



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
Amazon Web Services ジャパン株式会社

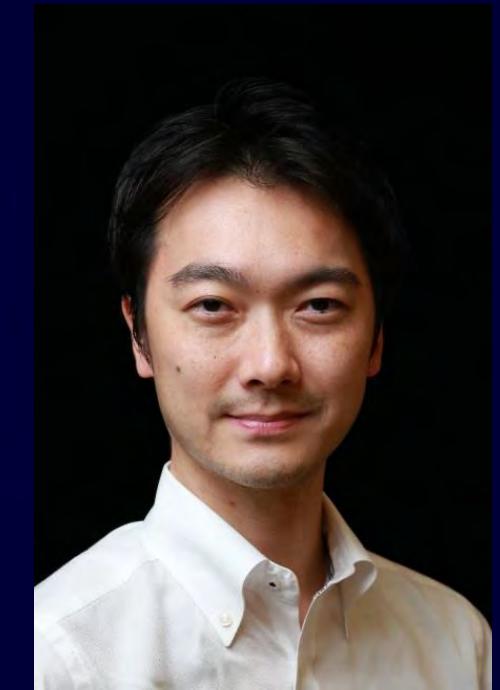


自己紹介

■ 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

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

増大する脅威を監視し対応するには (AWS Security Hub)

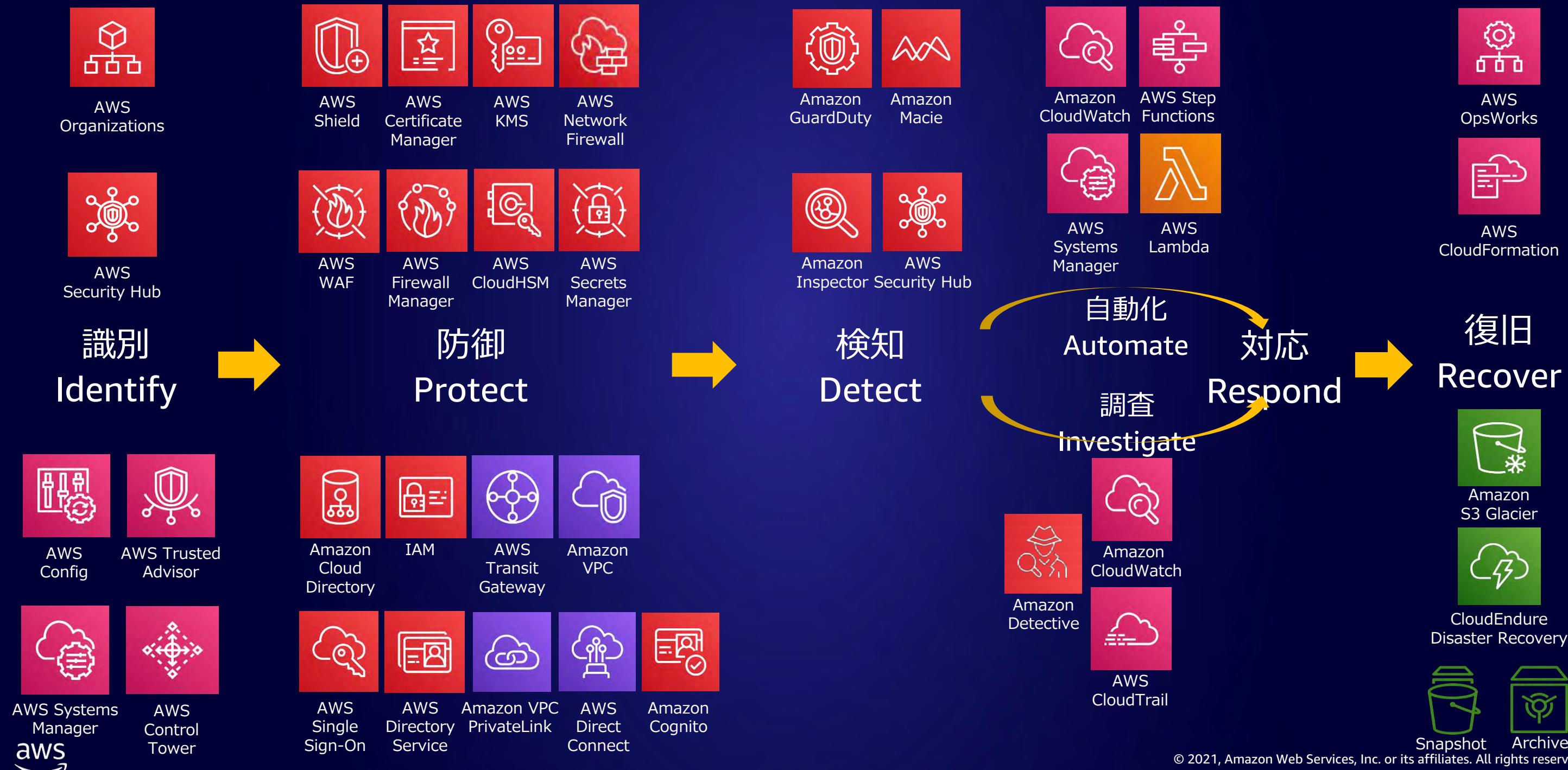
対応すべき脅威を調査するには (Amazon Detective)

