[AWS Black Belt Online Seminar]
AWS Security Hub

サービスカットシリーズ

Sr. Security Solutions Architect
桐山 隼人
2020/10/13

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

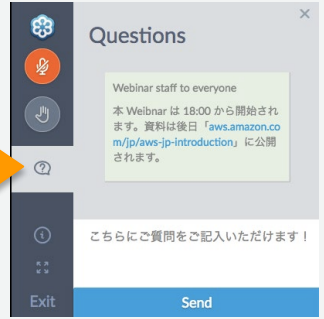
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
  お答えできませんのでご了承下さい

① 吹き出しをクリック
② 質問を入力
③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2020年10月13日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(http://aws.amazon.com)にてご確認ください。

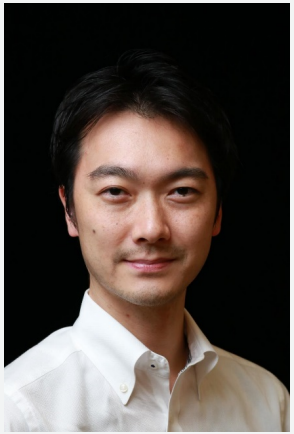
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。

- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

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

本セミナーの対象者とゴール

- 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・運用を管理する方
  - コンプライアンス遵守に関してAWS リソースの組織内ポリシーやルールへの準拠に責任を有する方
- ゴール
  - AWS サービスを用いて、企業におけるセキュリティとコンプライアンス対応の課題をどのように解決できるのかについて理解する
  - そのための AWS Security Hub の適した使い方 (ベストプラクティス) を習得する
- 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やコンプライアンス要件に関する基本的な説明
  - AWS Security Hub 以外の AWS サービスの細かな仕様や詳細解説 (AWS サービスの基本知識が前提)

本日のアジェンダ

- AWS Security Hub とは
- AWS Security Hub を使ってみる
  1. AWS Security Hub をデプロイする
  2. セキュリティツールと統合する
  3. セキュリティ基準を有効化する
  4. セキュリティ検出結果を取り扱う
  5. 対応を自動化する
  6. コスト管理をする
- まとめ

AWS Security Hub とは

セキュリティとコンプライアンス対応における課題

対応すべき
コンプライアンス
要件の多さ

多数のツールや
データによる
複雑性

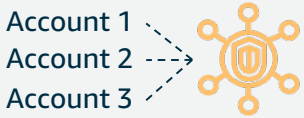
大量の
セキュリティ
アラート

統合的な
可視性の不足

AWS Security Hub とは

組織内の様々なセキュリティデータを集約して、一元的に可視化

AWS Security Hub 利用時の流れ



全 AWS アカウントで AWS Security Hub を有効化する(全体監視)

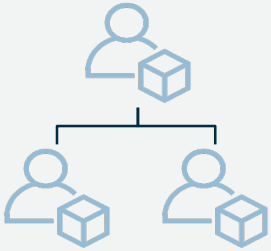
継続的にデータ集約し検出結果の優先順位をつける

コンプライアンスチェックを自動的に実行する

検出結果に基づいて効果的なアクションを行う

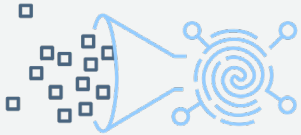
セキュリティ課題にまつわる可視性の向上 → コンプラアインス遵守状態のより簡単な維持

組織に求められるセキュリティ



組織全体の監視

データ集約と
セキュリティ評価



検出結果の
優先順位付け

効果的な対応

AWS Security Hub を使ってみる

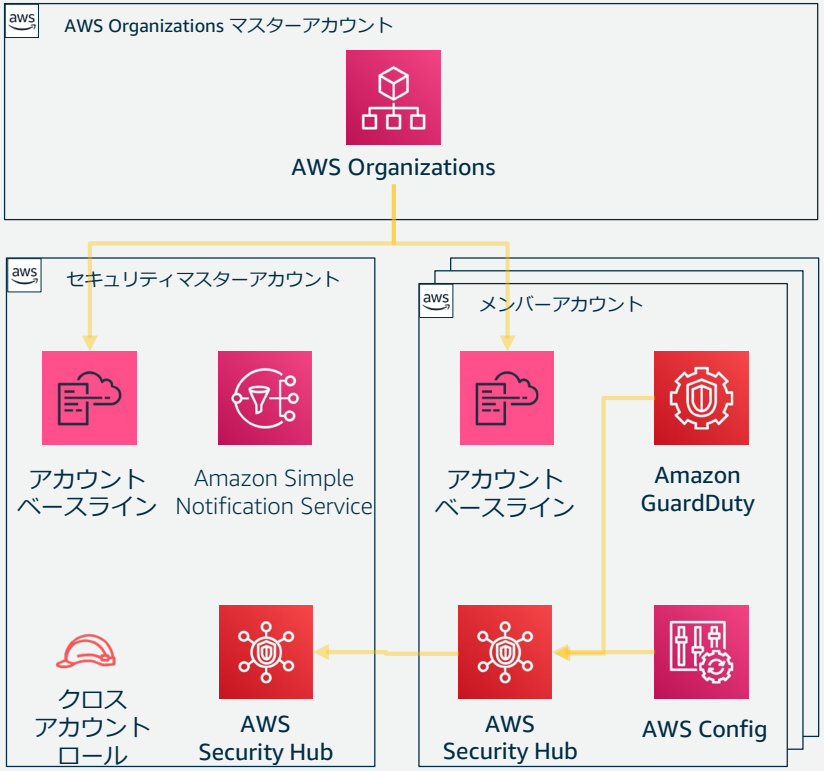
AWS Security Hub 利用の6つのステップ

1. AWS Security Hub をデプロイする
2. セキュリティツールと統合する
3. セキュリティ基準を有効化する
4. セキュリティ検出結果を取り扱う
5. 対応を自動化する
6. コスト管理をする

AWS Security Hub 利用の6つのステップ

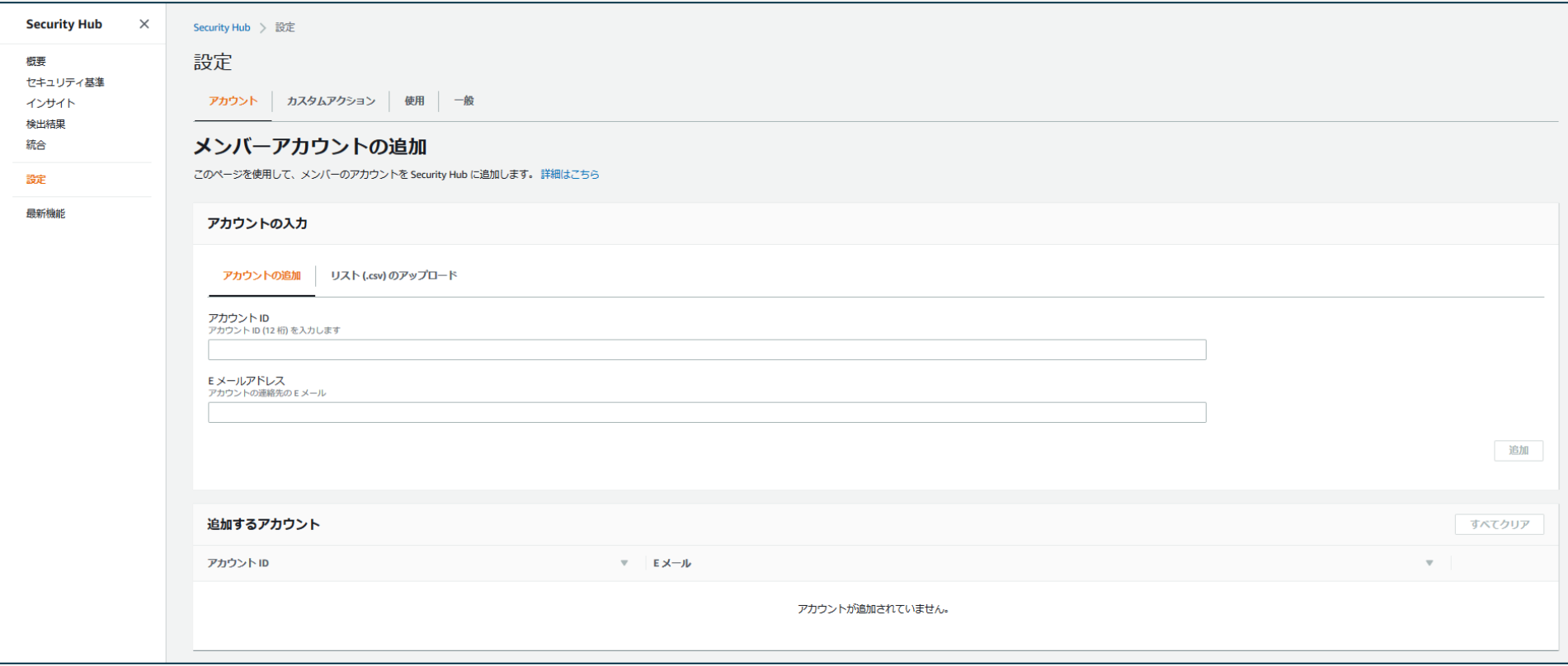
1. AWS Security Hub をデプロイする
2. セキュリティツールと統合する
3. セキュリティ基準を有効化する
4. セキュリティ検出結果を取り扱う
5. 対応を自動化する
6. コスト管理をする

AWS Security Hub デプロイのポイント



- 全リージョンと全AWSアカウントに対し、不正な振る舞いや構成ミスがないか継続的に監視する。通常、使用していないリージョンも有効化しておく
- AWS Config が有効化され、サポートする全リソース(グローバルリソースも含む)で記録開始されていること
- 監視対象のメンバーアカウントを招待することで Security Hub を有効化し、セキュリティマスターアカウントと関連付ける

管理画面でのメンバーアカウントの追加



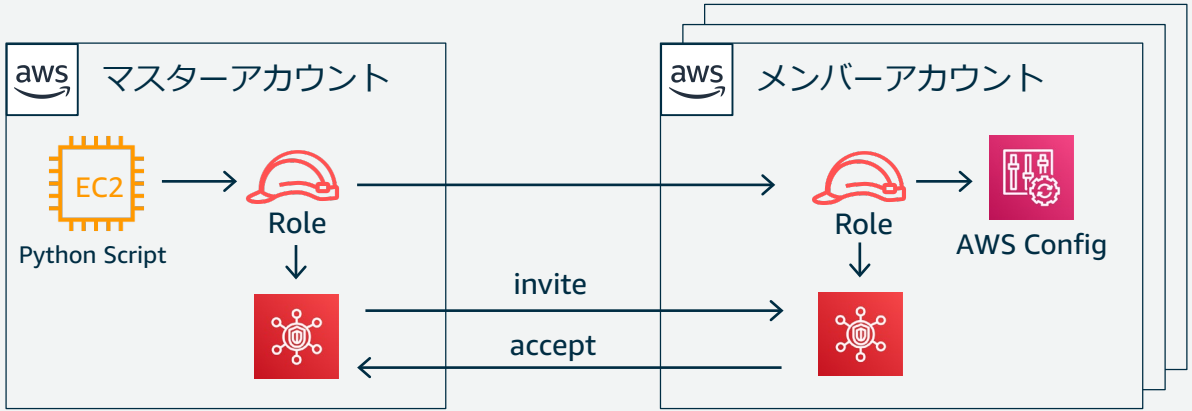
AWS Security Hub のマスターアカウントとメンバーアカウント
https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-accounts.html

