

# ワークショップ前提条件

<https://awssecworkshops.jp/>

- はじめに
  - AWS Accountの作成
  - AWS IAM Administrator作成 (root利用禁止)
  - クレジットの追加
- ワークショップ
  - AWS環境における脅威検知と対応

AWS環境における

# 脅威検知と対応ワークショップ

Tsuyoshi Shimizu

Partner Solutions Architect

Amazon Web Services





# 本日の内容

- オープニング (10分)
- Module 1：環境構築と設定 (20分)
- Module 2：攻撃シミュレーション (40分) (※安全)
- Module 3：検知、調査、対応 (50分)
- Module 4：レビュー、問題、環境クリーンアップ (15分)

# AWSアカウントについて

ご自身の持ち込みアカウントをご使用ください。なお、あなたの企業の本番環境アカウントは使用せず、本ワークショップ用に使用できるテスト用アカウントを使用してください。

AWSアカウントのルートユーザーを使用せず、管理用アクセス権を持ったAWS IAMユーザーを使用してください。

# (参考) AWSアカウントの準備

## AWSアカウントの作成 <https://aws.amazon.com/jp/getting-started/>

### ご利用開始のためのリソースセンター

主要な概念から初心者向けのチュートリアルまで、AWS で構築を開始するために必要な情報が見つかります。

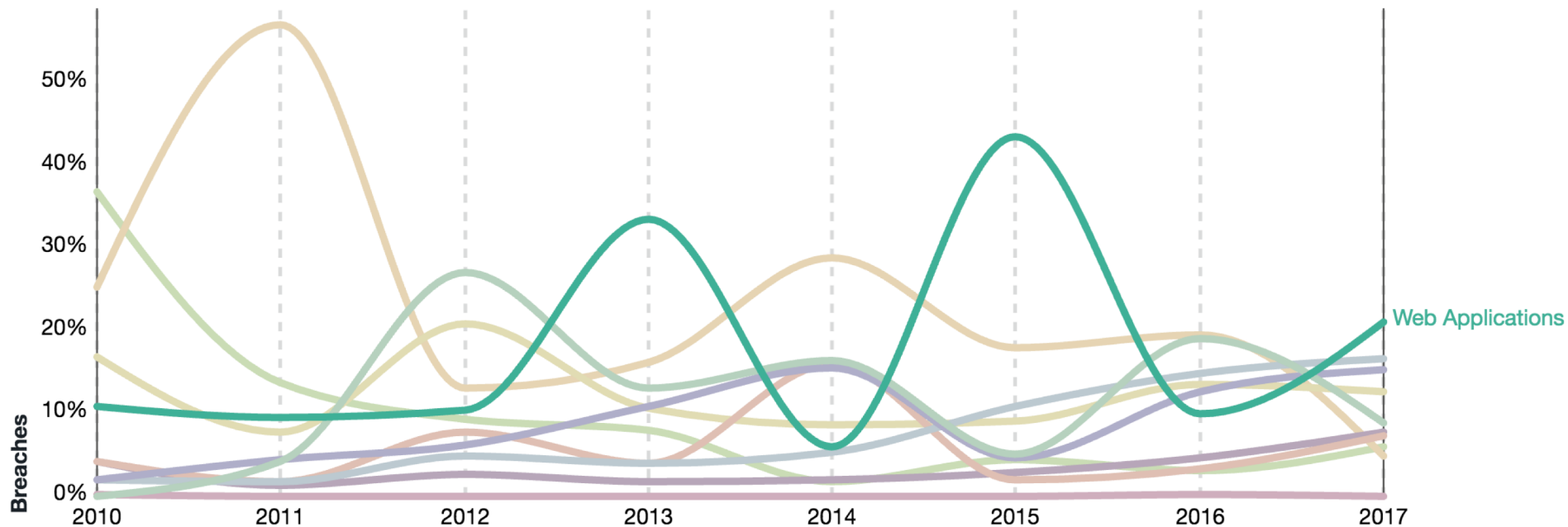
AWS アカウントを作成する

# (参考) 管理者用IAMユーザーの準備

1. AWS IAM コンソールを参照する
2. 左ナビゲーションの「ユーザー」をクリックし、ユーザーを追加する
3. ユーザー名を入力し、「AWS マネージメントコンソールへのアクセスをチェック」、「カスタムパスワード」を選択し、「次のステップ：アクセス権限」をクリック
4. 「既存のポリシーを直接アタッチ」をクリックし、「AdministratorAccess」をクリックして、「次のステップ：タグ」をクリック
5. 以降、デフォルト設定のまま進み、「ユーザーの作成」をクリック
6. 左ナビゲーションの「ダッシュボード」をクリックし、「IAMユーザーのサインインリンク」を使用して、ただいま作成した管理者ユーザーでログイン

# Verizon Report

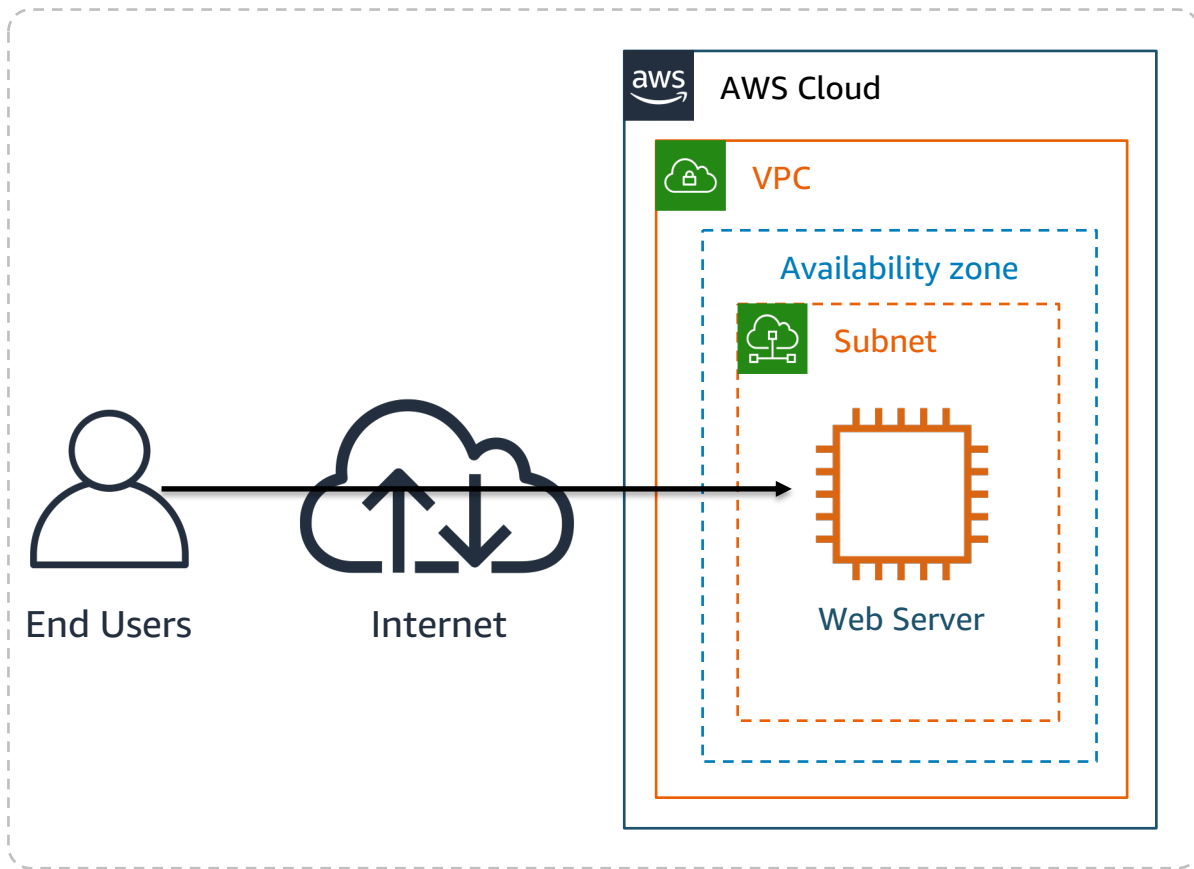
Verizon - 2018 Data Breach Investigations Report  
Data Breach Patterns



Source: 2018 Data Breach Investigation Report, Verizon, 11<sup>th</sup> edition 2018