まとめ



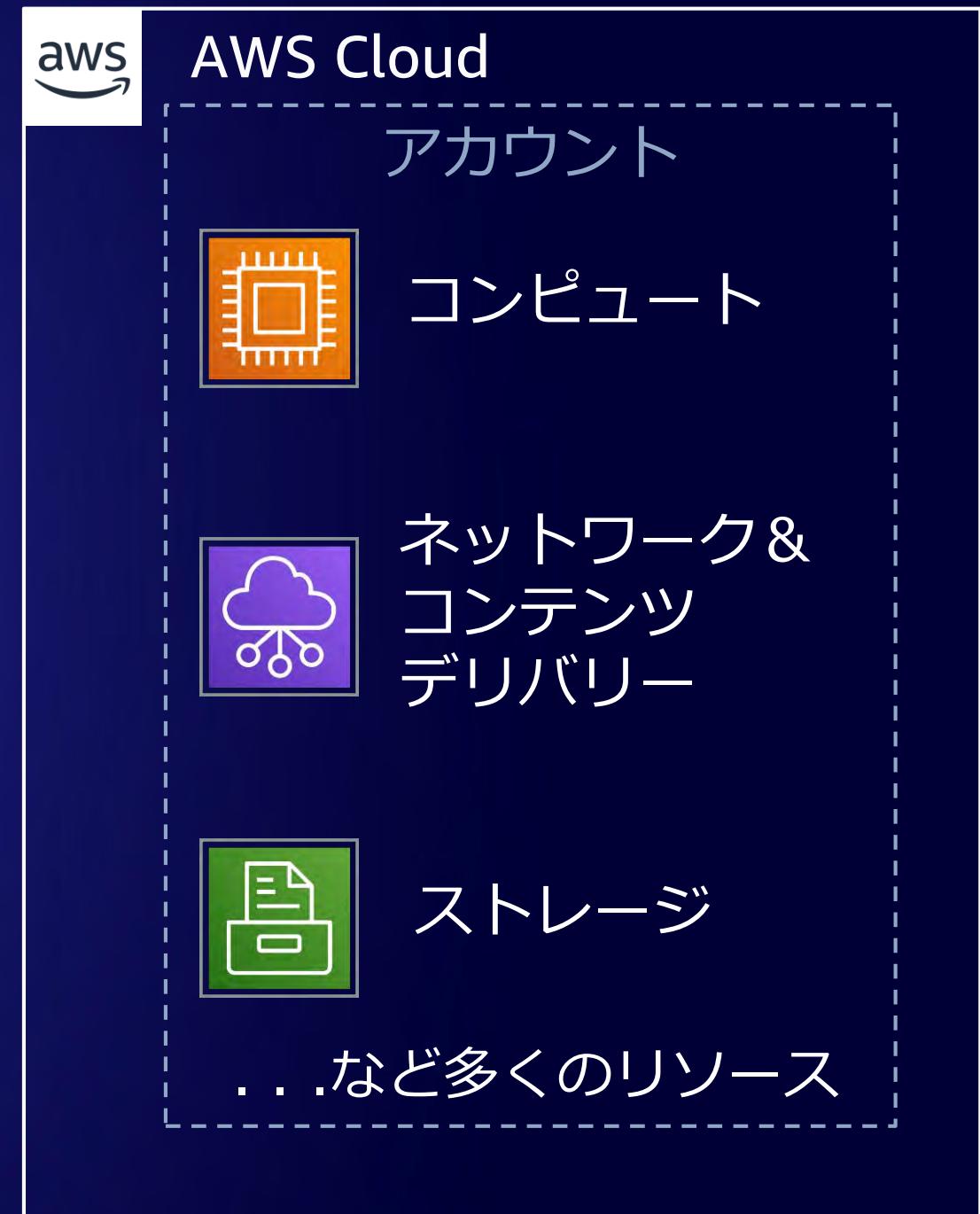
AWS セキュリティサービス による組織全体の保護

AWS セキュリティサービスによる多層防御

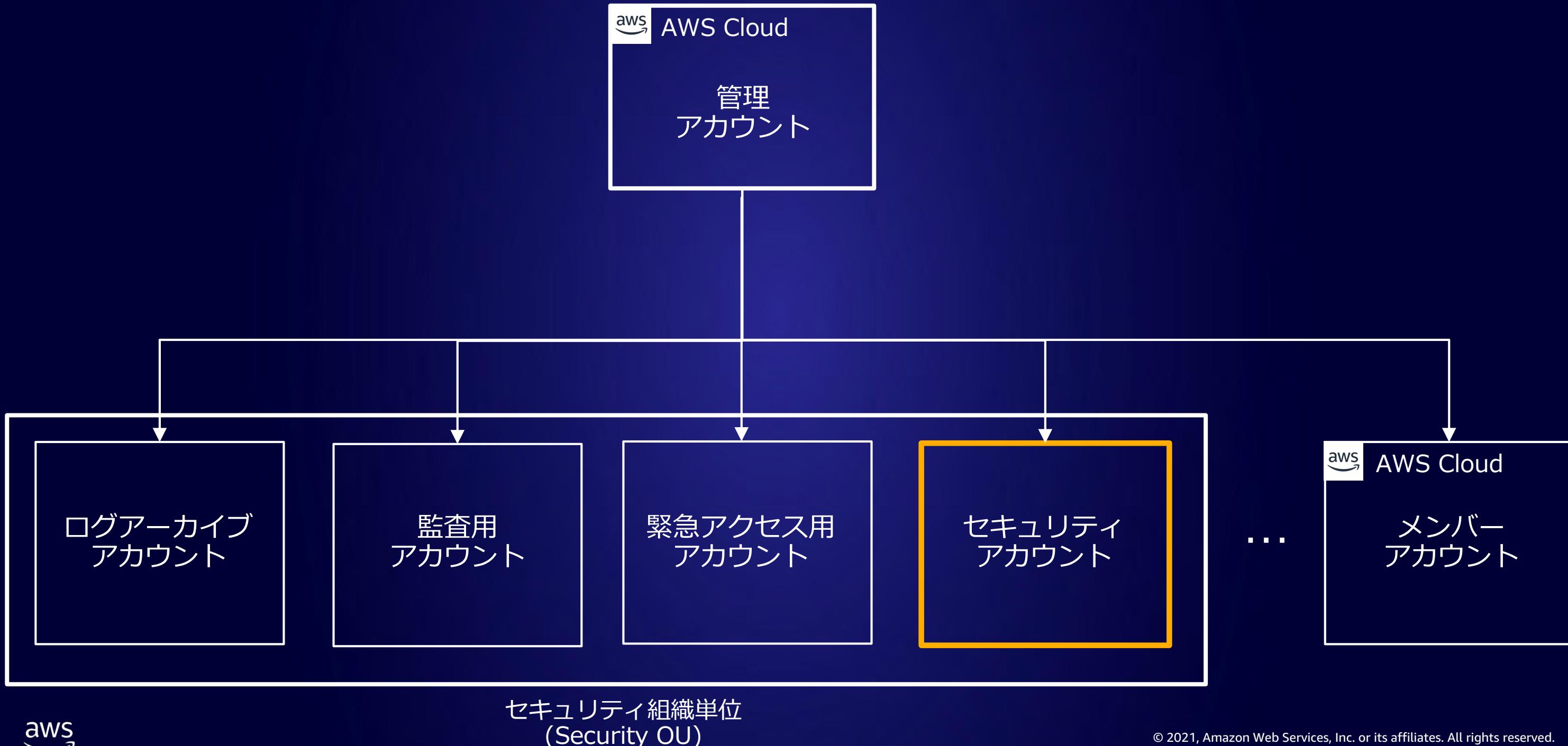


AWS アカウントの理解

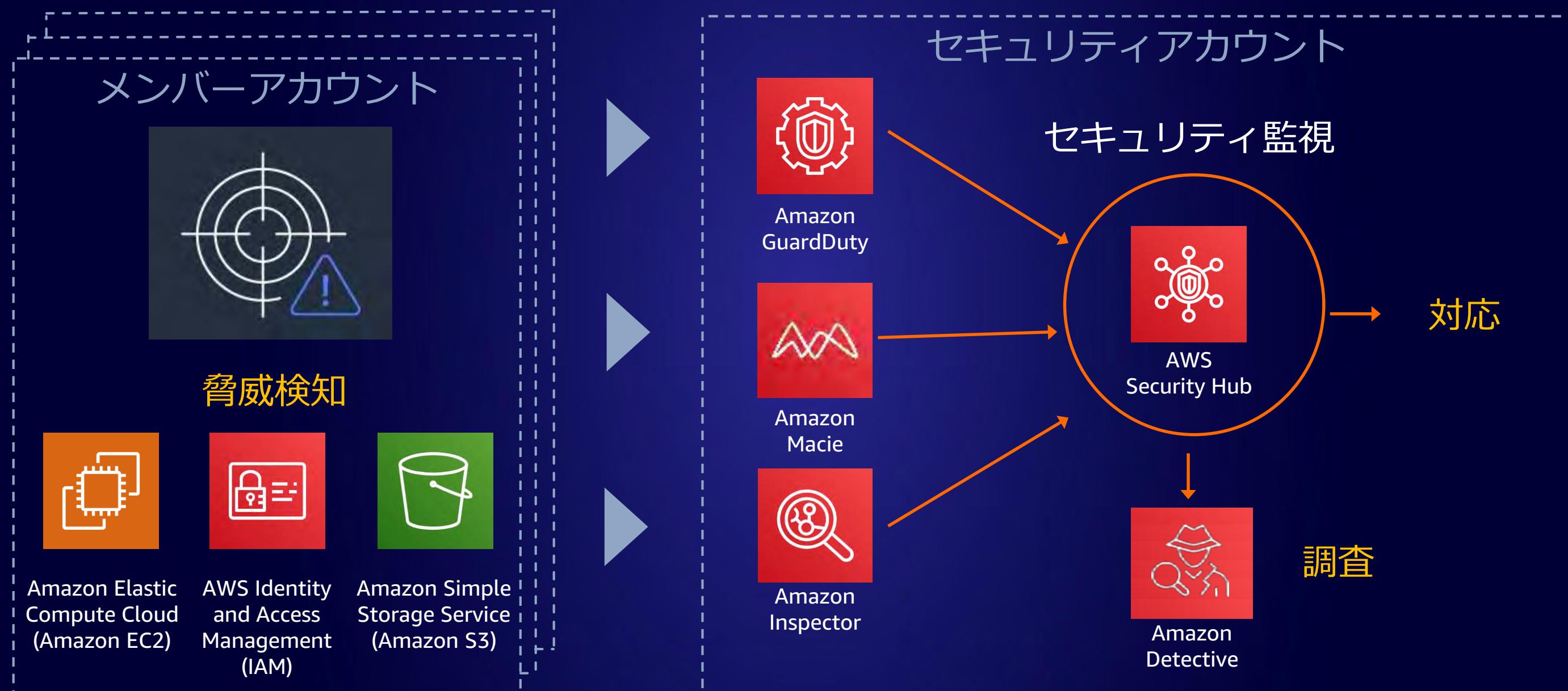
- AWS アカウントとは
 - AWS クラウドサービスのリソースコンテナ
 - 明示的なセキュリティ境界
 - コストの追跡と請求のためのコンテナ
 - 制限と閾値(サービススクオータや API 閾値など)を適用するメカニズム
- より多くのアプリケーションやサービスを運用するために、AWS アカウントを追加する (マルチアカウント)



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

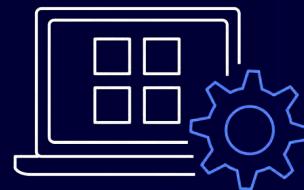




変化する環境において
脅威を検知するには
(Amazon GuardDuty)

