下のメカニズムを使用できます。すべてを網羅したリストではありませんが、以下の例を参考として役立ててください。

- ログとモニター - AWS ログ (Amazon CloudTrail、Amazon S3 アクセスログ、VPC フローログなど) とセキュリティモニタリングサービス (Amazon GuardDuty、 Amazon Detective、AWS Security Hub CSPM、Amazon Macie)。さらに、Amazon Route 53 ヘルスチェックや Amazon CloudWatch アラームなどのモニターを使用します。同様に、Windows イベント、Linux Syslog ログ、その他アプリケーション内で生成できるアプリケーション固有のログを使用し、CloudWatch エージェントを使用して Amazon CloudWatch にログを記録します。
- 請求アクティビティ - 請求アクティビティの突然の変化は、セキュリティイベントを示している可能性があります。
- 脅威インテリジェンス - サードパーティーの脅威インテリジェンスフィードを購読している場合、その情報を他のログ記録やモニタリングツールと関連付けて、イベントの潜在的な指標を特定できます。
- パートナーツール - AWS パートナーネットワーク (APN) のパートナーが提供している数百の製品をセキュリティ目標の達成に利用できます。詳細については、AWS Marketplace のセキュリティソリューションとセキュリティパートナーのソリューションを参照してください。
- AWS Outreach - AWS サポート が不正行為や悪意のある行為を特定した場合、お客様に連絡する場合があります。詳細については、「不正使用と侵害に対する AWS の対応」セクションを参照してください。
- 1 回限りの連絡 - 顧客、デベロッパー、または組織内の他のスタッフが異常に気付く可能性があるため、セキュリティチームへの一般的な連絡方法を周知させておくことが重要です。チケットシス

テム、連絡先の電子メールアドレス、ウェブフォームなどが一般的な方法です。組織が一般市民を対象としている場合は、一般向けのセキュリティ連絡メカニズムも必要になる場合があります。

オートメーションと検出のために AWS が提供しているツールの 1 つに AWS Security Hub CSPM があります。Security Hub を使用すると、AWS アカウント全体にわたって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 1 か所で包括的に確認できるため、これらの指標の可視性が向上します。AWS Security Hub CSPM は、セキュリティ情報イベント管理 (SIEM) ソフトウェアではなく、ログデータを保存しません。ただし、代わりに AWS の複数のサービスからセキュリティアラートや検出結果を集約して整理し、優先順位付けを行います。また、Security Hub では、複数のソースに基づくカスタムインサイトを作成することもできます。これにより、セキュリティオペレーションチームは、イベント発生時により多くの情報へのオプションとインサイトを得ることができます。Security Hub は、AWS のベストプラクティスや組織が従っている業界標準に基づく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できます。

これらのセキュリティやコンプライアンスに関する検出結果に対してアクションを起こすには、Amazon Detective や Amazon Athena で検出結果を調査します。または、Amazon CloudWatch Events やイベントバスのルールを使用して検出結果を送信します。送信先は、チケット発行、チャット、SIEM、SOAR (セキュリティオーケストレーションのオートメーションと対応)、インシデント管理の各ツール、またはカスタム修正プレイブックです。イベントベースのオートメーションにより、発生したインシデントやイベントに自動的に対応できます。このアプローチに従うと、オンプレミス環境と比べて、クラウド内ではセキュリティが変わり、イベントの処理方法も変わります。

クラウド機能を理解する

AWS には、すべてのドメインにわたってセキュリティイベントの調査に使用できる幅広いセキュリティ機能があります。例えば、AWS には、AWS CloudTrail ログ、Amazon CloudWatch Logs、Amazon S3 アクセスログなど、さまざまなログ記録メカニズムが用意されています。使用しているサービスで、関連するログが有効になっていることを確認してください。AWS は、集中ログ記録ソリューションも提供しています。このソリューションでは、一般的な種類のクラウドログを一元的に保存できます。これらのログ記録ソースを有効にしたら、Amazon Athena を使用して Amazon S3 バケット内のログをクエリするなど、ログを分析する方法を決める必要があります。

また、AWS パートナー製品も利用できます。AWS セキュリティコンピテンシープログラムで説明している製品など、これらのログの分析プロセスを簡略化できるパートナー製品が数多くあります。これらのデータから貴重なインサイトを汲み取るために役立つ AWS のサービスもいくつかあります。例えば、 Amazon GuardDuty (脅威検出サービス) や AWS Security Hub CSPM を使用すると、AWS アカウント全体にわたって優先度の高いセキュリティアラートやコンプライアンスステー

タスを包括的に確認できます。さらに、Amazon Detective を利用して AWS リソースからログデータを収集し、機械学習、統計分析、グラフ理論を使用して潜在的なセキュリティ問題や疑わしいアクティビティの根本原因を特定できます。調査に役立つ追加のクラウド機能の詳細については、「付録 A: クラウド機能の定義」を参照してください。

トピック

- データプライバシー
- 不正使用と侵害に対する AWS の対応

データプライバシー

AWS は、お客様がプライバシーとデータセキュリティに深い関心を持っていることを認識しています。そのため、お客様のコンテンツへの不正アクセスや漏えいを防ぐために設計された、高度な信頼できる技術的コントロールと物理的コントロールを実装しています。お客様の信頼を維持することは継続的な取り組みです。AWS のデータプライバシーに関する取り組みの詳細については、「データプライバシーのよくある質問」ページを参照してください。

このような意図的な自主規制により、AWS がお客様の環境内で対応を支援する能力が制限されます。そのため、責任共有モデル内での機能を理解して構築することが、AWS クラウド内で成功するための鍵となります。インシデントの発生前に AWS アカウントでログ記録とモニタリングの機能を有効にすることは重要ですが、インシデント対応には、ほかにもプログラムの成功に不可欠な要素があります。

カリフォルニア州消費者データプライバシー

2018 年のカリフォルニア州消費者プライバシー法 (CCPA) は、CCPA の対象となる「消費者に関連して企業が保有する個人情報に関する消費者のさまざまな権利」を認めています。CCPA の対象となるお客様に関連する AWS のプライバシーおよびデータセキュリティポリシーについては、「カリフォルニア州消費者プライバシー法に備える」ホワイトペーパーを参照してください。

一般データ保護規則

一般データ保護規則 (GDPR) は、2018 年 5 月 25 日から施行された欧州プライバシー法 (欧州議会および理事会の 2016 年 4 月 27 日の規則 2016/679) です。GDPR は、EU データ保護指令 (指令 95/46/EC) に取って代わるもので、各 EU 加盟国に拘束力を持つ唯一のデータ保護法を適用することにより、欧州連合 (EU) 全体でデータ保護法に親和性をもたせることを目的とします。GDPR に関連する AWS コンプライアンスについては、「AWS における GDPR コンプライアンスに関する情報提供」ホワイトペーパーを参照してください。

不正使用と侵害に対する AWS の対応

不正使用行為とは、AWS のお客様のインスタンスやその他のリソースで観察される、悪意のある行動、不快な行動、違法な行動、その他のインターネットサイトを損なう可能性のある行動です。AWS はお客様と協力して、お客様の AWS リソースからの疑わしい行為や悪意のある行為を検出して対処します。お客様のリソースからの予期しない行為や疑わしい行為は、AWS リソースが侵害されていることを示している可能性があり、これはお客様のビジネスに対する潜在的なリスクとなります。AWS アカウントには別の連絡方法があることに忘れないでください。連絡先を追加するときは、セキュリティと請求の両方の観点から、ベストプラクティスを必ず使用してください。お客様のルートアカウントの E メールは AWS からの通信のプライマリターゲットですが、AWS はセキュリティや請求に関する問題をセカンダリ E メールアドレスにも送信します。追加した E メールアドレスの受信者が 1 人だけである場合、AWS アカウントに単一障害点を追加したことになります。連絡先に配布リストを少なくとも 1 つ追加していることを確認します。

AWS は、以下のようなメカニズムを使用して、お客様のリソース内の不正使用行為を検出します。

- AWS 内部イベントモニタリング。
- AWS ネットワークアドレス空間に対する外部セキュリティインテリジェンス。
- AWS リソースに対するインターネット不正使用に関する苦情。

AWS の不正使用対応チームは、AWS で進行している不正使用行為を積極的にモニタリングしてシャットダウンしていますが、不正使用に関する苦情の大多数は AWS で正当な業務を行っているお客様に対するものです。意図しない不正使用行為の一般的な原因をいくつか以下に示します。

- 侵害されたリソース - パッチが適用されていない Amazon EC2 インスタンスは、ウィルスに感染してボットネットエージェントになる場合があります。
- 意図しない不正使用 - 過度に攻撃的なウェブクローラーは、一部のインターネットサイトでサービス拒否攻撃として分類される可能性があります。
- セカンダリ不正使用 - AWS のお客様が提供するサービスのエンドユーザーが、Amazon S3 のパブリックバケットにマルウェアファイルを投稿する場合があります。
- 虚偽の苦情 - インターネットユーザーが正当な活動を不正使用として誤って報告することがあります。

AWS は AWS のお客様と協力して、不正使用の防止、検出、軽減と、将来の再発防止に取り組むことをお約束します。AWS 利用規約を確認することをお勧めします。アマゾン ウェブ サービスおよび関連会社が提供するウェブサービスの禁止された使用について記載しています。AWS からの不

正使用の通知にタイムリーに対応できるように、AWS アカウントの連絡先情報が正確であることを確認してください。AWS から不正使用の警告を受け取ったら、お客様のセキュリティおよび運用スタッフはただちに事態を調査する必要があります。遅延は、悪評が長引いたり、自社や他社を法的問題に巻き込んだりする結果になります。さらに重要な点として、該当する不正使用リソースが悪意のあるユーザーから侵害されたり、侵害を無視すると、ビジネスへの被害が拡大したりする可能性があります。

準備 - 人材

自動化されたプロセスにより、組織はクラウド環境およびアプリケーションのセキュリティを向上させる対策に集中して時間を費やすことができます。インシデント対応を自動化すると、イベントの関連付け、シミュレーションの演習、新しい対応手順の考案、調査の実施、新しいスキルの開発、新しいツールのテストや構築を担当する人間も増やすことができます。自動化が進んでも、セキュリティ組織内のアナリストや対応者はまだやるべきことがたくさんあります。均質なチームでは盲点が生まれやすいため、多様なチームを構築して、異なる思考体系、文化的視点、複雑で流動的な状況での仕事と生活の経験をもたらすことが重要です。イベントの計画時に実行できる最もインパクトの強い事項の 1 つは、チームと対応計画に多様性を組み込むことです。多様な視点で構成されたチームは、見逃していた可能性がある盲点を特定し、他の方法では思い付かなかった可能性がある解決策を提示できる場合があります。

トピック

役割と責任の定義

インシデント対応のスキルとメカニズムは、新しいイベントや大規模なイベントを処理する場合に最も重要です。これらのイベントは、チームが開発した書面による基準と、チームが実践してきたプラクティスに依存します。イベントがどのような展開を見せるかを完全に予測または体系化することはできないため、インスタンスメモリや診断ログの収集など、単純で反復的なタスクはオートメーションに任せ、人間は難しい決定を担当できます。不明瞭なセキュリティイベントに対処するには、組織横断的な規律、決然とした行動、結果をもたらす能力が必要です。組織構造内には、人事 (HR)、経営陣、法務の代表者など、インシデントの実行責任者、説明責任者、相談先、報告先の役割を果たす多くの人が必要です。これらの役割と責任、さらにサードパーティーを関与させるかどうかを検討します。多くの地域では、許可事項と禁止事項を規定する現地の法律があることに注意してください。インシデントの実行責任者、説明責任者、相談先、報告先 (RACI) のチャートを作成するのは官僚的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、イベントの段階別にリーダーシップを明確に示すことができます。

信頼できるパートナーを調査や対応に関与させると、追加の専門知識や貴重な精査が得られます。これらのスキルが自社のチームにない場合は、外部の関係者を雇って支援を受けることができます。外部の関係者を雇う場合は、この関係者からチームメンバーがトレーニングを受けるようにします。これらの外部関係者が社内のデベロッパーやオペレーターと協力することで、チームメンバーのスキルを伸ばすことができ、新しい専門知識が将来の IR プログラムに価値をもたらす可能性があります。

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やデベロッパーを含めることが重要です。これらの人々は、対象分野の専門家 (SME) であり、情報とコンテキストを提供できます。デベロッパーやアプリケーション所有者の専門知識をインシデント対応に利用する前に、これらの人々と練習を行い、関係を構築してください。アプリケーションの所有者や SME は、環境に慣れていない、予期せぬ複雑さがある、または対応者がアクセスできない状況で行動することを求められる場合があります。アプリケーションの SME は、IR チームと連携する練習を行って慣れる必要があります。

トレーニングの提供

依存関係を減らし、対応時間を短縮するには、セキュリティチームと対応者がクラウドサービスに関するトレーニングを受け、組織で使用している特定のクラウドプラットフォームの実践練習をする機会があることを確認します。このトレーニングの一部は、プロセスの最初に行うチーム作りとランブックの作成を通じて行うことができます。できるだけ多くの人々を最初のランブックを作成するステップに関与させることで、社内チームの理解を深めることができます。これらのチームが机上訓練でこれらのランブックに従うようになると、このトレーニングはより現実的になります。

AWS およびその他のサードパーティーは、お客様がダウンロードして利用できるオンラインセキュリティワークショップ (AWS セキュリティワークショップ) も提供しています。組織は、スタッフに対して追加トレーニングを提供し、プログラミングスキル、開発プロセス (バージョン管理システムやデプロイの演習など)、インフラストラクチャの自動化を習得させることでメリットを得ることができます。

AWS では、デジタルトレーニング、クラスルームトレーニング、AWS パートナー、および認定を通じて、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。

対応メカニズムの定義

対応メカニズムは、ガバナンス、リスク、コンプライアンス (GRC) モデルによって異なります。理想的には、インシデント対応を計画する前に、GRC モデルを構築します。GRC の構築を開始していない場合は、適切なインシデント対応メカニズムを構築するための最初のステップとして必要です。

クラウド内でのインシデント対応アプローチを他のチーム (法律顧問、リーダー、ビジネスステークホルダーなど) と連携して検討する場合は、自分が持っているものと必要なものを理解する必要があります。ステークホルダーおよび関連する担当者を特定し、必要な対応を実行するための適切なアクセス権があることを確認します。

