JAWS DAYS 2025
connecting the dots

セキュリティイベントの調査に Amazon Detectiveって実際どこまで使えるの？

電通総研

自己紹介

- 氏名：福山 賢太
- 会社名：株式会社電通総研
- 所属部署：コーポレート本部 サイバーセキュリティ推進部
- 好きなAWSサービス

Amazon GuardDuty

AWS Security Hub

Amazon Detective

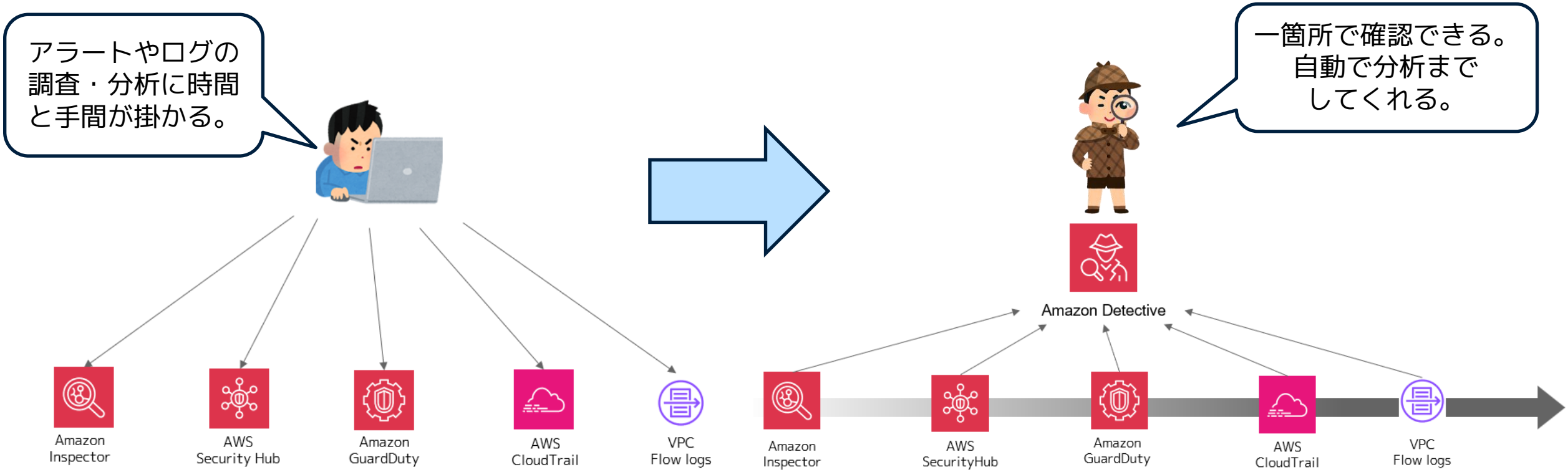
JAWS-UG