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



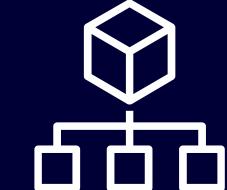
AWS アカウント
とリソースの
継続的監視



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



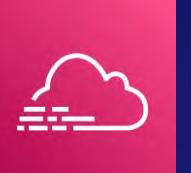
VPC フロー ログ

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

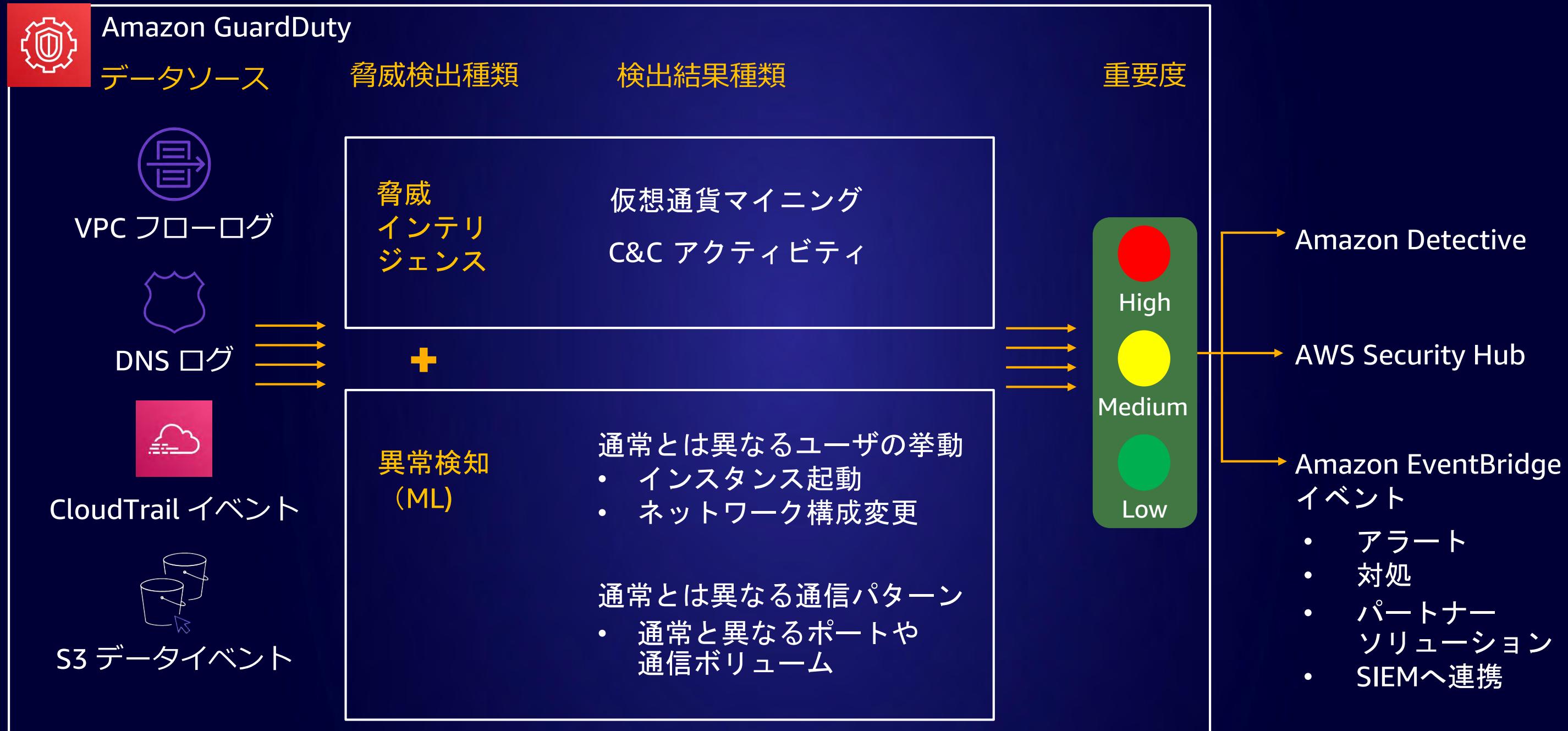


S3 データイベント

リソース内で実行される API の呼び出し履歴

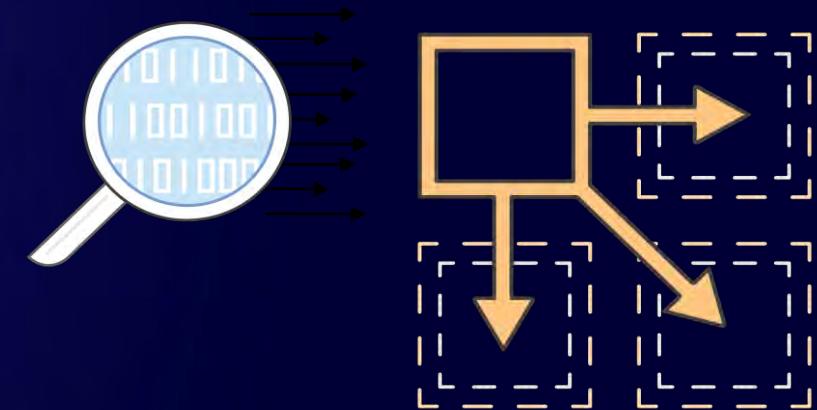
- GetObject
- ListObjects
- DeleteObject
- PutObject

Amazon GuardDuty 動作



Amazon GuardDuty が検出する既知の脅威

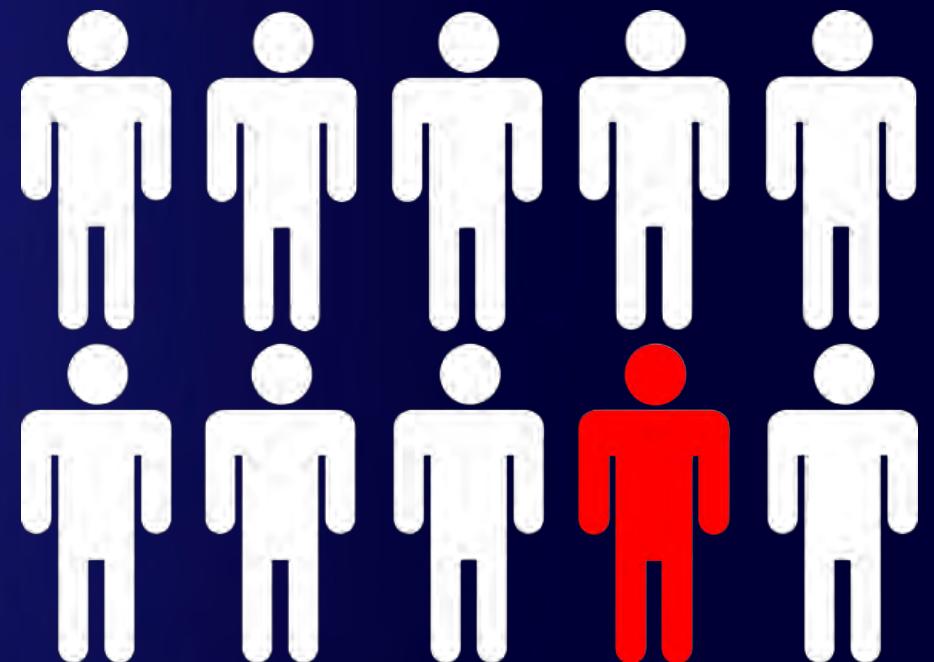
- ・ 様々なソースからの脅威インテリジェンスを活用
 - AWS 固有のインテリジェンス
 - AWS パートナーの脅威インテリジェンス (CrowdStrike, Proofpoint)
 - お客様が提供する脅威インテリジェンス
- ・ 脅威インテリジェンスを用いて GuardDuty が識別するもの
 - 既知のマルウェアに感染したホスト
 - 匿名プロキシ
 - マルウェアやハッカーツールをホストしているサイト
 - 暗号通貨マイニングプールとウォレット



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

GuardDuty X

Findings C

Showing 47 of 47 33 6 8

Actions Saved filters / Auto-archive Apply saved filters

Current Add filter criteria

Finding type	Reso...	Last seen	A	Count
UnauthorizedAccess:IAMUser/ConsoleLogin	admin:	an hour ago	114...	1
CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-094	24 days ago	114...	5
CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-094	24 days ago	114...	4
UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-0c9	24 days ago	943...	36
CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-094	24 days ago	114...	13
CryptoCurrency:EC2/BitcoinTool.B!DNS	Instance: i-094	24 days ago	114...	6
Backdoor:EC2/C&CActivity.B!DNS	Instance: i-094	24 days ago	114...	6
Trojan:EC2/DNSDataExfiltration	Instance: i-05a	a month ago	114...	29
Backdoor:EC2/C&CActivity.B!DNS	Instance: i-05a	a month ago	114...	1

CryptoCurrency:EC2/BitcoinTool... Q Q X

Finding ID: 42b587b2cb1dafddc1497861d3fc658e Feedback

 EC2 instance i-09457855ed83f3395 is querying a domain name that is associated with Bitcoin-related activity. [Learn More](#)

Severity	Region
HIGH Q Q	us-east-1

Count Account ID
5 11 [REDACTED] Q

Resource ID Created at
i-09457855ed83f3395 05-31-2019 12:37:24... [\[REDACTED\]](#)

Updated at
05-31-2019 13:28:42...

Resource affected

Resource role	Resource type
TARGET Q Q	Instance Q Q

検出結果の確認 : API/JSON 形式詳細

AWS 管理画面

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

EC2 Instance [Close](#) [Details](#) [Logs](#) [Metrics](#) [?](#)

i-e2f5f524
performing outbound port scans.

Recon:EC2/Portscan [Logs](#) [Metrics](#)

Actions [Edit](#) [Delete](#)

This finding was: [Up](#) [Down](#)

Alert EC2 Instance i-e2f5f524 is performing outbound port scans against remote host 10.0.0.158.

Severity	Region	Count
Medium Logs Metrics	us-west-2	1

Account ID [Logs](#) [Metrics](#)
Resource ID i-e2f5f524 [Logs](#) [Metrics](#)

Last seen
2017-11-01 15:53:28 (an hour ago)

Resource Affected [Edit](#)

Resource role	Resource type
ACTOR	Instance Logs Metrics

Instance ID [Logs](#) [Metrics](#) **i-e2f5f524** [Logs](#) [Metrics](#)
Port 38128 [Logs](#) [Metrics](#)

Image ID ami-494e7279
Launch time 2015-10-14 23:57:18

Tags
Name: tester
Inspector: Enabled

Private IP address [Logs](#) [Metrics](#)
Subnet ID subnet-d44ca8bc

Private dns name ip-10-0-1-224.us-west-2...
VPC ID vpc-de4ca8b6 [Logs](#) [Metrics](#)

API/JSON 形式

```
"type": "Recon:EC2/Portscan",
"resource": {
  "resourceType": "Instance",
  "instanceDetails": {
    "imageId": "ami-494e7279",
    "instanceId": "i-e2f5f524",
    "region": "us-west-2"
  }
},
"service": {
  "serviceName": "guardduty",
  "detectorId": "6caf9da04f873e4ab085519f3917fa88",
  "action": {
    "actionType": "NETWORK_CONNECTION",
    "networkConnectionAction": {
      "connectionDirection": "OUTBOUND",
      "remoteIpDetails": {
        "ipAddressV4": "10.0.0.158"
      }
    }
  }
},
"resourceRole": "ACTOR",
"additionalInfo": {
  "portsScannedSample": [
    146,
    83,
    119
  ]
},
"eventFirstSeen": "2017-11-01T22:52:36Z",
"eventLastSeen": "2017-11-01T22:53:28Z",
"severity": 5,
"createdAt": "2017-11-01T23:00:10.179Z",
"updatedAt": "2017-11-01T23:00:10.179Z",
"title": "EC2 Instance i-e2f5f524 performing outbound port scans",
"description": "EC2 Instance i-e2f5f524 is performing outbound port scans against remote host 10.0.0.158."}
```