クラウドはサービス API を通じて可視性と機能を向上させることができますが、GRC モデルはこれらを対応を活かす方法を示します。チームの AWS アカウント番号、仮想プライベートクラウド (VPC) の IP 範囲、対応するネットワーク図、ログ、データの場所、およびデータ分類を特定します。これらの技術的プロセスの多くは、「準備 - テクノロジー」セクションに記載してあります。次に、インシデント対応手順 (通常、手順またはランブックとも呼ばれます) の文書化を開始し、インシデントを調査および修正するステップを定義します。

受容性と適応性のあるセキュリティ文化を創り出す

AWS では、AWS のお客様や AWS 自身のセキュリティチームがどのようなときに最も成功するかを熟知しています。それは、セキュリティチームが自社のビジネスやデベロッパーにとって協力的なイネーブラーとなり、すべてのステークホルダーが協力して向上を重ね、俊敏で応答性の高いセキュリティ体制を維持する文化を育てたときです。このホワイトペーパーでは、組織のセキュリティ文化の向上は対象としていませんが、セキュリティチームの受容性が高いことが他のチームに伝われば、外部から適切な情報を得ることができます。セキュリティチームがオープンで近づきやすければ、リーダーからのサポートを受けて、セキュリティイベントに関する追加の通知、協力、対応を適時に得られる可能性が高くなります。

組織によっては、セキュリティ上の問題を報告すると、報復を受けるのではないかとスタッフが恐れる場合があります。問題を報告する方法を単に知らないという場合もあります。また、時間を無駄にしたくない、セキュリティインシデントとして報告したことが後で何でもなかったことがわかると恥ずかしいという場合もあります。リーダーシップチームから末端に至るまで、受容の文化を促進し、組織のセキュリティに誰もが貢献できるようにすることが重要です。潜在的なリスクや脅威があると思ったら、いつでも誰もが高重要度のチケットを開くことができる明確なチャネルを提供します。これらの通知を広い心で熱心に歓迎します。さらに重要なのは、セキュリティ担当以外のスタッフに対して、これらの通知を歓迎することを明確に伝えることです。潜在的な問題について通知をまったく受け取らないよりも、通知を過剰に受けることを希望していることを強調してください。研究者から公の記事で問題を指摘されるよりは、デベロッパー自身が自分の間違いを申告する方がはるかに増しです。

これらの通知は、ストレス下での迅速な調査を練習する貴重な機会となります。これらを重要なフィードバックループとして、対応手順の策定に活かすことができます。

対応の予測

すべての潜在的なイベントを予測することは不可能であるため、引き続き人間による分析に頼らざるを得ません。スタッフのトレーニングと組織の準備を時間をかけて慎重に行うと、予期しない事態に備えるのに役立ちます。ただし、組織の準備を単独で行う必要はありません。信頼できるセキュリティパートナーと協力して予期しないセキュリティイベントを特定することで、組織は追加の可視性とインサイトの恩恵を受けることができます。

パートナーと対応窓口

クラウドジャーニーは、組織ごとに異なります。ただし、他の組織が経験済みのパターンやプラクティスがあります。これらについて、信頼できるセキュリティパートナーから伝えてもらうことができます。対応能力を強化する外部の専門知識や異なる視点を提供できる外部の AWS セキュリティパートナーを見つけることをお勧めします。信頼できるセキュリティパートナーの支援を得て、よく知らない潜在的なリスクや脅威を特定できます。

1955 年、Joseph Luft と Harrington Ingham は、特性をカテゴリにマッピングするための演習として Johari ウィンドウを作成しました。このウィンドウは、次の図のような 4 つの格子で構成されたグリッドとして表されます。

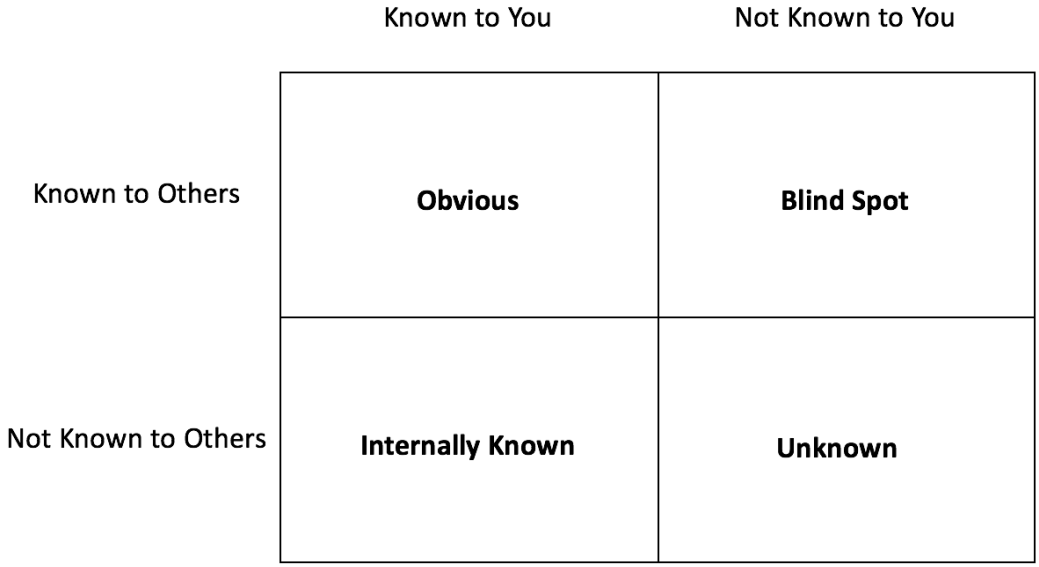

図 3: インシデント対応用に変更した Johari ウィンドウ

Johari ウィンドウは、情報セキュリティ用に意図されたものではありませんが、この概念を調整してシンプルなメンタルモデルとして使用し、組織の脅威を評価することの難しさを検討できます。変更した概念では、以下の 4 つの格子を使用します。

- 明白 - チームと AWS パートナーの両方が気付いているリスク。
- 内部で既知 - チームは気付いているが、AWS パートナーは気付いていないリスク。これは、社内の専門知識やチーム内の知識があることを意味する場合があります。
- 盲点 - AWS パートナーは気付いているが、チームは気付いていないリスク。
- 未知 - お客様も AWS パートナーも気付いていないリスク。

この図はシンプルですが、信頼できる AWS パートナーを持つことで達成できる価値を示しています。最も重要なのは、自分は気付いていないが、AWS パートナーから適切な専門知識を得られる盲点があり得ることです。明白の格子では、両者ともこれらのリスクに気付いているとしても、AWS パートナーは、お客様がよく知らないコントロールやソリューションを推奨できます。また、内部で既知の格子では、これらのリスクを AWS パートナーに知らせることができますが、AWS パートナーもそのリスクを軽減するための最適化されたコントロールを特定できる場合があります。改善に向けて自己評価を行う場合、AWS パートナーに連絡して専門的なアドバイスを受けてください。

未知のリスク

アラートの調整、自動化によるインシデント対応手順の改善、セキュリティ防御の改善に既に集中して取り組んでいる場合、次に何を改善すべきかと悩むことでしょう。図 3 の未知のカテゴリが示す未知のリスクについて気になるかもしれません。未知のリスクは、以下の方法で軽減できます。

- セキュリティアサーションを定義する - 何を真実としてアサートできるか。 環境で絶対的に真実であるべきセキュリティプリミティブは何であるか。 これらを明確に定義すると、逆のものを探すことができます。これは、セキュリティアサーションを後でリバースエンジニアリングするよりも、クラウドジャーニーの早い段階で行う方が簡単です。
- 教育、コミュニケーション、リサーチ - クラウドセキュリティのエキスパートをスタッフから生み出すか、エキスパートパートナーを参加させることで環境を精査してもらいます。前提を疑い、微妙な根拠に用心します。プロセスにフィードバックループを設け、エンジニアリングチームがセキュリティチームとコミュニケーションをとるメカニズムを提供します。また、アプローチを拡大して、関連するセキュリティメーリングリストや情報セキュリティの漏えいをモニタリングします。
- 攻撃面の減少 - 防御力を高めてリスクを回避し、未知の攻撃に備える時間を増やします。攻撃者をブロックして鈍化させ、目立たせます。

- 脅威インテリジェンス - 世界中の最新の脅威および関連する脅威、リスク、指標の継続的なフィードを購読します。
- アラート - 異常な、悪意のある、または費用のかかるアクティビティについて警告する通知を生成します。例えば、使用していないリージョンやサービスで発生したアクティビティに関する通知を作成できます。
- 機械学習 - 機械学習を使用して、特定の組織や個人のペルソナに関する複雑な異常を特定します。異常な動作を特定しやすくするために、ネットワーク、ユーザー、システムの正常な特性をプロファイリングすることもできます。

盲点や誰にも知られていない未知を考慮する場合は、脅威インテリジェンスが主要なトピックになります。Johari ウィンドウは知っていることと知らないことを分類する方法を示しますが、脅威インテリジェンスはまだ知らないことを説明する方法を示します。脅威インテリジェンスは、企業が脅威モデルを詳細に把握し、企業がまだ存在を認識していない可能性がある脅威を見つけるのに役立つ分野です。

通常、脅威インテリジェンスを構成する要素は以下のとおりです。

1. 新しい脅威の発見。
2. 新しいパターンの定義。
3. 新しい自動取得手法の定義
4. これらのプロセスの繰り返し。

この種の方法は役に立ちますが、脅威インテリジェンスチームのケアとメンテナンスは、大企業を含む多くのエンタープライズに過度な負担をかける可能性があります。最終的には、脅威モデル、規模、リスク回避を調和させることが問題になります。以下の質問を検討します。

- 脅威モデルは、自社が属する標準的な業種と大きく異なっているか?
- リスク選好度は、そのようなチームを必要とするほど低いか?
- チームを運営するのは自社にとって財政的に健全であるか?
- リスク特性は、自社の目的に適切な人材を引き付けるぐらい興味深いものであるか?

これらの質問のいずれかに「いいえ」と回答した場合は、ほぼ例外なく、脅威インテリジェンスパートナーを見つける必要があります。このサービスは、多くの大企業や有名企業が競合して提供しています。

AWS は、これらの問題を自分で管理するためのツールとサービスを提供しています。機械学習を使用して悪意のあるパターンを特定することは、よく調査された研究分野であり、対応パターンは、お客様、AWS Professional Services、AWS パートナーによって実装され、さらに Amazon GuardDuty や Amazon Macie などの AWS のサービスを通じて実装されています。これらのパターンの一部は、AWS re: Invent カンファレンスセッションで議論されています。詳細については、このホワイトペーパーの「メディア」セクションを参照してください。

また、お客様は、セキュリティデータレイクを開発する際に、従来のビジネス中心のデータレイクを拡張して同様のアーキテクチャパターンを活用しています。また、セキュリティ運用チームは、Amazon OpenSearch Service や OpenSearch Dashboards などの従来のログ記録やモニタリングツールの使用を、ビッグデータアーキテクチャにまで拡張しています。

これらのお客様は、AWS CloudTrail イベントログ、VPC フローログ、Amazon CloudFront アクセスログ、データベースログ、アプリケーションログから内部データを収集し、これらのデータをパブリックデータや脅威インテリジェンスと組み合わせています。お客様は、この貴重なデータを利用することで、セキュリティ運用チームにデータサイエンスとデータエンジニアリングのスキルを導入しています。また、Amazon EMR、Amazon Kinesis Data Analytics、Amazon Redshift、Amazon QuickSight、AWS Glue、Amazon SageMaker、Apache MXNet on AWS などのツールを活用して、自社のビジネス特有の異常を特定して予測するカスタムソリューションを構築するようになっています。

最後に、「セキュリティパートナーソリューション」を参照し、AWS パートナーが提供する数百の業界屈指の製品をご覧ください。これらの製品は、オンプレミス環境の既存のコントロールと同等、同一であるか、統合されています。これらの製品は、AWS の既存のサービスを補完し、クラウドとオンプレミスにわたって包括的なセキュリティアーキテクチャと、よりシームレスなエクスペリエンスをデプロイできるようにします。

準備 - テクノロジー

トピック

AWS アカウントへのアクセスを準備する

インシデントが発生したら、インシデント対応チームは、このインシデントに関連する環境やリソースにアクセスする必要があります。イベントが発生する前に、業務を遂行するための適切なアクセス権がチームにあることを確認します。そのためには、チームメンバーがどのレベルのアクセス権を必要とするか (どのように対処するかなど) を知り、事前にアクセス権をプロビジョニングしておく必要があります。このアクセス権は、企業のガバナンス、リスク管理、コンプライアンス (GRC) ポリシーから導き出されます。チームメンバーの認証と認可は、イベントが発生する前に文書化してテストし、遅滞なく適時に対応できるようにします。インシデントに正しく対応するには、準備の一環として、AWS アカウントがどのように配置されているか、クロスアカウントロールをどのように許可および構成するかを確認する必要があります。

この段階では、デベロッパー、アーキテクト、パートナー、ガバナンスチーム、コンプライアンスチームと緊密に連携して、対応者に必要なアクセスレベルを確認する必要があります。AWS アカウント戦略とクラウド ID 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、認証と認可の方法をどのように設定するかを確認します。以下のような方法があります。

- フェデレーション - ユーザーは、1 つの AWS アカウントで ID プロバイダーから IAM ロールを引き受けます。
- クロスアカウントアクセス - ユーザーは複数の AWS アカウントにわたって IAM ロールを引き受けます。
- 認証 - ユーザーは、単一の AWS アカウント内で作成された AWS IAM ユーザーとして認証します。

これらのオプションは、AWS への認証に関する技術的な選択肢と、対応時のアクセスを取得する方法を定義します。ただし、組織によっては、他のチームやパートナーに対応を依頼する場合があります。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アカウントには、十分な

アクセス権を確保するために、多くの場合、特権が付与されます。したがって、これらのユーザーアカウントの使用を制限し、日常業務には使用しないようにします。

新しいアクセスメカニズムを作成する前に、クラウドチームと協力して AWS アカウントをどのように構成および管理するかを確認します。多くのお客様は、請求の一元管理、AWS アカウント間でのリソースの共有、アクセス、コンプライアンス、セキュリティの制御に、AWS Organizations を役立てています。Organizations のコア機能は、これを活用してサービスコントロールポリシーをアカウントのグループに適用できることです。これにより、大規模なポリシー管理が可能になります。大規模なガバナンスメカニズムの実装の詳細については、「大規模な AWS ガバナンス」を参照してください。組織が AWS アカウントをどのように構成および管理しているかを理解したら、以下の一般化された対応パターンを検討して、組織に適したアプローチを特定するために役立てます。