AWS User Group - Japan

Amazon Detectiveとは

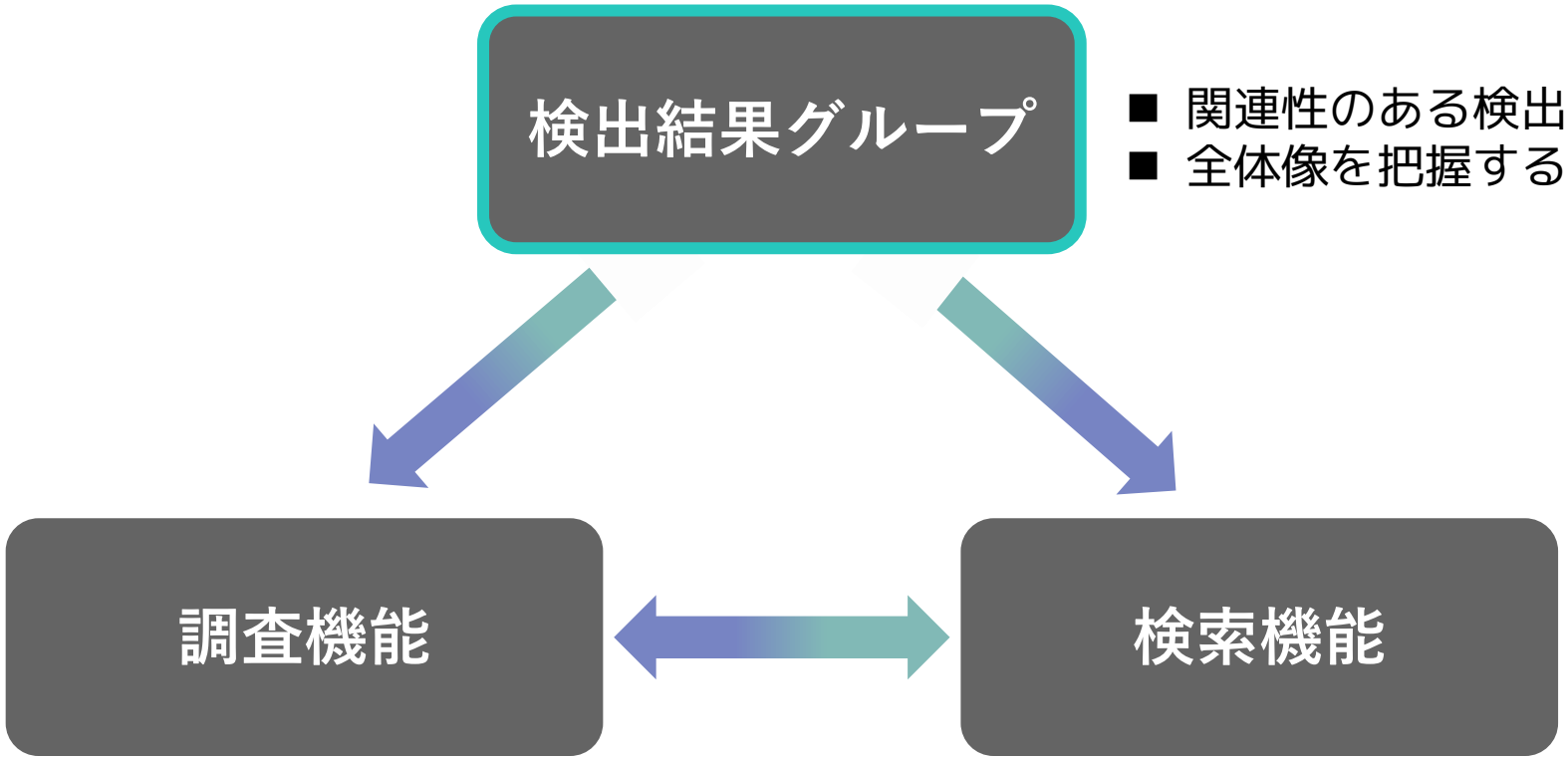
Amazon Detectiveを利用したセキュリティイベントの調査

■ 従来のセキュリティイベントの調査手法
⇒複数のサービスを横断しながら読み解いていく必要がある。

■ Amazon Detectiveを利用した調査手法
⇒各サービスの情報がDetectiveに自動で集約・分析され、セキュリティイベントの調査を一気通貫で進めることができる。