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





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



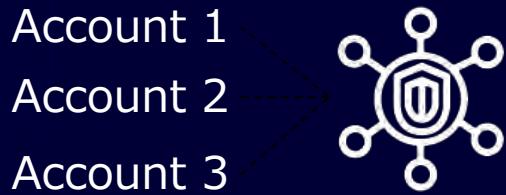
自動チェックで
セキュリティ体制
を改善



厳選された
セキュリティ
ベスト
プラクティス

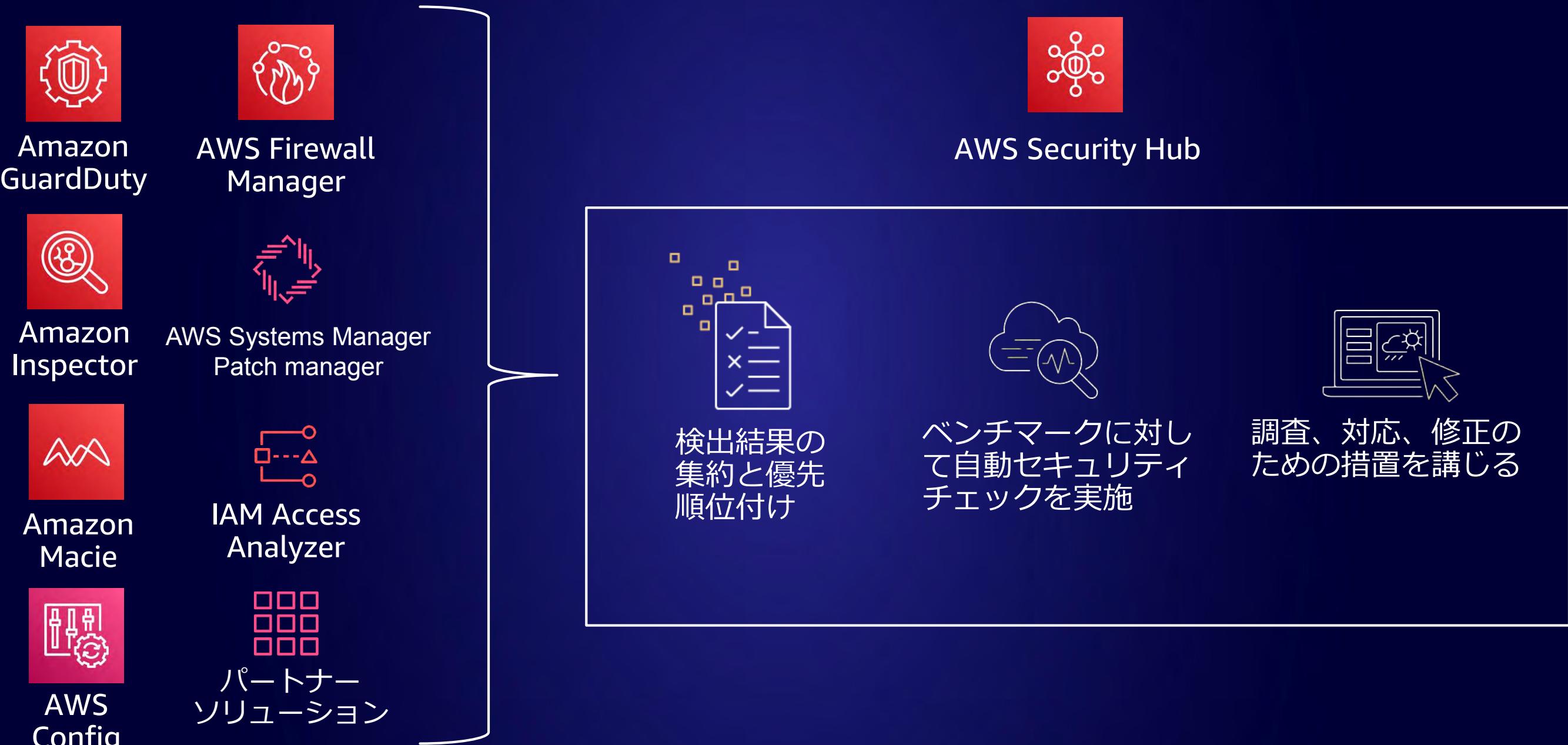


標準化された検出
結果フォーマット
とのシームレスな
統合



マルチアカウント
の統合

AWS Security Hub 動作概要



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

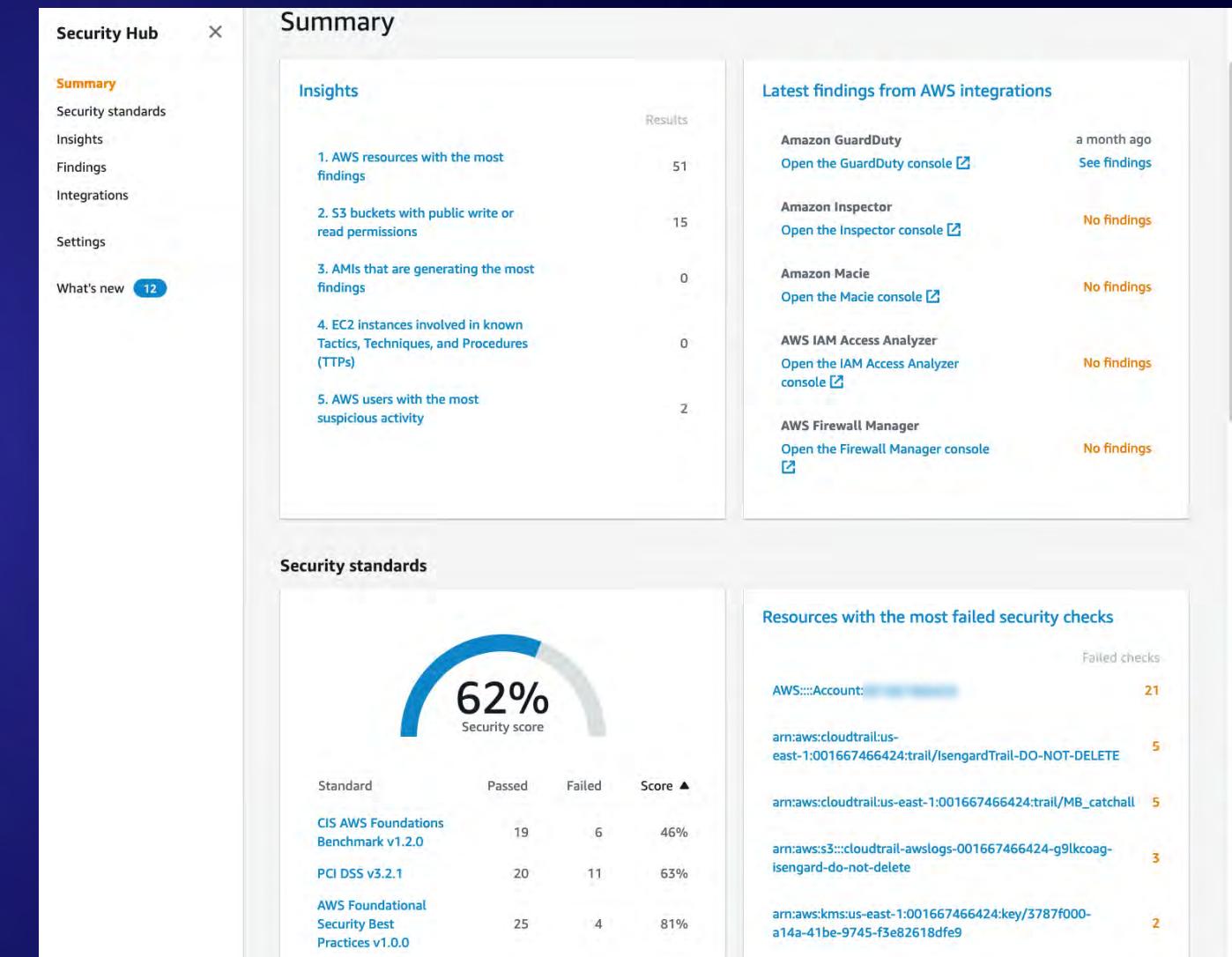
組織内の全ての AWS アカウントのセキュリティイベントを表示

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

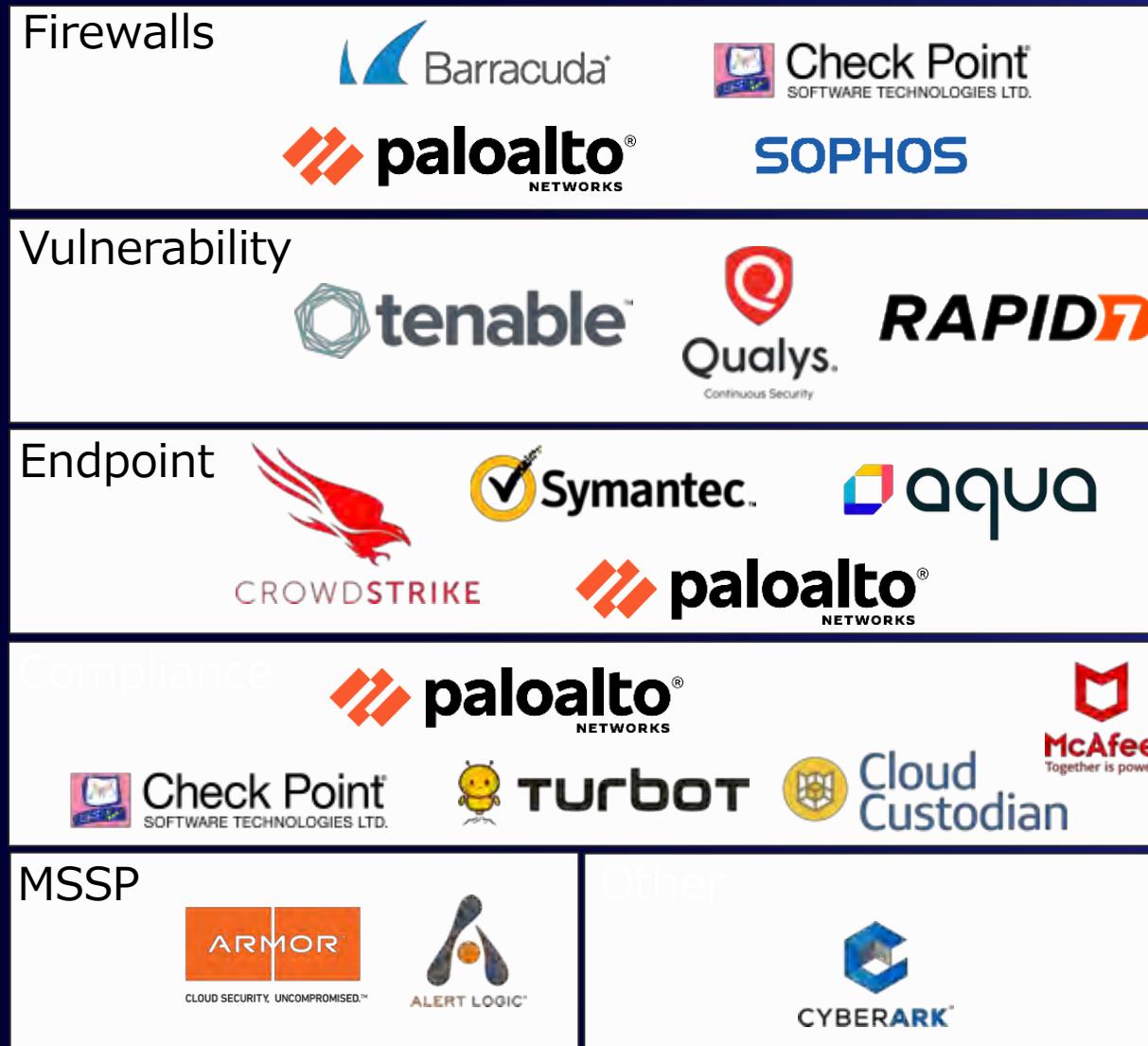
<https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-internal-providers.html>



