
aws
SUMMIT
ONLINE
JAPAN | MAY 11-12, 2021

AWS-39

AWS 環境における脅威検知と対応

桐山 隼人
シニアセキュリティソリューションアーキテクト
アマゾン ウェブ サービス ジャパン株式会社

自己紹介

- 氏名: 桐山 隼人

- 役割:
  - AWS 利用者のセキュリティにまつわる課題解決のご支援
  - クラウドセキュリティの考え方や実現方法のご提案

- 好きな AWS サービス:

AWS Security Hub　Amazon GuardDuty　Amazon Inspector　Amazon Macie　Amazon Detective

本セッションの対象者とゴール

- 対象者
  - アマゾンウェブサービス (AWS) 環境のセキュリティ対策に関する設計・実装を管理する方
  - 組織のセキュリティ監視と運用を行い、インシデントの検知や対応を実施する方

- ゴール
  - AWS サービスを用いて、高度な脅威検知とインシデント対応を実施方法を学び、組織全体のセキュリティ管理の仕方を理解する

- 本セッションでお話しないこと
  - 一般的なセキュリティ管理策に関する基本的な説明
  - AWS セキュリティサービス以外の細かな仕様や詳細解説 (AWS サービスの基本知識が前提)

目次

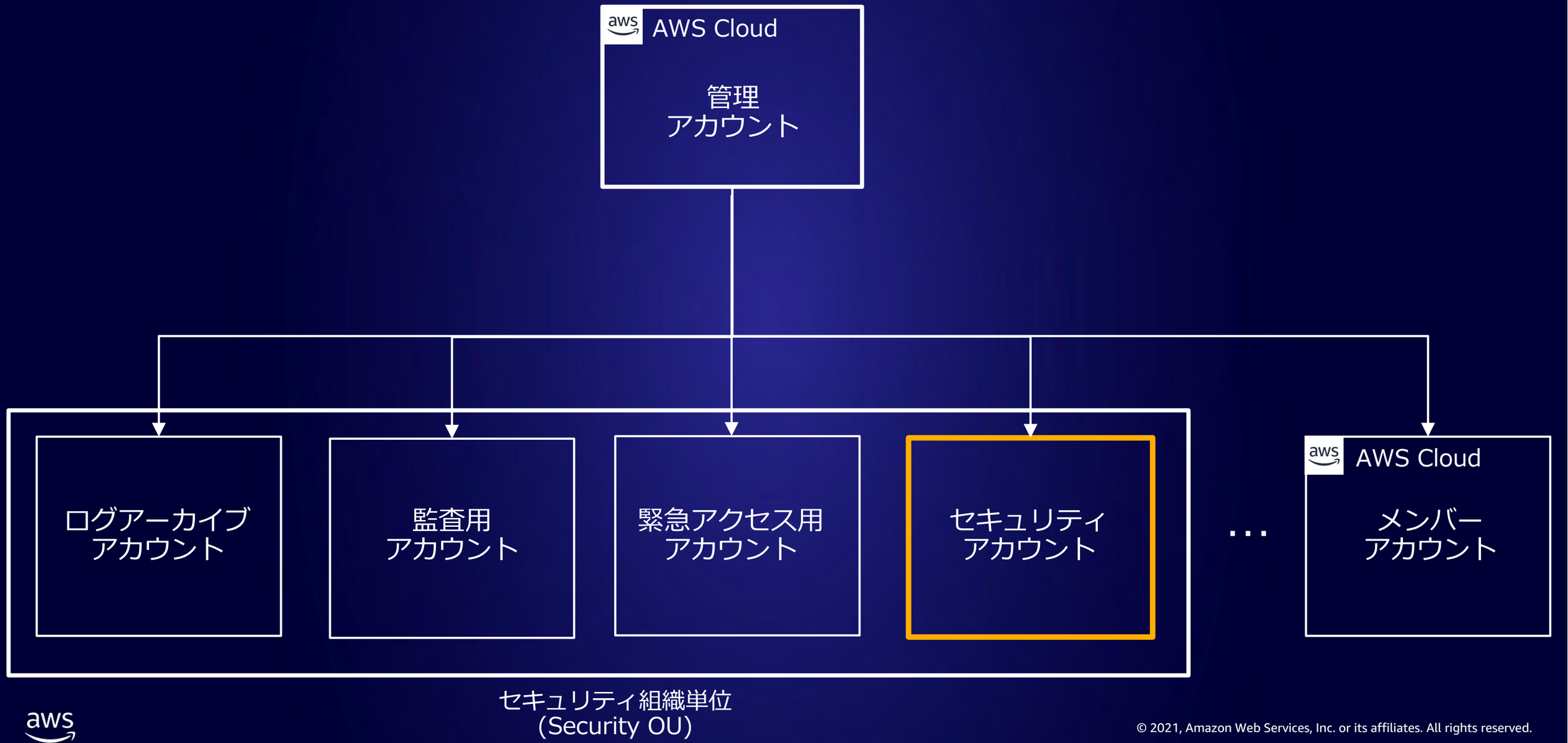
AWS セキュリティサービスによる組織全体の保護

AWS セキュリティサービスによる多層防御

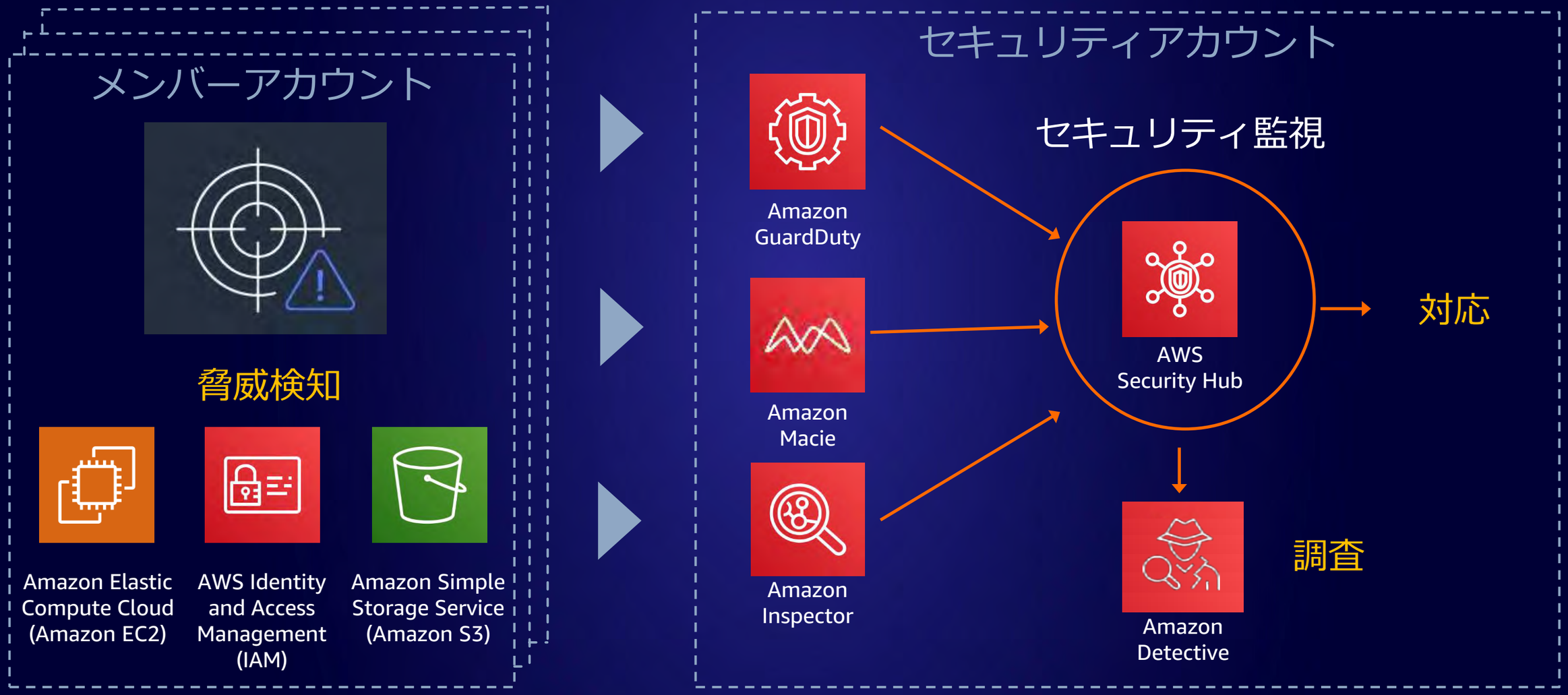
AWS アカウントの理解

- AWS アカウントとは
  - AWS クラウドサービスのリソースコンテナ
  - 明示的なセキュリティ境界
  - コストの追跡と請求のためのコンテナ
  - 制限と閾値(サービスクォータや API 閾値など)を適用するメカニズム
- より多くのアプリケーションやサービスを運用するために、AWS アカウントを追加する (マルチアカウント)