Amazon Detectiveを使った調査で利用する機能３つ



- 関連性のある検出結果をまとめて可視化
- 全体像を把握する

- IAMの侵害状況を自動でレポート化

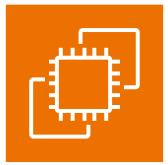
- 各エンティティ（リソースやアラートの単位）レベルで詳細分析

JAWS-UG
AWS User Group - Japan

実際に擬似攻撃を起こして Detectiveを使って調査してみた

原因不明のセキュリティイベント発生！

攻撃者
（福山）



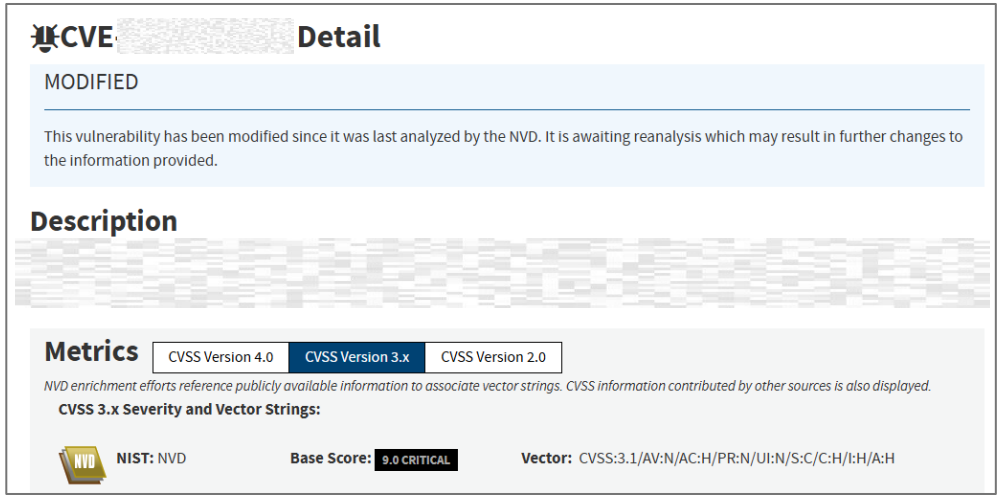
Amazon EC2

S3 Bucket

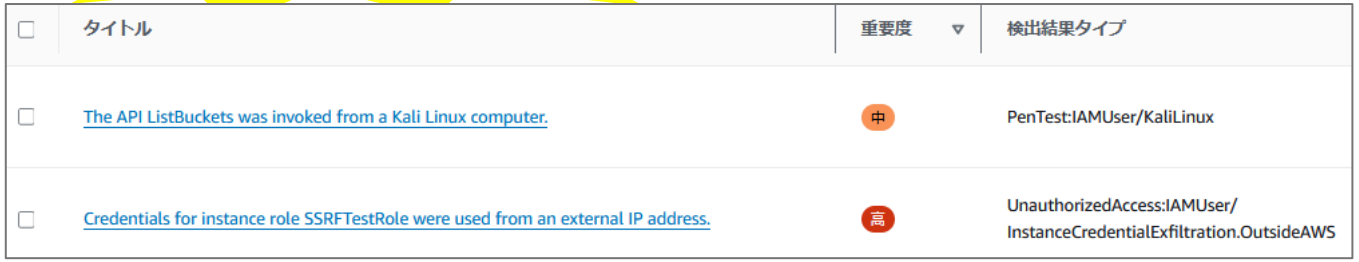
・インスタンスに紐づくIAMロールが外部のIPから利用された。

・S3バケットの一覧が取得された。

- PoCで利用した脆弱性



- 検出されたGuardDutyアラート



検出結果グループの確認①

Effects (1), Software and Configuration Checks (18), TTPs (1), UnusualBehavior:AllAccounts (2) 情報

高 アクティブ a1f43361-6cd6-499e-91c1-7c6a72594a22 関連

時間範囲 情報
2025/02/21 15:00 - 2025/02/21 15:59 UTC

概要 - *新規* 情報

Credentials exfiltration and vulnerabilities on i-052790e86fd21d5aa using SSRFTestRole

Credentials for role SSRFTestRole were exfiltrated from i-052790e86fd21d5aa to external IP 49.

Ports 80 and 3389 were externally reachable on i-052790e86fd21d5aa.

i-052790e86fd21d5aa had CVE vulnerabilities affecting Apache HTTP Server.

Discovery API call originated from potential penetration testing system at 49.