トピック

間接アクセス

間接アクセスを使用する場合、アカウント所有者またはアプリケーションチームは、セキュリティエキスパートであるインシデント対応チームからの戦術的なガイダンスに従って、AWS アカウントで認可済みの修正を実行する必要があります。この方法は、タスクの実行に時間がかかり、より複雑ですが、対応者がアカウントやクラウド環境に慣れていない場合に成功する可能性があります。

直接アクセス

インシデント対応者に直接アクセス権を付与するには、AWS アカウント内に AWS IAM ロールをデプロイし、セキュリティイベントの発生時にセキュリティエンジニアやインシデント対応者がこのロールを引き受けることができるようにします。インシデント対応者は、通常のフェデレーションプロセスを通じて認証します。または、インシデントが通常の認証プロセスに影響する場合は、特別な緊急プロセスを通じて認証します。インシデント対応の IAM ロールに付与する許可は、対応者が実行すると予想されるアクションによって異なります。

代替アクセス

セキュリティイベントがセキュリティ、アイデンティティ、または通信システムに影響を与えていると思われる場合は、代替のメカニズムやアクセス権を通じてその影響を調査して修正することが必要になる場合があります。新しい専用の AWS アカウントを使用することで、対応者間で協力し、代替の安全なインフラストラクチャから作業を実行できます。

例えば、対応者は、Amazon WorkSpaces を使用したリモートワークステーションや、Amazon WorkMail が提供する E メールサービスなど、クラウド内で起動された新しいインフラストラクチャを活用できます。安全な代替の AWS アカウントが、影響を受けた AWS アカウントに代わって許可を引き受けることができるように、適切なアクセスコントロール (IAM ポリシーを使用) を準備してアクセス権を委任する必要があります。

適切なアクセス権を委任したら、影響を受けたアカウントの AWS API を使用して、ログやボリュームスナップショットなどの関連データを共有し、隔離された環境で調査業務を実行できます。このクロスアカウントアクセスの詳細については、「チュートリアル: AWS アカウント間の IAM ロールを使用したアクセスの委任」を参照してください。

オートメーションアクセス

オートメーションの使用に切り替えてセキュリティイベントに対応する場合は、オートメーションリソース (Amazon EC2 インスタンスや AWS Lambda 関数など) 専用の IAM ロールを作成する必要があります。これにより、これらのリソースは IAM ロールを引き受けて、ロールに割り当てられた許可を継承できます。AWS 認証情報を作成して配布する代わりに、AWS Lambda 関数または Amazon EC2 インスタンスに許可を委任します。AWS リソースは一連の一時的な認証情報を自動的に受け取り、これらを使用して API リクエストに署名します。

また、Amazon EC2 インスタンスのオペレーティングシステム内でオートメーションやツールを安全に認証および実行する方法を検討することもできます。このオートメーションを実行できるツールは多くありますが、AWS Systems Manager Run Command の使用を検討してください。これを使用すると、Amazon EC2 インスタンスオペレーティングシステムにインストールしたエージェントを使用して、インスタンスをリモートから安全に管理できます。

AWS Systems Manager Agent (SSM Agent) は、Microsoft Windows Server や Amazon Linux など、一部の Amazon EC2 の Amazon マシンイメージ (AMI) にデフォルトでインストールされています。ただし、Linux インスタンスとハイブリッドインスタンスの他のバージョンには、エージェントを手動でインストールすることが必要になる場合があります。Run Command または別のツールを使用するかどうかにかかわらず、最初のセキュリティ関連のアラートを受け取って調査する前に、前提条件であるセットアップと設定を完了してください。

マネージドサービスへのアクセス

お客様の組織は、サービスおよびソリューションの管理を代行する情報技術プロバイダーと既に提携している場合があります。これらのパートナーとは組織のセキュリティをサポートする責任を共有するため、異常が発生する前にこの関係を明確に理解することが重要です。AWS マネージドサービスプロバイダー (MSP) パートナー、AWS Managed Services、またはマネージドセキュリティサービスパートナーのいずれかと既に提携しているかどうかにかかわらず、各パートナーの責任を明確にしておく必要があります。これらの責任は、クラウド環境、プロバイダーが既に持っているクラウドサービスへのアクセス権、プロバイダーに必要なアクセス権、サポートを依頼するときの連絡先やエスカレーションパスに関係してきます。最後に、これをパートナーと実際に練習して、対応計画が予測可能で正常に機能することを確認する必要があります。

プロセスの準備

適切なアクセス権をプロビジョニングしてテストしたら、インシデント対応チームは調査と修正に必要な関連プロセスを定義して準備する必要があります。この段階は、クラウド環境内でセキュリティイベントへの適切な対応を十分に計画する必要があるため、多大な労力を必要とします。

社内のクラウドサービスチームやパートナーと緊密に連携し、これらのプロセスが実現可能であることを確認するための必要なタスクを特定します。対応アクティビティのタスクで協働するか、タスクを相互に割り当てるとともに、必要なアカウント設定が整っていることを確認します。組織が以下の対応機能を実行できるようにする前に、プロセスと前提条件となる設定を準備しておくことをお勧めします。

トピック

- 意思決定ツリー
- 代替アカウントの使用
- データの表示またはコピー
- Amazon EBS スナップショットの共有
- Amazon CloudWatch Logs の共有
- イミュータブルストレージの使用
- イベントの近くでリソースを起動
- リソースの分離
- フォレンジックワークステーションの起動

意思決定ツリー

条件が異なれば、異なるアクションやステップが必要になることがあります。例えば、AWS アカウントのタイプ (開発と本番)、リソースのタグ、これらのリソースの AWS Config ルールコンプライアンスステータス、その他の入力に応じて、実行するアクションは異なる場合があります。

これらの決定の作成と文書化に役立てるために、他のチームやステークホルダーと一緒に意思決定ツリーのドラフトを作成することをお勧めします。フローチャートと同様に、意思決定ツリーは意思決定を支援するために活用できるツールであり、潜在的な条件と入力 (確率を含む) に基づいて最適なアクションと成果を決定するのに役立ちます。

代替アカウントの使用

影響を受けたアカウント内でイベントに対応することが必要な場合もありますが、影響を受けたアカウントの外部でデータを調査するのが理想的です。一部のお客様は、分離された AWS アカウント環境を個別に作成するプロセスを持っており、テンプレートを使用してプロビジョニングが必要なリソースを事前設定しています。これらのテンプレートは、AWS CloudFormation や Terraform などのサービスを通じてデプロイします。Terraform を使用すると、関連する AWS リソースのコレクションを簡単に作成し、整然とした予測可能な方法でプロビジョニングできます。

テンプレート化したメカニズムを使用してこれらのアカウントを事前設定すると、インシデントの初期段階で人的介入を排除できます。また、環境とリソースを繰り返し可能かつ予測可能な方法で準備し、監査によって検証できます。さらに、このメカニズムにより、フォレンジック環境のデータのセキュリティと封じ込めを維持する能力も向上します。

このアプローチでは、クラウドサービスチームやアーキテクトチームと協力して、調査に使用できる適切な AWS アカウントプロセスを決定する必要があります。例えば、クラウドサービスチームは AWS Organizations を使用することで、新しいアカウントを生成し、これらのアカウントをテンプレート化またはスクリプト化した方法で事前設定できます。

このセグメント化の方法は、大規模な組織を潜在的な脅威から切り離しておく必要がある場合に最適です。このセグメント化では、新しい、ほとんど接続されていない AWS アカウントを使用するため、マルチアカウントのドキュメントでセキュリティ組織単位 (OU) とラベル付けされた組織のユーザーは、このアカウント内に移動して、必要なフォレンジックアクティビティを実行し、必要に応じてアカウント全体をリーガルエンティティに引き渡すことができます。このフォレンジックとアトリビューションの方法は、大幅な見直しと計画が必要であり、エンタープライズの GRC ポリシーに沿っている必要があります。この作業は簡単ではありませんが、大規模なアカウントベースを構築する前に行う方がはるかに簡単です。

データの表示またはコピー

対応者は、分析するためにログやその他の証拠にアクセスする必要があり、データを表示またはコピーできることを確認する必要があります。対応者の IAM 許可ポリシーは、少なくとも読み取り専用アクセスを提供し、調査できるようにする必要があります。適切なアクセス権を有効にするには、SecurityAudit や ViewEnlyAccess などの事前に構築された AWS マネージドポリシーを検討できます。

例えば、対応者は、特定のアカウントの Amazon S3 バケットから別のアカウントの Amazon S3 バケットに AWS CloudTrail ログをコピーするなど、データのポイントインタイムコピーを作成できます。ReadOnlyAccess マネージドポリシーが提供する許可などを使用すると、対応者はこれらのアクションを実行できます。AWS コマンドラインインターフェイス (CLI) を使用してこれを実行する方法については、「ひとつの Amazon S3 バケットから別のバケットにすべてのオブジェクトをコピーするにはどうすればよいですか」を参照してください。

Amazon EBS スナップショットの共有

多くのお客様は、Amazon EC2 インスタンスに関連するセキュリティイベントの調査の一部に Amazon Elastic Block Store (Amazon EBS) スナップショットを役立てています。Amazon EBS ボリュームのスナップショットは増分バックアップです。Amazon EBS 増分スナップショットの詳細については、「Amazon EBS スナップショット」を参照してください。

分離した個別のアカウントで Amazon EBS ボリュームの調査を実行するには、スナップショットの許可を変更して、他の指定した AWS アカウントとスナップショットを共有する必要があります。認可されたユーザーは、共有したスナップショットに基づいて独自の EBS ボリュームを作成できます。元のスナップショットは影響を受けないまま残ります。詳細については、「Amazon EBS スナップショットの共有」を参照してください。

スナップショットが暗号化されている場合は、スナップショットの暗号化に使用したカスタムの AWS Key Management Service (AWS KMS) カスタマーマネージドキー (CMK) も共有する必要があります。カスタム CMK には、その作成時または作成後に、クロスアカウント許可を適用できます。スナップショットは、作成元のリージョンに制限されますが、別のリージョンにコピーすることで、コピー先のリージョンと共有できます。詳細については、「Amazon EBS スナップショットのコピー」を参照してください。

Amazon CloudWatch Logs の共有

Amazon CloudWatch Logs に記録されたログ (Amazon VPC フローログなど) は、CloudWatch Logs サブスクリプションを通じて別のアカウント (集中型セキュリティアカウントなど) と共有できま

す。例えば、ログイベントデータを集中型 Amazon Kinesis ストリームから読み取り、カスタム処理や分析を実行できます。カスタム処理は、多数のアカウントからログデータを収集する場合に特に便利です。理想的には、この設定をクラウドジャーニーの早い段階で作成し、セキュリティ関連のイベントの発生に備えます。詳細については、「サブスクリプションと共有するクロスアカウントのログデータ」を参照してください。

イミュータブルストレージの使用

ログやその他の証拠を別のアカウントにコピーした場合は、レプリケートしたデータを必ず保護してください。二次的な証拠を保護するだけでなく、コピー元のデータの整合性も保護する必要があります。このようなメカニズムはイミュータブルストレージと呼ばれ、データの改ざんや削除を防止することで、データの整合性を保護します。

Amazon S3 のネイティブ機能を使用して、データの整合性を保護するように Amazon S3 バケットを設定できます。例えば、S3 オブジェクトロックを使用すると、オブジェクトの削除や上書きを一定期間または無期限に防止できます。データの書き込みや読み取りを制限する他の方法としては、S3 バケットポリシーでのアクセス許可の管理、S3 バージョニングの設定、MFA Delete の有効化があります。この種の設定は、調査ログと証拠の保存に役立ち、書き込みは 1 回限りだが読み取りは何度でもできるライトワンスリードメニー (WORM) と呼ばれることもあります。データを保護するには、AWS Key Management Service (AWS KMS) によるサーバー側の暗号化を使用し、適切な IAM プリンシパルにのみデータの復号を許可することもできます。

また、調査の完了後にデータを長期ストレージに安全に保持したい場合は、オブジェクトライフサイクルポリシーを使用して Amazon S3 から Amazon S3 Glacier にデータを移動することを検討してください。Amazon S3 Glacier は、安全性と耐久性に優れ、きわめて低コストのクラウドストレージサービスで、データのアーカイブや長期バックアップに使用できます。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およびコンプライアンス機能を提供します。

さらに、Amazon S3 Glacier ボールトロックを使用して Amazon S3 Glacier 内のデータを保護できます。ボールトロックポリシーを使用すると、Amazon S3 Glacier ボールトごとにコンプライアンスコントロールを簡単にデプロイして適用できます。WORM などのセキュリティコントロールをボールトロックポリシーに指定して、ポリシーを将来の編集からロックできます。ロックしたポリシーは変更できなくなります。Amazon S3 Glacier は、ボールトロックポリシーに設定されたコントロールを適用することで、データ保持などのコンプライアンス目標の達成を支援します。AWS Identity and Access Management (IAM) ポリシー言語を使用して、さまざまなコンプライアンスコントロールをボールトロックポリシーにデプロイできます。

イベントの近くでリソースを起動

クラウドを初めて使用する対応者は、既存のツールがあるオンプレミスでクラウド調査を実施したくなるかもしれません。AWS の経験によると、インシデント対応にクラウドテクノロジーを使用している AWS のお客様の方がより良い成果を達成しています。クラウドでは、隔離の自動化、コピーの容易化、証拠の早期分析、分析の早期完了が可能です。

ベストプラクティスは、データが存在するクラウド内で調査とフォレンジックを実行することです。調査の前にデータをデータセンターに転送する必要はありません。クラウドの安全なコンピューティングおよびストレージ機能は、世界中のほぼどこででも使用でき、安全な対応業務を実行できます。多くのお客様は、調査用に別個の AWS アカウントを事前に作成していますが、同じ AWS アカウントで分析を実行することもできます。コンプライアンスや法的な理由で組織が記録を保持する必要がある場合は、長期保管と法的業務用に別々のアカウントを保持することが適切な場合があります。