# 状況

- オンプレからウェブサーバーへ移行PoC実施
- EC2/VPC/S3で構成
- セキュリティ管理者として想定脅威への対策をする



# Module 1

## 環境構築と設定

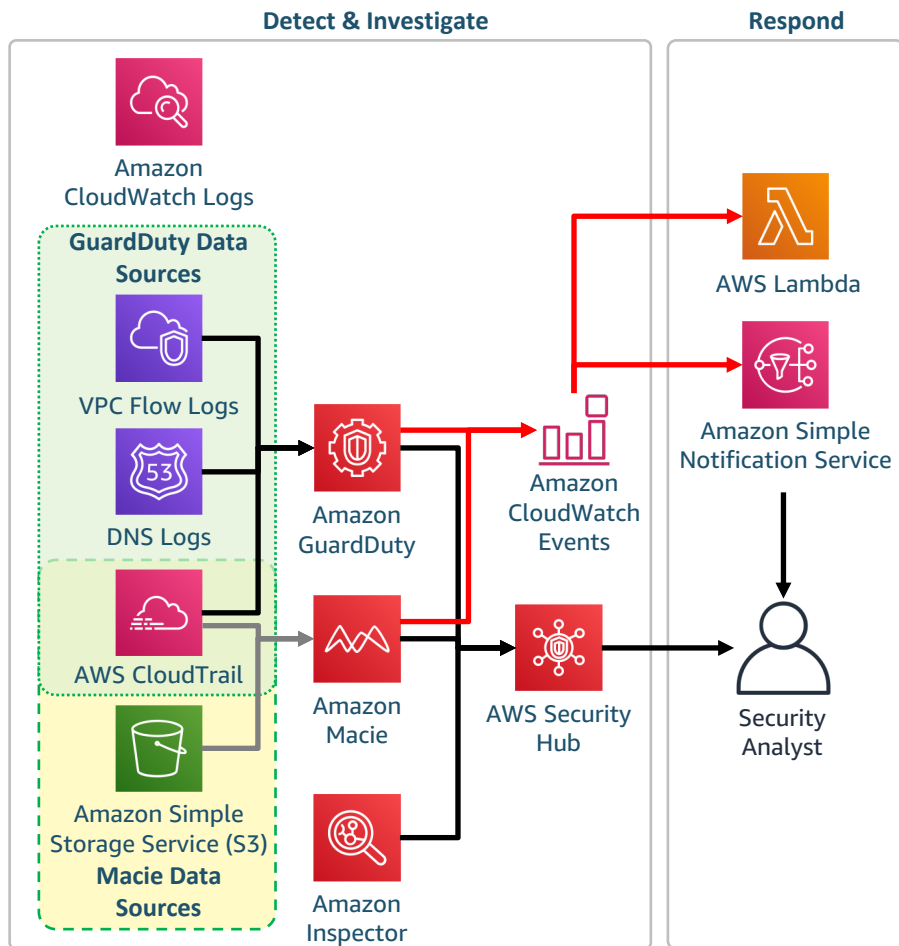


# Module 1 Agenda

- CloudFormation templateの実行 (~5 分)
- 各種設定 (~30 分)



# モジュール1 完了後



<https://scaling-threat-detection.awssecworkshops.jp/>

ワークショップ (35 min):

- **Module 1:環境構築**
  - AWS CloudFormation templateの実行(
    - 手作業セットアップ)

us-west-2 (オレゴン)

# Module 2

## 攻撃シミュレーションと講義



# Module 2 Agenda

- CloudFormation templateの実行 (~5分)
- 脅威検知と対応・講義 (~20分)
- 環境説明 (~10分)

<https://scaling-threat-detection.awssecworkshops.jp/>

- ワークショップ (5 min):
  - Module 1: 環境構築
  - **Module 2: 攻撃シミュレーション**
    - AWS CloudFormation templateの実行
    - 講義

# 脅威検知と対応

# なぜ脅威検知は難しい？



大量の  
データセット

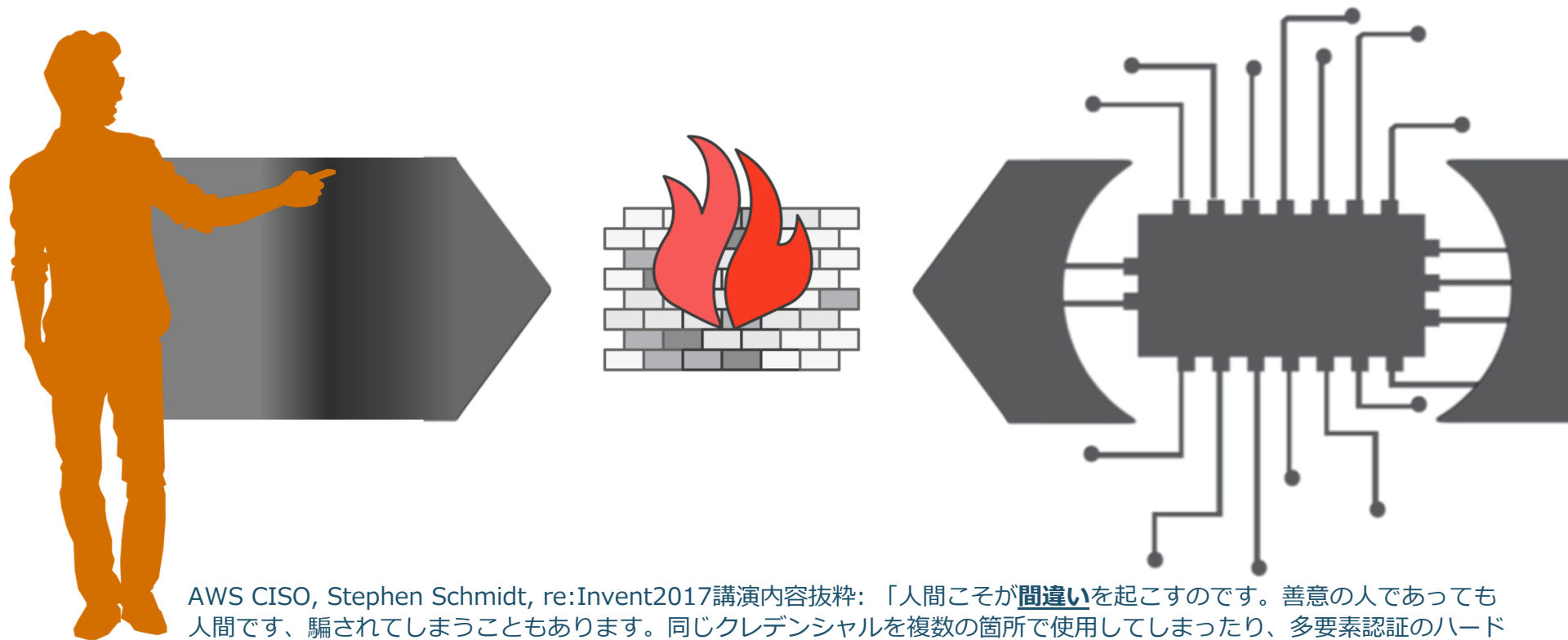


高い検知精度  
の要求



人材と  
スキル不足

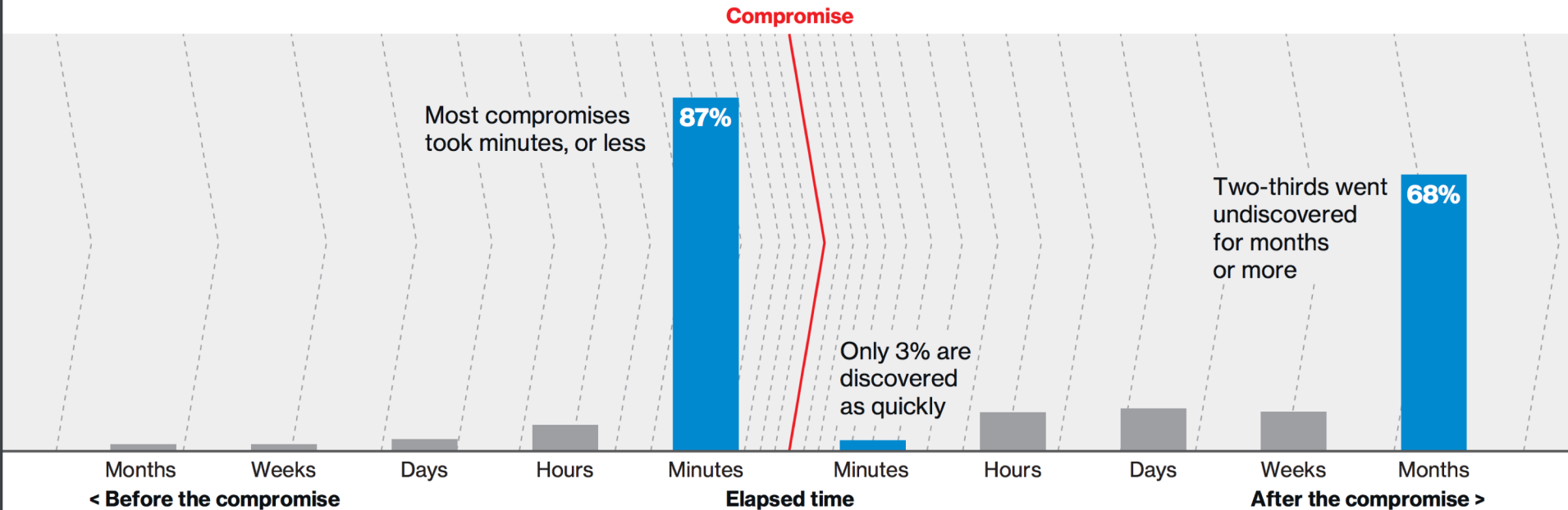
# 「人をデータから切り離す」



AWS CISO, Stephen Schmidt, re:Invent2017講演内容抜粋: 「人間こそが**間違い**を起こすのです。善意の人であっても人間です、騙されてしまうこともあります。同じクレデンシャルを複数の箇所で使用してしまったり、多要素認証のハードウェアトークンを使用しないのも人間です、、、人為的な要因をできる限りデータから隔離する必要があります。