マルチアカウントにおけるセキュリティ組織単位



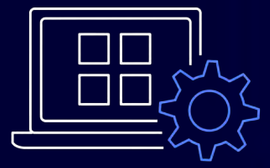
セキュリティアカウントによる検知・対応・調査



変化する環境において脅威を検知するには (Amazon GuardDuty)

Amazon GuardDuty

脅威インテリジェンスと継続的監視により
拡大していく AWS アカウントやリソースを効果的に保護

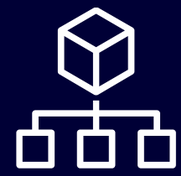


ワンクリックで
有効化
性能影響も無し

AWS アカウント
とリソースの
継続的監視

各リージョンの
結果による
グローバル対応

既知の脅威と
未知の脅威を
検出



組織全体の統合
と管理

Amazon GuardDuty データソース

VPC フローログ

VPC のネットワークインターフェースとの間で送受信される IP トラフィックに関する情報

DNS ログ

Amazon EC2 インスタンスから、既知および未知の疑わしいドメインに対して行われたクエリ

CloudTrail イベント

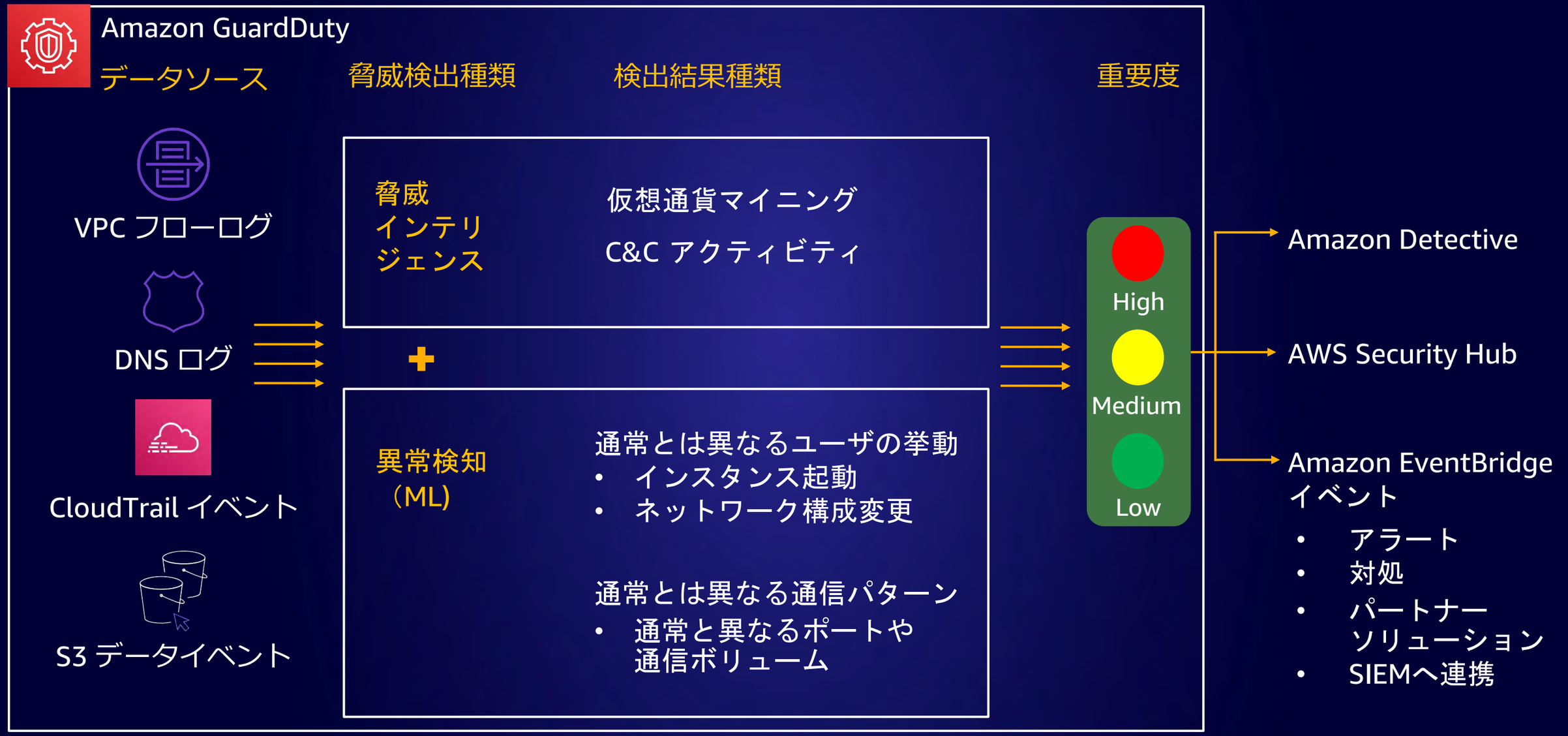
AWS マネジメントコンソール、SDK、および AWS CLI へのアクセスに使用されたAPI 呼び出しの履歴

S3 データイベント

リソース内で実行される API の呼び出し履歴

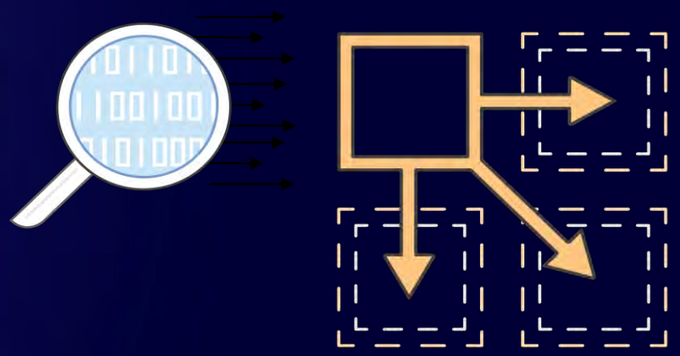
- GetObject
- ListObjects
- DeleteObject
- PutObject

Amazon GuardDuty 動作



Amazon GuardDuty が検出する既知の脅威

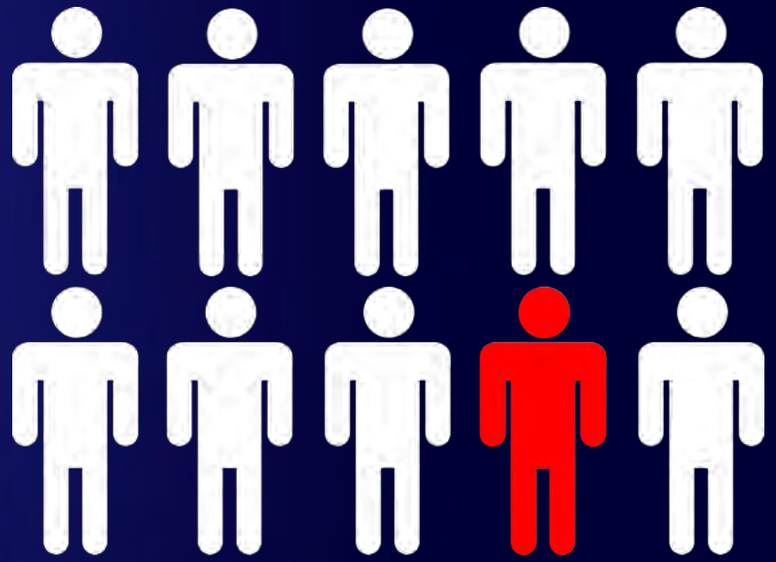
- 様々なソースからの脅威インテリジェンスを活用
  - AWS 固有のインテリジェンス
  - AWS パートナーの脅威インテリジェンス（CrowdStrike, Proofpoint）
  - お客様が提供する脅威インテリジェンス
- 脅威インテリジェンスを用いて GuardDuty が識別するもの
  - 既知のマルウェアに感染したホスト
  - 匿名プロキシ
  - マルウェアやハッカーツールをホストしているサイト
  - 暗号通貨マイニングプールとウォレット