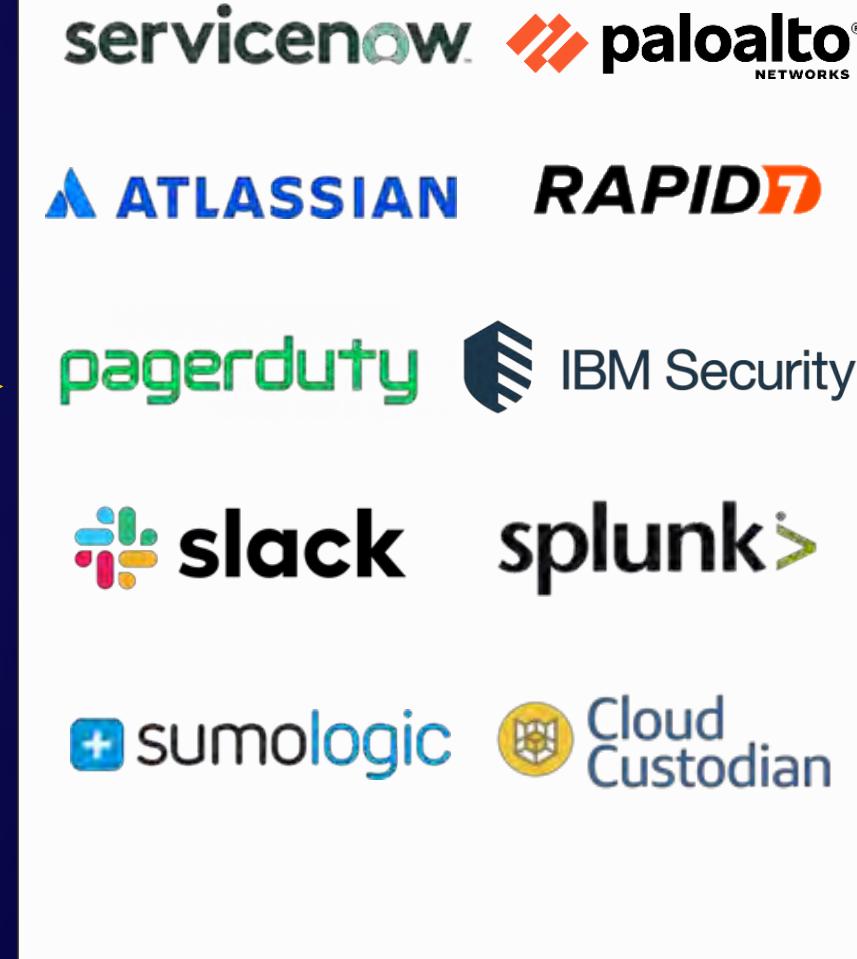
パートナー製品の統合

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



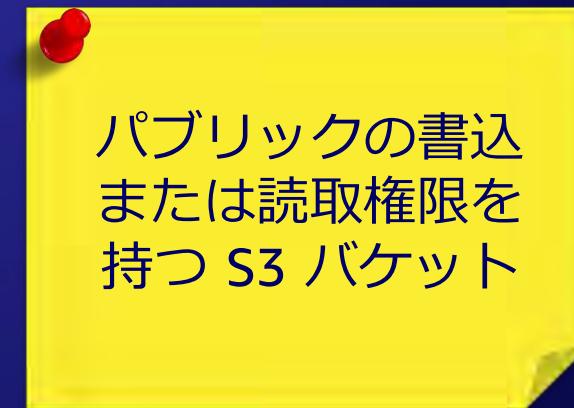
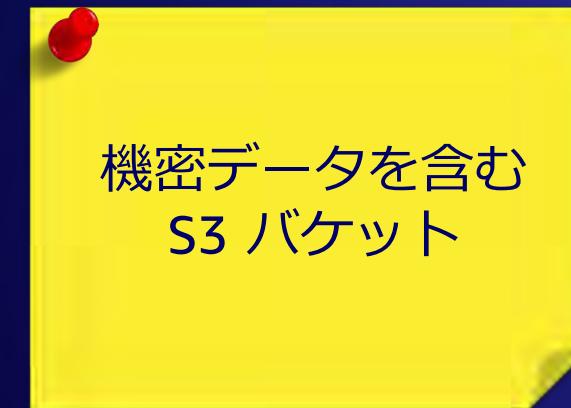
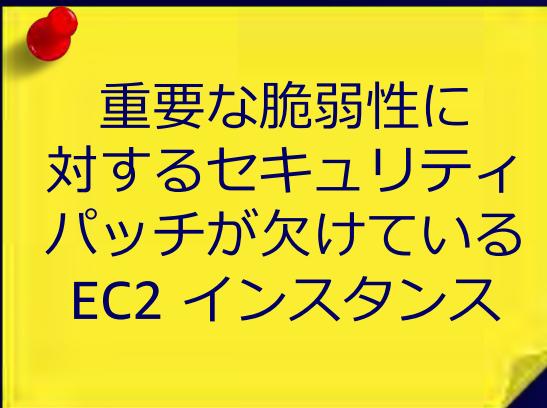
検出結果に基づいた対応アクション



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



*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



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

セキュリティ評価の自動化

Security Hub > セキュリティ基準

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 v1.0.0 AWS による

説明
AWS 基礎セキュリティのベストプラクティス標準は、AWS アカウントとデプロイされたリソースがセキュリティのベストプラクティスと一致しないことを検出する自動化されたセキュリティチェックのセットです。この標準は AWS セキュリティの専門家によって定義されたものです。この厳選された一連の統制は、AWS におけるセキュリティ体制の改善に役立ち、AWS で最も人気の高い基礎的なサービスを網羅しています。

セキュリティスコア
 62%

無効化 結果を表示する

CIS AWS Foundations Benchmark v1.2.0 AWS による

説明
Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 は、AWS のセキュリティ設定のベストプラクティスのセットです。この Security Hub 標準では、CIS 要件のサブセットに対するコンプライアンスの準備状況が自動的にチェックされます。

セキュリティスコア
 14%

無効化 結果を表示する

PCI DSS v3.2.1 AWS による

説明
Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 は、カード所有者データを保存、処理、転送するエンティティ向けの情報セキュリティ標準です。この Security Hub 標準では、PCI DSS 要件のサブセットに対するコンプライアンスの準備状況が自動的にチェックされます。

セキュリティスコア
 45%

無効化 結果を表示する

- 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やすやくアクセス可
- 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
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
イ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

Security Hub > Findings

Findings

Findings document a security or compliance issue.