マルチアカウント用スクリプトを活用する

マスターアカウント配下へ監視対象AWSアカウントの一斉追加

スクリプト実行により、マスターアカウントからの招待送付、メンバーアカウントでの自動的な招待受諾、デプロイリージョンの選択、AWS Config の有効化、セキュリティ基準の有効化を実施

```
enablesecurityhub.py --master_account 111122233344 --
assume_role sh-member-enable accounts.csv --enable_standards
standards/aws-foundational-security-best-practices/v/1.0.0
```



[GitHub] awslabs/aws-securityhub-multiaccount-scripts
https://github.com/awslabs/aws-securityhub-multiaccount-scripts/projects

[参考] GuardDutyのアカウント階層の活用

GuardDutyの既存のマスター/メンバーアカウント階層を出力する

```
aws guardduty list-members --detector-id <Detector ID>
--query "Members[].[AccountId, Email]" --output text |
awk '{print $1 "," $2}'
```

*上記コマンドにより*GuardDuty*メンバーアカウント*ID*と*E*メールアドレスのリストが出力される

AWS Security Hub 利用の6つのステップ

1. AWS Security Hub をデプロイする

2. セキュリティツールと統合する

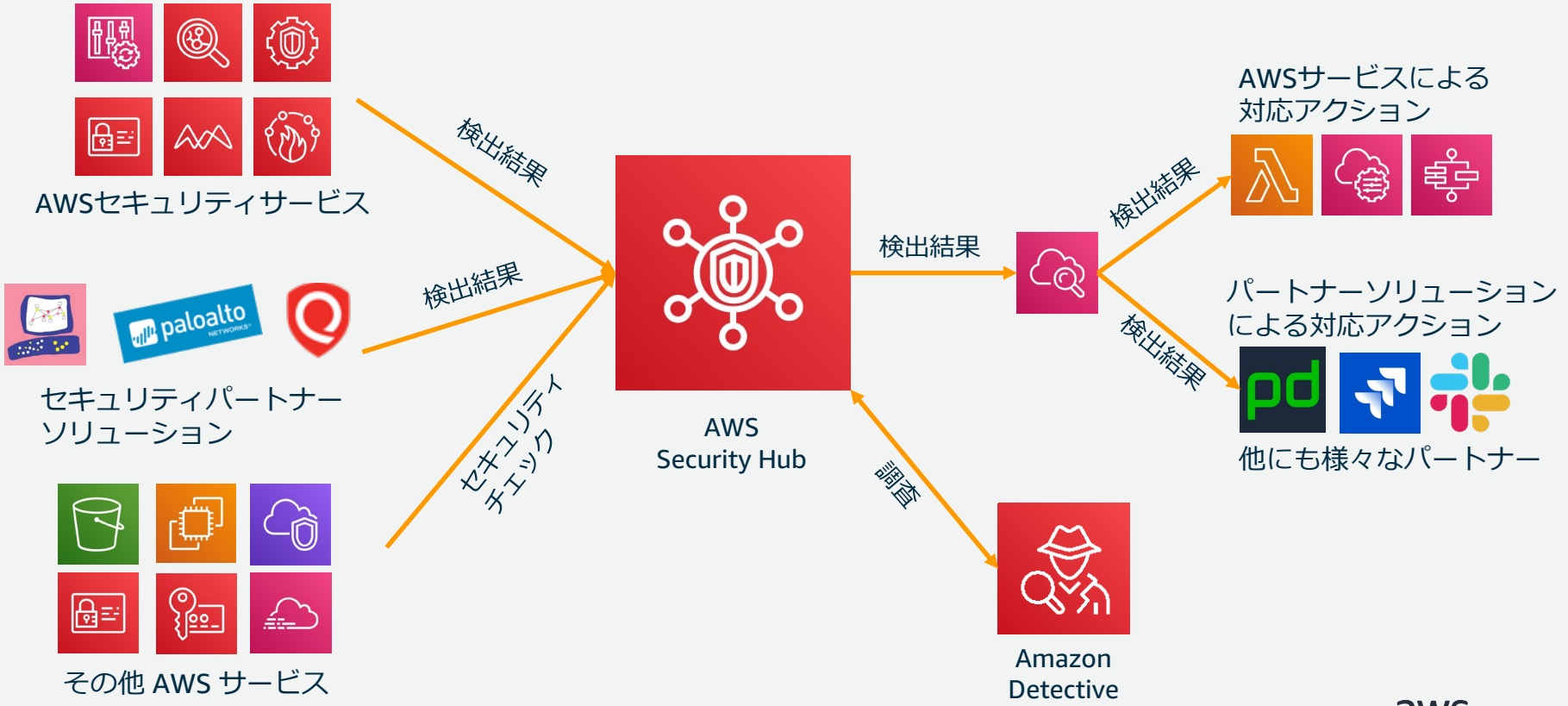
3. セキュリティ基準を有効化する

4. セキュリティ検出結果を取り扱う

5. 対応を自動化する

6. コスト管理をする

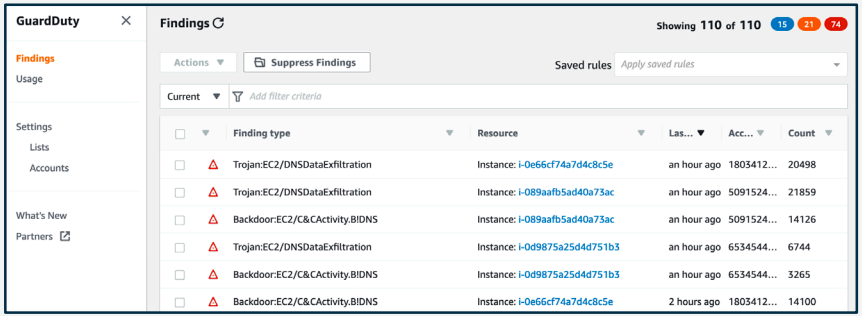
AWS Security Hub データの流れ



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 に送信し、一元的に可視化

Amazon GuardDuty
脅威検知に関する全ての検出結果

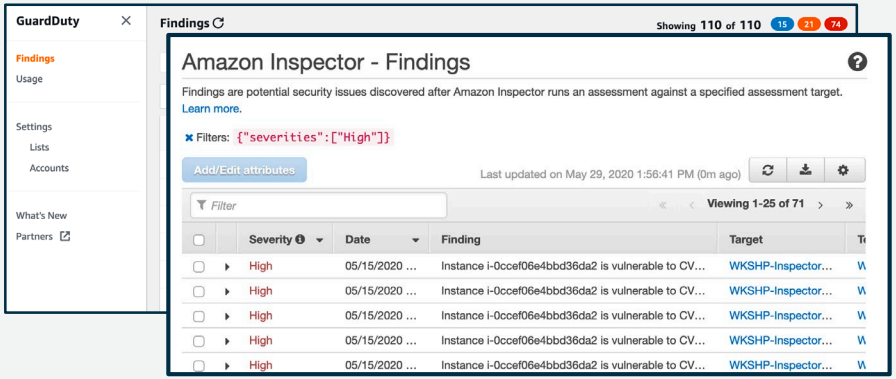


Available AWS service integrations
https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-internal-providers.html

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 に送信し、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

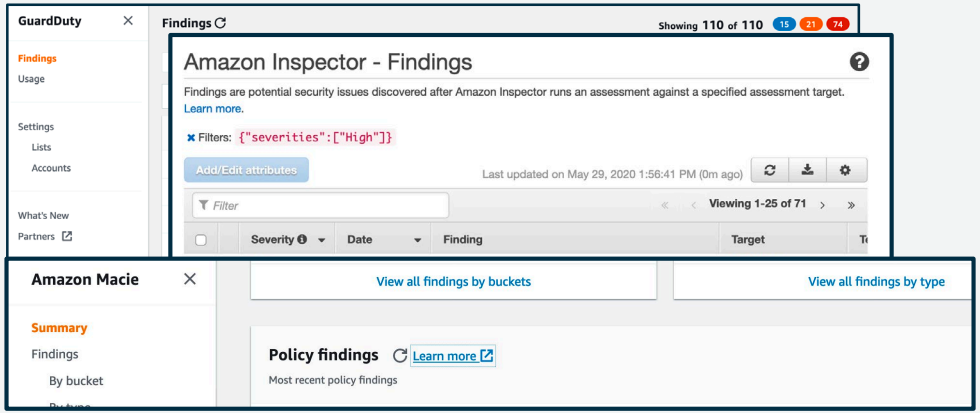


Available AWS service integrations
https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-internal-providers.html

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 に送信し、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