GuardDuty
アラートの要約

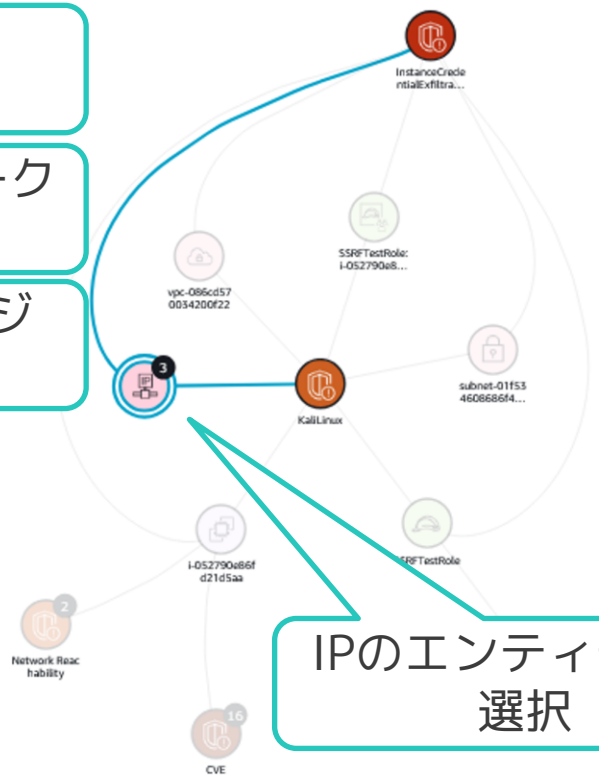
Inspectorネットワーク
到達可能性の要約

Inspectorパッケージ
脆弱性の要約

可視化 情報

このインタラクティブな可視化では、検出結果グループ内の各アイテムを選択して詳細を確認できます。エンティティまたは検出結果を選択すると、詳細が表示されます。Ctrl キーを押しながらクリックするか、Ctrl キーを押しながらドラッグすると、複数のエンティティと検出結果を選択できます。

ラジアル - 新規 ラベルを表示 凡例



概要

エンティティと検出結果を選択 (1)

IP アドレス (3)

10. IP アドレス

18. IP アドレス

49. IP アドレス

見覚えのないIP

IPのエンティティを
選択

検出結果グループの確認②

Effects (1), Software and Configuration Checks (18), TTPs (1) 情報

高 アクティブ a1f43361-6cd6-499e-91c1-7c6a72594a22 関連

時間範囲 情報
2025/02/21 15:59 - 2025/02/21 15:59 UTC

概要 - *新規* 情報

Credentials exfiltration and vulnerabilities on i-052790e86fd21d5aa using SSRFTestRole

Credentials for role SSRFTestRole were exfiltrated from i-052790e86fd21d5aa to external IP 49.

Ports 80 and 3389 were externally reachable on i-052790e86fd21d5aa.

i-052790e86fd21d5aa had CVE vulnerabilities affecting Apache HTTP Server.

Discovery API call originated from potential penetration testing system at 49.

関係するエンティティ | 関係する検出結果

エンティティ (8) 情報

これらのエンティティは、同じ基礎となるアクティビティと相関しています。エンティティのプロファイルにピボットして追加の詳細を確認するか、[関係する検出結果] タブから関係する検出結果を確認します。

エンティティを検索

1

関係するエンティティ	AWS アカウント	関係する検出結果	関係する検出結果の
i-052790e86fd21d5aa EC2 イ		CVE-2021-40438 ■ 重大 Software and Configuration Checks/Vulnerabilities/CVE CVE-2024-38476 ■ 重大 Software and Configuration Checks/Vulnerabilities/CVE CVE-2023-25690 ■ 重大 Software and Configuration Checks/Vulnerabilities/CVE さらに 17 の検出結果	20
SSRFTestRole AWS ロール		Credentials for instance role SSRFTestRole were used from an external IP address. ■ 高 UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS The API ListBuckets was invoked from a Kali Linux computer. ■ 中 PenTest:IAMUser/KaliLinux	2

EC2インスタンスにApacheの脆弱性があることがわかる

IAMロールが漏れていることがわかる

検出結果グループからインスタンスの調査に遷移する

Effects (1), Software and Configuration Checks (18), TTPs (1), UnusualBehavior:AllAccounts (2) 情報

高 アクティブ a1f43361-6cd6-499e-91c1-7c6a72594a22 関連

時間範囲 情報
2025/02/21 15:00 - 2025/02/21 15:59 UTC

概要 - *新規* 情報

Credentials exfiltration and vulnerabilities on i-052790e86fd21d5aa using SSRFTestRole

Credentials for role SSRFTestRole were exfiltrated from i-052790e86fd21d5aa to external IP 49.