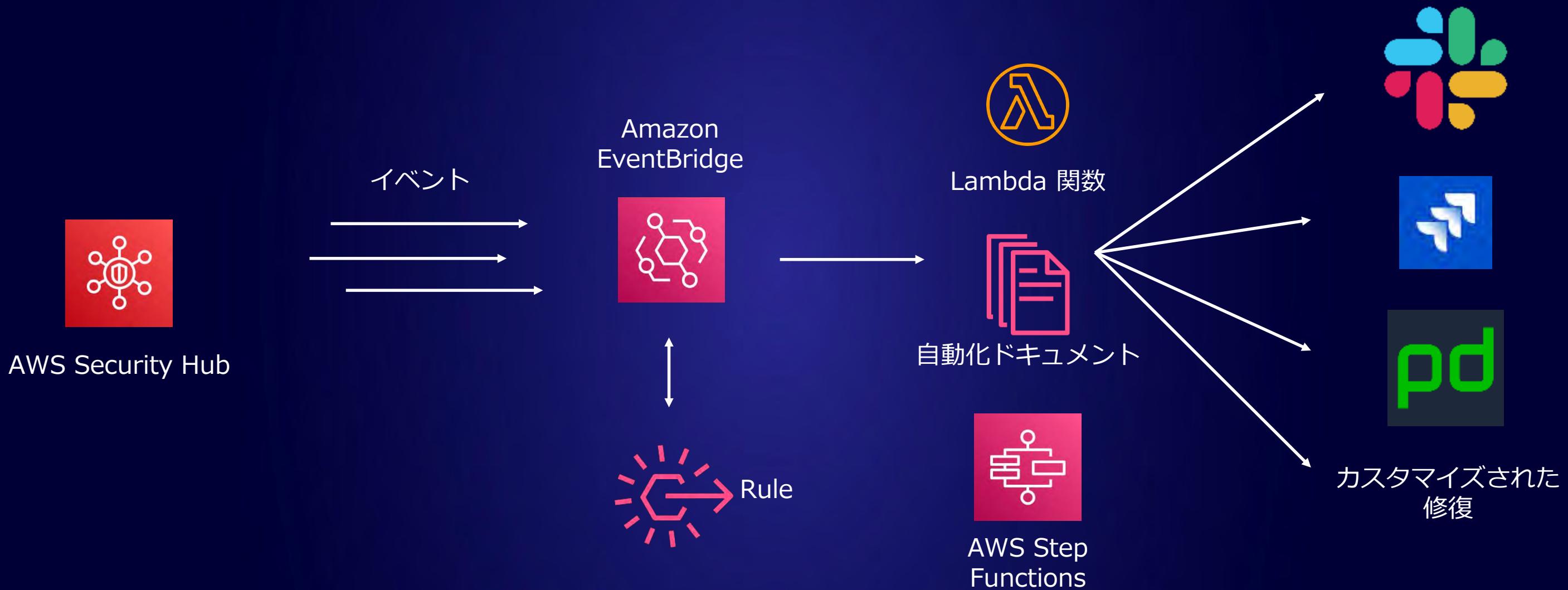
Actions ▾ Create Insight

Record state EQUALS ACTIVE X

< 1 >

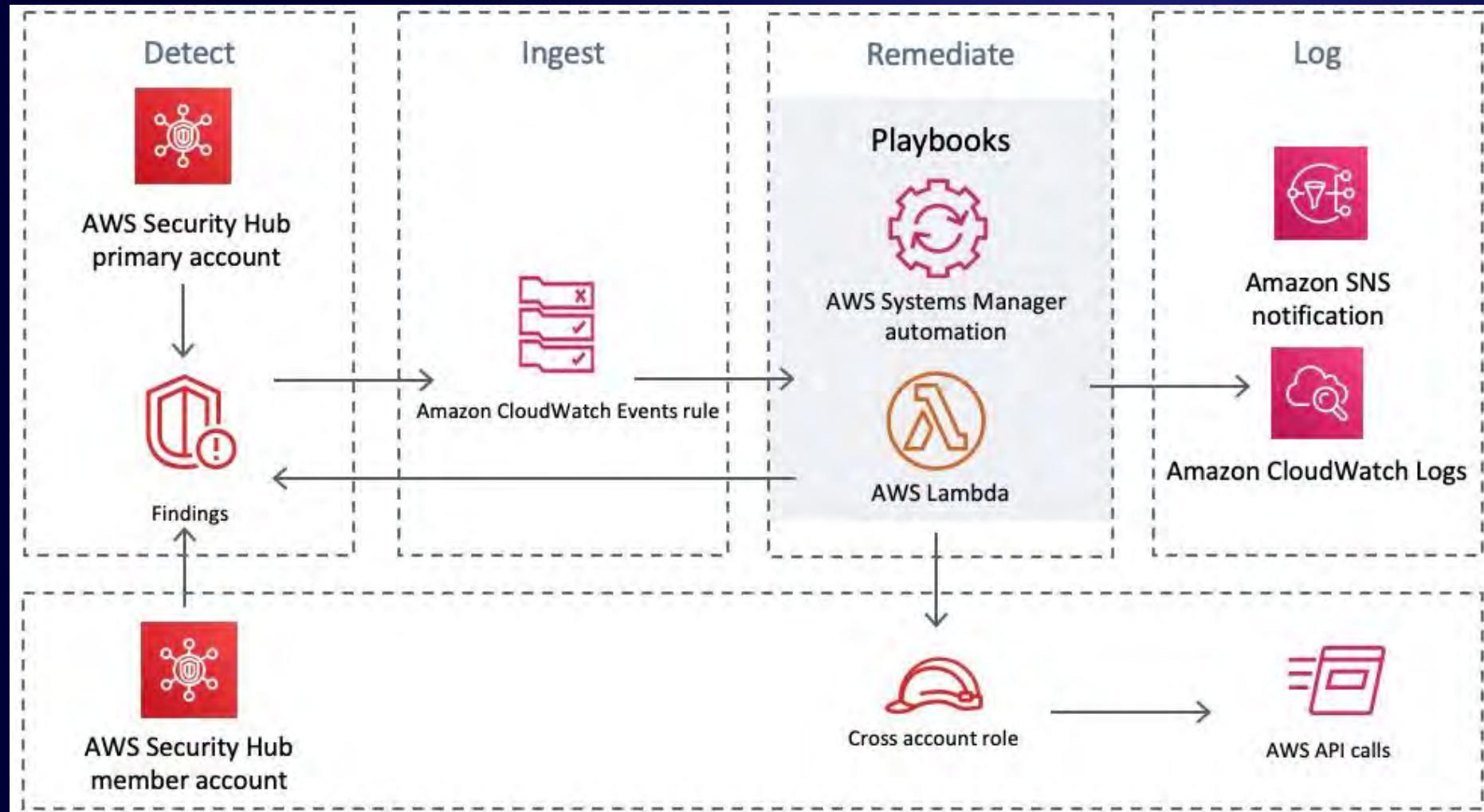
Severity	Company	Product	Title	Resource ID	Resource type	Status	Updated at
● MEDIUM	AWS	GuardDuty	Unusual console login was seen for principal SecurityHubDemo.	AWS::IAM::AccessKey: null	AwsIamAccessKey	-	a day ago
● MEDIUM	AWS	GuardDuty	Unusual console login was seen for principal SecurityHubDemo.	AWS::IAM::AccessKey: null	AwsIamAccessKey	-	a month ago
● MEDIUM	AWS	GuardDuty	Unusual console login was seen for principal SecurityHubDemo.	AWS::IAM::AccessKey: null	AwsIamAccessKey	-	2 months ago
● MEDIUM	AWS	GuardDuty	Unusual IAM user/group/policy change by SecurityHubDemo.	AWS::IAM::AccessKey: ASIARACJK4XV2YAKU KSB	AwsIamAccessKey	-	3 months ago
● LOW	AWS	Security Hub	1.10 Ensure IAM password policy prevents password reuse	AWS::Account:068873283051	AwsAccount	FAILED	6 hours ago
● LOW	AWS	Security Hub	2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs	AWS::Account:068873283051	AwsAccount	FAILED	6 hours ago
● LOW	AWS	Security Hub	2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs	arn:aws:cloudtrail:us-east-1:068873283051:trail/IsengardTrail-DO-NOT-DELETE	AwsCloudTrailTrail	FAILED	6 hours ago
● LOW	AWS	Security Hub	1.13 Ensure MFA is enabled for the "root" account	AWS::Account:068873283051	AwsAccount	FAILED	6 hours ago
● LOW	AWS	Security Hub	4.3 Ensure the default security group of every VPC restricts all traffic	arn:aws:ec2:eu-west-3:068873283051:security-group/sge-49e0c621	AwsEc2SecurityGroup	FAILED	6 hours ago
● LOW	AWS	Security Hub	4.3 Ensure the default security group of every VPC restricts all traffic	AWS::Account:068873283051	AwsAccount	FAILED	6 hours ago
● LOW	AWS	Security Hub	2.9 Ensure VPC flow logging is enabled in all VPCs	arn:aws:ec2:eu-west-3:068873283051:vpc/vpc-2a97ca43	AwsEc2Vpc	FAILED	6 hours ago
● LOW	AWS	Security Hub	2.9 Ensure VPC flow logging is enabled in all VPCs	AWS::Account:068873283051	AwsAccount	FAILED	6 hours ago
● LOW	AWS	Security Hub	1.14 Ensure hardware MFA is enabled for the "root" account	AWS::Account:068873283051	AwsAccount	FAILED	6 hours ago
● LOW	AWS	Security Hub	2.5 Ensure AWS Config is enabled in all regions	AWS::Account:068873283051	AwsAccount	FAILED	6 hours ago
● LOW	AWS	Security Hub	1.1 Avoid the use of the "root" account	AWS::Account:068873283051	AwsAccount	FAILED	6 hours ago

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/>



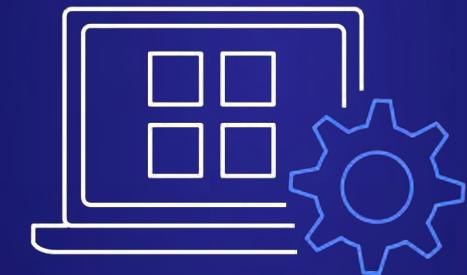
対応すべき脅威を調査するには
(Amazon Detective)