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

AWS セキュリティサービスとの統合

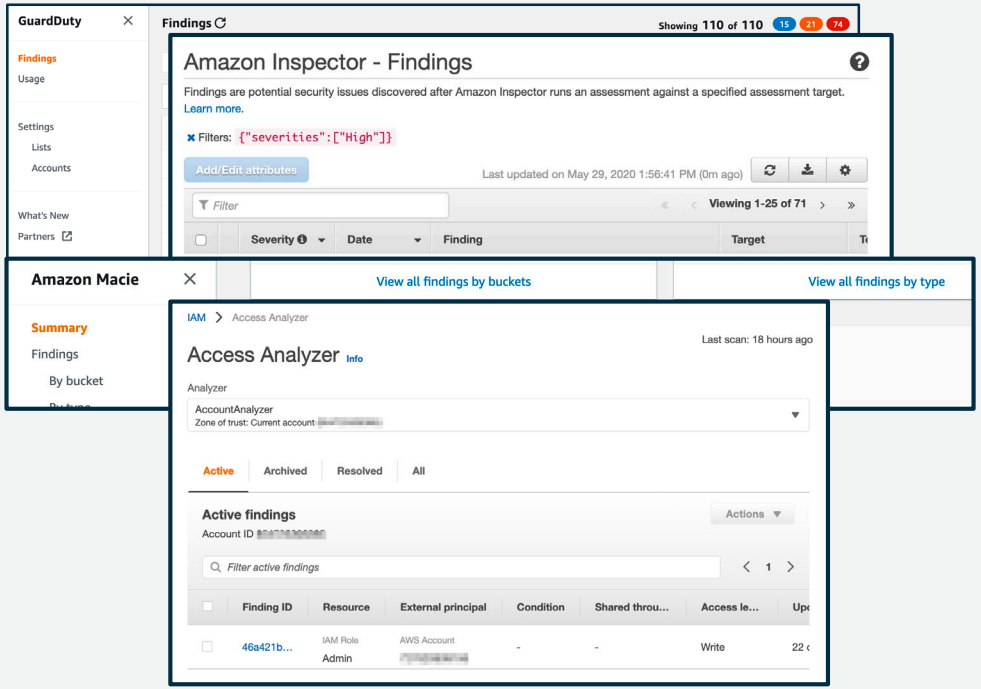
各サービスの検出結果を Security Hub に送信し、一元的に可視化

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



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

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 に送信し、一元的に可視化

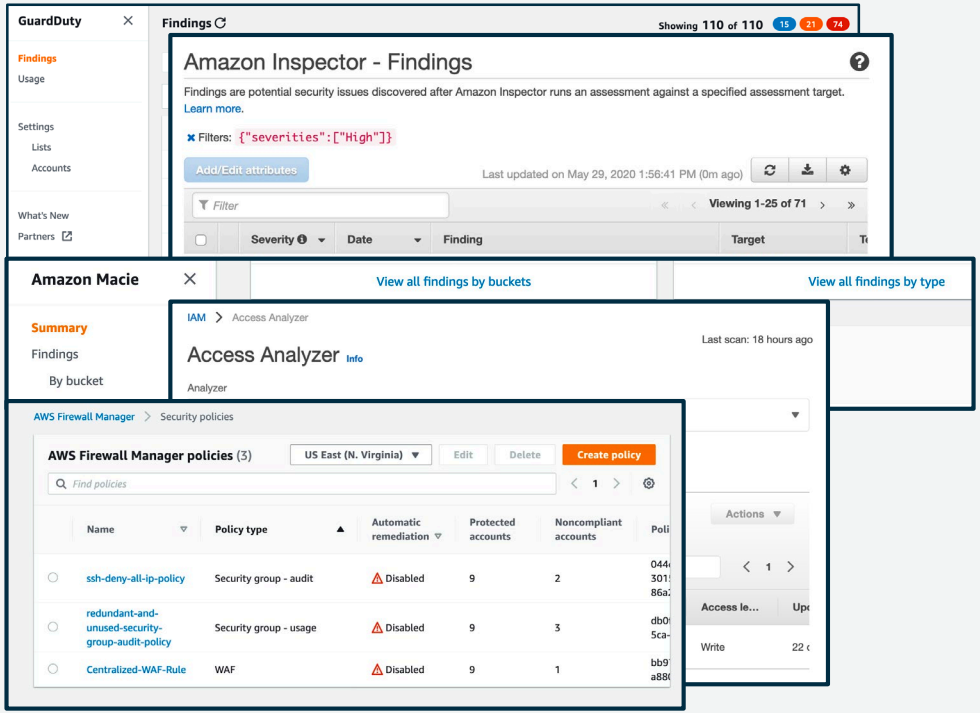
Amazon GuardDuty
脅威検知に関する全ての検出結果

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



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

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 に送信し、一元的に可視化

Amazon GuardDuty
脅威検知に関する全ての検出結果

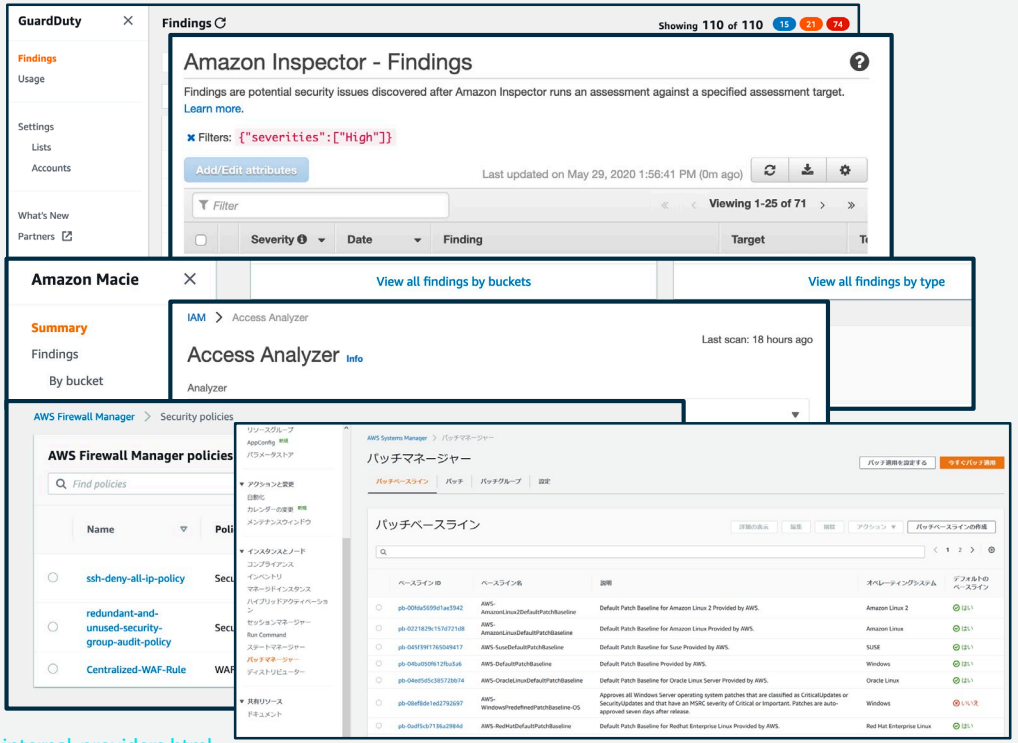
Amazon Inspector
セキュリティ評価による全ての検出結果

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

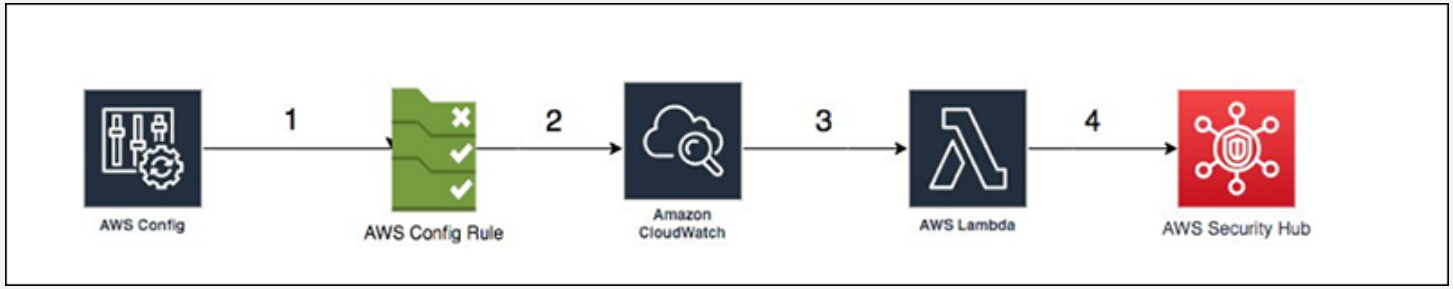
AWS Systems Manager Patch Manager
EC2インスタンスがパッチベースラインに基づくコンプライアンスルールに非準拠の時の検出結果



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

AWS Config カスタムルール検出結果の統合

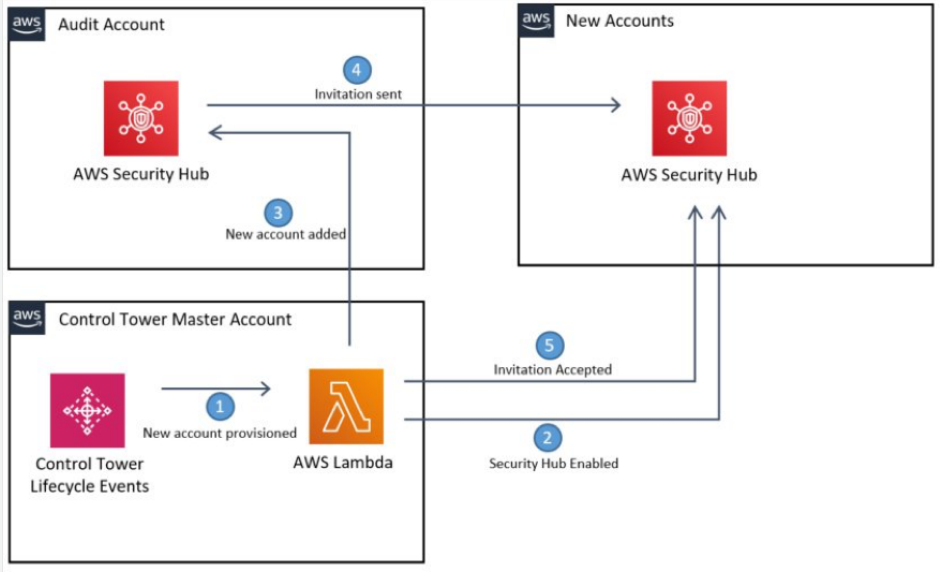
- カスタマイズされた Config ルールの結果を Security Hub の検出結果として統合することが可能
- 下記サンプルのAWS CloudFormationスタックをデプロイし、Config と Security Hub を統合するリソースを作成する



AWS Config ルールの評価結果を Security Hub にインポートする方法
https://aws.amazon.com/jp/blogs/news/how-to-import-aws-config-rules-evaluations-findings-security-hub/

AWS Control Tower ライフサイクルイベントによる AWS Security Hubの有効化

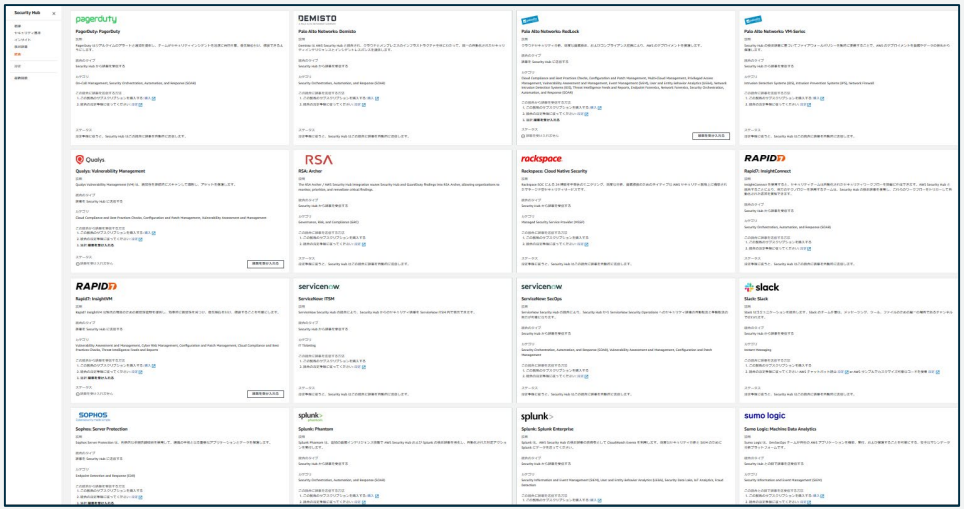
- Control Tower による AWS アカウント作成(プロビジョニング)のライフサイクルイベントをフック
- メンバーアカウントの Security Hub 自体とセキュリティ基準を有効化する
- Security Hub マスターアカウントとメンバーアカウントとの関連付けも自動で行う



Automating AWS Security Hub Alerts with AWS Control Tower lifecycle events
https://aws.amazon.com/jp/blogs/mt/automating-aws-security-hub-alerts-with-aws-control-tower-lifecycle-events/

既存のセキュリティパートナー製品の統合

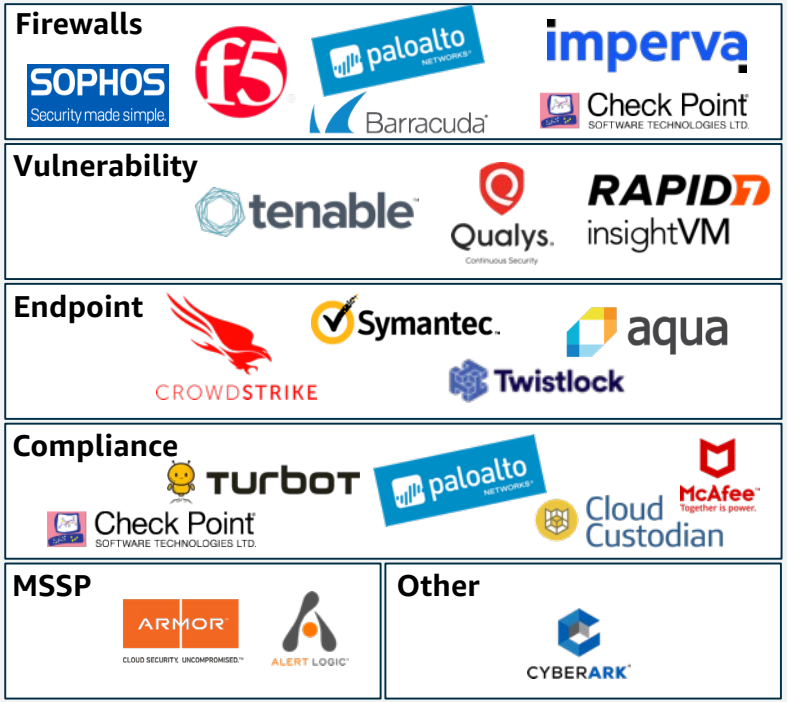
Security Hub との統合により各製品の検出結果フォーマットは AWS Security Finding Format (以下URL参照) に正規化され、管理画面上で一元的に可視化される