また、データを別の AWS リージョンにレプリケートせずに、イベントが発生したのと同じ AWS リージョンで調査を実施するのもベストプラクティスです。この方法をお勧めする主な理由は、リージョン間でのデータ転送には余分な時間がかかるためです。運用する AWS リージョンごとに、インシデント対応プロセスと対応者の両方が該当するデータプライバシー法に準拠していることを確認してください。リージョン間でデータを移動する必要がある場合は、管轄区域間でのデータ移動に伴う法的な影響を考慮してください。一般的には、同じ管轄区域内にデータを保持することがベストプラクティスです。

セキュリティイベントがセキュリティ、アイデンティティ、または通信システムに影響を与えていると思われる場合は、代替のメカニズムやアクセス権を通じてその影響を調査して修正することが必要になる場合があります。AWS では、新しいインフラストラクチャを迅速に立ち上げて、安全な代替作業環境で使用できるようにします。例えば、状況の潜在的な重要度を調査するときに、新しい AWS アカウントを作成して安全なツールを準備し、弁護士、広報、セキュリティチームが相互にコミュニケーションを取りながら作業を続行できるようにすることができます。AWS WorkSpaces (仮想デスクトップ用)、 AWS WorkMail (E メール用)、Amazon Chime (コミュニケーション用) などのサービスは、対応チーム、リーダー、その他の参加者に問題の伝達、調査、修正に必要な機能と接続を提供します。

リソースの分離

調査の過程で、セキュリティ異常への対応の一環として、リソースを分離することが必要になる場合があります。リソースを分離する目的は、潜在的な影響を制限し、影響を受けたリソースの伝播を防ぎ、意図しないデータ漏洩や不正なアクセスを防止することです。

すべての対応に共通することですが、ビジネス、規制、法律、その他の考慮事項が適用されます。予期した結果や予期しない結果に対する意図したアクションの効果を比較検討してください。クラウドチームがリソースタグを使用している場合は、これらのタグを利用してリソースの重要度や連絡先の所有者を特定できます。

フォレンジックワークステーションの起動

インシデント対応業務には、インシデントに関連するディスクイメージ、ファイルシステム、RAM ダンプ、その他のアーティファクトの分析が含まれる場合があります。多くのお客様は、影響を受けたデータボリュームのコピー (EBS スナップショットと呼ばれる) をマウントするために使用できるフォレンジックワークステーションを構築してカスタマイズしています。これを行うには、以下の基本的な手順に従います。

1. フォレンジックワークステーションとして使用できる基本の Amazon マシンイメージ (AMI) (Linux や Microsoft Windows など) を選択します。
2. その基本 AMI から Amazon EC2 インスタンスを起動します。
3. オペレーティングシステムを強化し、不要なソフトウェアパッケージを削除して、関連する監査およびログ記録メカニズムを設定します。
4. 希望するオープンソースのスイートやプライベートのツールキットと、必要なベンダーソフトウェアおよびパッケージをインストールします。
5. Amazon EC2 インスタンスを停止し、停止したインスタンスから新しい AMI を作成します。
6. 最新のソフトウェアパッチで AMI を更新および再構築するための週単位または月単位のプロセスを作成します。

AMI を使用してフォレンジックシステムをプロビジョニングすると、インシデント対応チームは、このテンプレートを使用して新しい AMI を作成し、調査ごとに新しいフォレンジックワークステーションを起動できます。AMI を Amazon EC2 インスタンスとして起動するプロセスは、事前に設定してデプロイプロセスを簡略化できます。例えば、必要なフォレンジックインフラストラクチャリソースのテンプレートをテキストファイルとして作成し、これを AWS CloudFormation で AWS アカウント内にデプロイできます。

テンプレートからリソースを迅速にデプロイできるようにすると、十分なトレーニングを受けたフォレンジックエキスパートは、インフラストラクチャを再利用せずに、新しいフォレンジックワークステーションを調査ごとに使用できるようになります。このプロセスにより、他のフォレンジック検査との相互汚染がないことを確認できます。

インスタンスタイプおよびロケーション

Amazon EC2 は、さまざまなユースケース向けに最適化したインスタンスタイプを幅広く取り揃えています。インスタンスタイプは、CPU、メモリ、ストレージ、ネットワーク容量のさまざまな組み合わせで構成されているため、アプリケーションのために適切な組み合わせのリソースを柔軟に選択できます。多くのインスタンスタイプには複数のインスタンスサイズが含まれているため、ターゲットワークロードの要件に合わせてリソースをスケールできます。インシデント対応インスタンスの場合は、本番インスタンスを実行するネットワークからの場所とセグメンテーションに関する自社の GRC ポリシーに従います。

AWS の拡張ネットワークは、シングルルート I/O 仮想化 (SR-IOV) を使用して、サポートされているインスタンスタイプで高性能ネットワーク機能を提供します。SR-IOV は、従来の仮想化ネットワークインターフェイスと比較し、I/O パフォーマンスが高く、CPU 利用率が低いデバイス仮想化の手法です。拡張ネットワークは、高い帯域幅、1 秒あたりのパケット (PPS) の高いパフォーマンス、常に低いインスタンス間レイテンシーを実現します。拡張ネットワークは追加料金なしで使用できます。10 Gbps または 25 Gbps のネットワーク速度をサポートするインスタンスタイプや、その他の高度な機能については、「Amazon EC2 インスタンスタイプ」を参照してください。

クラウドプロバイダーのサポート

トピック

- AWS Managed Services
- AWS サポート
- DDoS 対応のサポート

AWS Managed Services

AWS Managed Services (AMS) は、AWS インフラストラクチャの継続的な管理を提供するため、お客様はアプリケーションに集中できます。AMS は、ベストプラクティスを実装してインフラストラクチャを管理するため、運用のオーバーヘッドとリスクを削減できます。AMS は、変更リクエスト、モニタリング、パッチ管理、セキュリティ、バックアップサービスなどの一般的なアクティビティを自動化します。また、ライフサイクル全体にわたるサービスを提供して、インフラストラクチャをプロビジョニング、実行、サポートします。

AMS は、インフラストラクチャオペレーターとして、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負い、Follow-the-Sun (フォローザサン) モデルを使用して 24 時間 365 日のアラート

対応を提供します。アラートがトリガーされると、AMS は標準の自動および手動ランブックのセットに従い、一貫した対応を確実に行います。これらのランブックは、オンボーディング中に AMS のお客様と共有されるため、お客様は AMS と連携して対応を開発できます。実際のインシデントが発生する前に、お客様との共同のセキュリティ対応シミュレーションを実施し、運用力を高めることを AMS は推奨しています。

AWS サポート

AWS サポート は、AWS ソリューションの成功と運用のヘルスをサポートするツールや専門知識へのアクセスを提供する一連のプランを用意しています。すべてのサポートプランで、年中無休のカスタマーサービス、AWS ドキュメント、ホワイトペーパー、およびサポートフォーラムをご利用いただけます。AWS 環境の計画、デプロイ、最適化に役立つ技術サポートや追加のリソースが必要な場合は、お客様の AWS ユースケースに合った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、主な連絡先として AWS マネジメントコンソール のサポートセンターをご検討ください。AWS サポート へのアクセスは IAM によって制御されます。AWS サポート機能にアクセスする方法の詳細については、サポートへのアクセスを参照してください。

また、Amazon EC2 の悪用を報告する必要がある場合は、AWS の不正使用チームに連絡してください。

DDoS 対応のサポート

サービス拒否 (DoS) 攻撃を受けると、エンドユーザーはウェブサイトやアプリケーションを利用できなくなります。攻撃者は、さまざまな手法を駆使してネットワークの帯域幅やその他のリソースを消費し、正規のエンドユーザーのアクセスを妨げます。最もシンプルな DoS 攻撃では、単独の攻撃者が 1 つのソースから標的を狙います。

分散型サービス拒否 (DDoS) 攻撃では、攻撃者が複数のソースを使用して標的に対する攻撃を指揮します。これらのソースは、協力者のグループによって侵害または制御されている場合があります。DDoS 攻撃では、協力者または侵害されたホストが個別に攻撃に参加し、大量のパケットやリクエストを生成して標的に過重負荷をかけます。

AWS Shield は、AWS で実行しているウェブアプリケーションを保護するためのマネージド DDoS 保護サービスを提供します。AWS Shield で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常時稼働の検出と自動インライン緩和策を備えているため、DDoS からの保護を受けるために AWS サポート に依頼する必要はありません。AWS Shield にはスタンダードとアドバンストの 2 つの階層があります。

AWS のすべてのお客様は、AWS Shield Standard の自動保護の恩恵を無料で享受できます。AWS Shield Standard では、ウェブサイトやアプリケーションを標的とする、一般的かつ頻繁に発生するネットワーク層およびトランスポート層への DDoS 攻撃から防御します。AWS Shield Standard を Amazon CloudFront および Amazon Route 53 とともに使用すると、すべての既知のインフラストラクチャ (レイヤー 3 および 4) 攻撃に対して可用性が包括的に保護されます。

Amazon Elastic Compute Cloud (Amazon EC2)、Elastic Load Balancing (ELB)、Amazon CloudFront、Amazon Route 53 の各リソースで実行しているウェブアプリケーションを標的にした攻撃に対するさらに高度なレベルの保護をご希望の場合は、AWS Shield Advanced にサブスクライブできます。さらに、AWS Shield Advanced では AWS DDoS 対応チーム (DRT) に 24 時間 365 日アクセスできます。AWS Shield Standard と AWS Shield Advanced の詳細については、「AWS Shield」を参照してください。

シミュレーション

トピック

セキュリティインシデント対応のシミュレーション

セキュリティインシデント対応シミュレーション (SIRS) は、現実的なシナリオでインシデント対応計画や手順を試すための構造化された機会を提供する内部イベントです。基本的に SIRS イベントは準備を整え、対応能力を反復的に高めていくものです。お客様が SIRS アクティビティの実行に価値を見出す理由は、以下のとおいです。

- 準備態勢を検証する。
- シミュレーションやスタッフのトレーニングから学ぶことで自信を高める。
- コンプライアンスまたは契約上の義務に準拠する。
- 認定のためのアーティファクトを生成する。
- 俊敏性があり、集中して段階的に改善する。
- スピードとツールを改善する。
- コミュニケーションとエスカレーションを改善する。
- まれな事態や予期しない事態に備える。

このような理由から、SIRS のアクティビティへの参加には、ストレスの多いイベントで組織の有効性を高めるという価値があります。現実的で有益な SIRS アクティビティを開発するのは簡単な作業ではありません。よく理解しているイベントの処理手順やオートメーションを試すことには特定の利点がありますが、クリエイティブな SIRS アクティビティに参加して予期しない事態に対する準備体制を試すことも同様に重要です。

シミュレーションのステップ

独自の SIRS を設計する場合でも、信頼できるパートナーに基礎となる作業を依頼する場合でも、シミュレーションは通常、次のステップに従います。

1. 重要な課題を見つける - 対応を引き起こすトリガーを定義します。
2. 熟練したセキュリティエンジニアを特定する - シミュレーションにはビルダーとテスターが必要です。
3. 現実的なモデルシステムを構築する - シミュレーションは現実的で適切なものでなければなりません。現実的でなければ、参加者は演習に価値を認めない可能性があります。ささやかすぎると、演習は取るに足りないものと見なされる場合があります。簡単な演習から始めて、完全なイベントへと進めます。
4. シナリオ要素を構築してテストする - ロギングアーティファクト、E メール通知とアラート、潜在的なランブックなど、関連するシミュレーション資料の作成が必要になる場合があります。
5. 他のセキュリティ担当者や組織横断的な参加者を招待する - トレーニングと参加が必要な対象者全員を招待します。一般法務顧問、役員、広報担当者がシミュレーションに関与している場合は、彼らも招待する必要があります。
6. シミュレーションを実行する - スタッフに SIRS イベントを予告するか、シミュレーションを予告なしに実行するかを選択します。
7. 称賛する、測定する、改善する、繰り返す - シミュレーションにはストレス要因が伴うため、参加者の努力を奨励し、称賛することが重要です。奨励の後に、次のシミュレーションに向けた測定、改善、反復の機会が続きます。AWS は、これらのアクティビティを習慣化することをお勧めします。

> **Important**
>
> セキュリティインシデント対応シミュレーション (SIRS) を計画している場合は、「侵入テスト」の「その他のシミュレートされたイベント」セクションを参照し、手順に関する最新情報を確認してください。

シミュレーション例

期待する価値を提供するには、セキュリティシミュレーションを現実的なものにする必要があります。お客様やパートナーが独自のシミュレーションの作成に取り組む場合は、過去の実際のイベントをシミュレーション演習の貴重な情報源として常に参考にしてください。AWS のお客様が初期のシミュレーションに役立ったと報告している例をいくつか以下に示します。

- ネットワーク設定またはリソースに対する不正な変更。
- デベロッパーの設定ミスにより、誤って公開された認証情報。

- デベロッパーの設定ミスにより、誤って公開された機密性の高いコンテンツ。
- 悪意があると疑われる IP アドレスと通信しているウェブサーバーの隔離。

価値ある体験学習に加えて、SIRS アクティビティを実行すると、学習した教訓などの出力が生成され、プログラムの次のプロセスである反復への入力として使用できます。

反復

前のセクションでは、SIRS アクティビティの利点をいくつか定義しました。これらの利点の中には、段階的な改善による俊敏性の向上がありました。シミュレーションが生み出す価値ある成果を活用してセキュリティ対応を改善できます。シミュレーションは、何が機能して、何が機能しないかについて組織にフィードバックループを提供します。この知識に基づいて、新しい手順を段階的に作成したり、既存の手順を更新したりして、対応を改善できます。

トピック

ランブック

セキュリティ異常を検出した場合、イベントを封じ込め、既知の良好な状態に戻すことは、対応計画の重要な要素です。例えば、セキュリティ設定の誤りが原因で異常が発生している場合は、適切な設定でリソースを再デプロイして差異を取り除くだけで修復できることがあります。そのためには、事前に計画を立て、独自のセキュリティ対応手順を定義する必要があります。通常、この手順はランブックと呼ばれます。