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

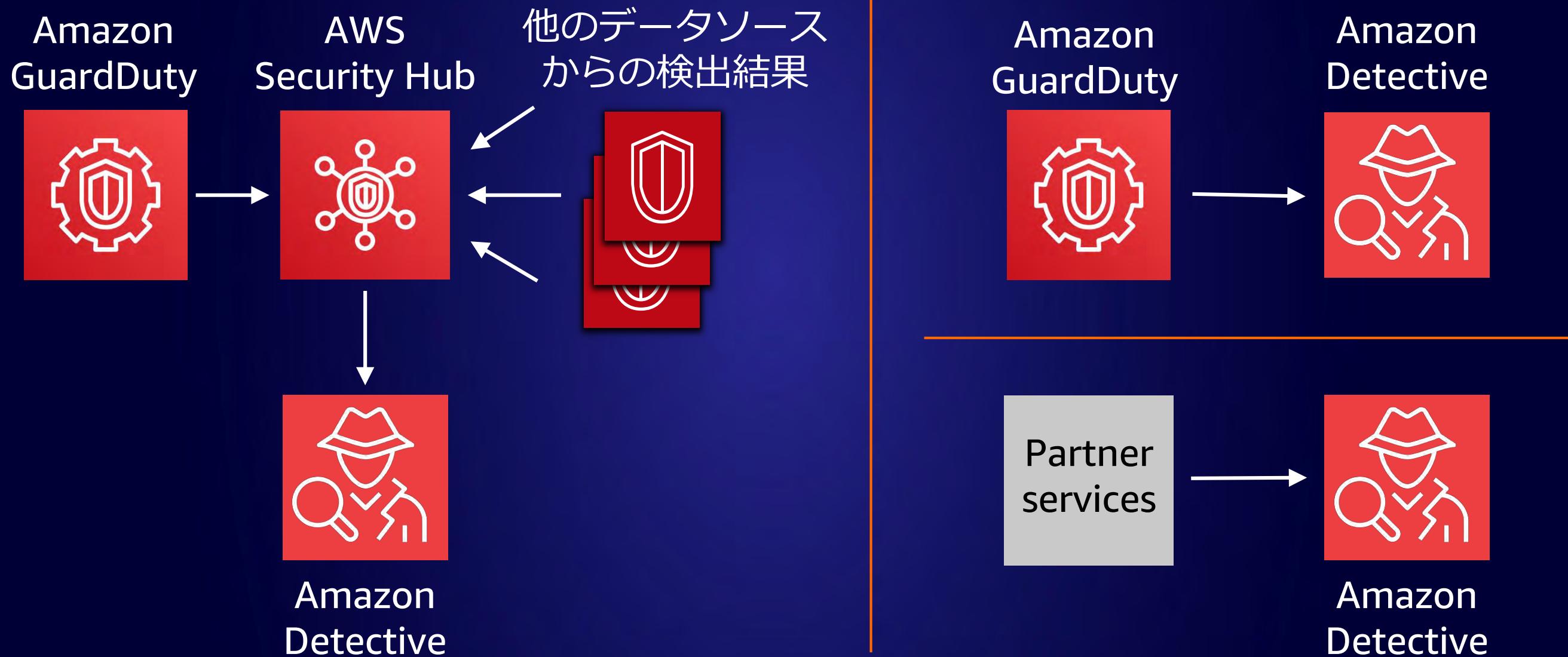


分析の
自動化

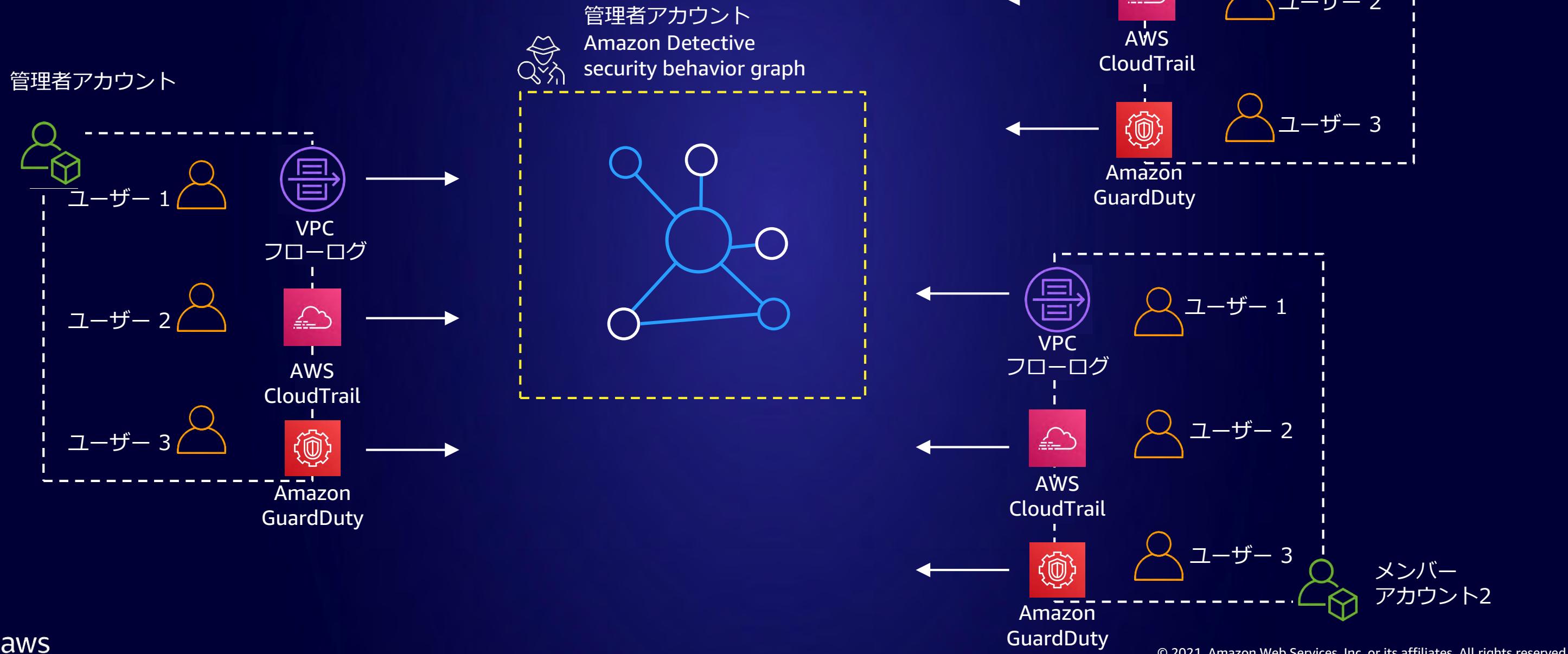


インサイトの
視覚化

Amazon Detective 利用フロー

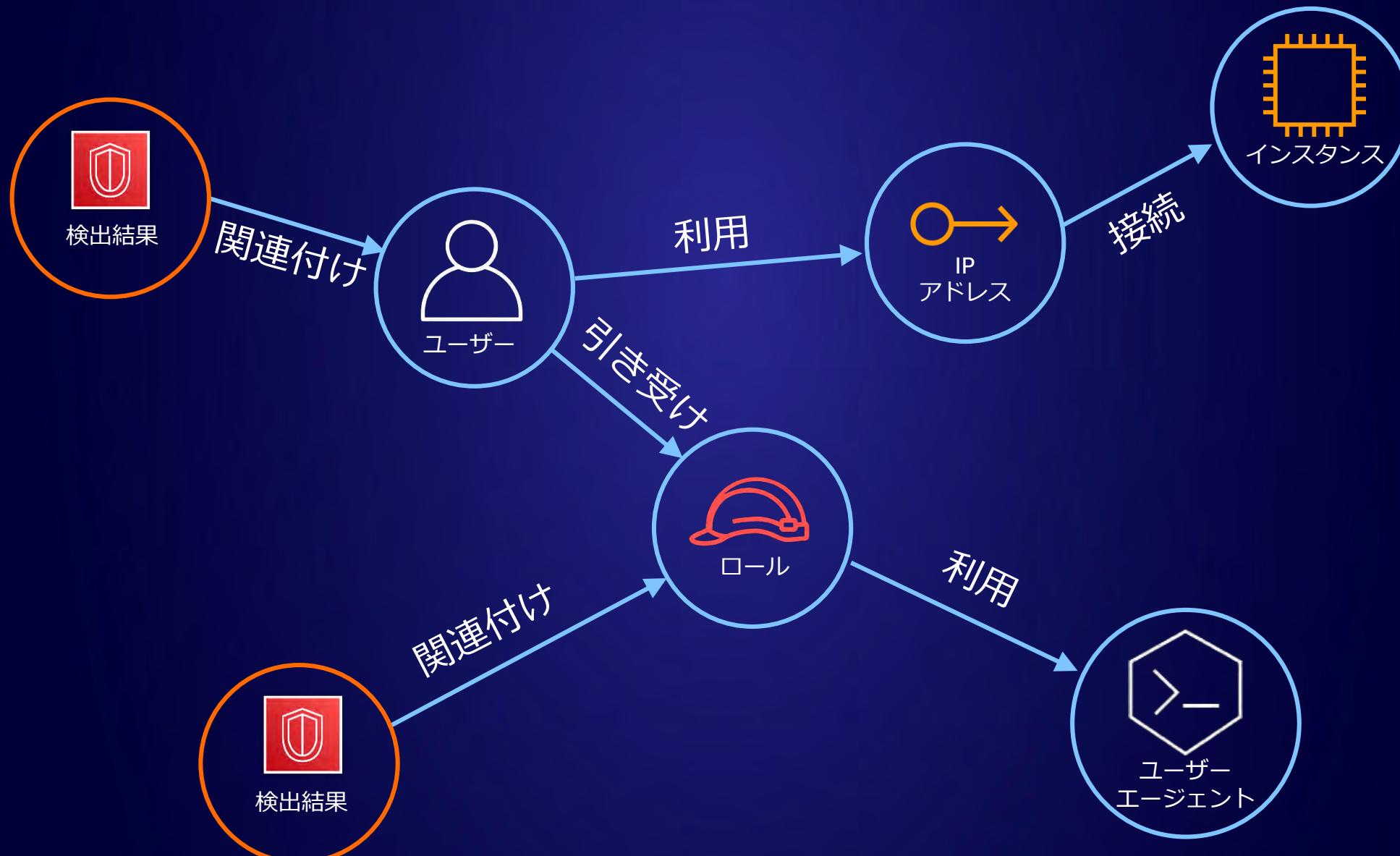


マルチアカウントの テレメトリデータ収集



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

Detective > 概要

概要 [情報](#)

[Detective の概要] ページは、追加の詳細を表示するエンティティを特定するのに役立ちます。これは、調査のための新たな開始点を提供します。

過去 24 時間の API 呼び出し量が最も多いロールとユーザー [情報](#)

プリンシパル (ロールまたはユーザー)	AWS アカウント	傾向 (7 日間)	成功	失敗	合計
AWSServiceRoleForConfig	AWS ロール		1,397	463	1,860
CodeBuild-role-CodeBuildService...	AWS ロール		1,388	449	1,837
AWSServiceRoleForAmazonMacie	AWS ロール		206	143	349
AWSServiceRoleForAccessAnalyzer	AWS ロール		174	63	237
AWSServiceRoleForTrustedAdvisor	AWS ロール		66	41	107
lambda-config-rules-role	AWS ロール		6	0	6
AWSServiceRoleForSecurityHub	AWS ロール		478	0	478

過去 24 時間に新たに観察された位置情報 [情報](#)

過去 24 時間に新たに観察された位置情報は観察されていません。

過去 24 時間のトラフィック量が最も多い EC2 インスタンス [情報](#)