AWS Security Finding Format (ASFF)
https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-findings-format.html

セキュリティパートナー製品例

AWS Security Hub へ検出結果を送信



AWS Security Hub

Amazon CloudWatch Events

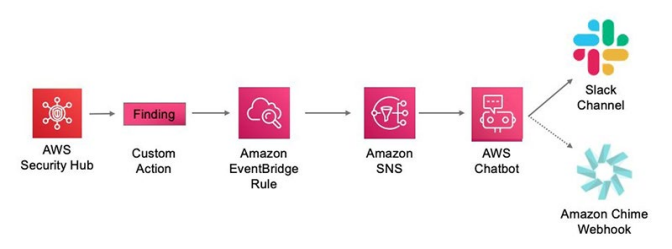
Event (event-based)

検出結果に基づいた対応アクション

aws

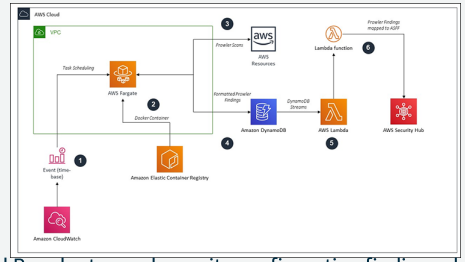
[参考] パートナー製品との統合例

Slack との統合例



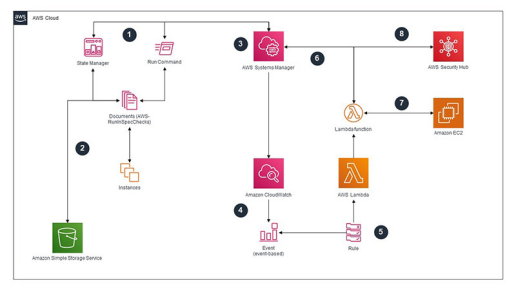
Enabling AWS Security Hub integration with AWS Chatbot
https://aws.amazon.com/blogs/security/enabling-aws-security-hub-integration-with-aws-chatbot/

Prowler との統合例



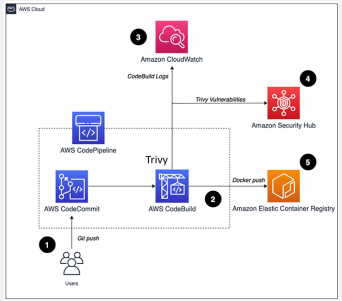
Use AWS Fargate and Prowler to send security configuration findings about AWS services to Security Hub https://aws.amazon.com/blogs/security/use-aws-fargate-prowler-send-security-configuration-findings-about-aws-services-security-hub/

Chef InSpec との統合例



Continuous compliance monitoring with Chef InSpec and AWS Security Hub
https://aws.amazon.com/blogs/security/continuous-compliance-monitoring-with-chef-inspec-and-aws-security-hub/

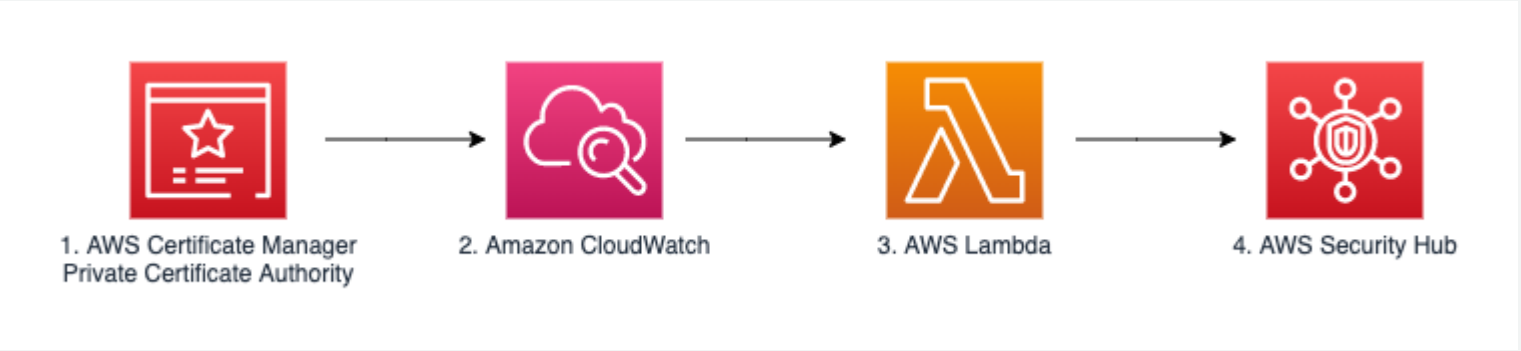
Trivy との統合例



How to build a CI/CD pipeline for container vulnerability scanning with Trivy and AWS Security Hub https://aws.amazon.com/blogs/security/how-to-build-ci-cd-pipeline-container-vulnerability-scanning-trivy-and-aws-security-hub/

AWS Certificate Manager Private CA の監視

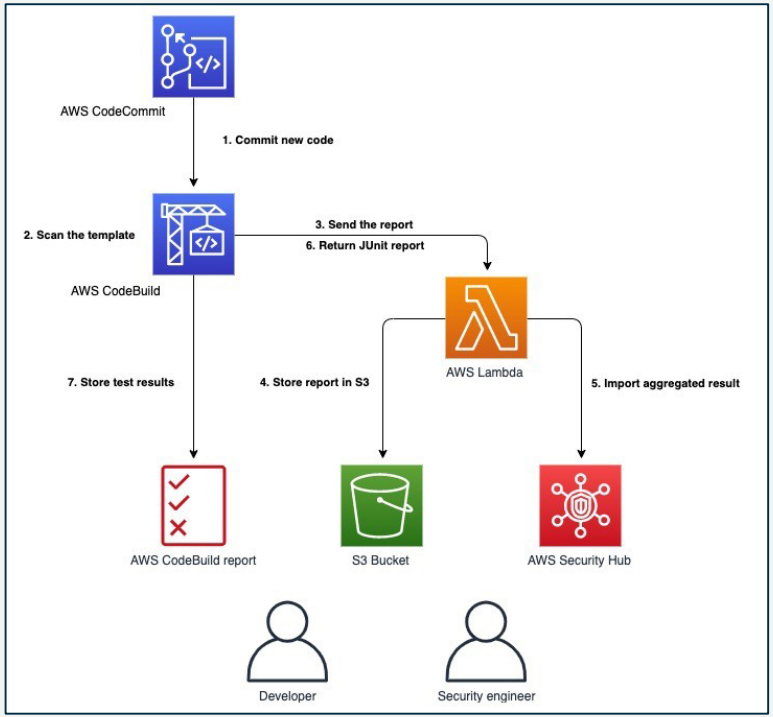
- Root CA が証明書発行する API コール監視
- CloudWatch Events により Lambda 関数を起動し、Amazon Security Finding Format (ASFF) に沿った Findings を生成する
- Security Hub に Findings を 送信し、Security Hub の一元的な View で対応



Monitoring AWS Certificate Manager Private CA with AWS Security Hub
https://aws.amazon.com/blogs/security/monitoring-aws-certificate-manager-private-ca-with-aws-security-hub/

AWS CloudFormation Guard による DevSecOps

- CodeCommit へのコードプッシュをきっかけに、セキュリティ評価プロセス開始
- CloudFormation Guard でテンプレートを評価し、結果レポートをLambdaに送信
- Lambda 関数内で 結果レポートをAmazon Security Finding Format (ASFF) に沿った Findings に変換
- Security Hub で一元的に可視化



Integrating AWS CloudFormation security tests with AWS Security Hub and AWS CodeBuild reports
https://aws.amazon.com/blogs/security/integrating-aws-cloudformation-security-tests-with-aws-security-hub-and-aws-codebuild-reports/

AWS Security Hub 利用の6つのステップ

1. AWS Security Hub をデプロイする
2. セキュリティツールと統合する
3. セキュリティ基準を有効化する
4. セキュリティ検出結果を取り扱う
5. 対応を自動化する
6. コスト管理をする

Security Hub セキュリティ基準の有効化

業界標準やベストプラクティスに基づいた自動コンプライアンスチェック

- AWS Foundational Security Best Practices v1.0.0
  - AWSセキュリティ専門家により定義された統制項目。セキュリティベストプラクティスに沿わないAWSアカウントやリソースを検知する
- CIS AWS Foundations Benchmark v1.2.0
  - Center for Internet Security が定義した要件の一部に対してチェックをする
- PCI DSS v3.2.1
  - クレジットカード情報を保存・処理・転送する組織が従うセキュリティ標準であるPCI DSS要件の一部に対してチェックする