# データ侵害の検知



Source: 2018 Data Breach Investigation Report, Verizon, 11<sup>th</sup> edition 2018

# AWS セキュリティソリューション

<https://www.nist.gov/cyberframework>



## 特定 (Identify)

AWS  
Systems Manager  
AWS Config



## 保護 (Protect)

AWS  
Systems Manager  
Amazon Inspector  
Amazon VPC  
AWS KMS  
AWS CloudHSM  
AWS IAM  
AWS Organizations  
AWS Cognito  
AWS Directory Service  
AWS Single Sign-On  
AWS Certificate Manager



## 検知 (Detect)

AWS CloudTrail  
AWS Config Rules  
Amazon  
CloudWatch Logs  
Amazon GuardDuty  
VPC Flow Logs  
Amazon Macie  
AWS Shield  
AWS WAF



## 対応 (Respond)

AWS Config Rules  
AWS Lambda  
AWS  
Systems Manager  
Amazon  
CloudWatch Events  
Pro Services AERO

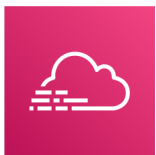


## 回復 (Recover)

AWS Lambda  
AWS DR and Backup  
Solutions

# 脅威検知サービス

# 脅威検知: ログデータソース



## AWS CloudTrail

ユーザー振る舞いとAPI使用を記録



## VPC Flow Logs

VPCネットワーク  
インターフェース  
でのIP通信ログ



## CloudWatch Logs

アプリケーションロ  
グファイルの監視保  
存



## DNS Logs

VPC内の  
DNSクエリログ

# 脅威検知: 機械学習



## Amazon GuardDuty

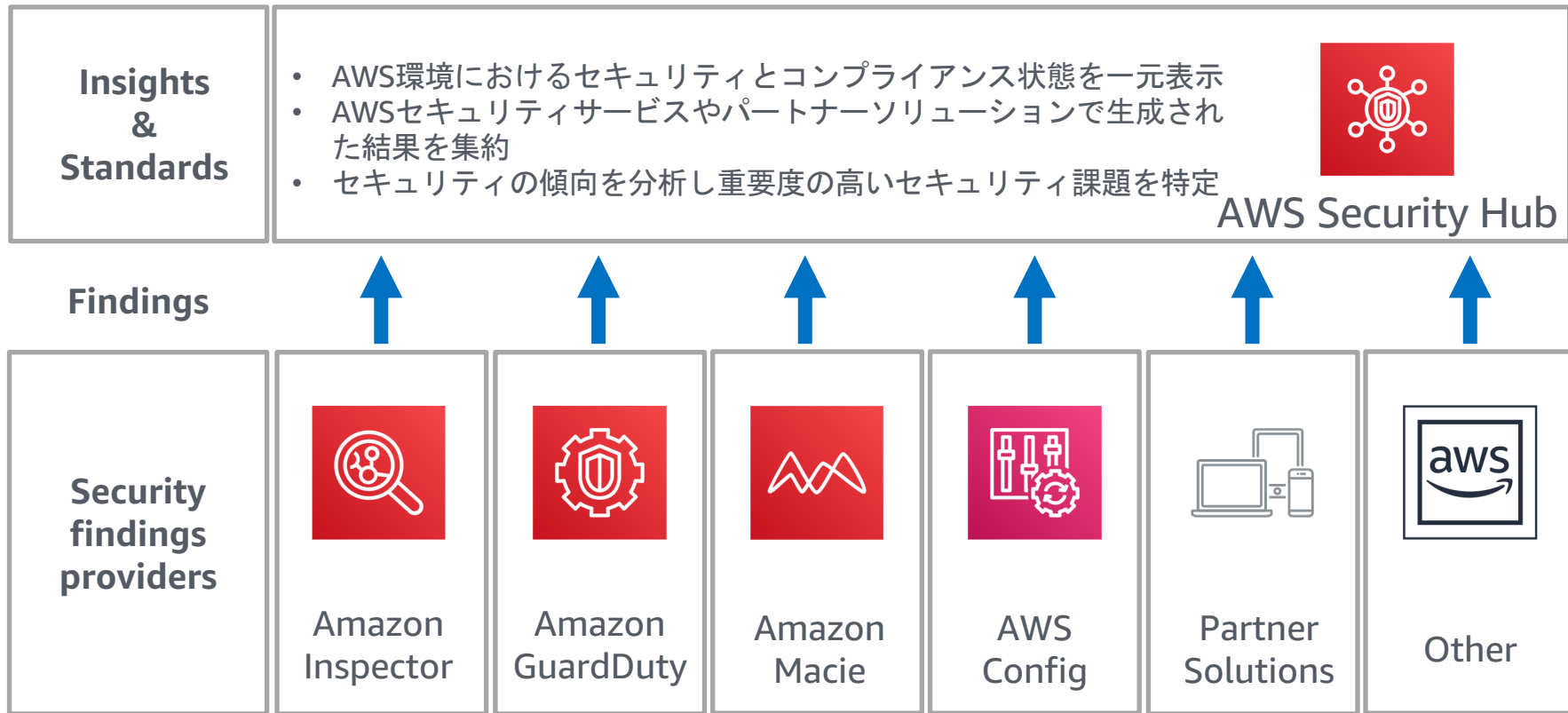
脅威インテリジェンスによる  
脅威検知や継続的監視により  
AWSアカウント/ワークロードを保護