EC2 インスタンス	AWS アカウント	傾向 (7 日間)	バイト (受信)	バイト (送信)	合計
i-00000000000000000			140 MB	143 MB	283 MB
i-00000000000000001			106 MB	61.2 MB	167 MB
i-00000000000000002			30.7 MB	15.5 MB	46.2 MB
i-00000000000000003			7.03 MB	9.97 MB	17 MB
i-00000000000000004			5.54 MB	9.74 MB	15.3 MB
i-00000000000000005			5.36 MB	6.27 MB	11.6 MB
i-00000000000000006			2.21 MB	2.48 MB	4.7 MB

Amazon Detective 概要画面

Detective > 概要

概要 [情報](#)

[Detective の概要] ページは、追加の詳細を表示するエンティティを特定するのに役立ちます。これは、調査のための新たな開始点を提供します。

過去 24 時間の API 呼び出し量が最も多いロールとユーザー [情報](#)

クリックし詳細画面へ

プリンシパル (ロールまたはユーザー)	AWS アカウント	傾向 (7 日間)	成功	失敗	合計
AWSServiceRoleForConfig AWS ロール			1,397	463	1,860
CodeBuild-role-CodeBuildService... AWS ロール			1,388	449	1,837
AWSServiceRoleForAmazonMacie AWS ロール			206	143	349
AWSServiceRoleForAccessAnalyzer AWS ロール			174	63	237
AWSServiceRoleForTrustedAdvisor AWS ロール			66	41	107
lambda-config-rules-role AWS ロール			6	0	6
AWSServiceRoleForSecurityHub AWS ロール			478	0	478

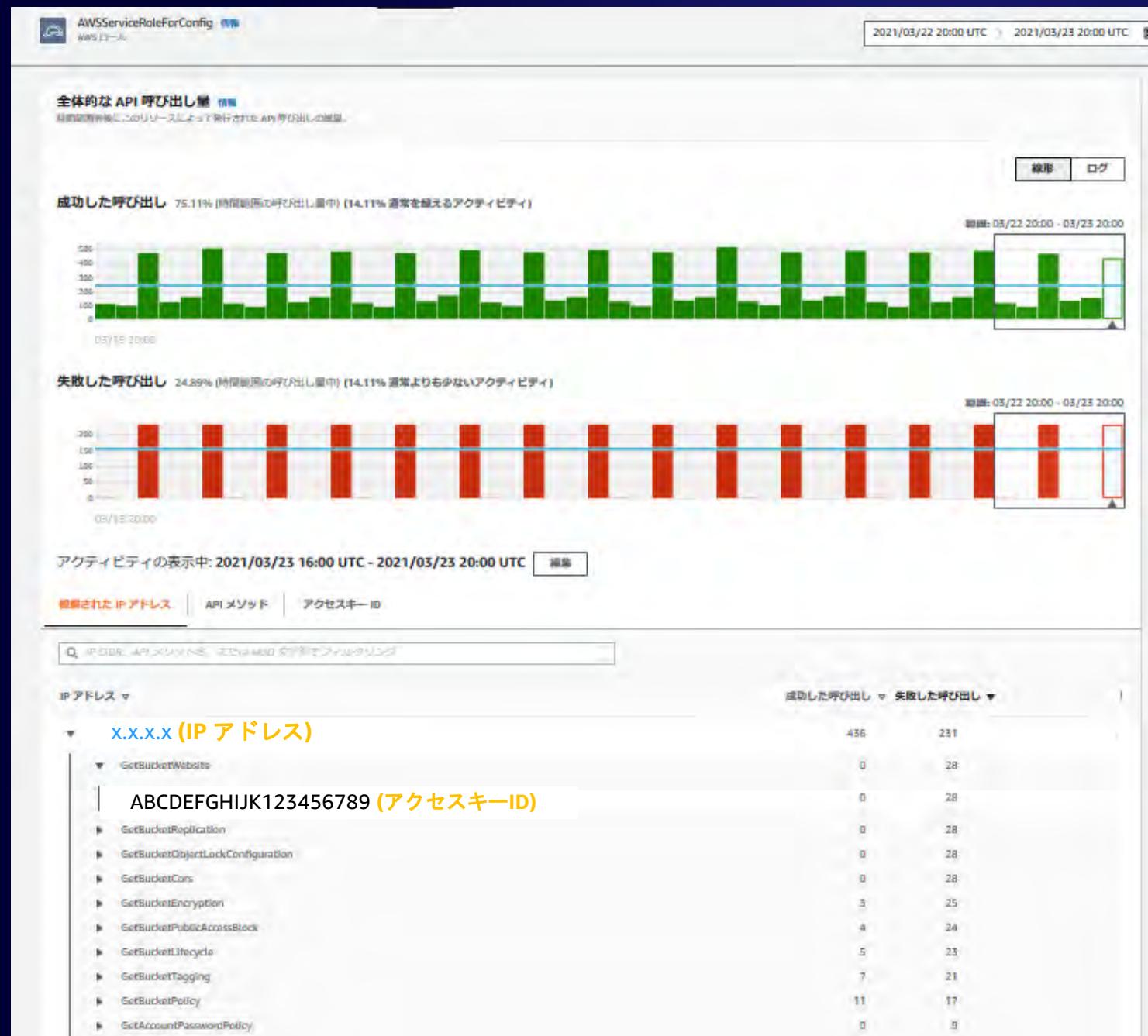
過去 24 時間に新たに観察された位置情報 [情報](#)

過去 24 時間以内に新たな位置情報は観察されていません。

過去 24 時間のトラフィック量が最も多い EC2 インスタンス [情報](#)

EC2 インスタンス	AWS アカウント	傾向 (7 日間)	バイト (受信)	バイト (送信)	合計
			140 MB	143 MB	283 MB
			106 MB	61.2 MB	167 MB
			30.7 MB	15.5 MB	46.2 MB
			7.03 MB	9.97 MB	17 MB
			5.54 MB	9.74 MB	15.3 MB
			5.36 MB	6.27 MB	11.6 MB
			2.21 MB	2.48 MB	4.7 MB

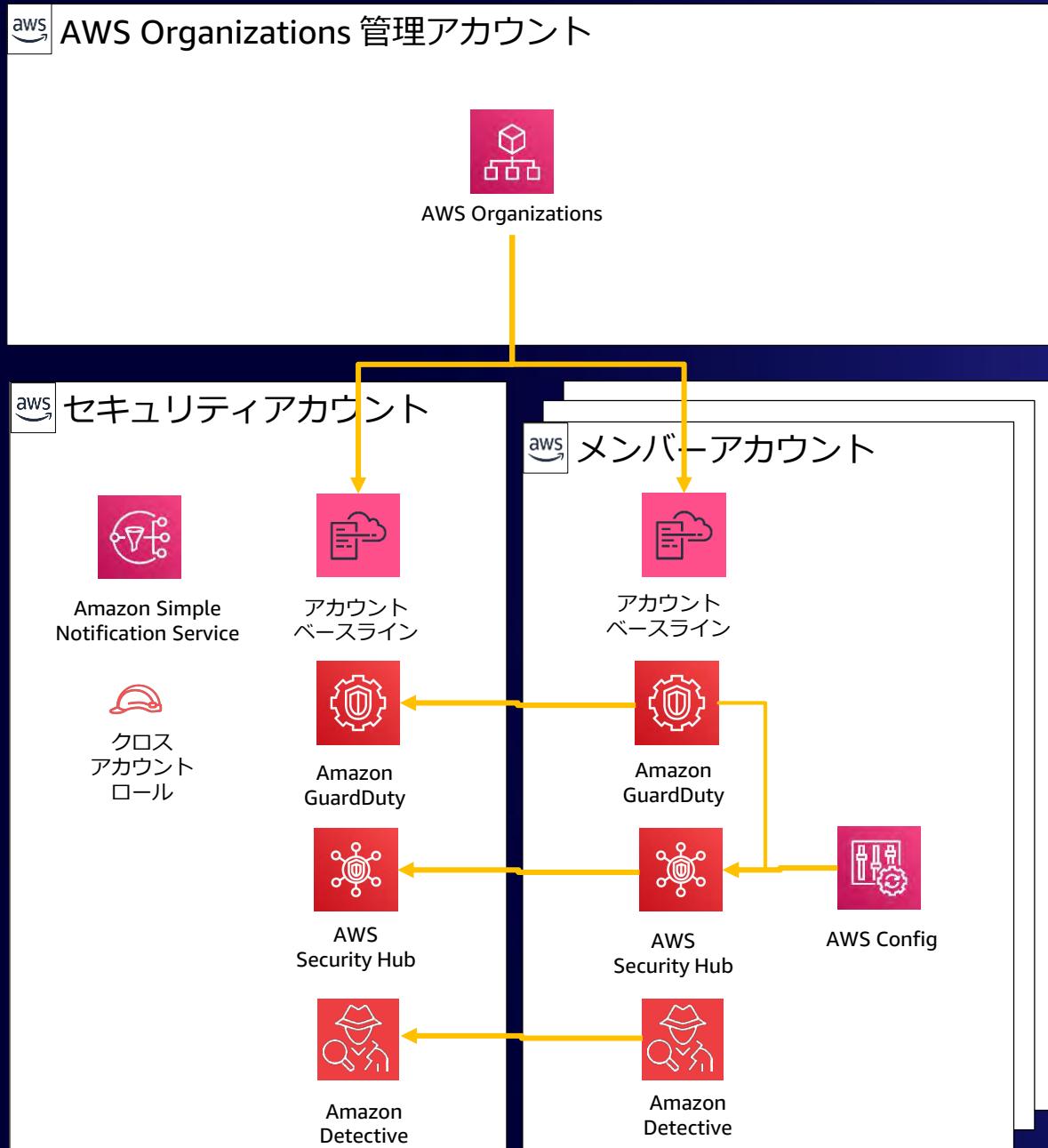
Amazon Detective 詳細画面



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

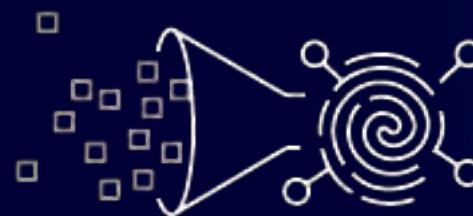
まとめ



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
Amazon Web Services 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