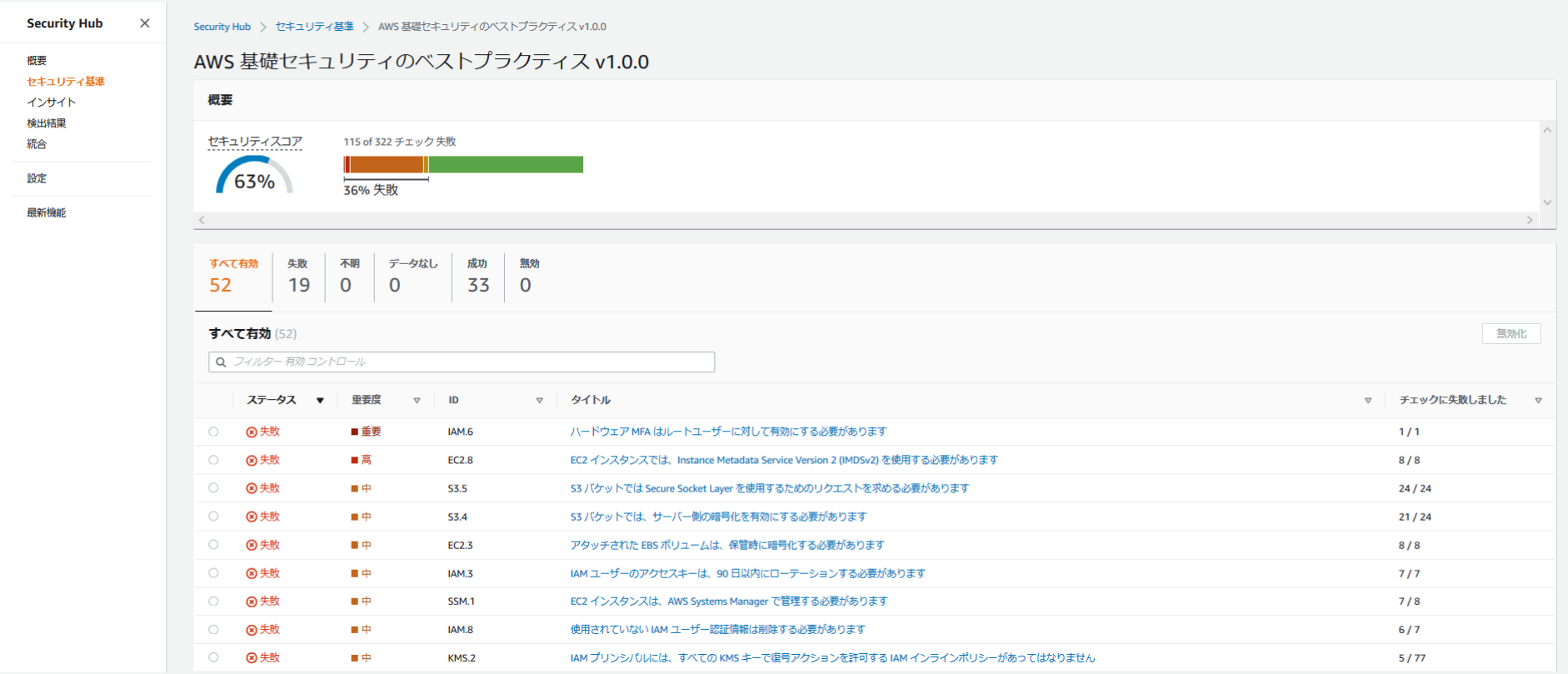
セキュリティ基準 デフォルト設定

Security Hubを有効化すると、
- AWS 基礎セキュリティのベストプラクティス
- CIS AWS Foundations Benchmark

がデフォルトで選択されている

PCI DSSが適用されるAWSアカウントにはPCI DSSの有効化が推奨

セキュリティ基準 画面例



新しいセキュリティ基準の有効化

Security Hub 管理画面の「セキュリティ基準」メニューにおいて、
新しいセキュリティ基準を有効化することが可能

AWS Security Hub 利用の6つのステップ

1. AWS Security Hub をデプロイする

2. セキュリティツールと統合する

3. セキュリティ基準を有効化する

4. セキュリティ検出結果を取り扱う

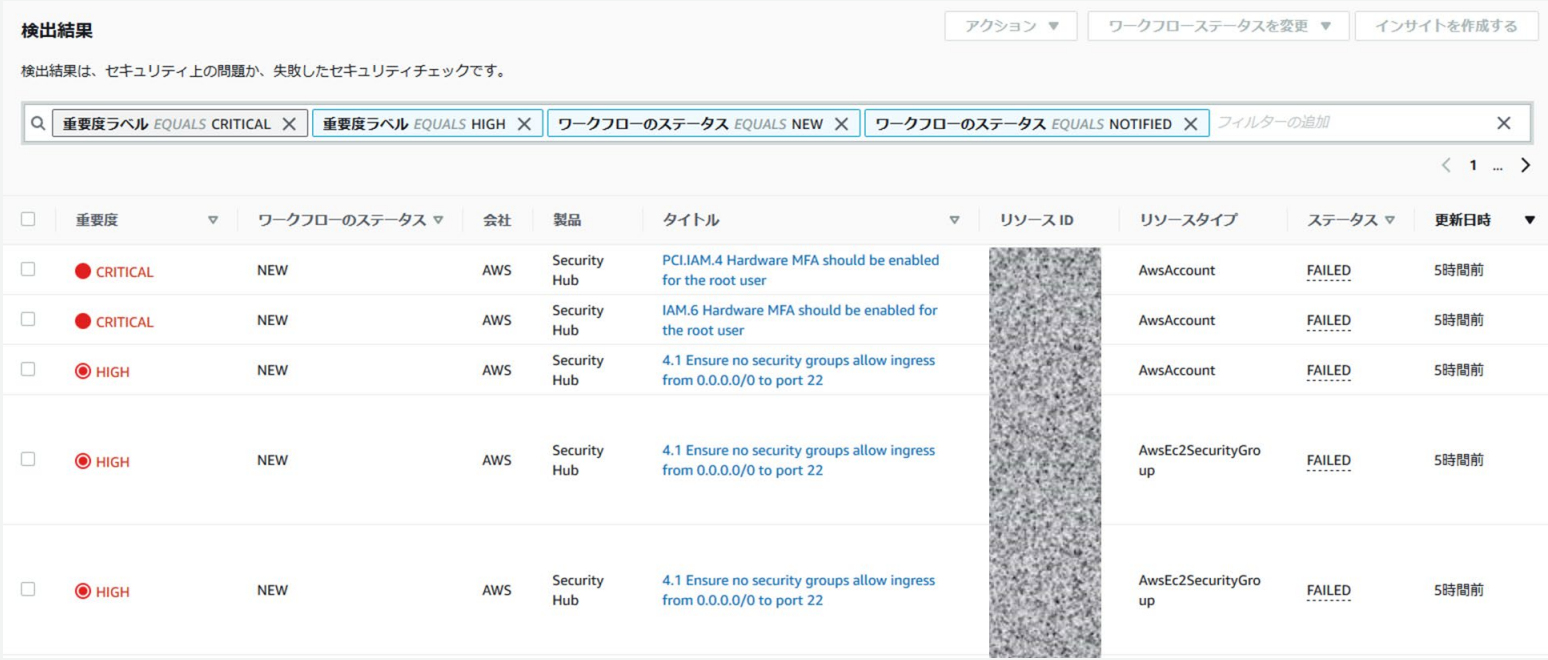
5. 対応を自動化する

6. コスト管理をする

対応すべき検出結果のフィルタリング

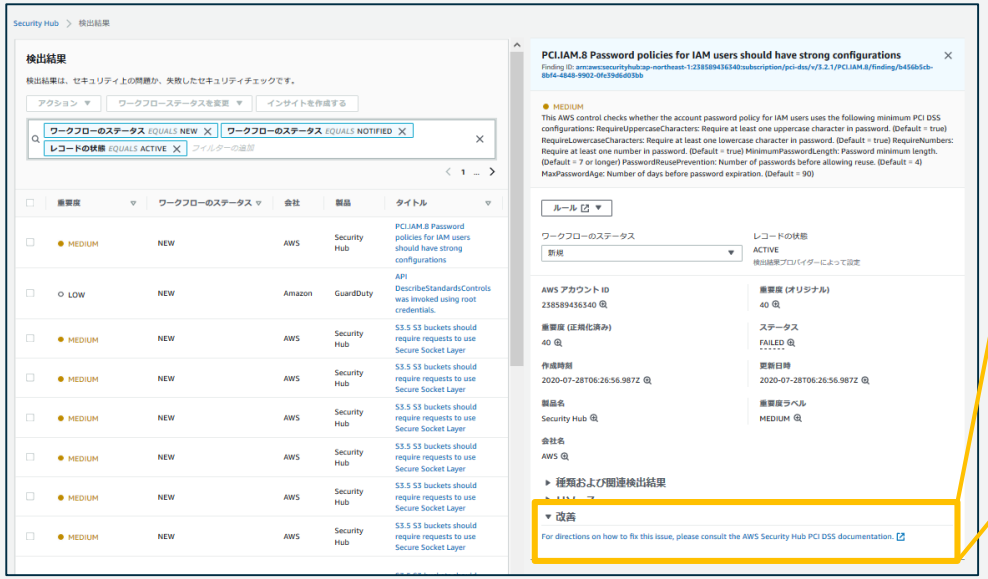
CRITICAL 及び HIGH の検出結果から優先的に対応する

”重要度ラベル”と”ワークフローのステータス”でフィルターする



改善アクションのガイダンス

セキュリティ基準に対する全ての検出結果は改善アクションのガイダンスが提供されている



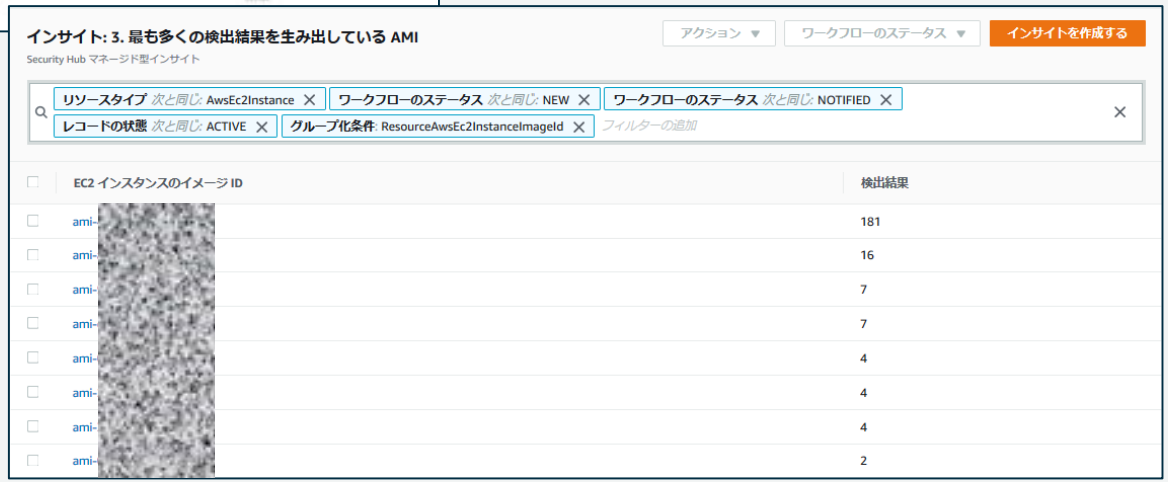
修復

ユーザーの MFA を設定するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. **[ユーザー]** を選択します。
3. MFA を設定するユーザーのユーザー名を選択します。
4. **[Security credentials (セキュリティ認証情報)]** を選択し、次に **[Assigned MFA device (割り当てられた MFA デバイス)]** の横にある **[管理]** を選択します。
5. **[Manage MFA Device (MFA デバイスの管理)]** ウィザードに従って、ご利用の環境に応じたデバイスのタイプを割り当てます。

ユーザーに MFA セットアップを委任する方法については、AWS セキュリティブログ記事の「AWS IAM ユーザーに多要素認証の管理を委任する方法」を参照してください。

“インサイト”による対応効率化



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

カスタマイズしたインサイトの作成

- インサイトは 「グループ化条件(Group By)」 フィルターによって生成される
- 注目したいインサイトをグループ化条件の前に追加する
  - 例: ステータス EQUALS FAILED
- 有用なインサイト例
  - リソースタイプ – AWS リソース毎に検出結果を集約
  - AWS アカウント ID – マルチアカウント環境においてAWSアカウント毎に検出結果を集約

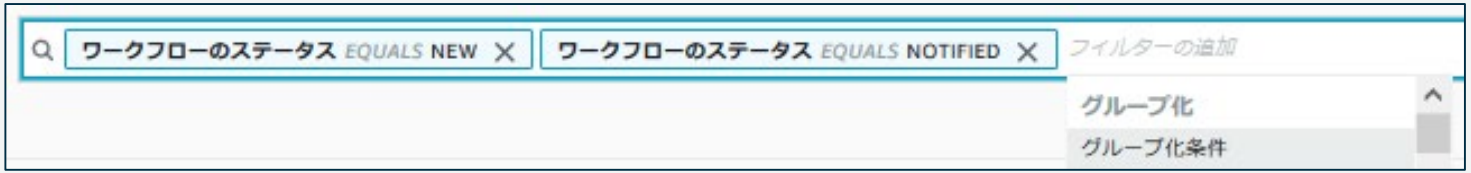
ワークフローステータス

ワークフローステータスにより検出結果の調査状況を追跡

ステータスの値

- 新規 (NEW)
- 通知済み (NOTIFIED)
- 抑制済み (SUPPRESSED)
- 解決済み (RESOLVED)