ランブックは、組織が 1 つのタスクや一連のタスクを実行するための手順をドキュメント形式にしたものです。このドキュメントは、通常、内部デジタルシステムに保存するか、用紙に印刷して保管します。現在、インシデント対応ランブックが既にあるか、新規に作成してセキュリティ保証フレームワークに準拠させようとしているかもしれません。ただし、作成したランブックの手順を手作業で実行すると、間違いを犯す可能性が高くなります。代わりに、繰り返し可能なタスクをすべて自動化することをお勧めします。自動化により、対応チームは一般的なタスクから解放され、イベントの関連付け、シミュレーションでの演習、新しい対応手順の考案、調査の実施、新しいスキルの開発、新しいツールのテストや構築など、より重要なタスクに取り組めるようになります。ただし、タスクをプログラマブルロジックに分解し、反復して適切に自動化するには、まずランブックを作成する必要があります。

ランブックの作成

クラウド用のランブックを作成するには、まず現在生成しているアラートに注目してください。アラートを生成した場合は、そのアラートを調査することが重要です。最初に、実行する手動プロセスの内容を定義します。その後、プロセスをテストし、ランブックパターンを反復して、対応のコ

アロジックを改善します。例外の定義およびそれらのシナリオに代わる解決方法を決定します。たとえば、開発環境では、設定ミスのある Amazon EC2 インスタンスを終了することができます。ただし、同じイベントが本番環境で発生した場合は、インスタンスを終了させずに停止し、ステークホルダーに重要なデータは失われないことを伝え、終了が許容されるかどうかを確認します。

最適なソリューションを決定したら、ロジックをコードベースのソリューションに分解します。多くの対応者は、このソリューションを対応プロセスを自動化し、差異や当て推量を取り除くためのツールとして使用できます。これにより、対応のライフサイクルが短縮されます。次の目標は、このコードを人間の対応者が実行するのではなく、アラートやイベント自体によって呼び出すことで、完全に自動化することです。

開始方法

どこから始めればよいかわからない場合はAWS Trusted Advisor、AWS Security Hub の基本的なセキュリティのベストプラクティス、AWS Config ルール (AWS Config ルール Github リポジトリを含む) で生成されるアラートから開始することを検討します。次に、該当するシステムを記述するサービスが生成するイベントに注目します。

Amazon GuardDuty と Access Analyzer は、アプリケーションが AWS で使用するドメインの多くを記述するため、一般的に推奨されています。ただし、データとエンドポイントに関する懸念があるドメインに対しては、Amazon Inspector と Amazon Macie が特化されています。Amazon GuardDuty の検出結果については、Amazon GuardDuty ユーザーガイドを参照してください。Access Analyzer の検出結果については、Amazon Access Analyzer ユーザーガイドを参照してください。Macie の検出結果については、Amazon Macie ユーザーガイドを参照してください。Amazon Inspector の検出結果については、Amazon Inspector ユーザーガイドを参照してください。Security Hub を使用すると、これらの検出結果を 1 か所に統合し、低レイテンシーで同時に対応できます。そのため、Security Hub は修復の中央場所として推奨されています。

上記のすべてのサービスは、新規アラートの生成や既存アラートの更新など、何らかの変化が検出結果やアラートに生じると、Amazon CloudWatch Events を通じて通知を送信します。Amazon CloudWatch Events ルールを設定し、AWS Lambda 関数をトリガーしてイベント駆動型の対応を実行できます。ただし、Security Hub を使用すると、カスタムインサイトを構築してアプリケーションドメインから独自の検出結果を追加できます。これだけでも、Security Hub を代わりに使用する大きな理由となります。詳細については、「イベント駆動型の対応」セクションを参照してください。

オートメーション

オートメーションは、何倍ものカを発揮できるようにします。つまり、組織のスピードに合わせて対応者の労力をスケールします。手動プロセスから自動プロセスに移行すると、AWS クラウド環境のセキュリティ強化に、より多くの時間を費やすことができます。

トピック

- インシデント対応の自動化
- イベント駆動型の対応

インシデント対応の自動化

セキュリティエンジニアリングとオペレーションの機能を自動化するには、AWS の包括的な API とツールのセットを使用できます。アイデンティティ管理、ネットワークセキュリティ、データ保護、モニタリングの各機能を完全に自動化できます。セキュリティのオートメーションを構築すると、人間がセキュリティ体制をモニタリングして手動でイベントに対応する代わりに、システムがモニタリングしてレビューし、対応を開始できます。

インシデント対応チームが同じ方法でアラートに対応し続けると、アラート疲れになるリスクがあります。時間の経過とともに、チームはアラートに対する感度が鈍くなり、通常の状況の処理で間違いを犯したり、異常なアラートを見逃したりする可能性があります。自動化を利用すれば、繰り返し発生する通常のアラートを処理する機能を使用してアラート疲れを回避し、機密性の高いインシデントや独自のインシデントの処理を人間に任せることができます。

プロセス内のステップをプログラムで自動化すれば、手動プロセスを改善できます。イベントに対する修復パターンを定義したら、そのパターンを実行可能なロジックに分解して、ロジックを実行するコードを記述できます。その後、対応者は、そのコードを実行して問題を修正します。時間の経過とともに、より多くのステップを自動化し、最終的には一般的なインシデントのクラス全体を自動的に処理できるようになります。

ただし、お客様の目的は、検出メカニズムと対応メカニズムとの時間ギャップをさらに短縮することです。過去の経験から、この時間ギャップは数時間、数日、さらには数か月に及ぶことがあります。2016年に SANS が実施したインシデント対応調査では、21% の回答者が検出に 2 ~ 7 日を費やしていること、および同じ時間枠内でイベントを修正できたのは回答者の 29% に過ぎなかったことがわかりました。クラウド内では、イベント駆動型の対応機能を構築することで、対応の時間ギャップを数秒に短縮できます。

トピック

- 対応の自動化オプション
- スキャン方法間のコスト比較

対応の自動化オプション

エータープライズ実装と組織構造の間でバランスを取ることが重要です。図 4 は、AWS に実装した自動対応オプションごとに技術属性の違いをレーダーチャートで示しています。チャートでは、自動対応オプションの技術属性がチャートの中心から離れるほど、その技術属性は強くなります。例えば、AWS Lambda はスピードで優り、より少ない技術スキルセットを必要とします。AWS Fargate は柔軟性で優り、より少ないメンテナンスと技術スキルセットを必要とします。表 1 に、これらのオートメーションオプションの概要と、オプションごとの技術属性の要約を示します。

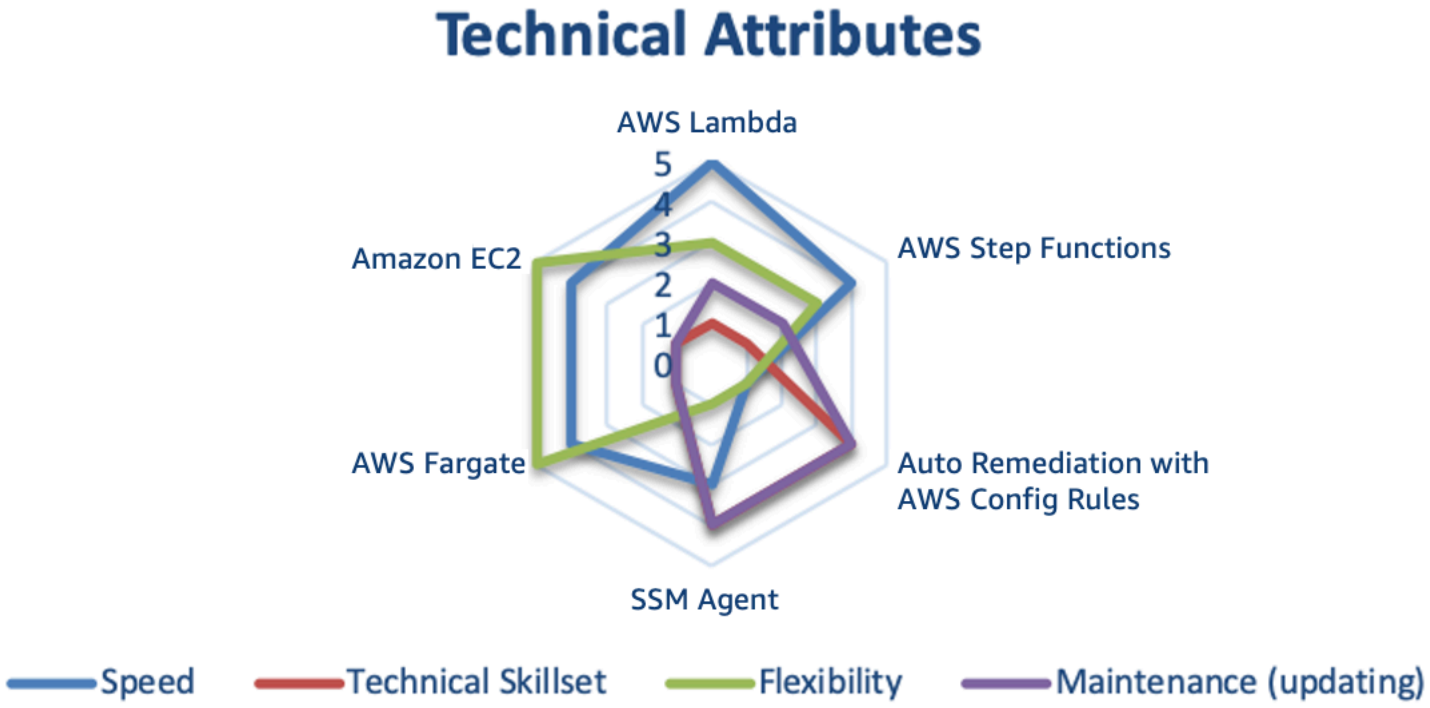

図 4: 自動対応アプローチ間の技術属性の違い

表 1: 自動対応のオプション

AWS のサービスまたは機能	説明	属性の要約*
AWS Lambda	AWS Lambda のみを使用するシステム。組織のエンタープライズ言語を使用します。	スピード 柔軟性 メンテナンス

AWS のサービスまたは機能	説明	属性の要約*
		スキルセット
AWS Step Functions	AWS Step Functions 、Lambda、SSM Agent を使用するシステム。	スピード 柔軟性 メンテナンス スキルセット
AWS Config ルール による自動修復	AWS Config ルール と自動修復のセット。環境を評価し、承認済みの仕様内に環境を戻します。	メンテナンスとスキルセット スピードと柔軟性
SSM Agent	オートメーションルールとドキュメントのセット。環境と内部システムの多くの部分をレビューし、修正を行います。	メンテナンスとスキルセット スピード 柔軟性
AWS Fargate	AWS Fargate システム。オープンソースのステップ関数コードと Amazon CloudWatch や他のシステムからのイベントを使用して、検出と修復を促進します。	柔軟性 スピード メンテナンスとスキルセット
Amazon EC2	フルインスタンスで実行するシステム。AWS Fargate オプションと似ています。	柔軟性 スピード メンテナンス スキルセット

* 属性は、サービスまたは機能ごとに降順で示しています。例えば、AWS Lambda はスピードで優り、より少ない技術スキルセットを必要とします。AWS Fargate は柔軟性で優り、より少ないメンテナンスと技術スキルセットを必要とします。

これらのオートメーションオプションを AWS 環境で検討する場合は、一元化とスキャン期間 (1 秒あたりのイベント数 (EPS)) も考慮する必要があります。

一元化とは、中央アカウントを通じて組織のすべての検出と修復を推進することです。このアプローチは、すぐに使用できる最良の選択肢と思われ、これが現在のベストプラクティスになっています。ただし、状況によっては、このアプローチから逸脱する必要があります。どのような場合に逸脱するかは、下位アカウントの処理方法によって異なります。まず、AWS Organizations のマルチアカウントフレームワークまたは AWS Control Tower でセキュリティツールアカウントのアプローチを活用することから開始することをお勧めします。

表 2: 一元化の長所と短所

	一元化	分散化
長所	シンプルな設定管理 対応をキャンセルまたは変更できない	シンプルなアーキテクチャ より高速な初期設定
短所	アーキテクチャが複雑化する アカウントとリソースのオンボーディング/オフボーディング	管理すべきリソースが増える ソフトウェアベースラインの維持が困難

これらの実装間のコストを比較すると、エンタープライズとして最適なオプションを決定する際に役立つ場合があります。1 秒あたりのイベント数 (EPS) は、コストを最適に見積もるために役立つメトリクスです。最終的には、集中型または分散型のアプローチを使用する方がはるかに簡単で安価になる可能性がありますが、お客様がそのコストをお客様のアカウントでどのように具体的に評価するかは、AWS では確認できません。これらのイベントを中央アカウントに送信して対応する場合は、EPS を必ず考慮してください。EPS の数が多いほど、これらのイベントを一元化されたアカウントに送信するコストが高くなります。

スキャン方法間のコスト比較

コストは、異常を検出するスキャン方法と、検証間の期間に基づいてより正確に決定されます。スキャン方法については、イベントベースまたは定期的スキャンレビューのどちらかを選択できます。表 3 に、両方のアプローチの長所と短所を示します。

表3: さまざまなスキャン方法の長所と短所

	イベントベース	定期的スキャン
長所	イベントから対応までの時間を短縮 追加の API コールをクエリする必要性が限定的	特定の時点での全体像
短所	リソースに関する状態コンテキストが限定される すぐには利用できないリソースに対してイベントがトリガーされる可能性がある	大規模なアカウントに対するサービスの制限 大量の API コールが原因でスロットリングが発生する可能性がある

多くの場合、完全に成熟した組織では、両方のスキャン方法を組み合わせることが最適な選択となります。AWS Security Hub CSPM と AWS の基本的なセキュリティのベストプラクティス標準では、両方のスキャン方法を組み合わせて提供しています。

図 5 は、オート–メーションアプローチごとに 1 秒あたりのイベント数 (EPS) のコスト比較をレーダーチャートで示しています。例えば、Amazon EC2 および AWS Fargate は 0 ~ 10 EPS の実行コストが最も高く、AWS Lambda および AWS Step Functions は 76 以上の EPS の実行コストが最も高くなっています。

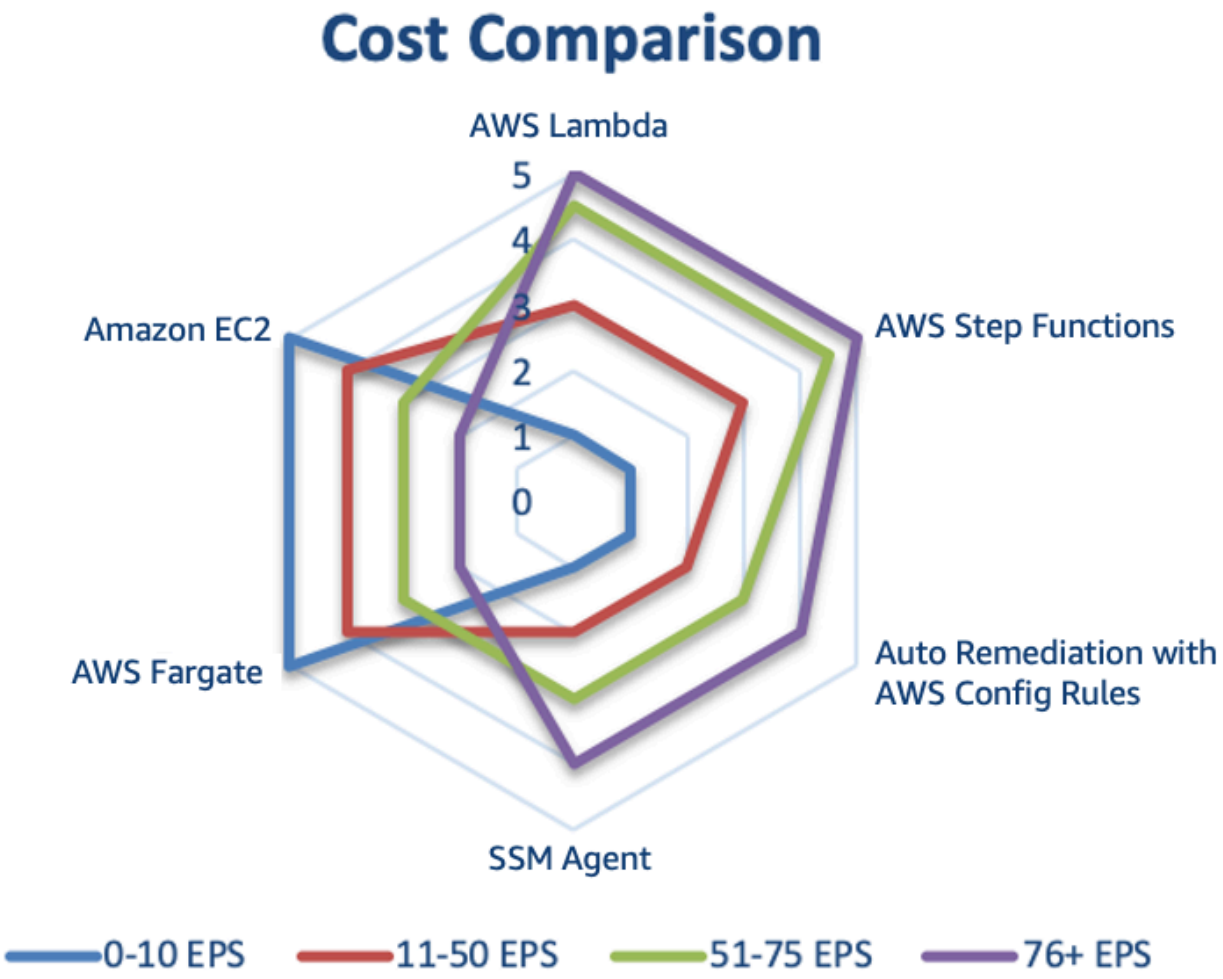

図 5: オートメーションオプションのスキャン方法 (1 秒あたりのイベント数 (EPS)) のコスト比較

イベント駆動型の対応

イベント駆動型の対応システムでは、検出メカニズムが対応メカニズムをトリガーして、イベントを自動的に修正します。イベント駆動型の対応機能を使用して、検出メカニズムから対応メカニズムまでの価値創出に要する時間を短縮できます。このイベント駆動型アーキテクチャを作成するには、AWS Lambda を使用できます。AWS Lambda は、イベントに応答してコードを実行し、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。

例えば、AWS CloudTrail サービスが有効になっている AWS アカウントがあるとします。AWS CloudTrailが (`cloudtrail:StopLogging`API を介して) 無効化されることがあった場合、対応プロシージャはサービスを再度有効にして、AWS CloudTrail ログ記録を無効化したユーザーを調査します。これらの手順を AWS マネジメントコンソール で手動で実行する代わりに、プログラムによっ

てログ記録を (cloudtrail:StartLogging API を介して) 再び有効にすることができます。これをコードで実装する場合、対応の目的は、このタスクをできるだけ早く実行して、対応を実行したことを対応者に通知することです。

これらのタスクを処理するには、ロジックを単純なコードに分解して AWS Lambda 関数で実行できます。次に、Amazon CloudWatch Events を使用して特定の cloudtrail:StopLogging イベントをモニタリングし、イベントが発生した場合に関数を呼び出すことができます。この AWS Lambda レスポンダー関数を Amazon CloudWatch Events で呼び出して、特定のイベントの詳細を渡すことができます。詳細には、AWS CloudTrail を無効化したプリンシパルの情報、無効化された日時、影響を受けた特定のリソース、その他の関連情報を含めます。これらの情報を使用して、ログからの検出結果を充実させ、対応アナリストが必要とする特定の値のみを含む通知やアラートを生成できます。

イベント駆動型の対応の目標は、理想的には、Lambda レスポンダー関数で対応タスクを実行し、異常が正常に解決されたことを、関連するコンテキスト情報とともに対応者に通知することです。その後、イベントが発生した理由を確認し、将来の再発を防止する方法を判断するのは、人間の対応者の役割です。このフィードバックループにより、クラウド環境のセキュリティがさらに向上します。この目標を達成するには、セキュリティチームが開発チームや運用チームと緊密に連携できる文化が必要です。

インシデント対応の例

トピック

サービスドメインのインシデント

通常、サービスドメインのインシデントは AWS API でのみ処理します。

アイデンティティ

AWS が API を提供しているクラウドサービスは、数百万のお客様が新しいアプリケーションを構築したり、ビジネスの成果を高めたりするために使用しています。これらの API は、ソフトウェア開発キット (SDK)、AWS CLI、AWS マネジメントコンソール など、さまざまな方法で呼び出すことができます。これらの方法を通じて AWS とやり取りするには、IAM サービスを利用して AWS リソースへのアクセスを安全にコントロールできます。IAM により、アカウントレベルでリソースの使用を許可するために誰を認証 (サインイン) し、誰を認可 (許可を付与) するかを制御できます。IAM で使用できる AWS のサービスのリストについては、「IAM と連携する AWS のサービス」を参照してください。

AWS アカウントを初めて作成する場合は、アカウントですべての AWS のサービスとリソースに対して完全なアクセス権限を持つ Single Sign-On (SSO) アイデンティティを使用して始めます。このアイデンティティは、AWS アカウントのルートユーザーと呼ばれます。ルートユーザーにアクセスするには、AWS アカウントの作成時に使用した E メールアドレスとパスワードを使用してサインインします。日常的なタスク、特に管理タスクにはルートユーザーを使用しないことを強くお勧めします。代わりに、ルートユーザーの使用に関するベストプラクティスに従って、ルートユーザーの使用は最初の IAM ユーザーの作成、ルートユーザーの認証情報の安全な保存、いくつかのアカウントやサービス管理タスクの実行に限定することをお勧めします。詳細については、「個々の IAM ユーザーを作成する」を参照してください。

これらの API は何百万ものお客様に価値をもたらしますが、悪意のある個人が IAM アカウントやルート認証情報へのアクセス権を取得すると、一部の API が不正使用されるおそれがあります。例えば、API を使用して、AWS CloudTrail などのアカウント内の口グ記録を有効化できます。ただし、攻撃者が認証情報を入手した場合、攻撃者も API を使用してこれらの口グを無効化できます。この種の不正使用を防ぐには、最小特権モデルに従った適切な IAM 許可を設定し、IAM 認証情報

を適切に保護します。詳細については、AWS Identity and Access Management ユーザーガイドの「IAM のベストプラクティス」を参照してください。この種のイベントが発生した場合は、AWS CloudTrail、AWS Config、AWS Trusted Advisor、Amazon GuardDuty、AWS CloudWatch Events など、AWS CloudTrail のログ記録が無効化されたことを確認する複数の検出コントロールがあります。

リソース

不正使用または誤設定されるその他の機能は、各お客様がクラウド内でどのように動作するかによって、組織ごとに異なります。例えば、特定のデータやアプリケーションを公的にアクセス可能にする組織もあれば、アプリケーションやデータを内部専用の機密扱いとする組織もあります。すべてのセキュリティイベントが本質的に悪意があるわけではありません。故意でない設定や不適切な設定が原因で発生するイベントもあります。どの API や機能が、組織に与える影響が大きいか、使用頻度が高いか低いかを検討します。

セキュリティ関連の誤設定の多くは、ツールとサービスを使用して特定できます。例えば、AWS Trusted Advisor には、ベストプラクティスに関する多くのチェックが用意されています。AWS パートナーも業界をリードする数百の製品を提供しており、これらはオンプレミス環境の既存のコントロールと同等または同一であるか、これらと統合できます。これらの製品やソリューションの多くは、AWS パートナーコンピテンシープログラムによって事前に認定されています。AWS セキュリティコンピテンシープログラムの「設定と脆弱性の分析」セクションにアクセスし、これらのソリューションを参照して、お客様の要件を満たすことができるかどうかを確認することをお勧めします。

インフラストラクチャドメインのインシデント

インフラストラクチャドメインには、通常、アプリケーションのデータやネットワークに関連するアクティビティが含まれます。VPC 内の Amazon EC2 インスタンスへのトラフィックや、Amazon EC2 インスタンスのオペレーティングシステムで実行しているプロセスなどが該当します。

例えば、モニタリングソリューションから Amazon EC2 インスタンスの潜在的なセキュリティ異常の通知を受けたとします。この問題に対処する一般的な手順は次のとおりです。

1. 環境を変更する前に、Amazon EC2 インスタンスからメタデータをキャプチャします。
2. インスタンスの終了保護を有効にして、Amazon EC2 インスタンスを誤って終了しないように保護します。
3. VPC セキュリティグループを切り替えて Amazon EC2 インスタンスを隔離します。ただし、VPC 接続の追跡やその他の封じ込め手法に注意してください。

4. Amazon EC2 インスタンスをあらゆる AWS Auto Scaling グループからデタッチします。
5. 関連する Elastic Load Balancing サービスから Amazon EC2 インスタンスの登録を解除します。
6. EC2 インスタンスにアタッチされた Amazon EBS データボリュームのスナップショットを作成し、保存とフォローアップ調査を行います。
7. Amazon EC2 インスタンスに対して調査のために隔離済みとしてタグ付けし、調査に関連するトラブルチケットなど、関連するメタデータを追加します。

上記のすべてのステップは、AWS API、AWS SDK、AWS CLI、AWS マネジメントコンソール を使用して実行できます。これらの方法を使用して AWS とやり取りするには、IAM サービスを使用して AWS リソースへのアクセスを安全にコントロールできます。IAM を使用して、アカウントレベルでリソースの使用を許可するために誰を認証および認可するかを制御します。IAM サービスは、お客様がこれらのアクションを実行し、サービスドメインとやり取りするための認証と認可を提供します。

Amazon EBS ボリュームのスナップショットは、EBS データボリュームの特定の時点におけるブロックレベルのコピーです。非同期のコピーであり、完了までに時間がかかる場合がありますが、特定の時点の前と後の差分となります。これらのコピーから新しい EBS ボリュームを作成して、フォレンジック EC2 インスタンスにマウントし、フォレンジック調査員がオフラインで詳細に分析できます。次の図は、簡略化した結果です。すべてのネットワークコンポーネント (サブネット、ルーティングテーブル、ネットワークアクセスコントロールリストなど) を網羅しているわけではありません。

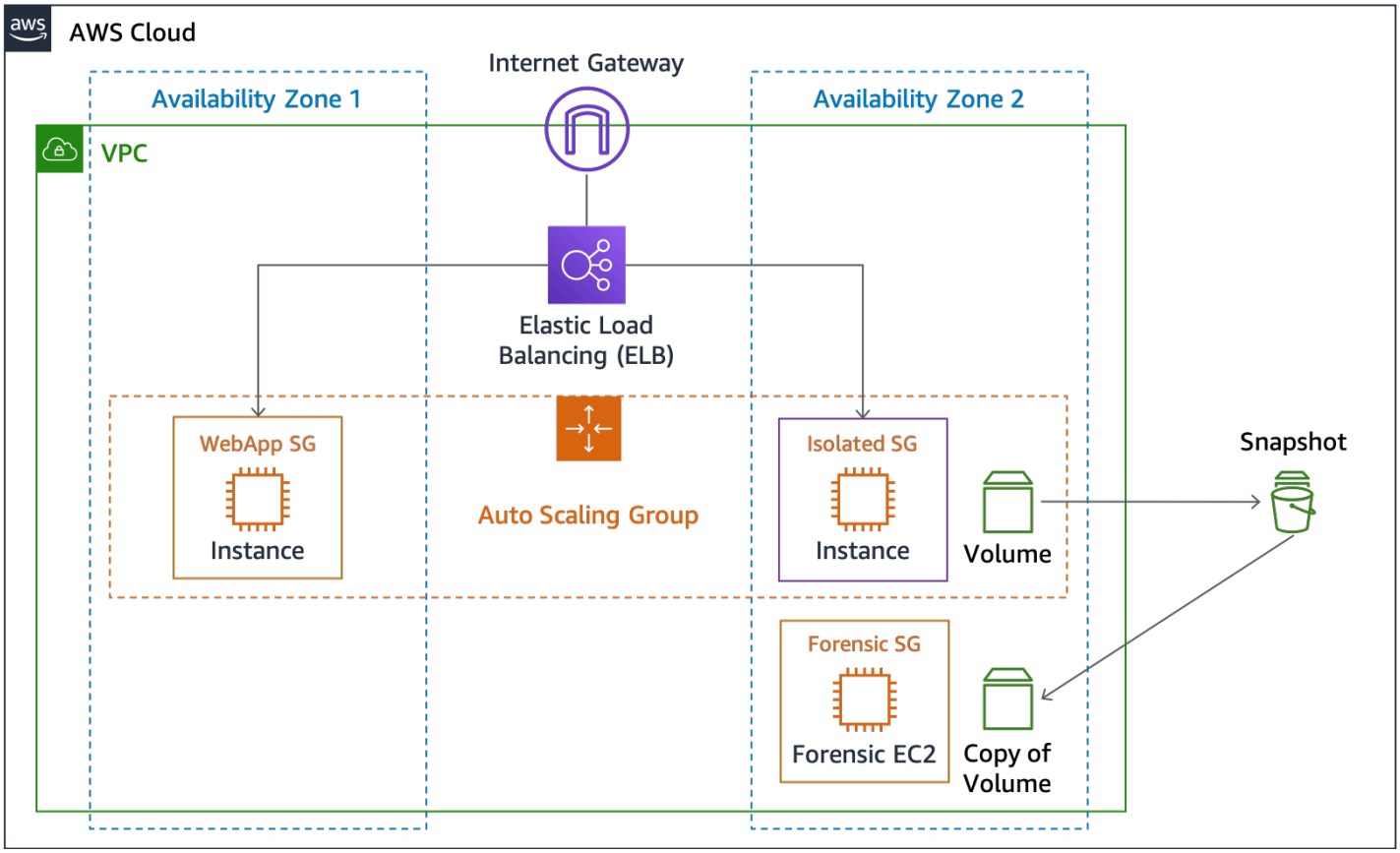

図 6: EC2 インスタンスの分離とスナップショット

トピック

- 調査の決定
- 揮発性データのキャプチャ
- AWS Systems Manager の使用
- キャプチャの自動化

調査の決定

この時点で、オフライン調査 (インスタンスを即時シャットダウン) またはオンライン調査 (インスタンスの実行を維持) のいずれかを選択できます。オフライン調査の利点の 1 つは、インスタンスのシャットダウン後に、既存の環境が影響を受けなくなることです。また、影響を受けたインスタンスのコピーを EBS スナップショットから作成し、このコピーを調査専用の隔離した環境の隔離した AWS アカウントで確認することもできます。ただし、オンライン調査により、メモリやネットワークトラフィックなどの揮発性の証拠をホスト OS から取得できる可能性がある場合は、インスタンスをすぐにシャットダウンしないことを選択できます。

揮発性データのキャプチャ

オンライン調査の実行を選択しない場合がありますが、インスタンスから揮発性データをキャプチャするために必要なメカニズムを理解しておくことが重要です。オンライン調査では、Amazon EC2 インスタンスで実行しているオペレーティングシステムとのやり取りが必要です。このシナリオでは、Amazon EC2 インスタンスでタスクを実行するために、AWS IAM サービス以外のサービスも必要です。マシンに対して直接認証するために、標準的な方法 (Linux セキュアシェル (SSH) や Microsoft Windows リモートデスクトップ (RDP) など) を使用することもできますが、オペレーティングシステムとの手動のやり取りはベストプラクティスではありません。オートメーションツールをプログラムで使用して、ホスト上でタスクを実行することをお勧めします。

AWS Systems Manager の使用

AWSSystems Manager Run Command は、Linux シェルスクリプトと Windows PowerShell コマンドをターゲットインスタンスで実行するオンデマンドの変更をリモートで安全に実行するのに役立ちます。Run Command コマンドは、AWS IAM サービスの許可から呼び出すことができますが、まずは Amazon EC2 インスタンスをマネージドインスタンスとしてアクティベートし、SSM Agent をマシンにインストールして (デフォルトでインストールされていない場合)、AWS IAM の許可を設定する必要があります。Run Command をオートメーションアクティビティや対応アクティビティに使用する場合は、調査を実行する前に前提条件となるアクティビティを必ず完了してください。

Run Command を含む AWS Systems Manager は、AWS CloudTrail と統合されています。このサービスは、Systems Manager 自体が行った API コールまたは Systems Manager に代わって行われた API コールをキャプチャし、そのログファイルを指定先の Amazon S3 バケットに渡します。AWS CloudTrail が収集した情報を使用して、リクエストの内容、リクエスト元のソース IP アドレス、リクエスト者、リクエスト日時などを確認できます。CloudTrail は、Systems Manager のすべての API アクションのログを作成します。これには、Run Command を使用してコマンドを実行するための API リクエストや、Systems Manager ドキュメントを作成するための API リクエストなどが含まれます。

AWS Systems Manager Run Command サービスを使用して SSM Agent を呼び出し、Linux シェルスクリプトや Windows PowerShell コマンドを実行できます。これらのスクリプトは、Linux Memory Extractor (LIME) カーネルモジュールなどのホストから追加データをキャプチャする特定のツールをロードして実行できます。その後、メモリキャプチャを VPC ネットワーク内のフォレンジック Amazon EC2 インスタンスに転送したり、Amazon S3 バケットに転送して永続的に保存したりできます。

キャプチャの自動化

SSM Agent を呼び出す方法の 1 つは、インスタンスに特定のタグが付いている場合に、Amazon CloudWatch Events を介して Run Command をターゲットにすることです。例えば、影響を受けるインスタンスに `Response=Isolate+MemoryCapture` タグを適用した場合、次の 2 つのアクションをトリガーするように Amazon CloudWatch Events を設定できます。

- 分離アクティビティを実行する Lambda 関数
- SSM Agent を介して Linux メモリをエクスポートするシェルコマンドを実行する Run Command

このタグ駆動型の対応は、イベント駆動型の対応の別の方法です。

まとめ

クラウドジャーニーを進めるにあたり、AWS 環境における前述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、小規模から始めて、徐々にオートメーション機能を導入しながら対応速度を高めることで、セキュリティイベントの発生に備えることができます。

その他のリソース

詳細については、以下の資料を参照してください。

- AWS Well-Architected
- AWS クラウド導入フレームワークのページ
- AWS 集中ロギングソリューション
- AWS Glue と Amazon QuickSight を使用した AWS CloudTrail ログの視覚化
- ホストベースの侵入検知システムのアラートを Amazon EC2 インスタンスでモニタリングする方法
- Amazon CloudWatch で OS とアプリケーションログファイルを保存およびモニタリングする
- Amazon S3 の Identity and Access Management
- バージョニングの使用 (Amazon S3)
- MFA Delete の使用
- AWS KMS マネージドキー (SSE-KMS) によるサーバー側の暗号化を使用してデータを保護する
- AWS コンソールと CLI を使用したインシデント対応
- カリフォルニア州消費者プライバシー法に備える

メディア

- AWS re: Invent 2014 (SEC402): クラウド内での侵入検知
- AWS re:Invent 2014 (SEC404) クラウド内でのインシデント対応
- AWS re: Invent 2015 (SEC308): クラウド内でのセキュリティイベントのラングリング
- AWS re: Invent 2015 (SEC316): セキュリティインシデント対応シミュレーションでアーキテクチャを強化
- AWS re:Invent 2016 (SEC313): アイデアからコード、実行に至るまでのセキュリティ対応イベントを自動化する
- AWS re: Invent 2017 (SID302): 自動化と Alexa でセキュリティチームの能力を倍加する
- AWS re: Invent 2016 (SAC316): セキュリティオートメーション: アプリケーションのセキュリティ保護に費やす時間を短縮
- AWS re: Invent 2016 (SAC304): 予測セキュリティ:ビッグデータを使用して防御を強化する

- AWS re: Invent 2017 (SID325): Amazon Macie: セキュリティおよびコンプライアンスワークロードのための機械学習を活用したデータ可視性
- AWS ロンドンサミット 2018: AWS でのインシデント対応とフォレンジックの自動化

サードパーティー製ツール

サードパーティー製ツールへの以下のリンクは外部サイトであり、AWS が承認しているものではありません。AWS は、これらのツールやページについて、いかなる保証も表明も行いません。

- AWS_IR - ホストとキーの侵害を軽減する、Python でインストール可能なコマンドラインユーティリティ。
- MargaritaShotgun - リモートメモリ取得ツール。
- ThreatPrep - インシデント処理の準備状況について AWS アカウントのベストプラクティスを評価する Python モジュール。
- ThreatResponse Web - AWS_IR コマンドラインツール用のウェブベースの分析プラットフォーム。
- GRR Rapid Response - インシデント対応のリモートライブフォレンジック。
- Linux Write Blocker - Linux ソフトウェアの書き込みブロックを有効にするカーネルパッチおよびユーザースペースツール。

業界リファレンス

- NIST SP 800-61R2: コンピュータセキュリティインシデント処理ガイド

ドキュメントの改訂

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードをサブスクライブしてください。

update-history-change	update-history-description	update-history-date
マイナーな更新	バグ修正と多くのマイナーな変更。	2021 年 6 月 2 日
マイナーな更新	壊れたリンクを修正しました。	2021 年 3 月 5 日
ホワイトペーパーの更新	壊れたリンクを修正し、テキストの変更を繰り返して読みやすくしました。	2020 年 11 月 23 日
マイナーな更新	「AWS コンソールと CLI を使用したインシデント対応」へのリンクを修正しました。	2020 年 6 月 30 日
ホワイトペーパーの更新	新しいセキュリティサービス、脅威インテリジェンス、コンテナの責任共有、オートメーション、CCPA について更新しました。サンプルの意思決定ツリーとランブックの付録を追加しました。	2020 年 6 月 11 日
初版発行	ホワイトペーパーの初版発行	2019 年 6 月 1 日

付録 A: クラウド機能の定義

AWS は 150 を超えるクラウドサービスと数千の機能を提供しています。これらの多くは、検出、予防、対応機能をネイティブに備えています。その他は、カスタムセキュリティソリューションの設計に使用できます。このセクションでは、クラウド内でのインシデント対応に最も関連するサービスの一部を紹介します。

トピック

ログ記録とイベント

AWS CloudTrail - AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を可能にするサービスです。CloudTrail を使用すると、AWS インフラストラクチャ全体のアクションに関連するアカウントアクティビティをログに記録し、継続的にモニタリングして、保持できます。CloudTrail は、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。これには、AWS マネジメントコンソール、AWS SDK、コマンドラインツール、その他の AWS のサービスを通じて実行したアクションが含まれます。このイベント履歴を活用して、セキュリティ分析、リソース変更の追跡、トラブルシューティングを簡素化できます。

ログファイルの検証は、セキュリティおよびフォレンジック調査で非常に重要です。CloudTrail が配信したログファイルが後で変更、削除、または変更されていないかどうかを判断するには、CloudTrail ログファイルの整合性の検証を使用できます。この機能は、業界標準のアルゴリズム (ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256) を使用して組み込まれています。これにより、検出されずに CloudTrail ログファイルを変更、削除、または偽造することはコンピューティング的に不可能になります。

デフォルトでは、CloudTrail からバケットに配信されるログファイルは、Amazon サーバー側の暗号化で暗号化されます。オプションとして、AWS Key Management Service (AWS KMS) マネージドキー (SSE-KMS) を CloudTrail ログファイルに使用できます。

Amazon CloudWatch Events - Amazon CloudWatch Events は、AWS リソースの変更や、AWS CloudTrail が API コールをいつ発行したかを記述するシステムイベントのストリームをほぼリアルタイムで配信します。すぐに設定できる簡単なルールを使用して、ルールに一致したイベントを 1 つ以上のターゲット関数またはストリームに振り分けることができます。CloudWatch Events は、運用上の変更が発生すると、これを認識します。CloudWatch Events は、これらの運用上の変更に応答し、是正措置として、必要に応じて環境への応答メッセージの送信、機能のアクティブ化、変更の実施、状態情報のキャプチャを行います。Amazon GuardDuty などの一部のセキュリティサービスは、CloudWatch Events の形式で出力を生成します。

AWS Config - AWS Config は、AWS リソースの設定を評価、監査、審査するためのサービスです。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、記録した設定を望ましい設定と照らし合わせて評価する作業を自動化できます。Config を使用すると、設定や AWS リソース間の関係の変更を、手動または自動で確認できます。リソース設定の詳細な履歴を確認し、社内ガイドラインで指定し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、運用のトラブルシューティングを簡素化できます。

Amazon S3 アクセスログ - Amazon S3 バケットに機密情報を保存する場合、S3 アクセスログを有効にして、データの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、バケット自体に変更 (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 ログとは別個に追加されます。

Amazon CloudWatch Logs - Amazon CloudWatch Logs を使用すると、CloudWatch Logs エージェントを使用して Amazon Elastic Compute Cloud (Amazon EC2) インスタンスからのログファイル (オペレーティングシステム、アプリケーション、カスタムのログファイルなど) をモニタリング、保存、アクセスできます。さらに、Amazon CloudWatch Logs は、AWS CloudTrail、Amazon Route 53 の DNS クエリ、VPC フローログ、Lambda 関数、その他のソースからのログをキャプチャできます。その後に、関連するログデータを CloudWatch Logs から取得できます。

Amazon VPC フローログ - VPC フローログを使用すると、VPC 内のネットワークインターフェイスとの間で行き来する IP トラフィックの情報をキャプチャできます。フローログを作成すると、そのデータを Amazon CloudWatch Logs で表示および取得できます。VPC フローログは、いくつかのタスクで役立つ場合があります。例えば、フローログを使用してインスタンスに到達していない特定のトラフィックのトラブルシューティングを行うことができます。これは、制限が過度に厳しいセキュリティグループルールの診断に役立ちます。また、フローログをセキュリティツールとして使用し、インスタンスへのトラフィックをモニタリングすることもできます。

AWS WAF ログ - AWS WAF は、サービスで検査したすべてのウェブリクエストの完全なログ記録をサポートするようになりました。これらのログは、コンプライアンスと監査のニーズに合わせて

Amazon S3 に保存したり、デバッグや追加のフォレンジックに役立てたりすることができます。これらのログを参照して、特定のルールがトリガーされた理由や、特定のウェブリクエストがブロックされた理由を理解できます。また、ログを SIEM ツールやログ分析ツールと統合することもできます。

その他の AWS ログ - イノベーションのペースに合わせて、AWS はほぼ毎日お客様向けの新しい機能をデプロイし続けています。したがって、ログ記録およびモニタリング機能を提供する AWS のサービスは何十種類もあります。AWS のサービスごとに利用できる機能については、そのサービスに関する AWS 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 CSPM - AWS Security Hub CSPM は、AWS アカウント全体にわたって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の包括的なビューを提供します。Security Hub を使用すると、複数の AWS のサービス (Amazon GuardDuty、Amazon Inspector、Amazon Macie など) および AWS パートナーソリューションからのセキュリティアラートや検出結果を 1 つの場所で集約、整理、優先順位付けできます。検出結果は、統合されたダッシュボードで実用的なグラフと表を使って視覚的にまとめられます。AWS のベストプラクティスと所属組織が従う業界標準に基づく自動化されたコンプライアンスチェックを使用して、継続的に環境をモニタリングすることもできます。

Amazon GuardDuty - Amazon GuardDuty はマネージド脅威検出サービスです。悪意のある行為や不正行為を継続的にモニタリングし、AWS アカウントやワークロードを保護できるようにします。アカウント侵害の可能性を示す異常な API コールや不正なデプロイなどのアクティビティをモニタリングします。GuardDuty は、インスタンスへの侵入の可能性や攻撃者による偵察も検出します。

GuardDuty では、統合された脅威インテリジェンスフィードを使用して疑わしい攻撃者を特定し、機械学習を使用してアカウントやワークロードアクティビティの異常を検出します。潜在的な脅威を検出すると、GuardDuty コンソールと AWS CloudWatch Events に詳細なセキュリティアラートを配信します。これにより、アラートに基づく対処が可能になり、既存のイベント管理システムやワークフローシステムにアラートを統合しやすくなります。

Amazon Macie - Amazon Macie は AI を活用したセキュリティサービスで、AWS に保存した機密データを自動的に検出、分類、保護してデータ損失を防止できます。Amazon Macie では、機械学習を使用して、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ます。また、このようなデータを組織内のどこに保存し、どのように利用し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えいのリスクを検出すると、アラートを配信します。

AWS Config ルール - AWS Config ルールは、リソースの望ましい設定を表し、これらの設定と AWS Config に記録された関連リソースの設定変更を照合して評価します。ルールとリソースの設定を照合して評価した結果はダッシュボードで確認できます。Config ルールを使用することで、設定の観点から全体的なコンプライアンスおよびリスクステータスを評価し、経時的なコンプライアンス傾向を確認できます。また、どの設定変更がリソースのルール違反をもたらしたかを特定できます。

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、パフォーマンスとセキュリティを向上させるオンラインリソースです。Trusted Advisor は、AWS のベストプラクティスに従ってリソースをプロビジョニングする際に役立つガイダンスをリアルタイムで提供します。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は、CloudWatch Events の統合を含め、Trusted Advisor のすべてのチェックを利用できます。

Amazon CloudWatch - Amazon CloudWatch は、AWS クラウドリソースと AWS で実行するアプリケーションをモニタリングするサービスですAmazon CloudWatch を使用すると、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、および AWS リソースへの変更に対する自動的な対応が可能です。Amazon 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 リソースをモニタリングできます。さらに、アプリケーションやサービスが生成するカスタムメトリクスと、アプリケーションが生成するあらゆるログファイルもモニタリングできます。Amazon CloudWatch を使用して、システム全体のリソース使用率、アプリケーションパフォーマンス、オペレーションヘルスを可視化できます。これらのインサイトを使用して適切に対応し、アプリケーションのスムーズな動作を維持できます。

Amazon Inspector - Amazon Inspector は、AWS にデプロイしたアプリケーションのセキュリティとコンプライアンスを向上させるための自動化されたセキュリティ評価サービスです。Amazon Inspector は、アプリケーションの脆弱性やベストプラクティスからの逸脱を自動的に評価します。Amazon Inspector は、評価の実行後に、セキュリティの評価結果を重要度の順に詳細なリストとして表示します。これらの結果は直接確認できます。または、Amazon Inspector コンソールや API を介して詳細な評価レポートの一部としても確認できます。

Amazon Detective - Amazon Detective はセキュリティサービスであり、AWS リソースからログデータを自動的に収集し、機械学習、統計的分析、グラフ理論を使用して、リンクされたデータセットを構築します。これにより、迅速かつ効率的なセキュリティ調査を簡単に実施できます。Amazon Detective は、Virtual Private Cloud (VPC) フローログ、AWS CloudTrail、Amazon GuardDuty などの複数のデータソースからの数兆個のイベントを分析できます。また、リソースとユーザー、および両者間の経時的なやり取りのインタラクティブな統合ビューを自動的に生成します。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 か所で可視化できます。これにより、調査結果の原

因の候補を絞り込み、関連する履歴アクティビティを詳しく調査して、根本原因をすばやく判断できます。

オートメーション

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、他の AWS のサービスをカスタムロジックで拡張したり、AWS のスケール、パフォーマンス、セキュリティで動作する独自のバックエンド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すべての管理を自動的に行います。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オートスケーリング、コードとセキュリティパッチのデプロイ、コードのモニタリングとログ記録が含まれます。お客様はコードを提供するだけで済みます。

AWS Step Functions - AWS Step Functions を使用すると、視覚的なワークフローを使用して、分散アプリケーションとマイクロサービスのコンポーネントを簡単に調整できます。Step Functions では、グラフィカルコンソールを使用して、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して可視化できます。これにより、複数のステップからなるアプリケーションを簡単に構築および実行できます。Step Functions は、各ステップが自動的にトリガーおよび追跡し、エラーが発生した場合は再試行するため、アプリケーションが整然と意図したとおりに実行します。

Step Functions は、各ステップの状態をログに記録し、問題が発生した場合は、問題をすばやく診断してデバッグできます。コードを書かなくても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簡単に進化させ、イノベーションを迅速化できます。AWS Step Functionsは AWS サーバーレスプラットフォームの一部であり、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トできます。Step Functions は、Amazon EC2 や Amazon ECS などのコンピューティングリソースを使用したマイクロサービスのオーケストレーションにも使用できます。

AWS Systems Manager - AWS Systems Manager を使用すると、AWS でインフラストラクチャを可視化および制御できます。Systems Manager では、統合されたユーザーインターフェイスを使用して、複数の AWS のサービスからの運用データを表示し、AWS リソース全体にわたって運用タスクを自動化できます。Systems Manager では、リソースをアプリケーションごとにグループ化し、運用データを表示してモニタリングとトラブルシューティングを行い、リソースのグループに対してアクションを実行できます。Systems Manager は、インスタンスを定義したままの状態に保ち、オンデマンド変更 (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) を行ったり、その他のオートメーションやパッチ適用のタスクを実行したりできます。

安全なストレージ

Amazon S3 - Amazon S3 は、任意の量のデータの保存と取得をどこからでも行えるように設計されたオブジェクトストレージです。これは 99.999999999% の耐久性を提供するように設計されています。このストレージに保存した何百万というアプリケーションのデータは、あらゆる業界のマーケットリーダーに使用されています。Amazon S3 は包括的なセキュリティを提供し、お客様の規制要件を満たすように設計されています。お客様は現在使用している方法でデータを柔軟に管理し、コスト最適化、アクセスコントロール、コンプライアンスを達成できます。Amazon S3 にはクエリインプレース機能があり、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ます。Amazon S3 は最もサポートされているクラウドストレージサービスであり、サードパーティーソリューションの最大のコミュニティ、システムインテグレーターパートナー、その他の AWS のサービスと統合されています。

Amazon S3 Glacier - Amazon S3 Glacier は、安全性と耐久性に優れた、きわめて低コストのクラウドストレージサービスであり、データのアーカイブや長期バックアップに使用できます。99.999999999% の耐久性を実現するように設計され、包括的なセキュリティを提供します。また、規制要件を満たすように設計されています。Amazon S3 Glacier にはクエリインプレース機能があり、保管中のアーカイブデータに対して強力な分析を直接実行できます。Amazon S3 Glacier は、低コストに抑えつつさまざまな取り出しニーズに対応する目的で、アーカイブへのアクセス時間が数分から数時間までの 3 つのオプションを提供しています。

カスタム

前述のサービスと機能は、すべてを網羅したものではありません。AWS は継続的に新しい機能を追加しています。詳細については、「AWS の新機能」および「AWS クラウドセキュリティ」のページを参照してください。AWS がネイティブクラウドサービスとして提供するセキュリティサービスに加えて、AWS のサービス上に独自の機能を構築することもできます。

AWS CloudTrail、Amazon GuardDuty、Amazon Macie などのセキュリティサービスの基本セットをアカウント内で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付加価値を引き出すこともできます。AWS セキュリティコンピテンシープログラムに記載しているものなど、多数のパートナーツールを利用できます。また、独自のクエリを作成してログを検索することもできます。AWS が提供する膨大な数のマネージドサービスを使用すれば、このカスタマイズは従来とは比較にならないほど容易になっています。このホワイトペーパーの対象ではありませんが、Amazon Athena、Amazon OpenSearch Service、Amazon QuickSight、Amazon Machine Learning、Amazon EMR など、調査に役立つ他の AWS のサービスが数多くあります。

付録 B: サンプルコード

AWS CloudTrail イベントの例

次の例は、Alice という名前の IAM ユーザーが AWS CLI で ec2-stop-instances を使用して Amazon EC2 の StopInstancesaction を呼び出したことを示しています。

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
    },
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        },
        "previousState": {
            "code": 16,
            "name": "running"
        }
    }]}}
}]}
```

AWS CloudWatch Event の例

次の Amazon CloudWatch Event の例は、jane-roe-test という名前の AWS IAM ユーザーが www.github.com に公開された状態であることが判明し、権限のないユーザーに悪用される可能性があることを示しています。

```
{
  "check-name": "Exposed Access Keys",
  "check-item-detail": {
    "Case ID": "02648f3b-e18f-4019-8d68-ce25efe080ff",
    "Usage (USD per Day)": "0",
    "User Name (IAM or Root)": "jane-roe-test",
    "Deadline": "1440453299248",
    "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
    "Time Updated": "1440021299248",
    "Fraud Type": "Exposed",
    "Location": "www.github.com"
  },
  "status": "ERROR",
  "resource_id": "",
  "uuid": "cce6d28f-e44b-4e61-aba1-5b4af96a0f59"
}
```

インフラストラクチャドメイン CLI アクティビティの例

次の AWS CLI コマンドは、インフラストラクチャドメイン内のイベントに対応する例を示しています。この例では、AWS API を使用して、このホワイトペーパーで説明しているインシデント対応の初期アクティビティの多くを実行しています。

```
# Anomaly detected on IP X.X.X.X. Capture that instance's metadata
> aws ec2 describe-instances --filters "Name=ip-address,Values=X.X.X.X"
```

```
# Protect that instance from accidental termination
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute
 disableApiTermination --value true
```

```
# Switch the EC2 instance's Security Group to a restricted Security Group
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4
```

```
# Detach from the Auto Scaling Group
> aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name
 web-asg
```

```
# Deregister the instance from the Elastic Load Balancer
> aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-
balancer-name web-load-balancer
```

```
# Create an EBS snapshot
> aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-
REFERENCE-ID"
```

```
# Create a new EC2 instance from the Forensic Workstation AMI
> aws ec2 run-instances --image-id ami-4n6x4n6x --count 1 --instance-type c4.8xlarge --
key-name forensicPublicKey --security-group-ids sg-1a2b3c4d --subnet-id subnet-6e7f819e
```

```
# Create a new EBS volume copy from the EBS snapshot
> aws ec2 create-volume --region us-east-1 --availability-zone us-east-1a --snapshot-id
 snap-abcd1234 --volume-type io1 --iops 10000
```

```
# Attach the volume to the forensic workstation
> aws ec2 attach-volume --volume-id vol-1234abcd --instance-id i-new4n6x --device /dev/
sdf
```

```
# Create a security group rule to allow the new Forensic Workstation to communicate to
 the contaminated instance.
> aws ec2 authorize-security-group-ingress --group-id sg-a1b2c3d4 --protocol tcp --port
 0-65535 --source-group sg-1a2b3c4d
```

```
# Tag the contaminated instance with the ticket or reference ID
> aws ec2 create-tags -resources i-abcd1234 -tags
 Key=Environment,Value=Quarantine:REFERENCE-ID
```

付録 C: ランブックの例

次のランブックの例は、より大きなランブックの 1 つのエントリを表しています。このランブックは非公式であり、例としてのみ提供しています。 ランブックを作成していくうちに、各シナリオは進化して大規模化し、前提や侵害の指標は異なってきますが、いずれも結果や是正措置は似た内容になります。ランブックで変化を達成すると、他の状況でもより優れた対応やインサイトに富む対応ができるようになります。

インシデント対応ランブック - ルートの使用

目的

このランブックの目的は、AWS ルートアカウントの使用を管理する方法に関する具体的なガイダンスを提供することです。このランブックは、詳細なインシデント対応戦略に代わるものではありません。このランブックでは、以下の IR ライフサイクルに焦点を当てます。

- コントロールを確立する。
- 影響を判断する。
- 必要に応じて復旧する。
- 根本原因を調査する。
- 改善する。

侵害の指標 (IOC)、初期ステップ (被害を食い止める)、およびこれらのステップを実行するために必要な詳細な CLI コマンドを以下に示します。

前提

- CLI が設定およびインストール済みである。
- 報告プロセスが設定済みである。
- Trusted Advisor がアクティブになっている。
- Security Hub がアクティブになっている。

侵害の指標

- アカウントでの異常なアクティビティ。

  - IAM ユーザーの作成。
  - CloudTrail がオフになっている。
  - Cloudwatch がオフになっている。
  - SNS が一時停止している。
  - Step Functions が一時停止している。
- 新しい AMI または予期しない AMI の起動。
- アカウントでの連絡先の変更。

修正ステップ - コントロールの確立

侵害された可能性があるアカウントに関する AWS ドキュメントでは、以下の具体的なタスクを挙げています。侵害された可能性のあるアカウントに関するドキュメントは、「AWS アカウントの不正なアクティビティに気付いた場合、どうすればよいですか?」にあります。

1. できるだけ早く AWS サポート と TAMに連絡する。
2. ルートパスワードの変更とローテーションを行い、ルートに関連する MFA デバイスを追加する。
3. 修正ステップに関連するパスワード、アクセス/シークレットキー、CLI コマンドをローテーションする。
4. ルートユーザーが実行したアクションを確認する。
5. これらのアクションのランブックを開く。
6. インシデントを閉じる。
7. インシデントを確認し、何が起きたかを理解する。
8. 根本的な問題を修正して、改善を実装し、必要に応じてランブックを更新する。

その他のアクション項目 - 影響を判断する

作成済みの項目と変化している呼び出しを確認します。将来アクセスできるように項目が作成済みになっている場合があります。以下を確認します。

- IAM クロスアカウントロール。
- IAM ユーザー。
- S3 バケット。
- EC2 インスタンス。

- [このリストは、アプリケーションとインフラストラクチャで使用します。]

注意

お客様は、この文書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明しており、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤーまたはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または暗示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で締結されるいかなる契約の一部でもなく、その内容を修正するものでもありません。