Ports 80 and 3389 were externally reachable on i-052790e86fd21d5aa.

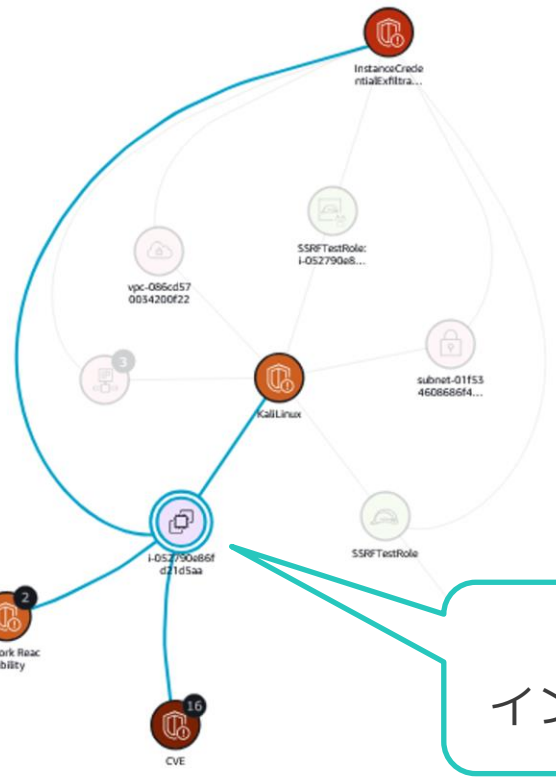
i-052790e86fd21d5aa had CVE vulnerabilities affecting Apache HTTP Server.

Discovery API call originated from potential penetration testing system at 49.

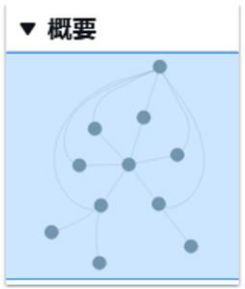
可視化 情報

このインタラクティブな可視化では、検出結果グループ内の各アイテムを選択して詳細を確認できます。エンティティまたは検出結果を選択すると、詳細が表示されます。Ctrl キーを押しながらクリックするか、Ctrl キーを押しながらドラッグすると、複数のエンティティと検出結果を選択できます。

ラジアル - 新規 ラベルを表示 凡例



▼ 概要



エンティティと検出結果を選択 (1)

i-052790e86fd21d5aa
i-052790e86fd21d5aa
EC2 インスタンス

ターゲットの
インスタンスを選択

インスタンスに関連付けられた検出結果

i-052790e86fd21d5aa
EC2 インスタンス 情報

時間範囲 情報
2025/02/21 15:00 UTC > 2025/02/21 16:00 UTC

EC2 インスタンスの詳細 情報

EC2 インスタンス
i-052790e86fd21d5aa

AWS アカウント
[redacted]

ノード
-

検出結果グループ
Effects (1), Software and Configuration Checks (18), TTPs (1)

作成日
2025/02/18 21:55 UTC

ARN
arn:aws:ec2:eu-central-1:[redacted]:instance/i-052790e86fd21d5aa

作成者:
[redacted]

関連付けられた VPC
vpc-086cd570034200f22

ロール
AmazonEC2ReadOnlyAccess
,
SSMManaged
,
SSRFTestRole

コンテナクラスター
-

このリソースに関連付けられた検出結果 情報

以下の検出結果は、時間範囲前後にこのリソースで発生しました。

検出結果を検索　4 一致

製品 = Security Hub　フィルターをクリア　1

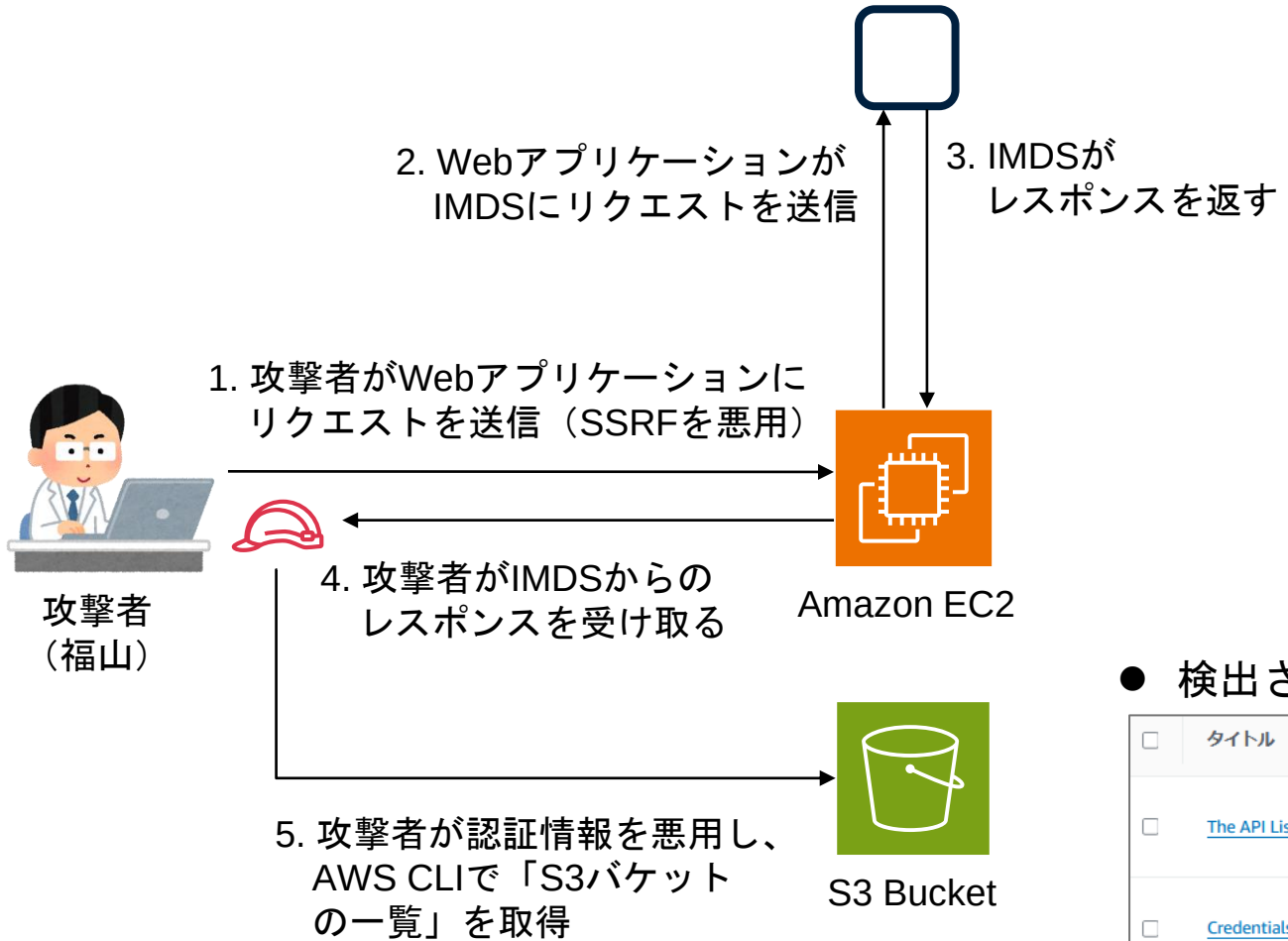
タイトル	製品	AWS アカウント	検出結果タイプ	最初に観察された時点:	最終観察時点:	検出結果の重大度
EC2 instances should not have a public IPv4 address	Security Hub		ation egulatory			
EC2 instances should not have a public IPv4 address	Security Hu		ation egulatory			
EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	Security Hub	[redacted]	Software and Configuration Checks/Industry and Regulatory Standards	2025/02/18 21:56 UTC	2025/02/21 16:19 UTC	■ 高