調査効率化のため、カスタムインサイト作成時のフィルターとして利用可能



BatchUpdateFindings API

API(や同等のCLI)から検出結果(Findings)の各フィールドを更新可

マスターアカウントはメンバーアカウントのアカウントの検出結果を更新可

使い方例：

- Workflowフィールド
  ワークフローステータスを一括更新
- Noteフィールド
  対応内容メモを記載する

```
PATCH /findings/batchupdate HTTP/1.1
Content-type: application/json

{
  "Confidence": number,
  "Criticality": number,
  "FindingIdentifiers": [
    {
      "Id": "string",
      "ProductArn": "string"
    }
  ],
  "Note": {
    "Text": "string",
    "UpdatedBy": "string"
  },
  "RelatedFindings": [
    {
      "Id": "string",
      "ProductArn": "string"
    }
  ],
  "Severity": {
    "Label": "string",
    "Normalized": number,
    "Product": number
  },
  "Types": [ "string" ],
  "UserDefinedFields": {
    "string" : "string"
  },
  "VerificationState": "string",
  "Workflow": {
    "Status": "string"
  }
}
```

[API Reference] BatchUpdateFindings
https://docs.aws.amazon.com/securityhub/1.0/APIReference/API_BatchUpdateFindings.html

aws

[参考] Amazon Detective

Security Hub と連携し、セキュリティ問題の根本原因の調査・特定を行うサービス

Amazon Detective では、潜在的なセキュリティ問題や不審なアクティビティの根本原因を簡単に分析、調査し、すばやく特定できます。Amazon Detective は、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、より迅速かつ効率的なセキュリティ調査を簡単に行えます。

Amazon GuardDuty、Amazon Macie、AWS Security Hub などの AWS セキュリティサービス、およびパートナーセキュリティ製品を使用して、潜在的なセキュリティの問題を特定したり、調査結果を取得したりできます。これらのサービスは、何か問題がある場合にアラートを受け取り、修正箇所を指摘してもらうのにとても便利です。けれども、セキュリティに関する調査結果を受け取って、さらに深く掘り下げてより多くの情報を分析することで、根本原因を特定して対処する必要がある場合もあるかもしれません。セキュリティの発見の根本原因を特定することは、多くの場合、多くの個別のデータソースからログを収集して結合することを伴う複雑なプロセスになる可能性があります。その際、抽出、変換、および読み込み (ETL) ツールまたはカスタムスクリプトを使用してデータを整理してから、セキュリティアナリストがデータを分析して長時間の調査を行う必要があります。

Amazon Detective は、セキュリティチームが簡単に調査し、発見の根本原因にすばやく到達できるようにすることで、このプロセスを簡素化します。Amazon Detective は、Virtual Private Cloud (VPC) Flow Logs、AWS CloudTrail、Amazon GuardDuty などの複数のデータソースから数兆個のイベントを分析し、リソース、ユーザー、およびそれらの間の経時的な相互作用の統一されたインタラクティブなビューを自動的に生成できます。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 か所で視覚化して、調査結果の根本的な理由を特定し、関連する履歴アクティビティにドリルダウンして、根本原因を迅速に特定できます。

AWS Security Hub 利用の6つのステップ

1. AWS Security Hub をデプロイする

2. セキュリティツールと統合する

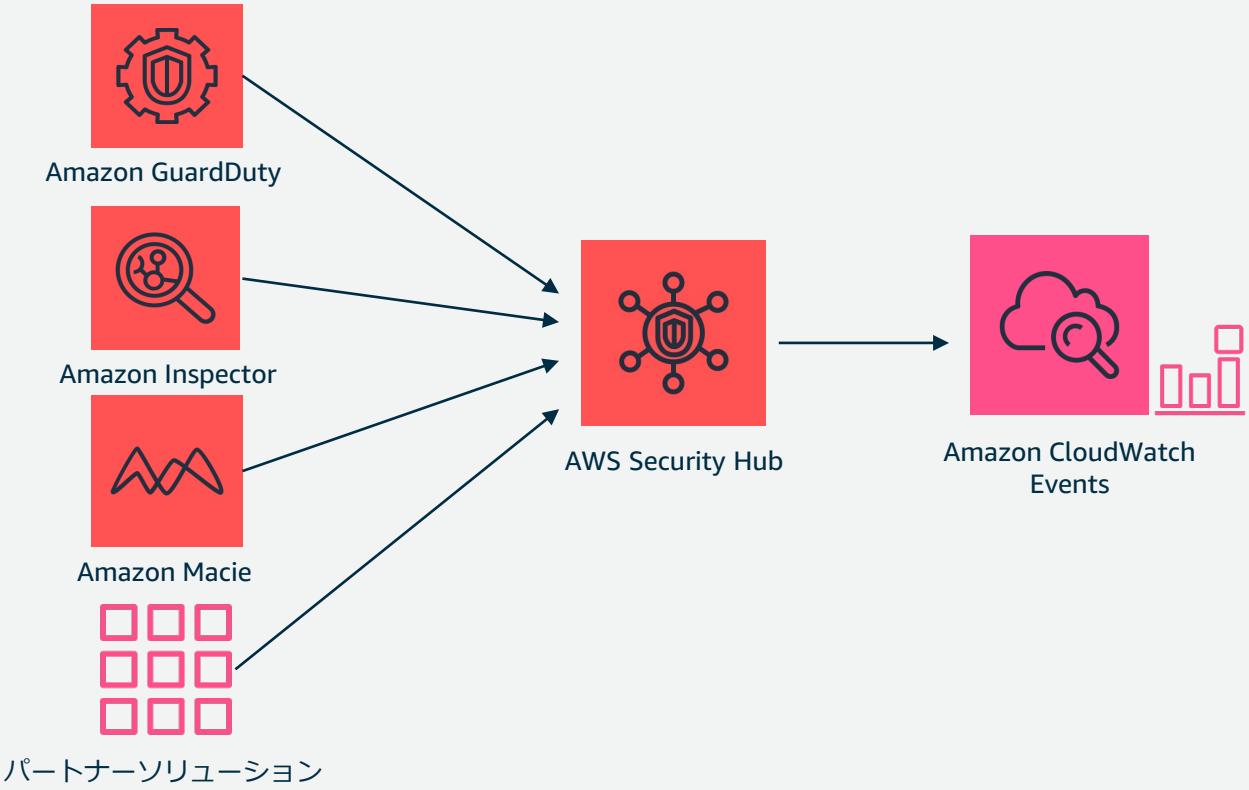
3. セキュリティ基準を有効化する

4. セキュリティ検出結果を取り扱う

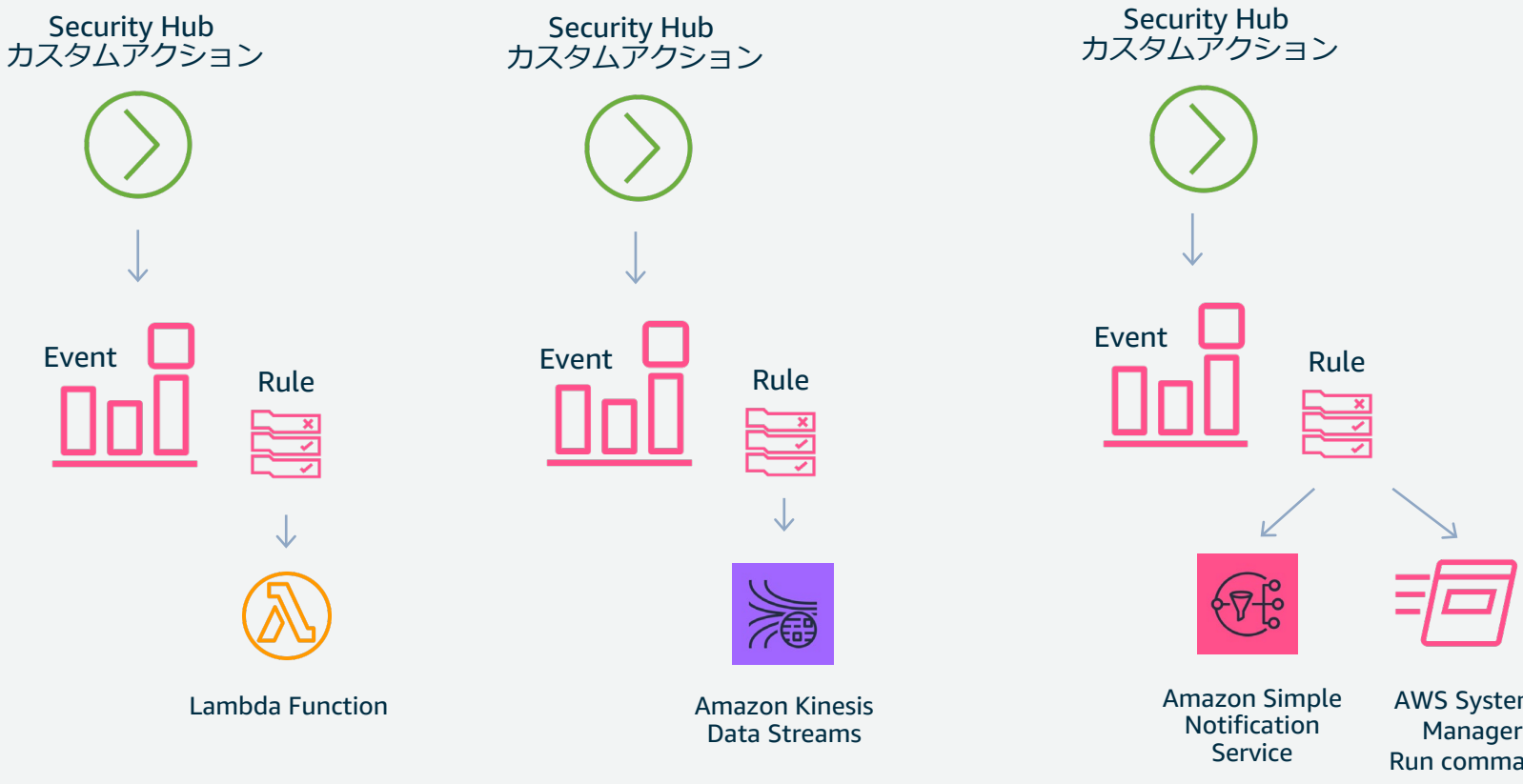
5. 対応を自動化する

6. コスト管理をする

検出結果に基づいた対応



カスタムアクションによる自動化の開始



Security Hub カスタムアクション作成1

Security Hub カスタムアクション画面

ここではメール通知用のカスタムアクションを想定

CloudWatch イベントによる AWS Security Hub の自動化
https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-cloudwatch-events.html