## Amazon Macie

機械学習による機密情報  
の検出、分類、保護

# AWS Security Hub



# 脅威検知: 通知/トリガー



## AWS Config rules

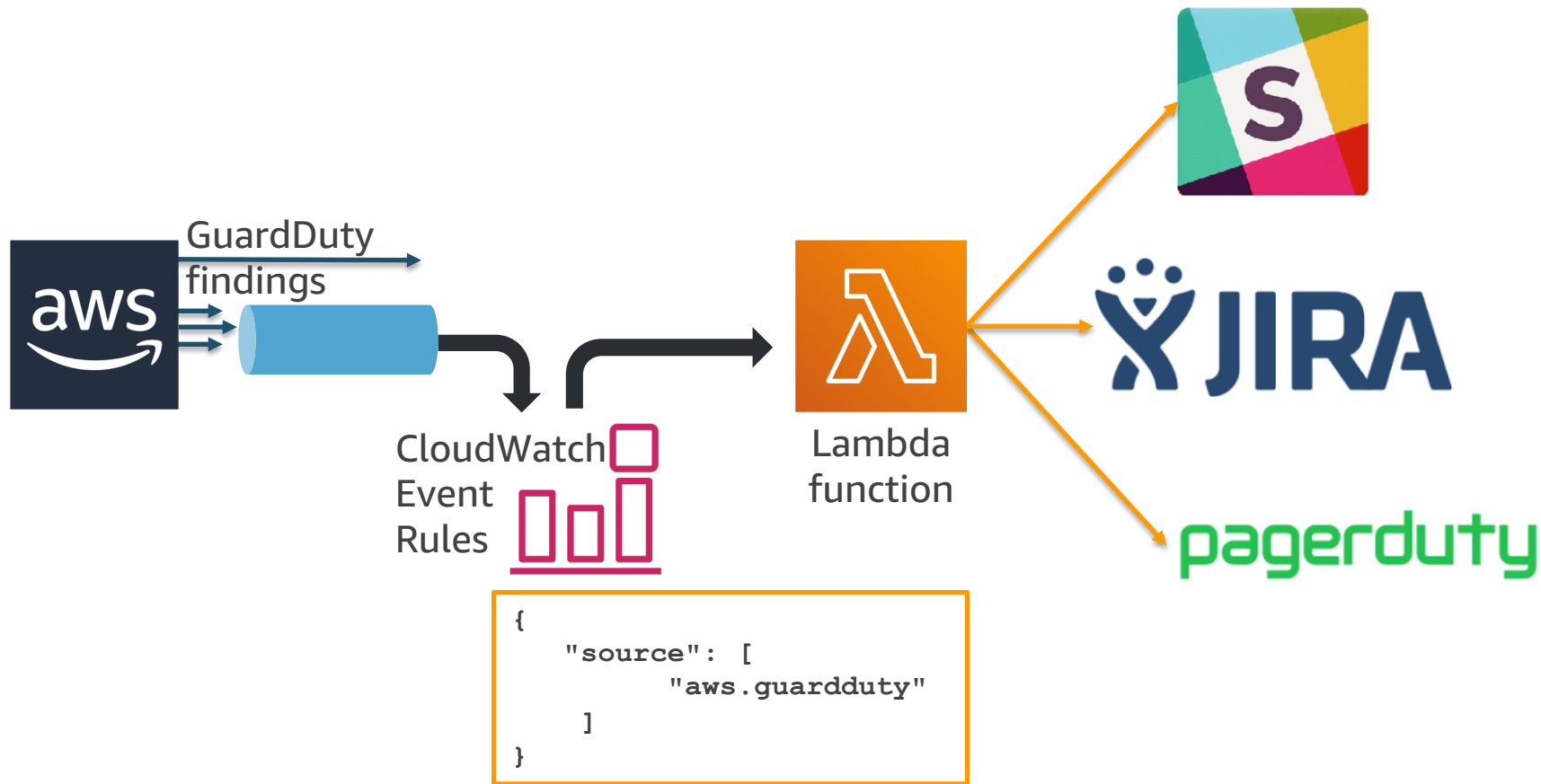
継続的にリソース変更を監視し  
定義ルールへの準拠状況を通知



## Amazon CloudWatch Events

AWSリソースの変更イベントを  
ニアリアルタイムで通知

# Amazon CloudWatch Events





# 脅威対応サービス

# 脅威対応サービス



## AWS Lambda

アプリケーションや  
バックエンドサービス  
のコードを自動実行



## AWS Systems Manager

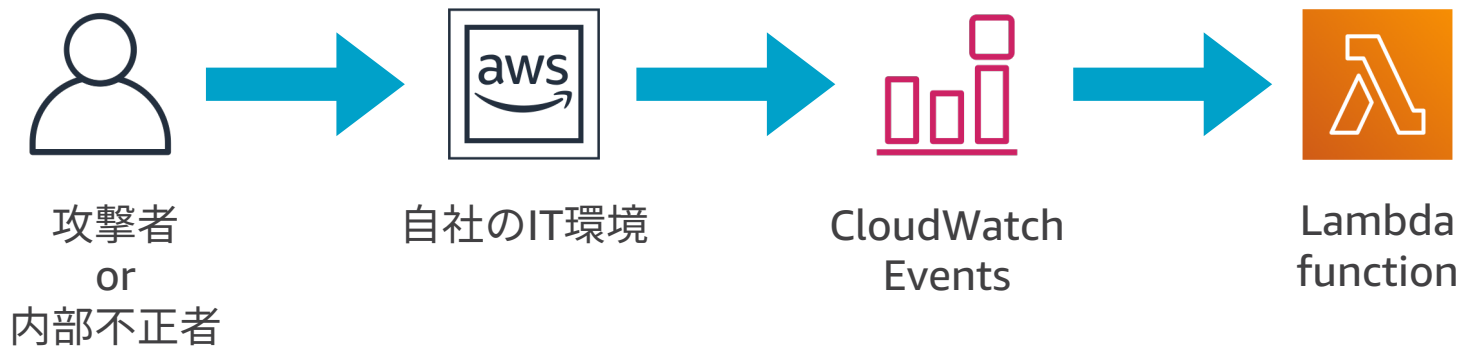
AWSリソースに関する  
運用情報取得や実行  
(エージェント)



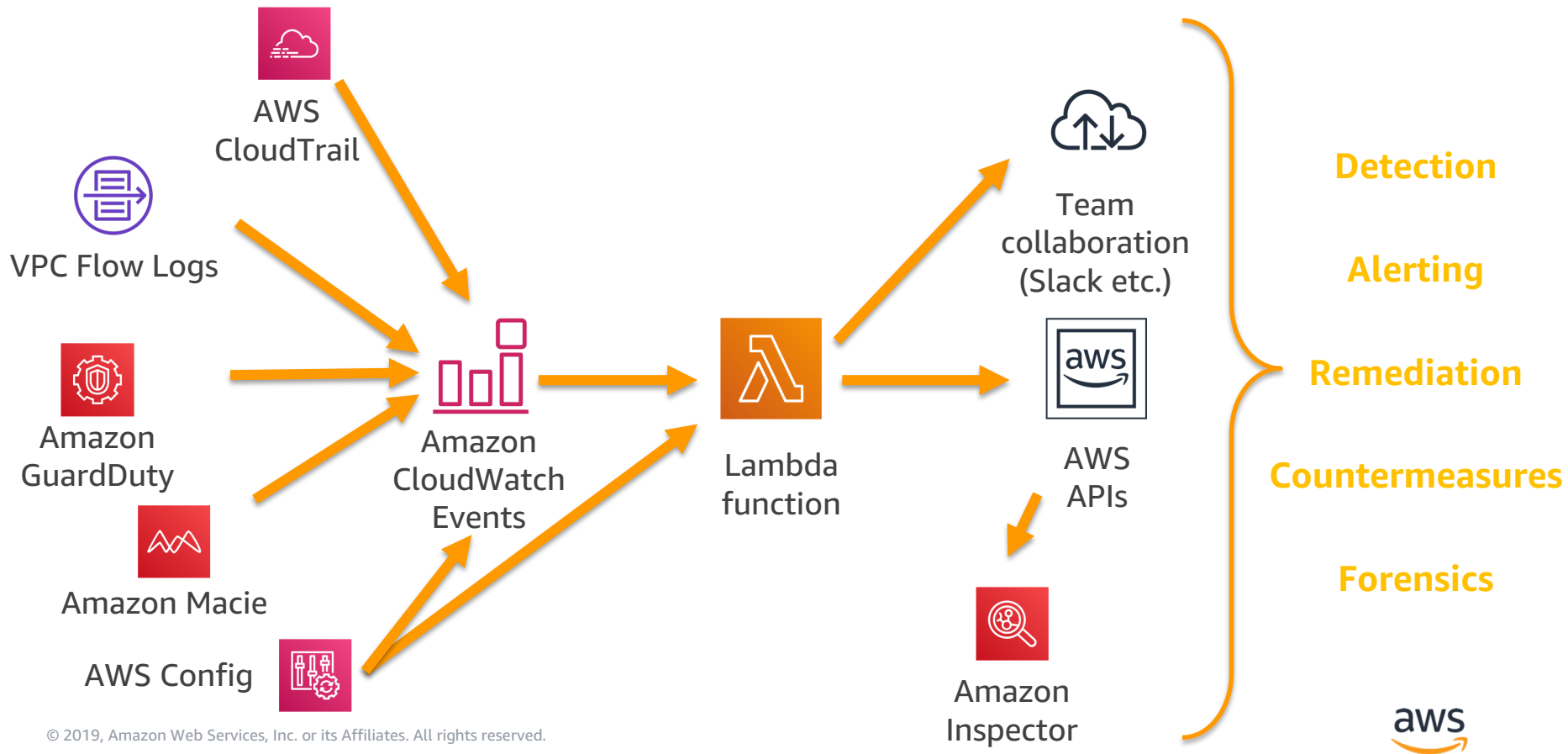
## Amazon Inspector

EC2インスタンスへ  
の自動セキュリティ  
評価  
(エージェント)

# 想定シナリオ

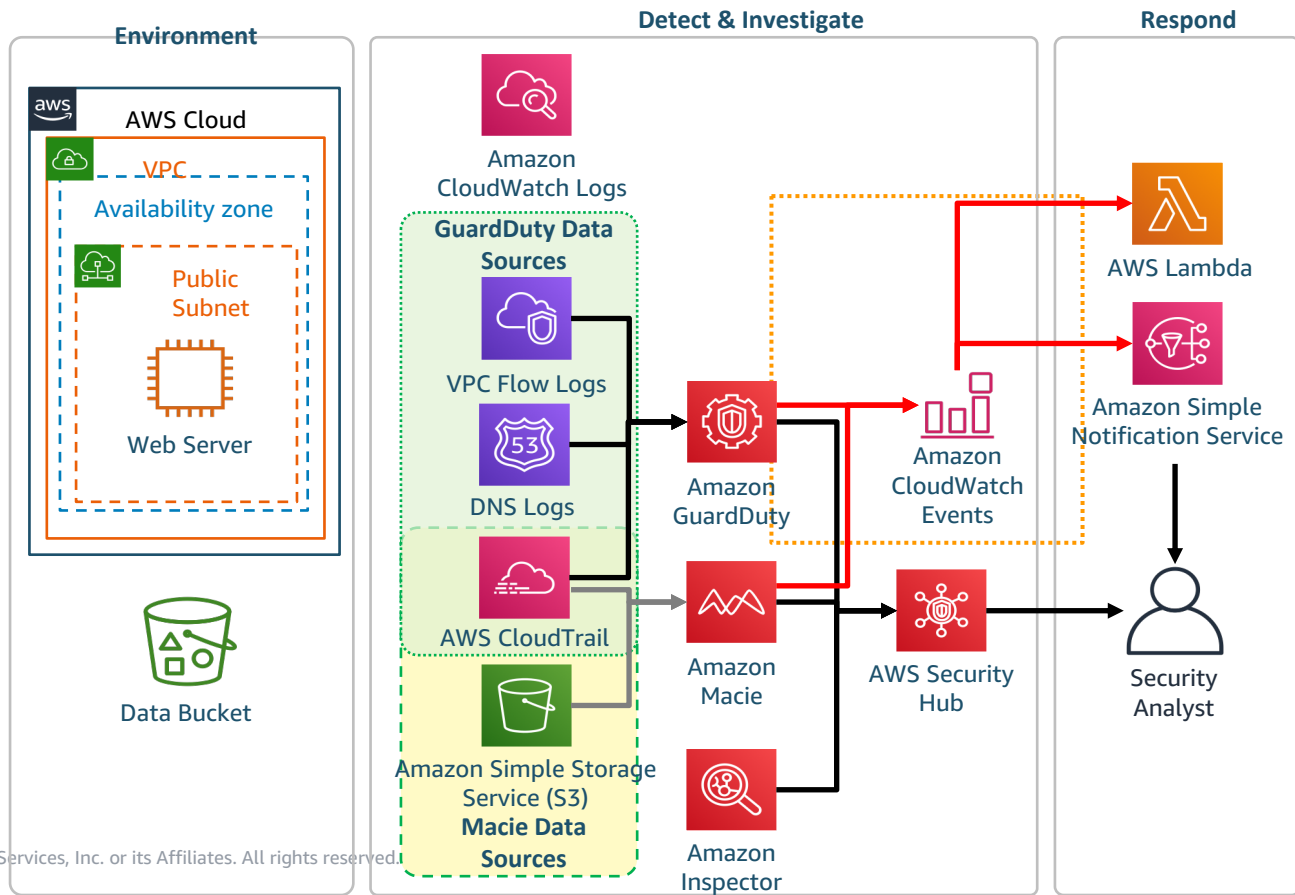


# 想定シナリオ・パターン



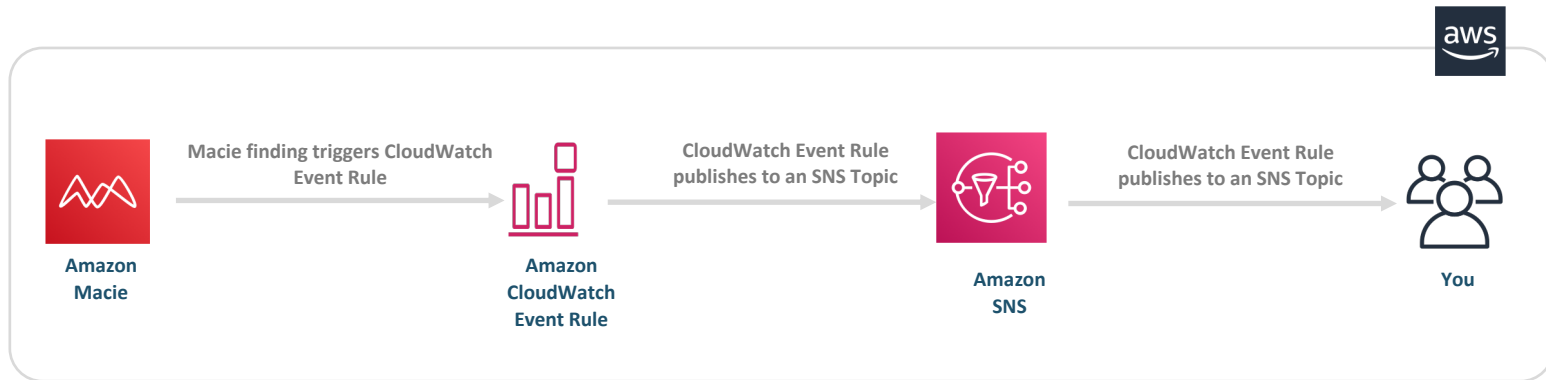
# ライブ・ロールプレイング

# 環境説明



# 対応自動化

CloudWatch Event Rule: *threat-detection-wksp-macie-alert*



# 対応自動化

CloudWatch Event Rule: *threat-detection-wksp-macie-alert*

## Event Pattern

```
{
  "detail-type": [
    "Macie Alert"
  ],
  "source": [
    "aws.macie"
  ]
}
```

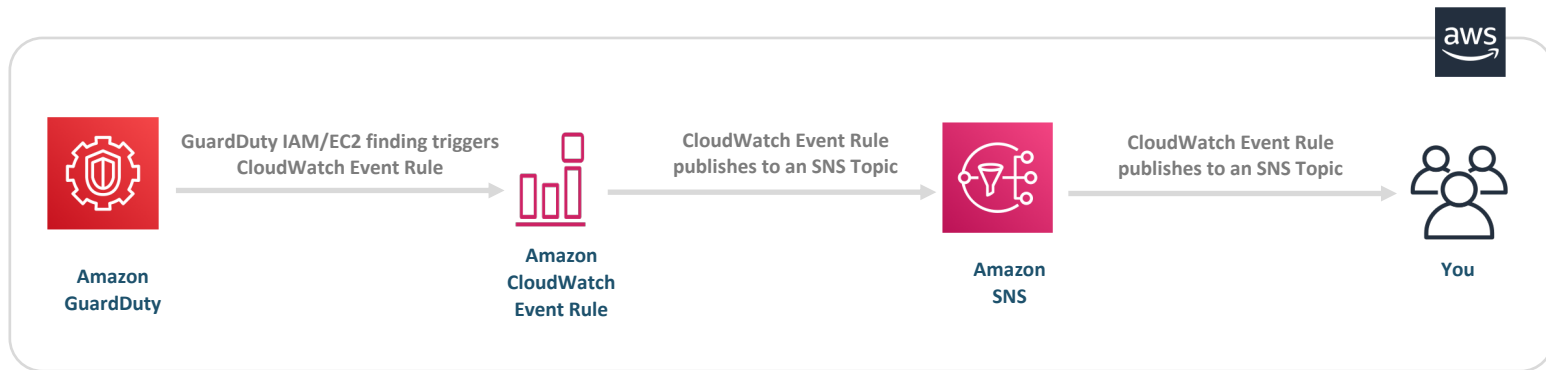
## Input Transformer

```
InputTransformer:
  InputTemplate: '"Amazon Macie Alert: <macdesc>"'
  InputPathsMap:
    macdesc: "$.detail.summary.Description"
```



# 対応自動化

CloudWatch Event Rule: *threat-detection-wksp-guardduty-iam-finding*  
*threat-detection-wksp-guardduty-ec2-finding*



# 対応自動化

CloudWatch Event Rule: *threat-detection-wksp-guardduty-iam-finding*

## Event Pattern

```
{
  "detail-type": [
    "GuardDuty Finding"
  ],
  "source": [
    "aws.guardduty"
  ],
  "detail": {
    "resource": {
      "resourceType": [
        "AccessKey"
      ]
    }
  }
}
```

## Input Transformer

### InputTransformer:

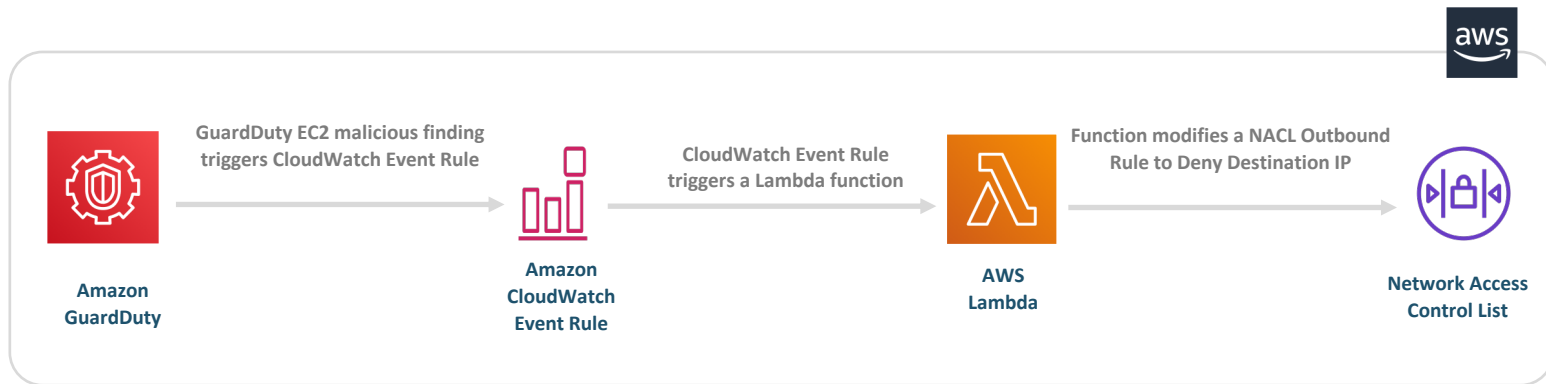
**InputTemplate:** "\"Amazon GuardDuty Finding :  
<type>\"\\\"\\\"\\\"Account : <account>\"\\\"\\\"Region :  
<region>\"\\\"\\\"Description : <description>\"\\\"\\\"Access Key ID :  
<accessKey>\"\\\"\\\"User Type : <userType>\"\\\""

### InputPathsMap:

type: "\$.detail.type"  
description: "\$.detail.description"  
account: "\$.account"  
region: "\$.region"  
accessKey: "\$.detail.resource.accessKeyDetails.accessKeyId"  
userType: "\$.detail.resource.accessKeyDetails.userType"

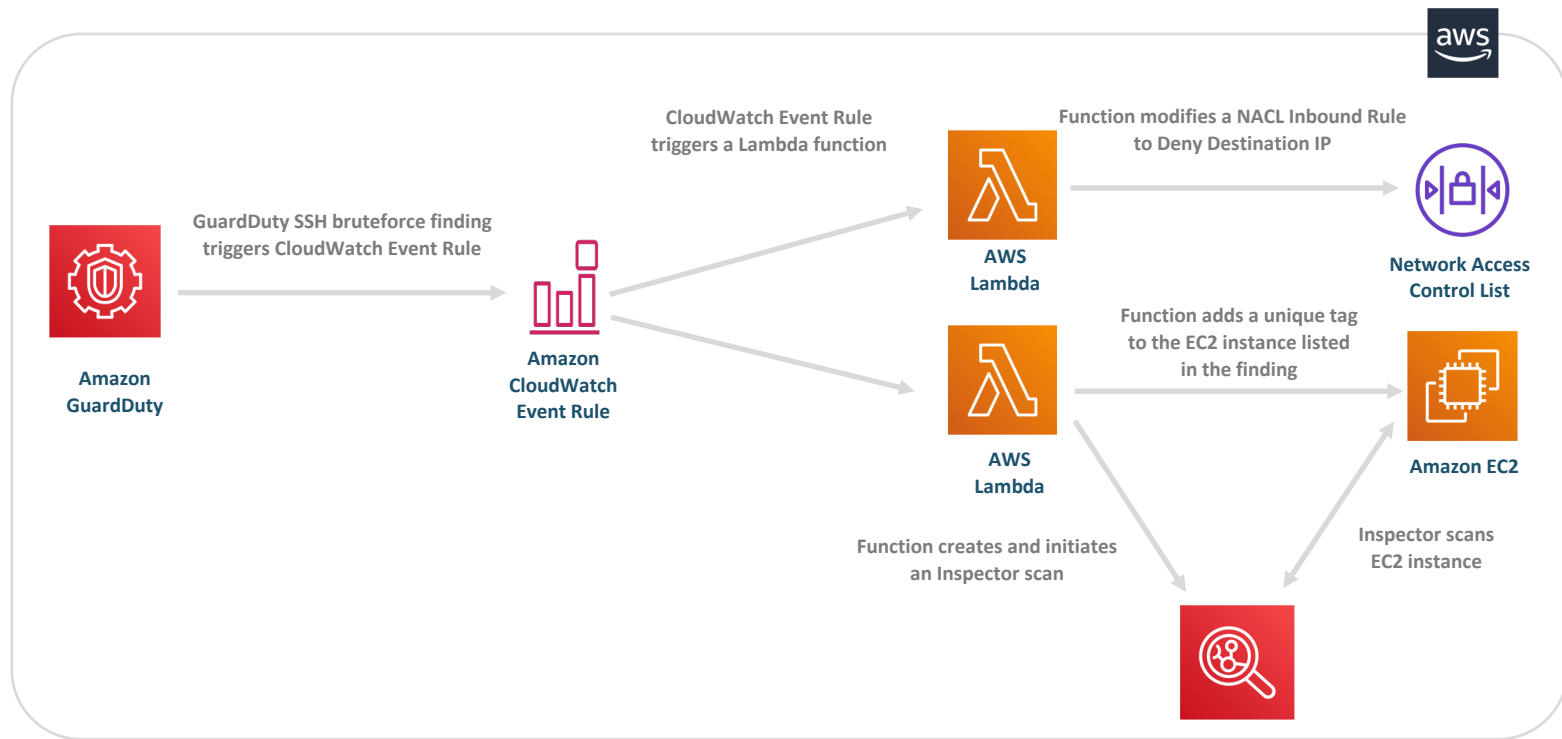
# 対応自動化

CloudWatch Event Rule: *threat-detection-wksp-guardduty-finding-ec2-maliciousip*



# 対応自動化

CloudWatch Event Rule: **threat-detection-wksp-guardduty-finding-sshbruteforce**



# 対応自動化

CloudWatch Event Rule: **threat-detection-wksp-guardduty-finding-sshbruteforce**

## Event Pattern

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail": {
    "type": [
      "UnauthorizedAccess:EC2/SSHBruteForce"
    ]
  }
}
```

# おさらい

1. CloudTrailを利用した解析におけるGuardDutyとMacieの違いは何ですか？
2. AWS Security Hub に自動的に結果を送る脅威検知サービスは何ですか？
3. 対応の自動化に重要なサービスは何ですか？
4. あなたのアカウントが100以上のVPCを持っている時に、GuardDutyはどのくらいパフォーマンスに影響を与えますか？
5. どのサービスがあなたのAmazon EC2 インスタンスに直接アクセスしますか？

# Module 3

## 検知と対応



<https://scaling-threat-detection.awssecworkshops.jp/>

- Workshops (75 min):
  - Module 1: 環境構築
  - Module 2: 攻撃シミュレーション
  - **Module 3: 検知と対応**
    - Part 1: 侵害されたAWS IAM クレデンシャル
    - Part 2: 侵害された EC2 instance
    - Part 3: 侵害された S3 Bucket



# Module 4

## レビュー、ディスカッション、 クリーンアップ



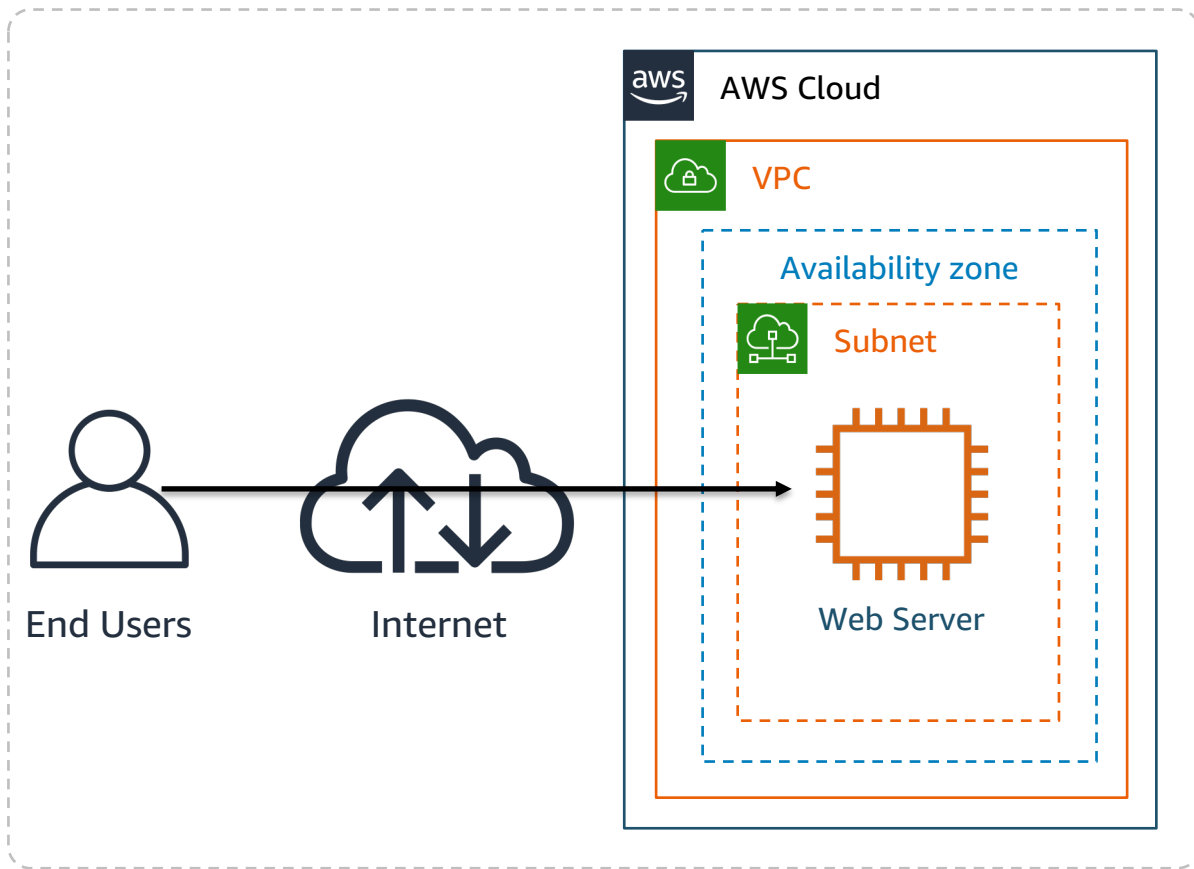
# Module 4 Agenda

- レビュー ( 5 min)
- ディスカッション ( 10 min)
- クリーンアップ

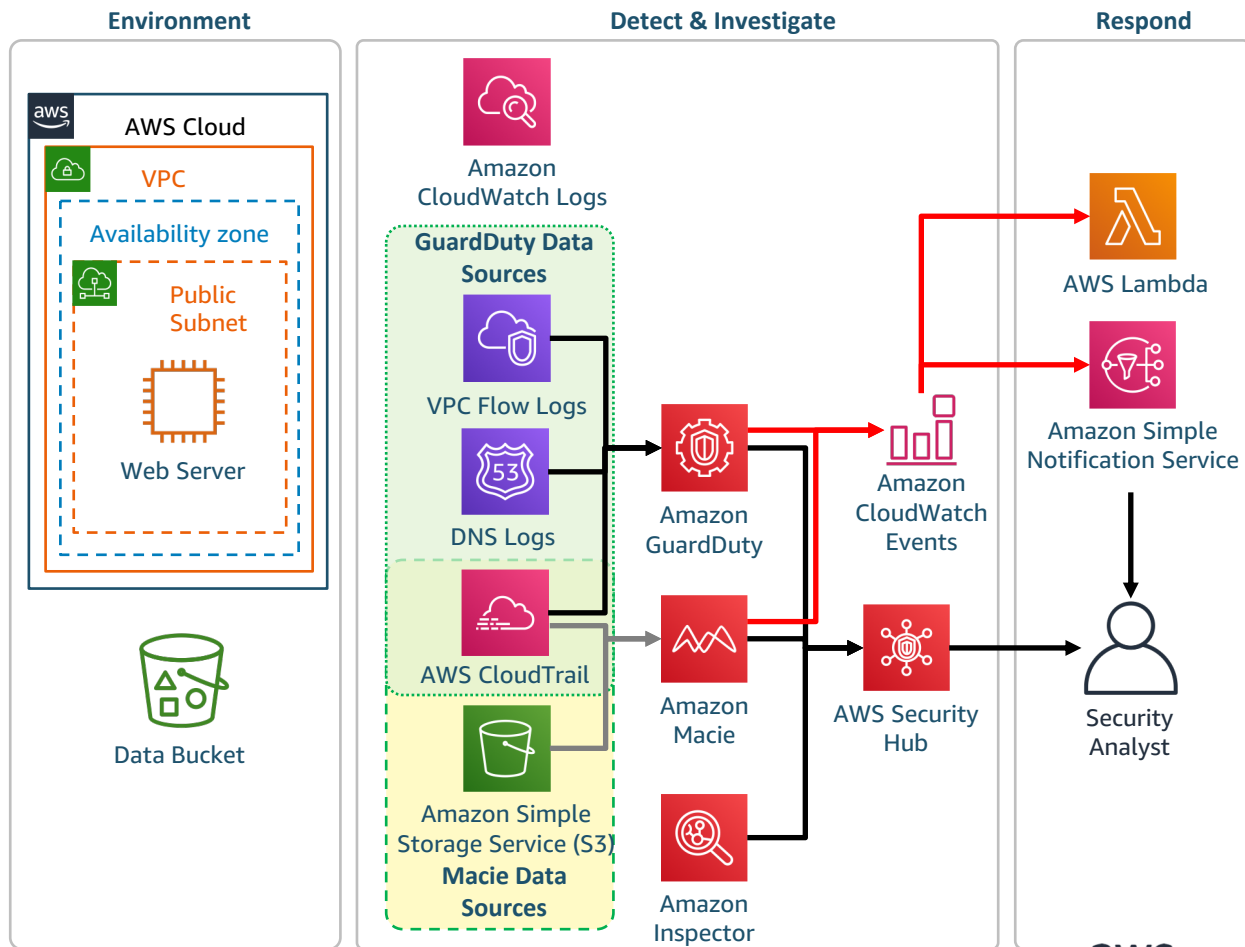
# <https://awssecworkshops.jp/>

- ワークショップ(45 min):
  - Module 1: 環境構築
  - Module 2: 攻撃シミュレーション
  - Module 3: 検知と対応
  - **Module 4: ディスカッション**

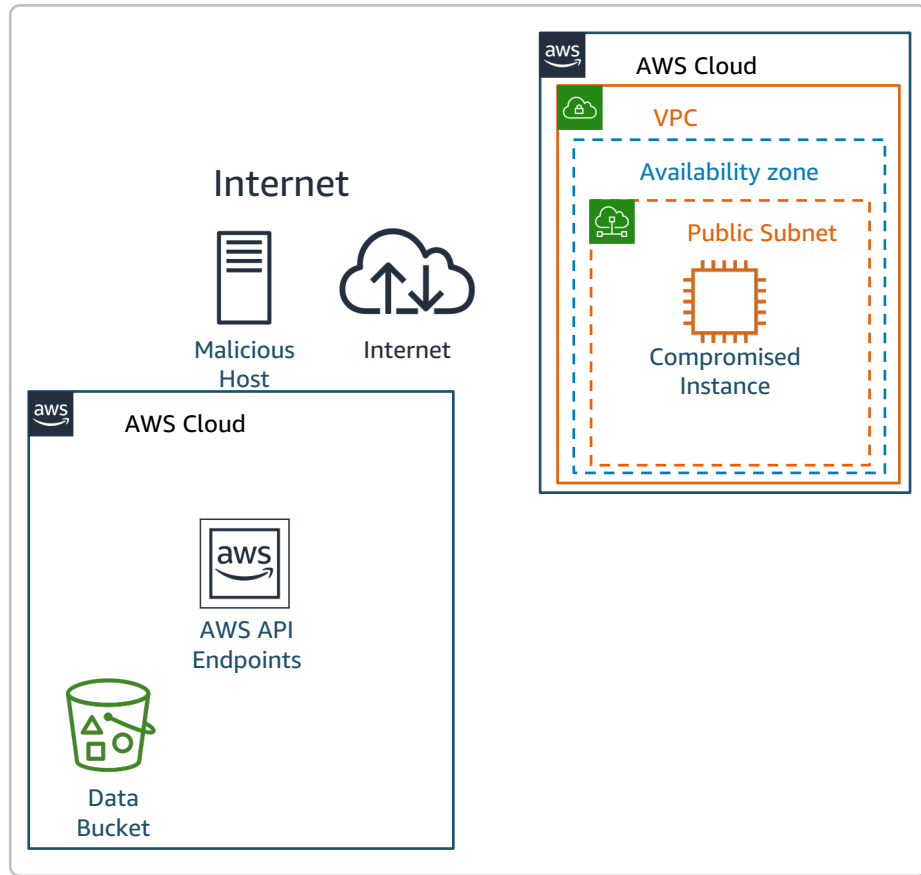
# 攻撃対象



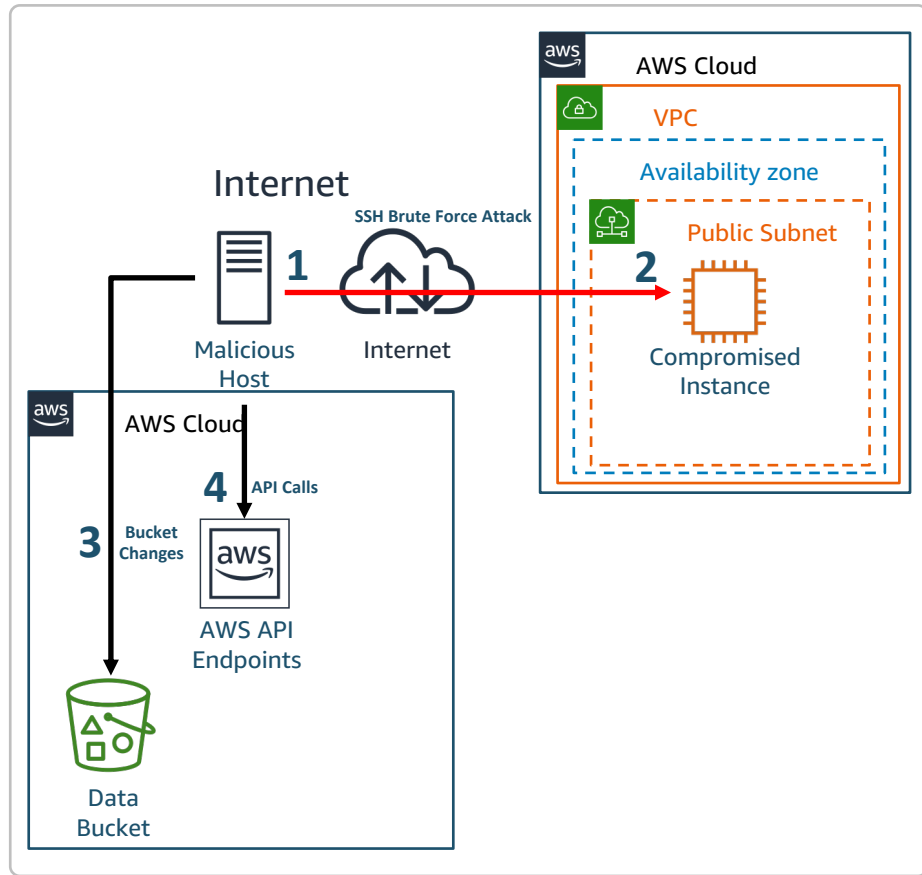
# モジュール2 完了後



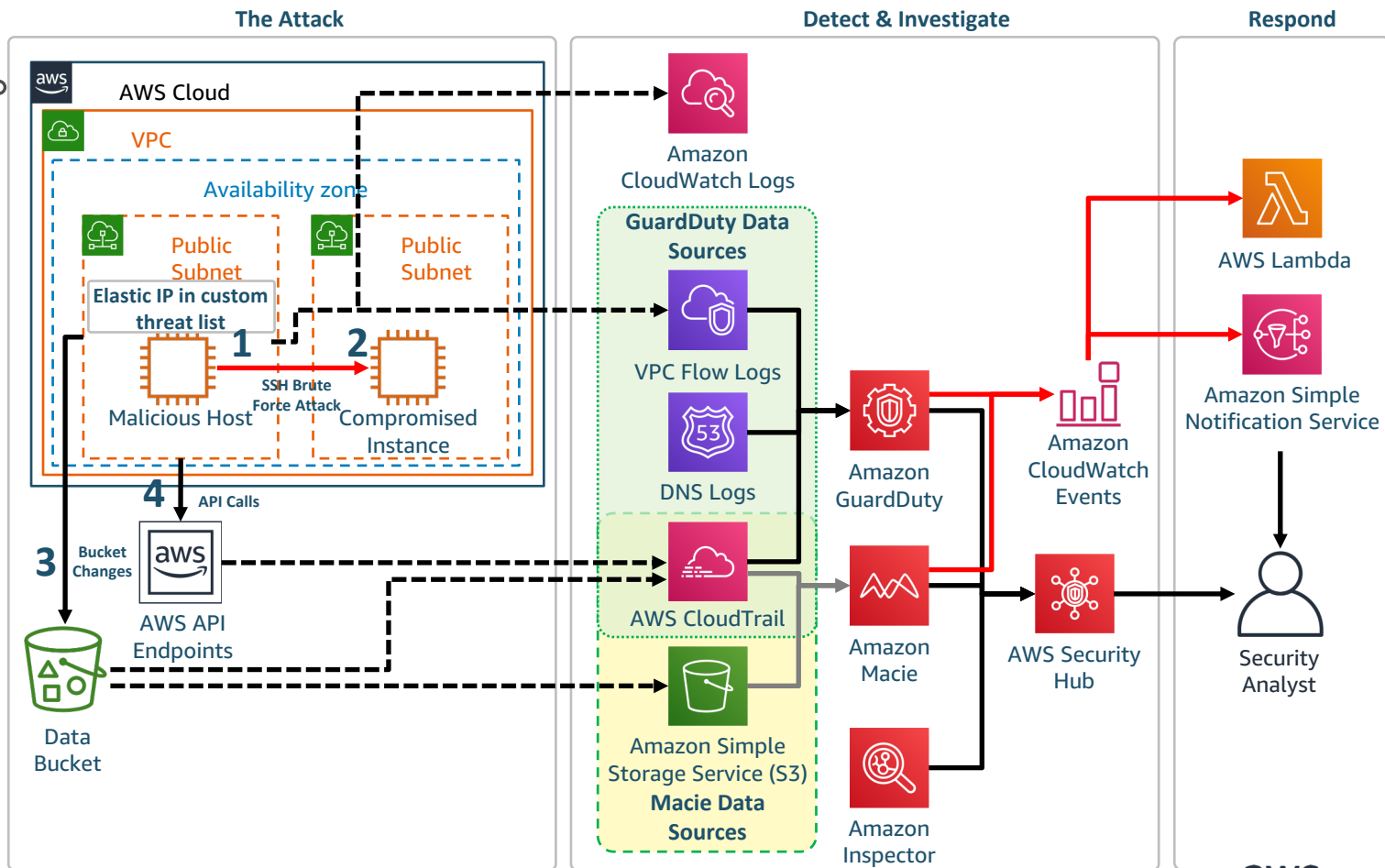
# 攻撃シミュレーション



# 攻撃シミュレーション



# ワーク ショップ 全体像





# ワークショップ 質問

# Question 1

なぜ、“攻撃ホスト“からAWS API CallはGuardDuty findingsを生成したのでしょうか？

# Question 2

ユニークなAWS API Callは攻撃ホストからいくつ生成されましたか？

また、それらをどうやって識別しましたか？

# Question 3

このワークショップにおいて重要度高のSSH ブルートフォースアタックの検知結果を無視できるのはなぜか？

重要度低のブルートフォース検知結果との違いはどのようなものか？

# Question 4

IAM Roleのすべてのセッションを取り消すと、アプリケーションの可用性に影響があるリスクがあります。

このリスクを軽減するような修復方法を何が考えられますか？

# Question 4

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Deny",
    "Action": [
      "*"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "DateLessThan": {
        "aws:TokenIssueTime": "2018-12-30T04:29:04.801Z"
      },
      "StringEquals": {
        "aws:userId": ["AR0AI2X7ZKTD3E4SA0HTE:i-06e8a8b87f7106582"]
      }
    }
  }
]
```

# Question 5

S3バケットを作ることやオブジェクトへの不特定多数のアクセスから守るために有効な方法は何でしょうか？

# Question 5 Block public access

パブリックアクセス設定

アクセスコントロールリスト

バケットポリシー

CORS の設定

## このバケットのパブリックアクセス設定

Amazon S3 ブロックのパブリックアクセス設定を使用して、バケットのデータへのパブリックアクセスを許可しないようにします。Amazon S3 ブロックのパブリックアクセス設定は、アカウントレベルでも行うことができます。 [詳細はこちら](#)


### このバケットのパブリックアクセスコントロールリスト (ACL) を管理する


アクセスコントロールリスト (ACL) は、基本的な読み取り/書き込みアクセス許可を他の AWS アカウントに付与するために使用されます。

更新

キャンセル


保存


☒ 新規のパブリック ACL と、パブリックオブジェクトのアップロードをブロックする (推奨) 

☒ パブリック ACL を通じて付与されたパブリックアクセスを削除する (推奨) 

### このバケットのパブリックバケットポリシーを管理する

バケットポリシーでは、JSON ベースのアクセスポリシー言語を使用して、Amazon S3 リソースへの高度なアクセス許可を管理します。

☐ 新規のパブリックバケットポリシーをブロックする (推奨) 

☐ バケットにパブリックポリシーがある場合、パブリックアクセスとクロスアカウントアクセスをブロックする (推奨) 



# Question 6

どのタイプのサーバーサイド暗号化がデータバケットのオブジェクト暗号化に使われているか？

SSE-KMSを使っている場合に、Macieはオブジェクトの識別できるか？

# Question 7

このワークショップで調査したS3バケットについて、Macieは“S3 Bucket IAM policy grants global read rights.”というアラートを出しましたか？ そのオブジェクトは実際外からアクセス可能でしたか？

そのバケットがグローバル読み取り権限が許可されていたポリシーを持っていた場合は、暗号化オブジェクトにはアクセス可能ですか？

# Cleanup

# 関連参考リンク

**AWSクラウドセキュリティ**

<https://aws.amazon.com/jp/security/>

**Verizon 2018 Data Breach Investigations Report**

[https://www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2018\\_Report\\_en\\_xg.pdf](https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf)

**NIST Cyber Security Framework**

<https://www.nist.gov/cyberframework>

**[Whitepaper] AWS Cloud Adoption Framework Security Perspective**

[https://d0.awsstatic.com/whitepapers/AWS\\_CAF\\_Security\\_Perspective.pdf](https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf)

**GuardDuty All Findings**

[https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\\_findings.html](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings.html)

**GuardDuty to Slack Integration**

<https://github.com/aws-samples/amazon-guardduty-to-slack>

**GuardDuty Multi-Account script**

<https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts>

**GuardDuty Testing Scripts**

<https://github.com/aws-labs/amazon-guardduty-tester>

**Macie blog with test data**

<https://aws.amazon.com/blogs/security/classify-sensitive-data-in-your-environment-using-amazon-macie/>

ありがとうございました