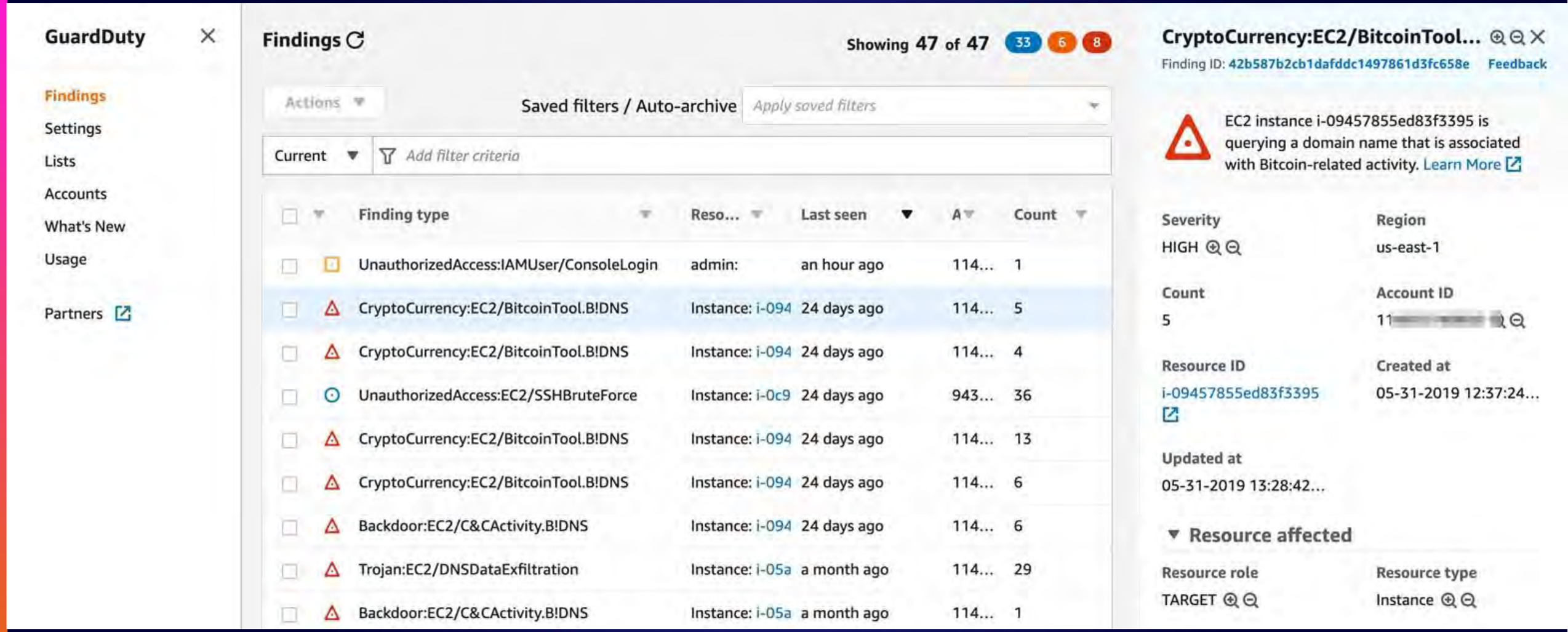
Amazon GuardDuty が検出する未知の脅威

異常な振る舞いを検出するためのアルゴリズム

- ヒューリスティックのための信号パターンの検査
- 正常なプロファイリングと偏差の確認
- 機械学習による分類



検出結果の確認：Amazon GuardDuty 管理画面

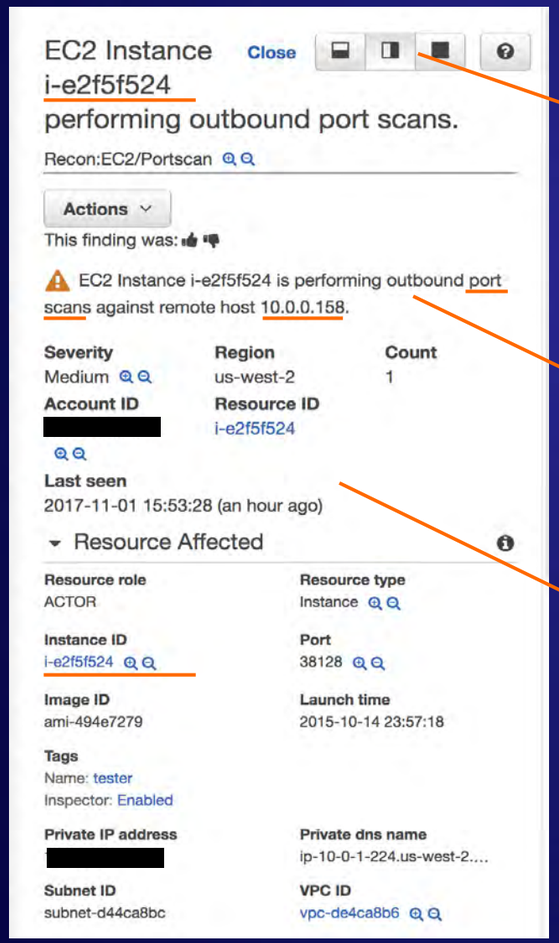


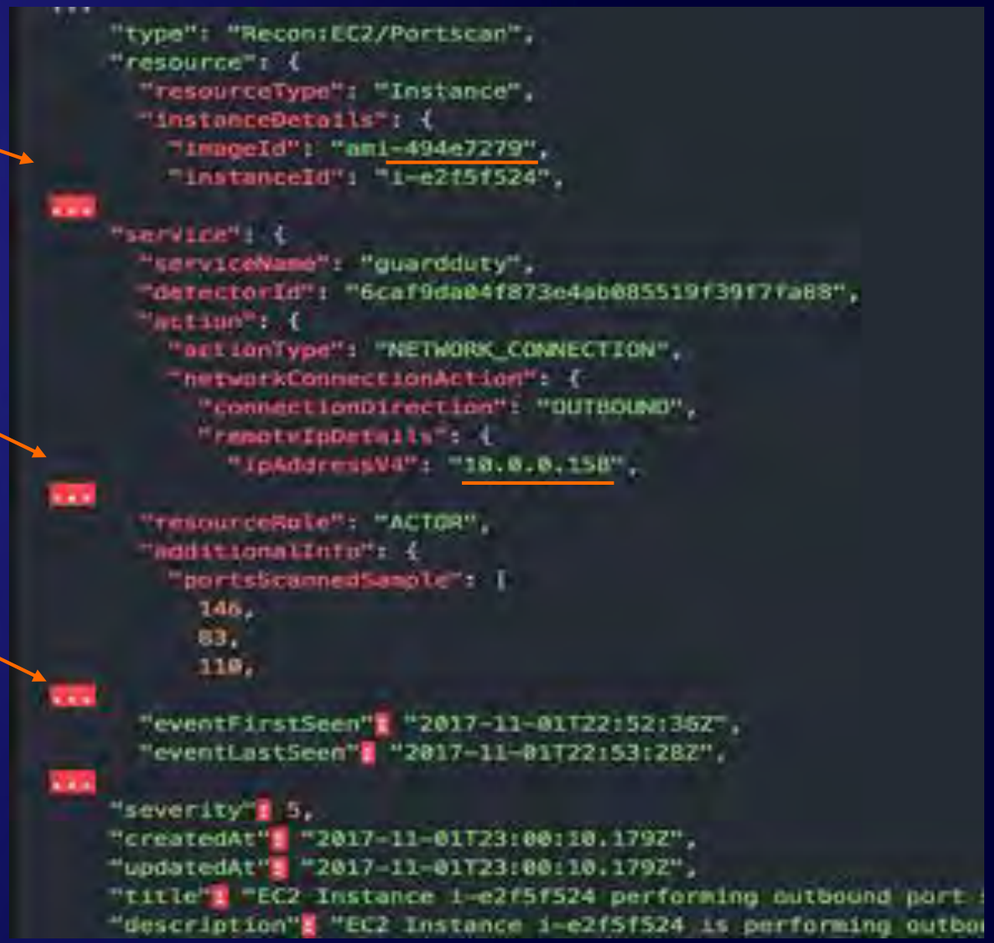
検出結果の確認：API/JSON 形式詳細

AWS 管理画面

API/JSON 形式

脅威情報
- 重要度
- リージョン
- 数/頻度
- 脅威種類
- 影響するリソース
- 脅威ソース





検出結果の確認：**Amazon EventBridge** イベント

- GuardDuty が送信する一つのイベントには、脅威を検出してから5分間の情報が集約される
- EventBridge イベントは、グラフ化、保存、エクスポート、分析などに利用される


```
{
 "version": "0",
 "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
 "detail-type": "GuardDuty Finding",
 "source": "aws.guardduty",
 "account": "111122223333",
 "time": "1970-01-01T00:00:00Z",
 "region": "us-east-1",
 "resources": [],
 "detail": {COMPLETE_GUARDDUTY_FINDING_JSON}
}
```


Amazon GuardDuty に紐付くイベント例

検出結果に基づくアクション

検知

Amazon GuardDuty

集約

AWS Security Hub

検出結果とインサイト

通知

Amazon EventBridge

イベント

対応

増大する脅威を監視し対応するには **(AWS Security Hub)**

AWS Security Hub

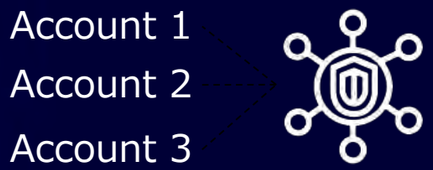
組織内の様々なセキュリティデータを集約
一元的に可視化してリスクを評価

調査結果を集約し
時間を節約

自動チェックで
セキュリティ体制
を改善

厳選された
セキュリティ
ベスト
プラクティス

標準化された検出
結果フォーマット
とのシームレスな
統合



マルチアカウント
の統合

AWS Security Hub 動作概要

Amazon GuardDuty

AWS Firewall Manager

Amazon Inspector

AWS Systems Manager Patch manager

Amazon Macie

IAM Access Analyzer

AWS Config

パートナーソリューション

AWS Security Hub

検出結果の集約と優先順位付け

ベンチマークに対して自動セキュリティチェックを実施

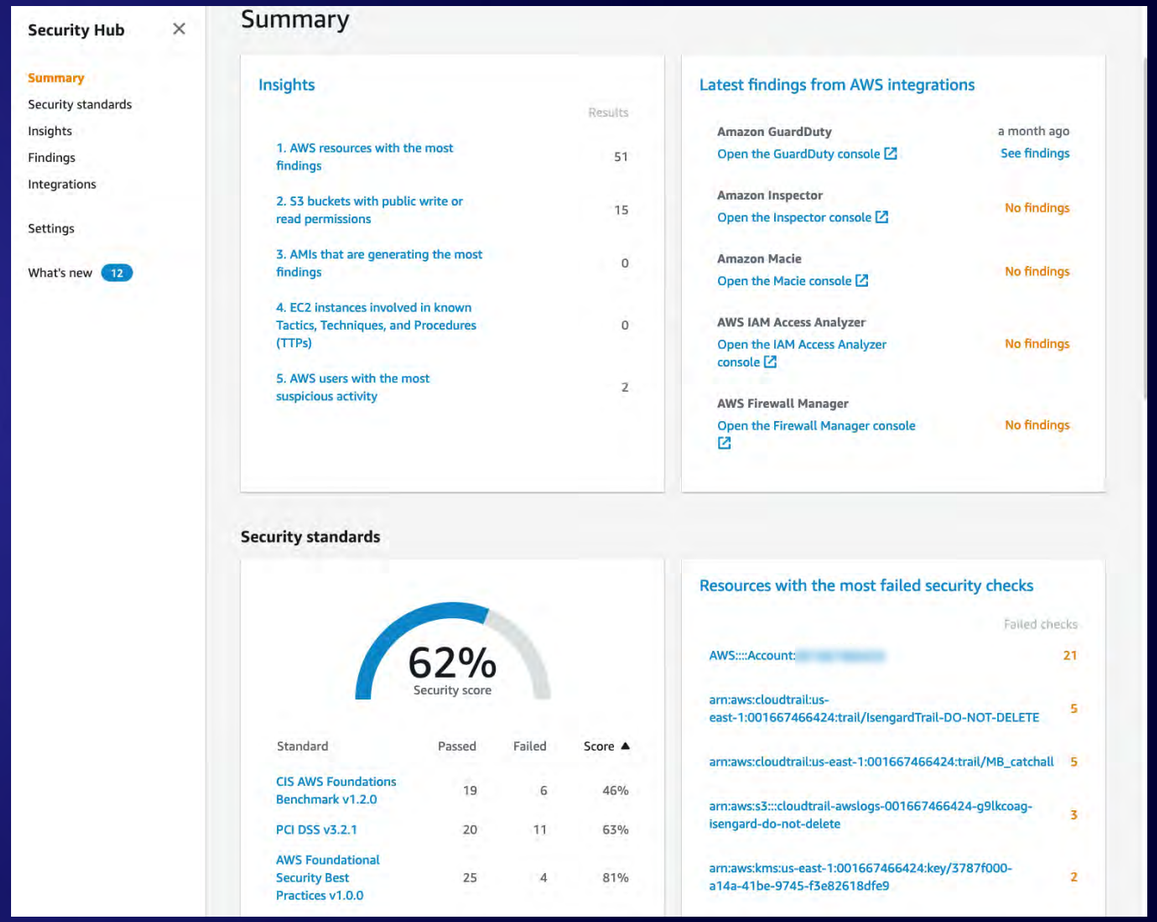
調査、対応、修正のための措置を講じる

ユースケースの概要

1. **検出結果の優先順位付けとアクションの実行**
   組織内の全ての AWS アカウントのセキュリティイベントを表示

2. **統合と連携**
   正規化された共通形式で、イベントをSIEMまたはログ管理ツールに送信

3. **可視性**
   組織内の全ての AWS アカウントのコンプライアンス遵守状況を可視化



AWS セキュリティサービスとの統合

各サービスの検出結果を Security Hub に集約し、一元的に可視化

Amazon GuardDuty
- 脅威検知に関する全ての検出結果

Amazon Inspector
- セキュリティ評価による全ての検出結果

Amazon Macie
- ポリシー違反時の検出結果

AWS IAM Access Analyzer
- 自身のアカウント内のリソースに対して、外部からのアクセスを許可するポリシー記述を検出した時の検出結果

AWS Firewall Manager
- AWS WAF ポリシーや Web ACL ルールのコンプライアンス非準拠時の検出結果
- AWS Shield Advanced によりリソース保護されていない、または攻撃を検知した時の検出結果

AWS Systems Manager Patch Manager
- EC2インスタンスがパッチベースラインに基づくコンプライアンスルールに非準拠の時の検出結果

Available AWS service integrations
https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-internal-providers.html

パートナー製品の統合

50以上のサードパーティ製品とオープンソースツール

AWS Security Hub へ検出結果を送信

Firewalls

Barracuda
Check Point SOFTWARE TECHNOLOGIES LTD.
paloalto NETWORKS
SOPHOS

Vulnerability

tenable
Qualys. Continuous Security
RAPID7

Endpoint

CROWDSTRIKE
Symantec
aqua
paloalto NETWORKS

Compliance

paloalto NETWORKS
McAfee Together is power.
Check Point SOFTWARE TECHNOLOGIES LTD.
turbot
Cloud Custodian

MSSP

ARMOR CLOUD SECURITY, UNCOMPROMISED.
ALERT LOGIC

Other

CYBERARK

AWS Security Hub

Amazon EventBridge

Event (event-based)

検出結果に基づいた対応アクション

servicenow
paloalto NETWORKS
ATLASSIAN
RAPID7
pagerduty
IBM Security
slack
splunk>
sumologic
Cloud Custodian

aws

AWS Security Hub インサイト

グループ化条件(Group By)によってフィルターされる検出結果

- フィルタリング後の上位結果をダッシュボードに表示
- 32の事前定義インサイトが AWS および AWS パートナーから提供
- 利用者が独自のインサイトを作成可能

重要な脆弱性に対するセキュリティパッチが欠けているEC2 インスタンス

機密データを含むS3 バケット

パブリックの書込または読取権限を持つ S3 バケット

検出結果数別の上位AMI*

*Amazon Machine Image

AWS Security Hub のインサイト
https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-insights.html

セキュリティ評価の自動化

- 150以上のセキュリティ項目の継続的評価を自動化
- 評価結果はダッシュボードに表示されすばやくアクセス可
- コンプライアンス遵守に役立つベストプラクティス情報の提供

セキュリティ基準

AWS 基礎セキュリティのベストプラクティス

- AWS アカウントとリソースが、AWS セキュリティベストプラクティスと一致していないことを検出する一連の自動セキュリティチェック
- AWS セキュリティの専門家によって定義
- 基本的な AWS サービスをカバー、AWS 環境におけるセキュリティの改善に役立つ

EBS スナップショットはパブリックであってはなりません

S3 ブロックパブリックアクセス設定を有効にする必要があります

VPC のデフォルトのセキュリティグループ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を許可しない必要があります

Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります

セキュリティ基準

CIS AWS Foundations Benchmark

- Center for Internet Security (CIS) が定義した、AWS のセキュリティ設定のベストプラクティス
- CIS 要件の一部に対するコンプライアンス遵守状況を自動的にチェック

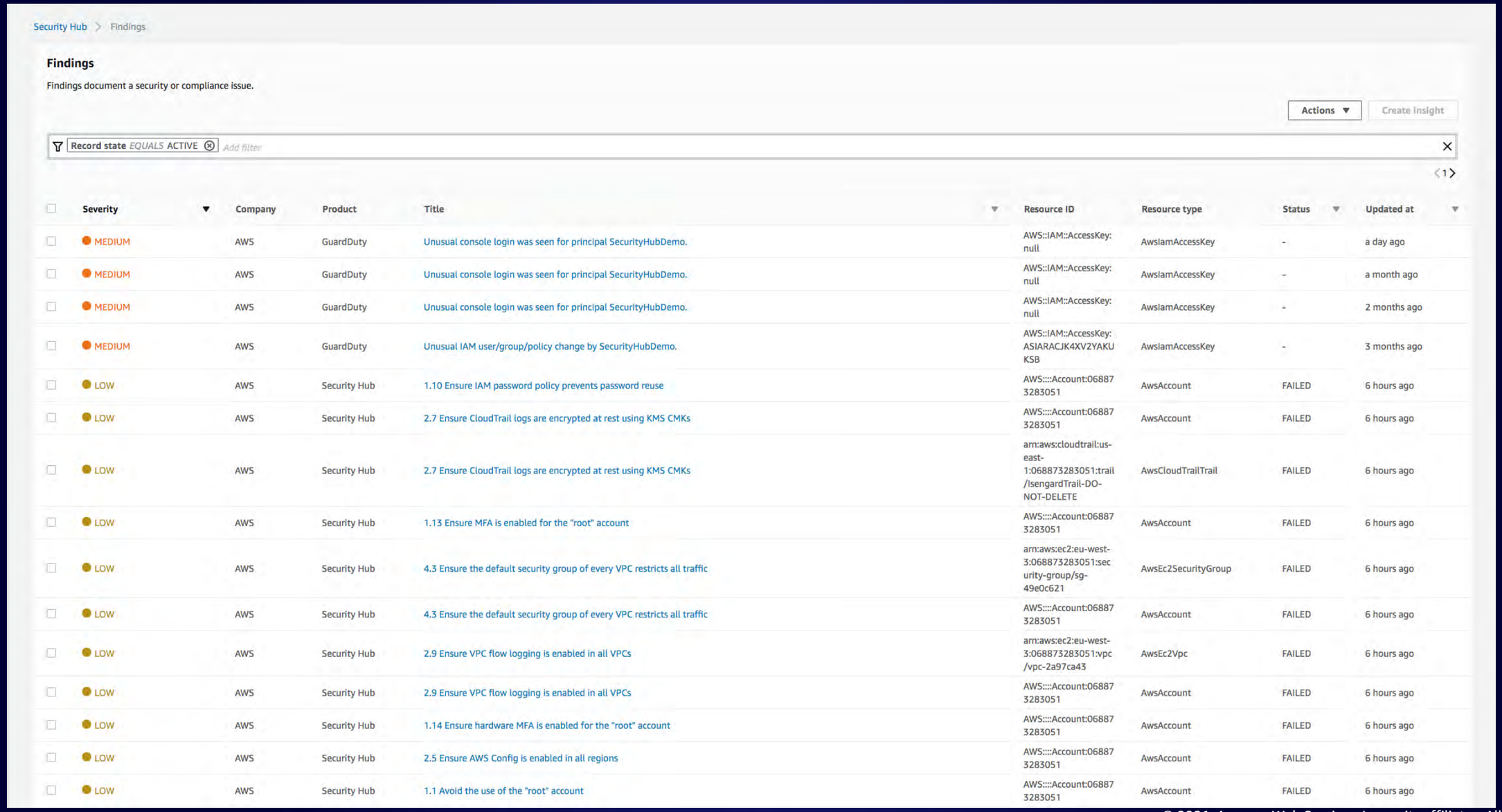
「ルート」アカウントの使用を避ける

CloudTrail がすべてのリージョンで有効であることを確認する

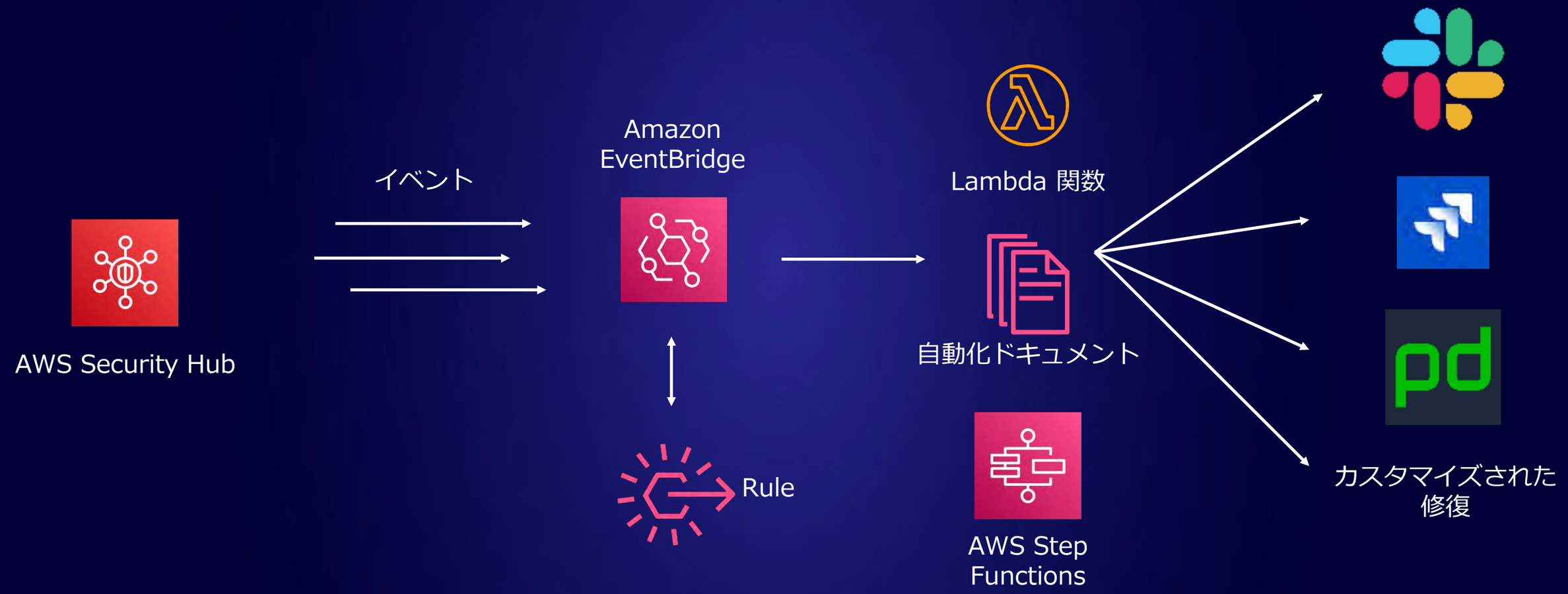
どのセキュリティグループも 0.0.0.0/0 からポート 22 への侵入を許可していないことを確認する

完全な「*:*」管理権限を許可する IAM ポリシーが作成されていないことを確認する

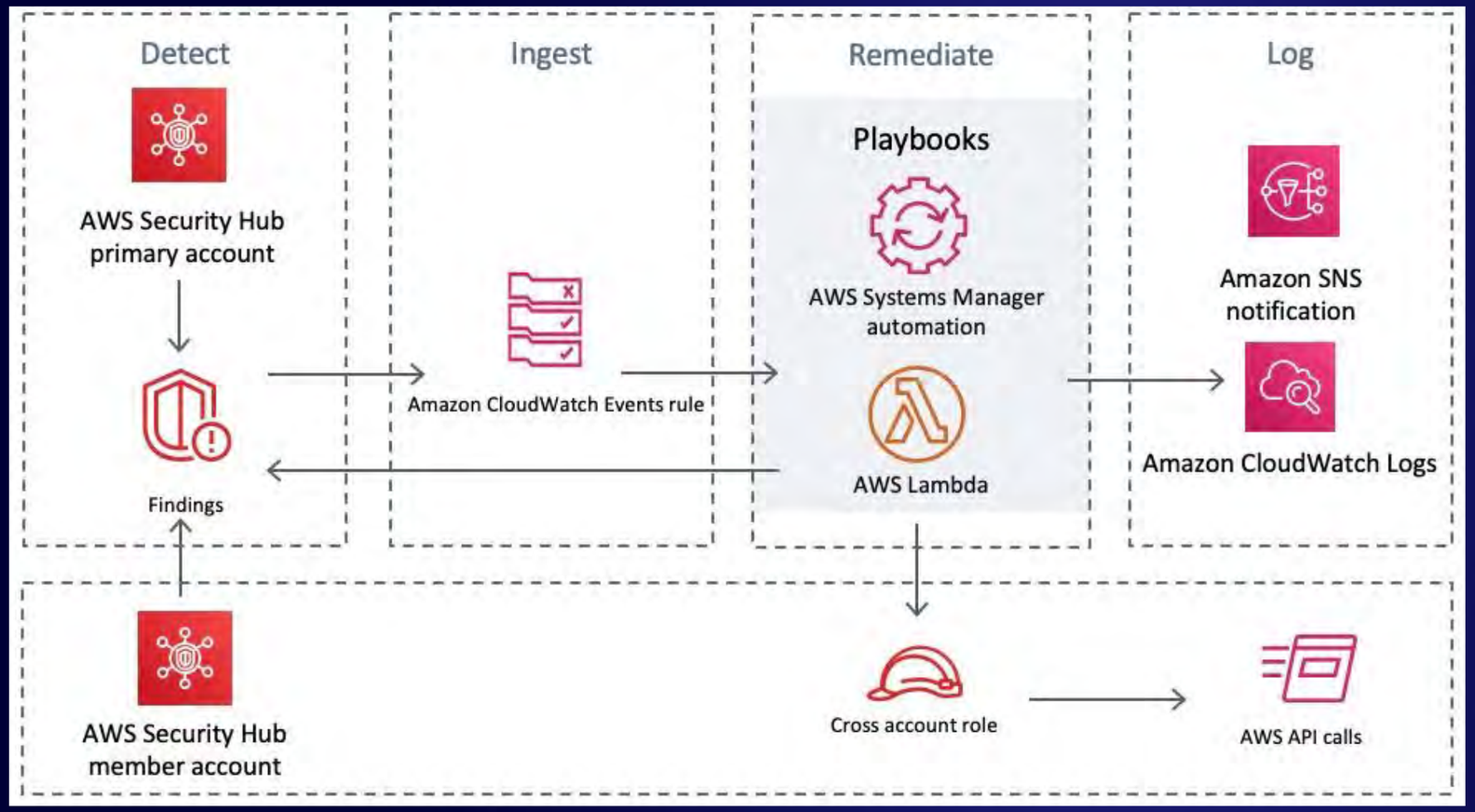
検出結果の表示例



カスタマイズ可能な対応と修復アクション



AWS ソリューション
AWS Security Hub の自動化された応答と修復



以下の典型的な使い方を示すテンプレートを提供するソリューション
(下URL参照)

- セキュリティイベント検出
- 結果の取り込み
- 自動修正
- 対応の記録

AWS Security Hub Automated Response and Remediation
https://aws.amazon.com/solutions/implementations/aws-security-hub-automated-response-and-remediation/

対応すべき脅威を調査するには
(Amazon Detective)

Amazon Detective とは

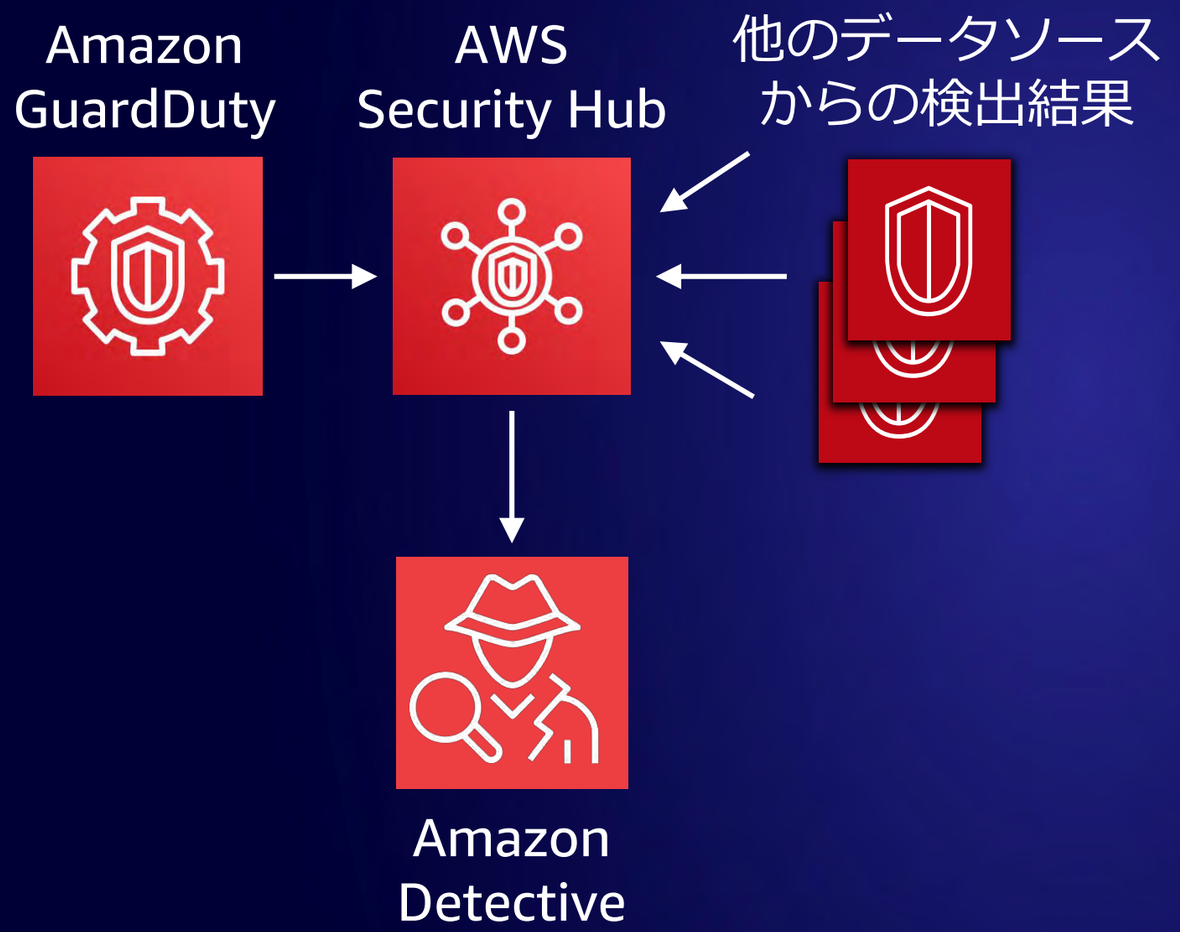
セキュリティ問題の根本原因を迅速に分析、調査、特定

ビルトインされた
データ収集

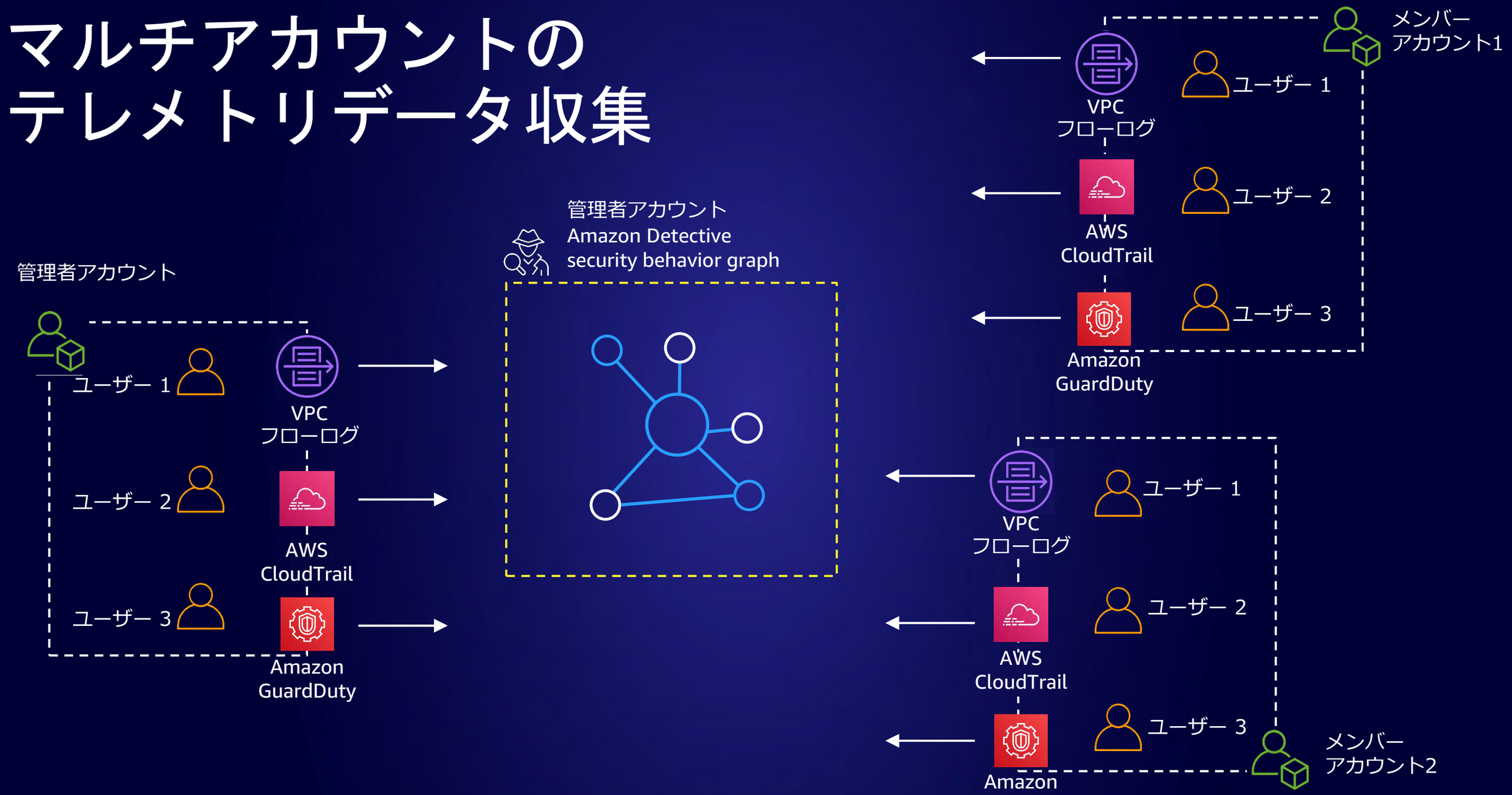
分析の
自動化

インサイトの
視覚化

Amazon Detective 利用フロー



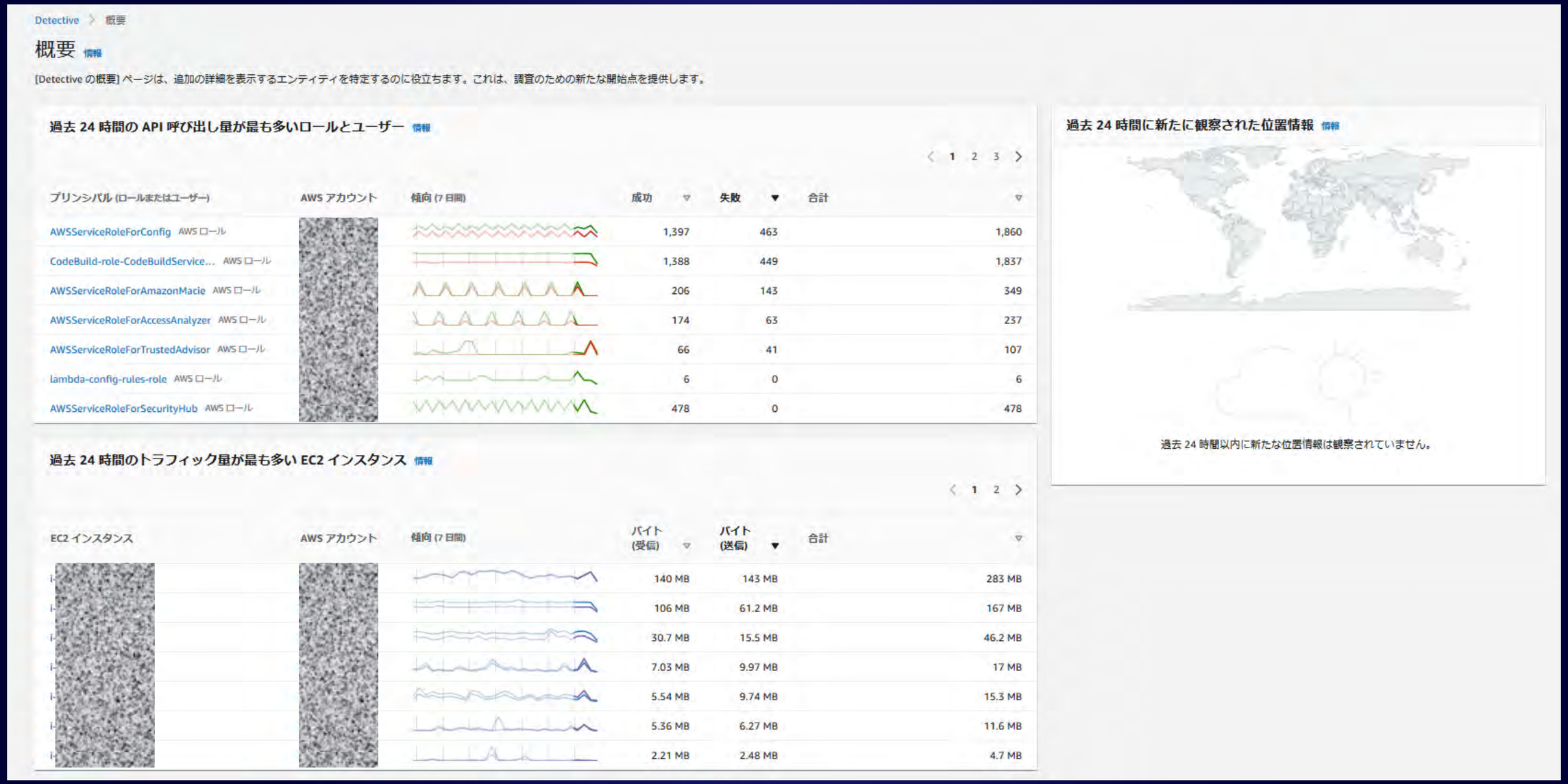
マルチアカウントの
テレメトリデータ収集



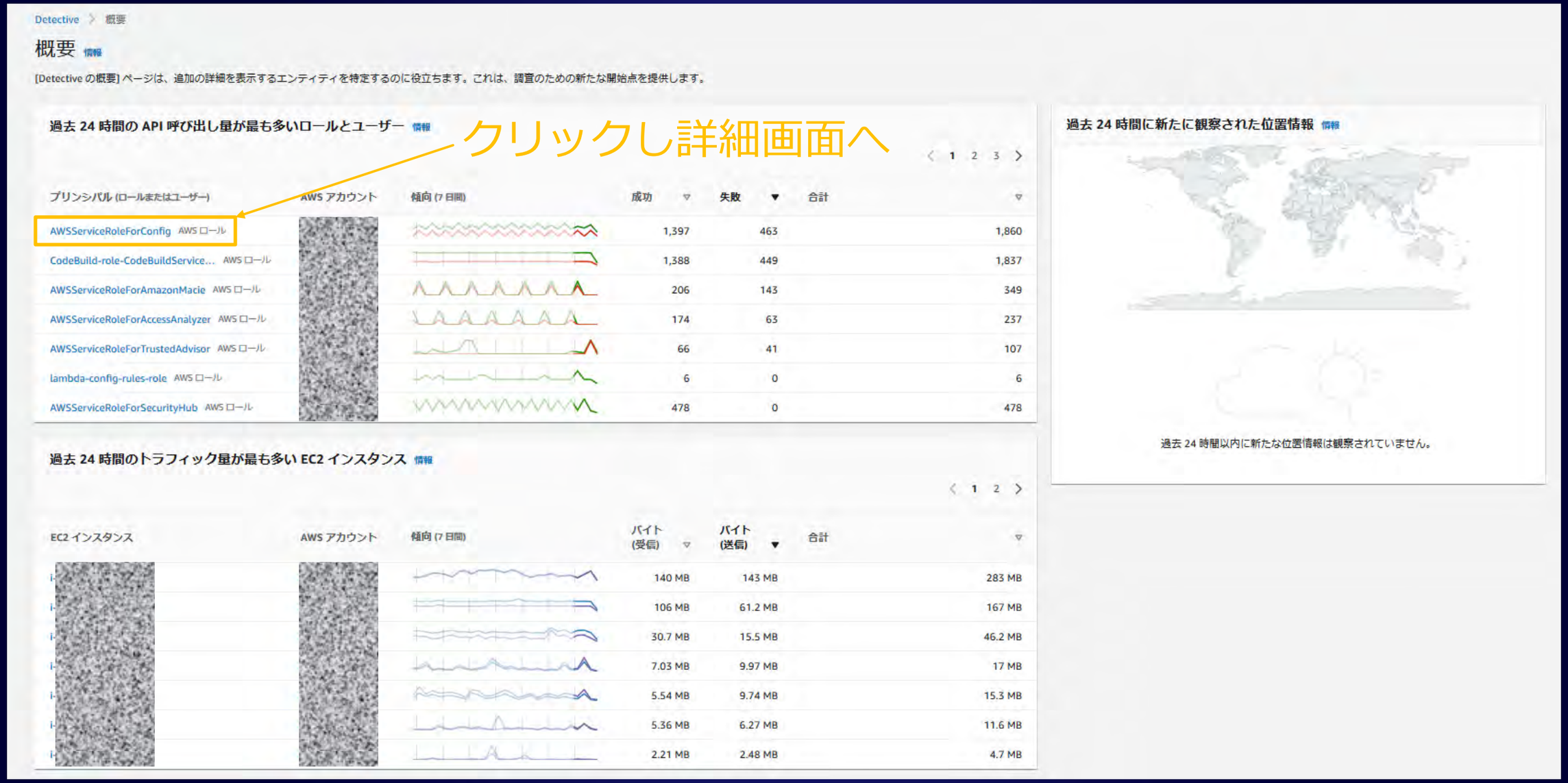
継続的な集約とグラフモデルへの変換

Security Behavior Graph

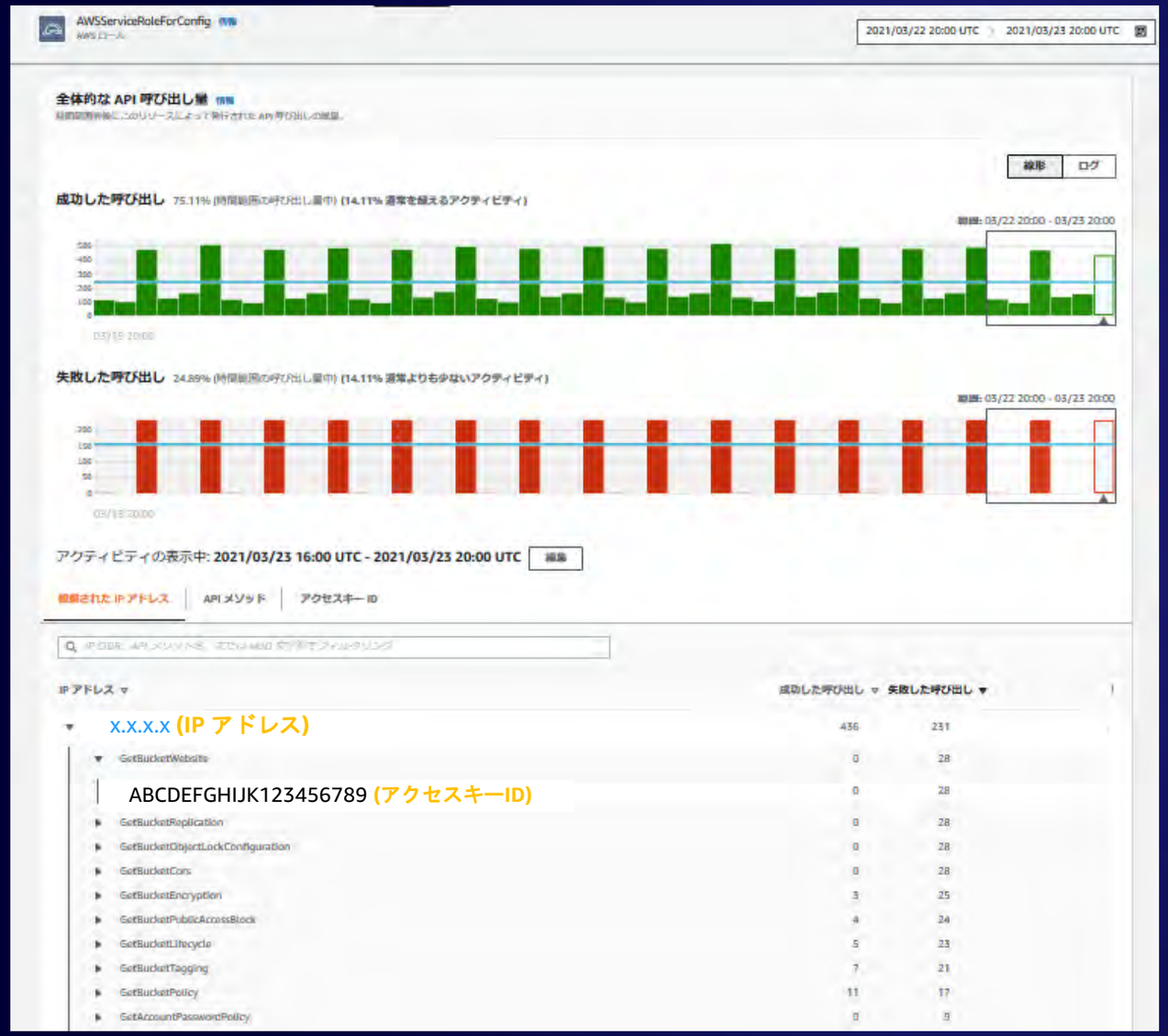
Amazon Detective 概要画面



Amazon Detective 概要画面



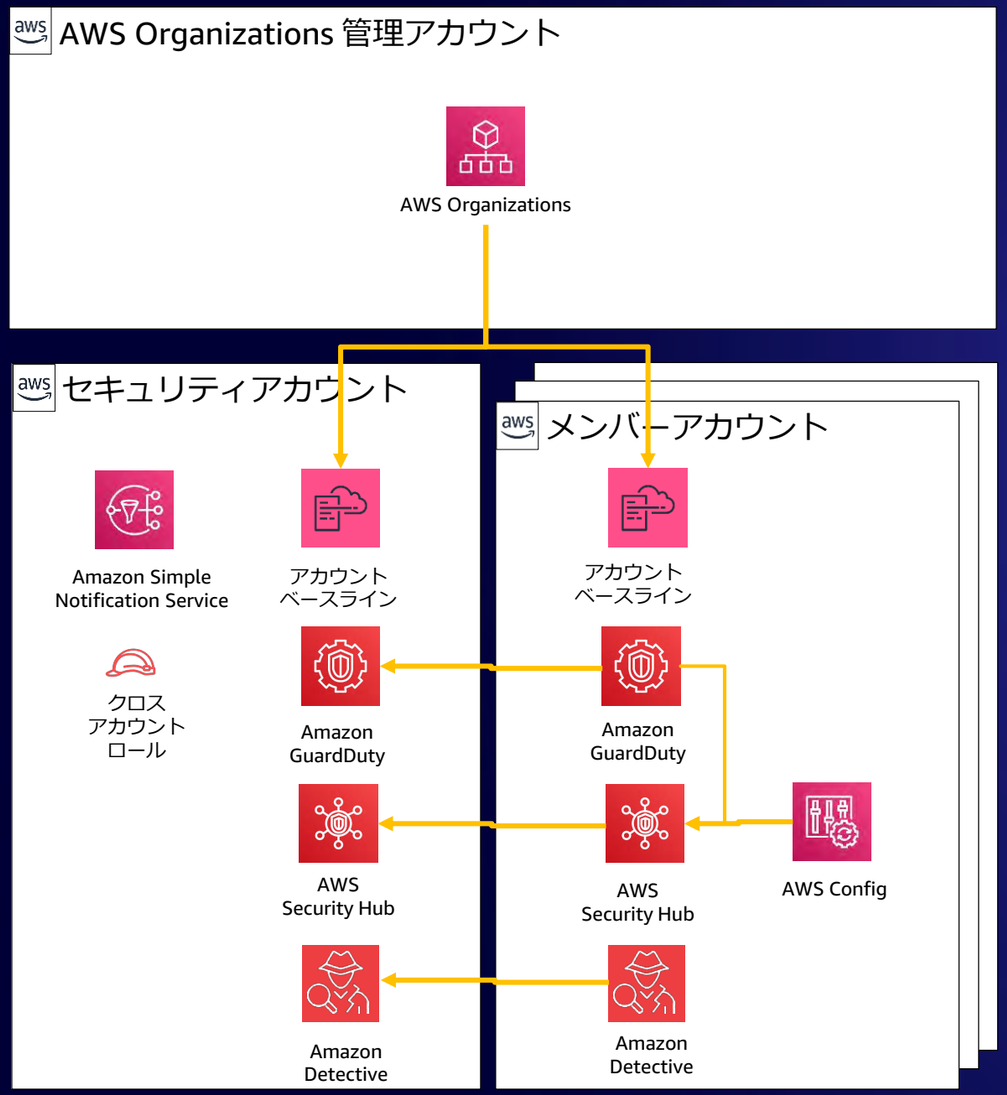
Amazon Detective 詳細画面



指定したプリンシパルにおける API コールの時系列データを確認

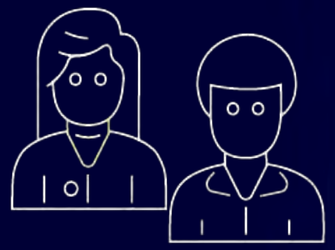
成功(もしくは失敗)API コールの IP アドレスやアクセスキー ID を調査

セキュリティアカウントによる集中管理



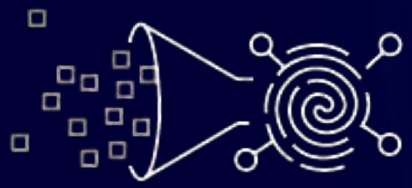
- Amazon GuardDuty, AWS Security Hub, Amazon Detective の権限移譲された管理アカウント (Delegated Administrator) にセキュリティアカウントを指定する
- AWS Organizations 配下のメンバーアカウントに対して、Amazon GuardDuty, AWS Security Hub を一括自動有効化可能
- Amazon Detective のメンバーアカウントは、セキュリティアカウントから招待することで関連付ける

まとめ



組織全体のセキュリティを保護するには
全ての AWS アカウントをセキュリティ監視対象とする

脅威の検知、対応、調査を実施するには
Amazon GuardDuty, AWS Security Hub, Amazon Detective など AWS で利用可能なセキュリティサービスを理解する



AWS セキュリティサービスを活用するには
AWS マルチアカウント環境において、AWS セキュリティサービスを有効化するだけでスケーラブルに展開する

セキュリティ関連セッション

セッションID	セッションタイトル
AWS-37	入門！ AWS アイデンティティサービス
AWS-38	AWSにおけるネットワーク＆アプリケーション保護のすすめ
AWS-39	AWS環境における脅威検知と対応
AWS-48	ISMAPに基づくクラウドコンプライアンスの向上
AWS-52	AWSアカウントを守るためにおさえておきたいセキュリティ対策
AWS-55	AWSにおける安全なWebアプリケーションの作り方

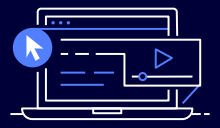
Thank you!

桐山 隼人

シニアセキュリティソリューションアーキテクト
アマゾン ウェブ サービス ジャパン株式会社

AWS トレーニングと認定

AWS クラウドをキャリアに活用してください



デジタルトレーニング

クラウドのスキルを構築する無料のオンデマンドコースを探索する

クラスルームトレーニング

エキスパートインストラクターによるトレーニングに参加する

AWS 認定の取得

業界で認められている認定を取得する

教育プログラム

AWS のスキルと経験を持つ人材に出会える

エンタープライズリソース

学習ニーズ分析とAWSランプアップガイドを活用する

詳細はこちら　https://aws.amazon.com/jp/training/