Security Hub カスタムアクション作成 2

CloudWatch Events ルール作成画面

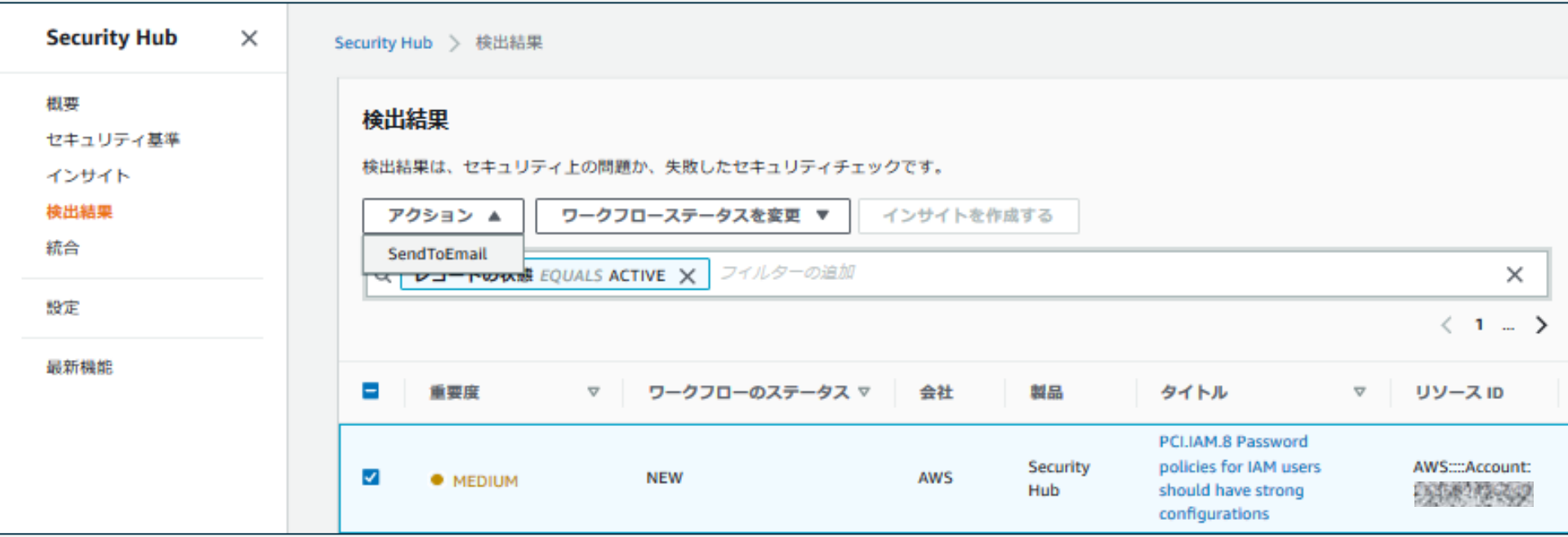
Security Hub カスタムアクションARNを指定

ここでは管理者メールアドレスに
通知するトピックが定義されている想定

CloudWatch イベント による AWS Security Hub の自動化
https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-cloudwatch-events.html

Security Hub カスタムアクション作成３

Security Hub 検出結果 アクション選択画面

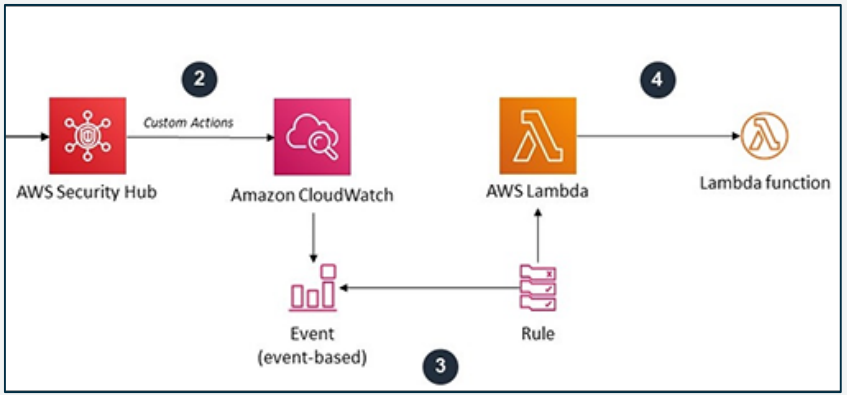


CloudWatch イベントによる AWS Security Hub の自動化
https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-cloudwatch-events.html

[参考] サンプルカスタムアクション

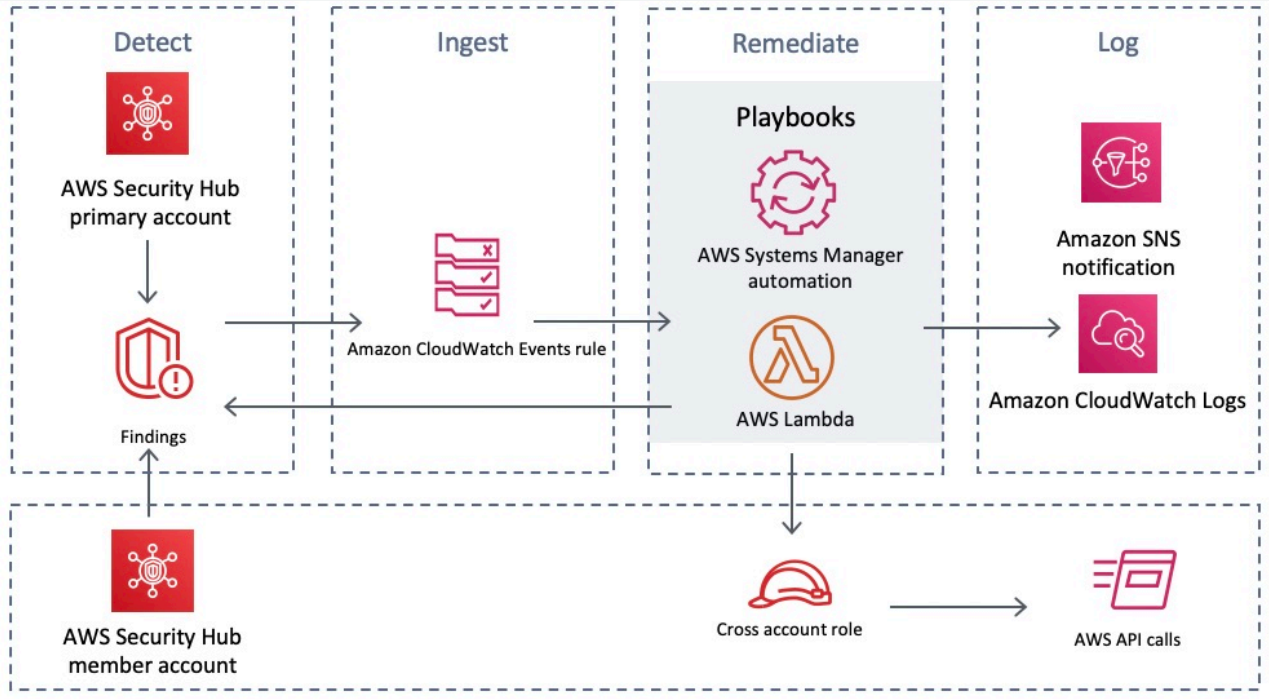
CIS AWS Foundations Benchmark

1.3 – “Ensure credentials unused for 90 days or greater are disabled”
1.4 – “Ensure access keys are rotated every 90 days or less”
1.5 – “Ensure IAM password policy requires at least one uppercase letter”
1.6 – “Ensure IAM password policy requires at least one lowercase letter”
1.7 – “Ensure IAM password policy requires at least one symbol”
1.8 – “Ensure IAM password policy requires at least one number”
1.9 – “Ensure IAM password policy requires a minimum length of 14 or greater”
1.10 – “Ensure IAM password policy prevents password reuse”
1.11 – “Ensure IAM password policy expires passwords within 90 days or less”
2.2 – “Ensure CloudTrail log file validation is enabled”
2.3 – “Ensure the S3 bucket CloudTrail logs to is not publicly accessible”
2.4 – “Ensure CloudTrail trails are integrated with Amazon CloudWatch Logs”*
2.6 – “Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket”*
2.7 – “Ensure CloudTrail logs are encrypted at rest using AWS KMS CMKs”
2.8 – “Ensure rotation for customer created CMKs is enabled”
2.9 – “Ensure VPC flow logging is enabled in all VPCs”*
4.1 – “Ensure no security groups allow ingress from 0.0.0.0/0 to port 22”
4.2 – “Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389”
4.3 – “Ensure the default security group of every VPC restricts all traffic”



AWS Security Hubによる自動対応と修復
https://aws.amazon.com/jp/blogs/news/automated-response-and-remediation-with-aws-security-hub/

自動対応と修正ソリューション

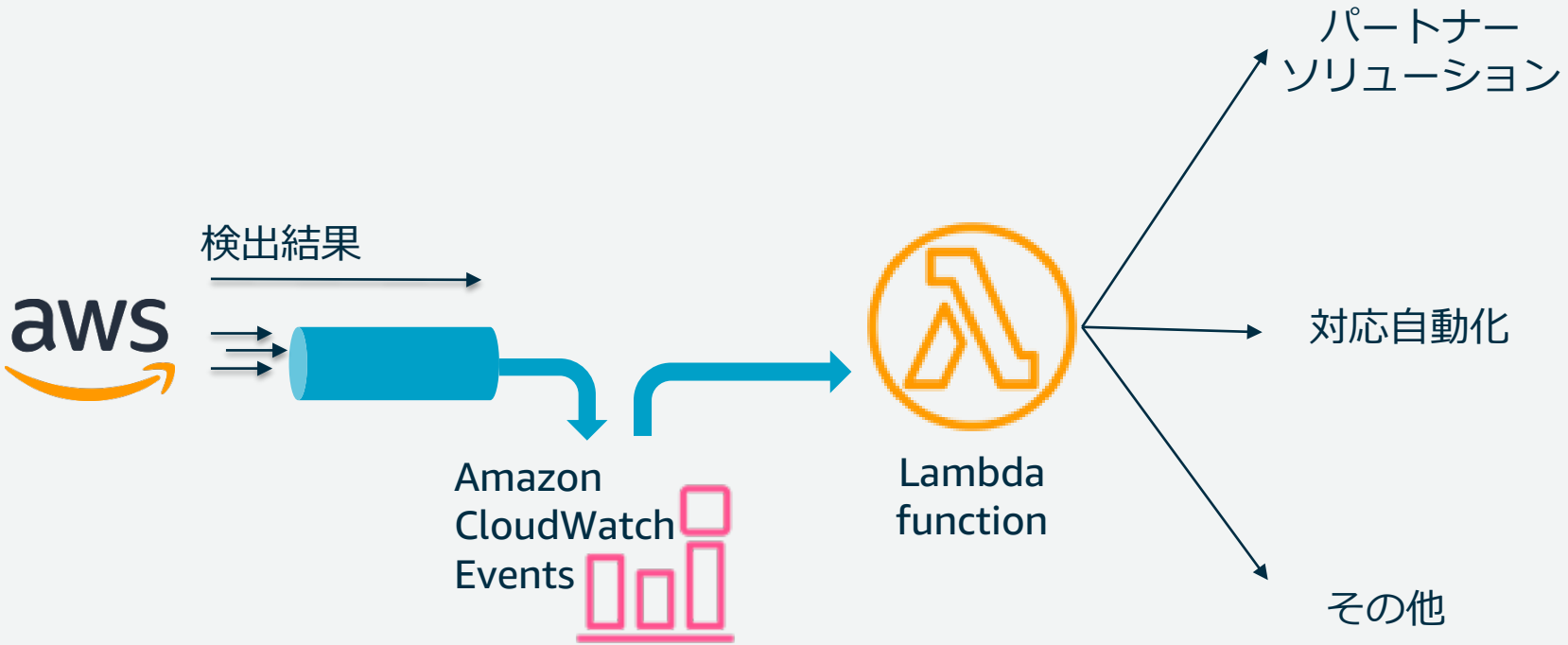


以下の典型的な使い方を示すテンプレートを提供するソリューション(下URL参照)