IMDSv1とv2の両方が有効であることがわかる

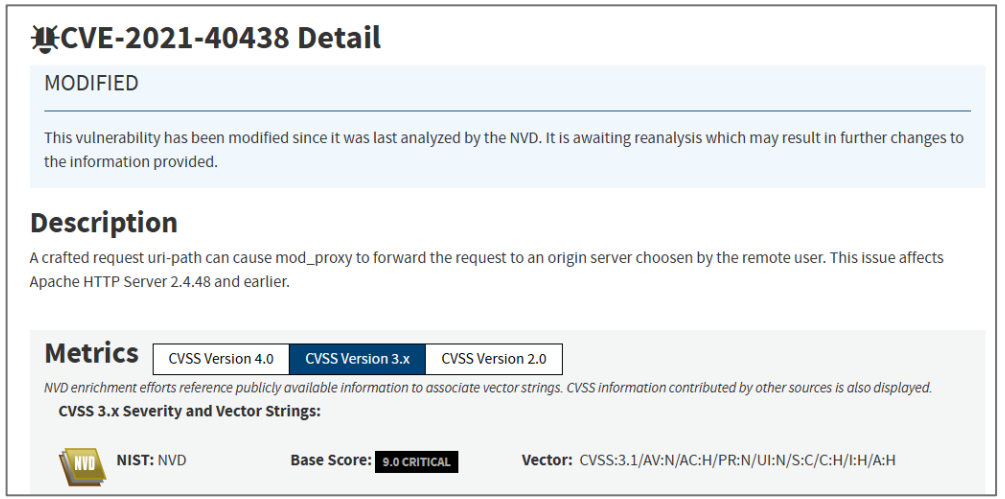
IMDS（Instance Metadata Service）とは
・インスタンス自身の設定情報を保有する
・インスタンスの設定や管理に使用される

まとめ

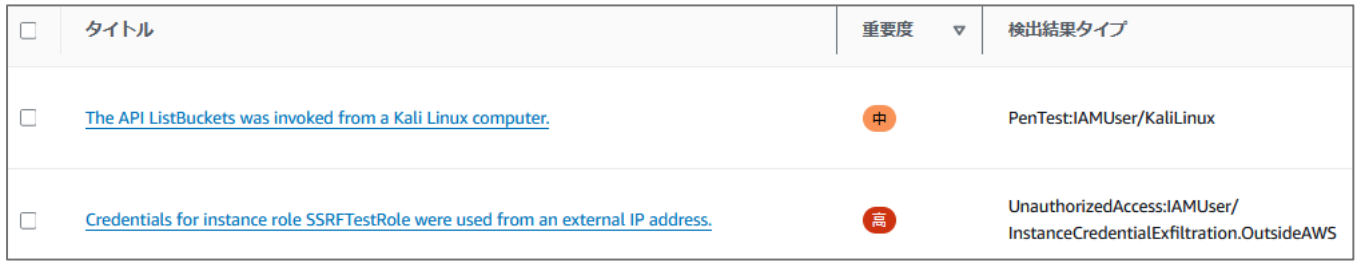
種明かし



- PoCで利用したApacheの脆弱性



- 検出されたGuardDutyアラート



セキュリティイベントの調査にAmazon Detectiveは役に立ちそう

■ Detectiveを使うことで、複数のAWSサービスを横断して調査することによる手間が掛からない

- ✓ 80番ポートがインターネットからアクセス可能であることを確認できた（Inspector）
- ✓ EC2インスタンスで使用しているApacheの脆弱性を確認できた（Inspector）
- ✓ IMDSv1とv2の両方が有効であることを確認できた（Security Hub）
- ✓ インスタンスに紐づくIAMロールが外部から悪用されていることを確認できた（GuardDuty）

つまり・・

SSRFの脆弱性を突かれて認証情報を取得され
S3バケットにアクセスされた！

■ 検出結果グループで全体像を把握した上で、各エンティティを調査する方法がおすすめ

■ Detectiveについてもっと詳しく知りたい方は

電通総研　Detective