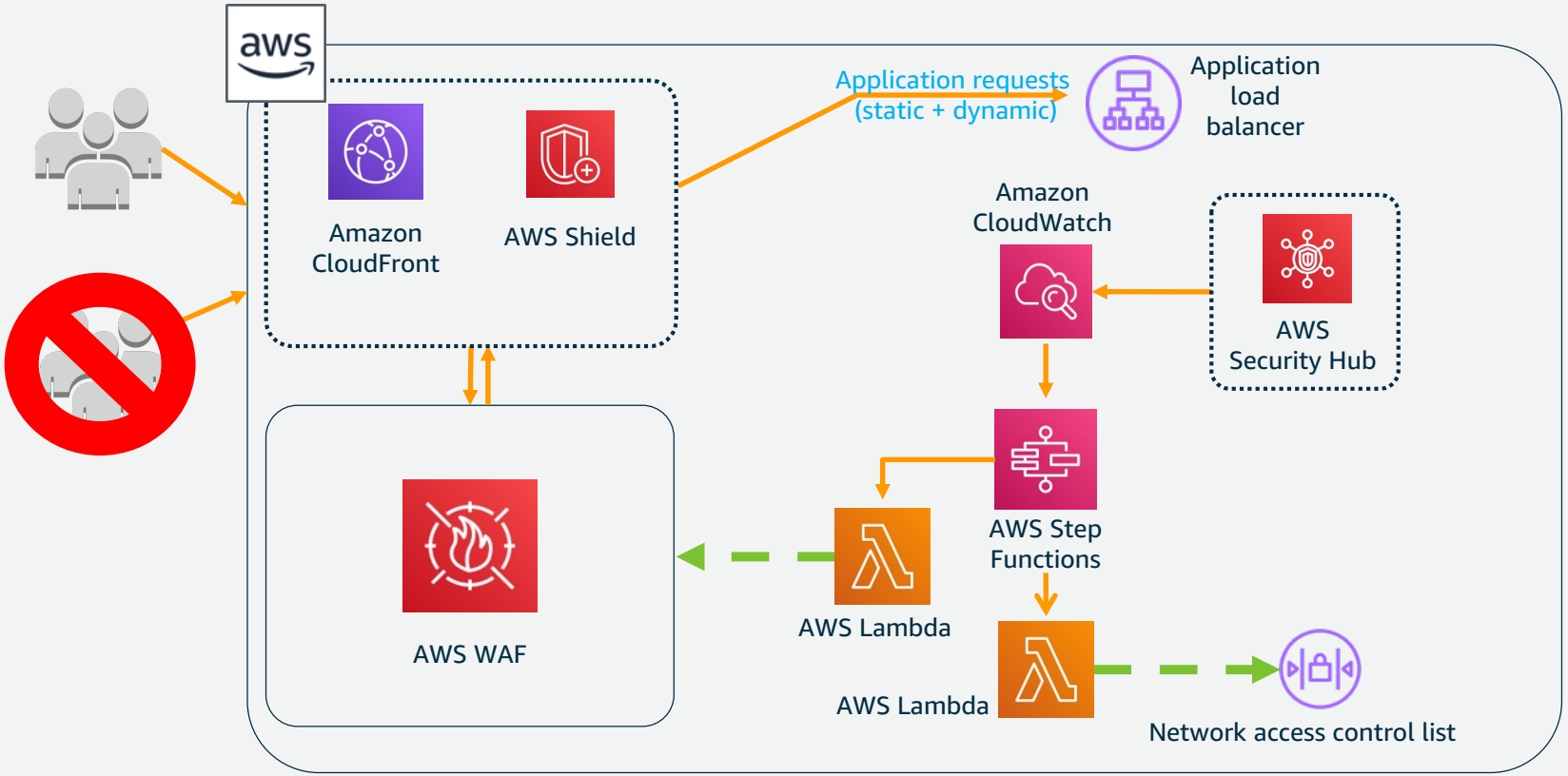
- セキュリティイベント検出
- 結果の取り込み
- 自動修正
- 対応の記録

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

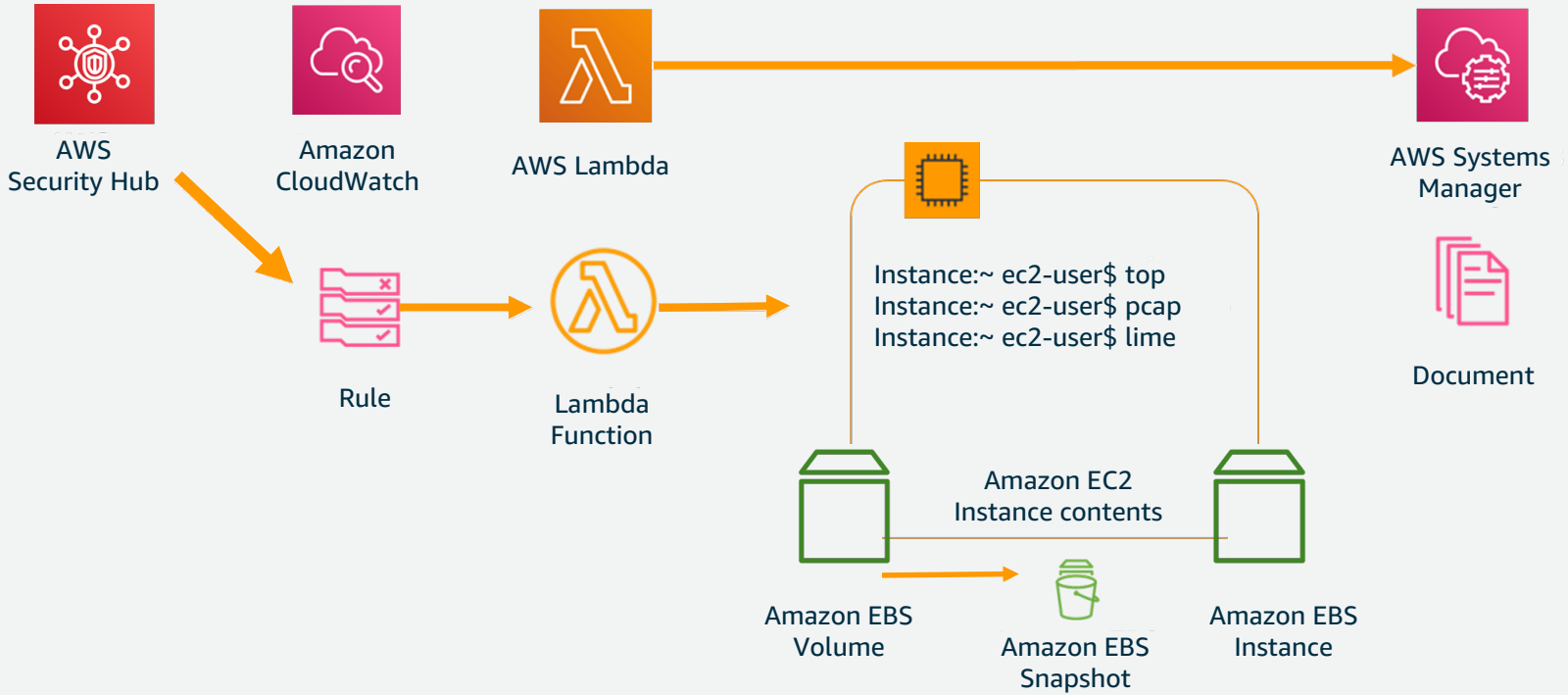
インシデントレスポンスの自動化



Network ACL+AWS WAF によるリソース保護



Systems Manager によるデータ収集



AWS Security Hub 利用の6つのステップ

1. AWS Security Hub をデプロイする

2. セキュリティツールと統合する

3. セキュリティ基準を有効化する

4. セキュリティ検出結果を取り扱う

5. 対応を自動化する

6. コスト管理をする

無料期間を用いたコスト試算

- 全てのリージョン、全てのアカウントに対して30日間の無料期間あり
- Security Hub 管理画面 > 設定 > 使用 から予測コストを確認

セキュリティチェック対象の選別

有効化されたセキュリティ基準のうち、個別のセキュリティチェックを無効化することが可能(コスト最適化)

[CIS.1.16] IAM ポリシーがグループまたはロールだけにアタッチされていることを確認する

[CIS.1.22] 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

▶ Config によるグローバルリソースの記録をしていないリージョンで無効化

[CIS.2.3] CloudTrail ログを保存するために使用される S3 バケットが一般にアクセス可能ではないことを確認する

[CIS.2.6] CloudTrail S3 バケットで S3 バケットアクセスログが有効であることを確認する

▶ CloudTrail ログ保存用 S3 バケットが無いリージョンやアカウントで無効化

aws

まとめ

AWS Security Hub 利用のベストプラクティス

- 全リージョン、全アカウントでSecurity Hub, Configを有効化する
- セキュリティマスターアカウントを指定する

- GuardDuty, Inspector, Macie, IAM Access Analyzer, Firewall Manager, Systems Manager などのAWSサービスを統合する
- パートナーソリューションを統合する

- 「AWS 基礎セキュリティのベストプラクティス」や「CIS AWS Foundations Benchmark」などのセキュリティ基準を有効化する

- 高い重要度の検出結果を優先し、改善ガイダンスに従って対応する
- カスタムインサイトやワークフローステータスを使い、調査を効率化する

- カスタムアクションを定義し、対応を自動化する

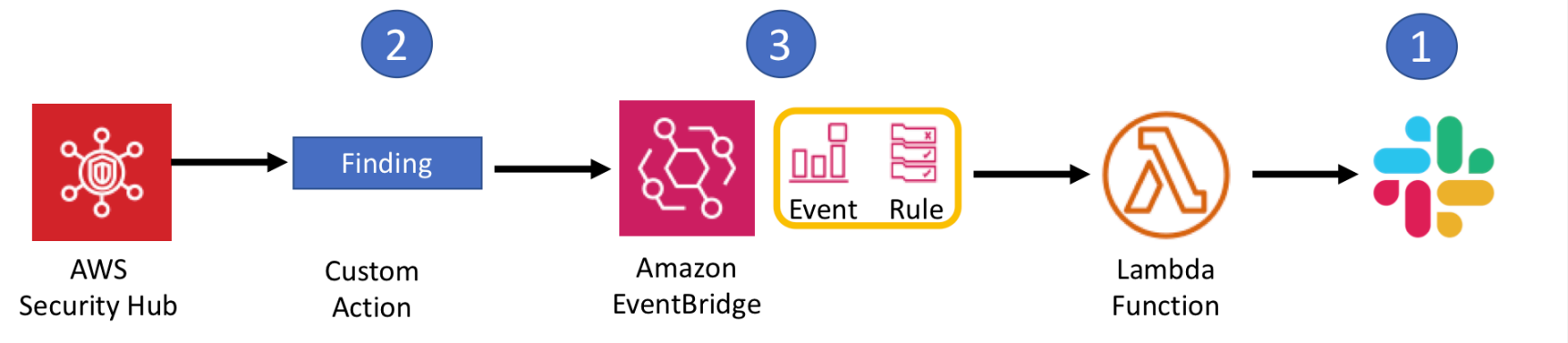
- 無料期間を利用してコスト試算する
- セキュリティチェック項目を選別し、コスト最適化する

aws

[参考] AWS Security Hub ワークショップ

- レベル：中級
- 想定時間：2-3時間
- 事前準備：AWSアカウント、IAM管理ユーザー

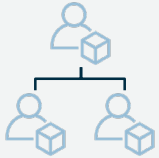
統合された各種サービスからSecurity Hubに送られてくるFindingsに対して、カスタムインサイト/カスタムアクションなど用いて対応するサンプル(下URL参照)



[Workshop] Integration, Prioritization, and Response with AWS Security Hub
https://security-hub-workshop.awssecworkshops.com/

まとめ

1. 組織のセキュリティとコンプライアンスの課題に対応するためには、以下を継続的・自動的に行う



組織全体の監視

データ集約と
セキュリティ評価

検出結果の優先順位付け

効果的な対応

2. 以下のベストプラクティスのポイントを参考に、AWS Security Hub を効果的に活用する

1. デプロイ	2. ツール統合	3. セキュリティ基準	4. 検出結果	5. 対応自動化	6. コスト管理

Q&A

お答えできなかったご質問については
AWS Japan Blog 「https://aws.amazon.com/jp/blogs/news/」にて
後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に対策などを相談することも可能
- 申込みはイベント告知サイトから

(https://aws.amazon.com/jp/about-aws/events/)

AWS イベント で[検索]

ご視聴ありがとうございました

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive