



[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>



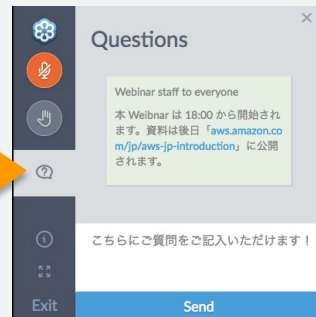
AWS Black Belt Online Seminar とは

「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

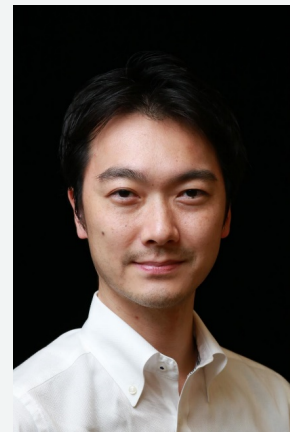
- 本資料では2020年10月13日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっております。日本居住者のお客様には別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available 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



Account 1
Account 2
Account 3

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

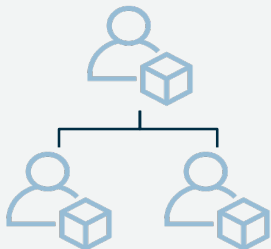


検出結果に基づいて
効果的なアクション
を行う

セキュリティ課題にまつわる可視性の向上

コンプライアンス遵守状態のより簡単な維持

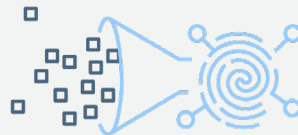
組織に求められるセキュリティ



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

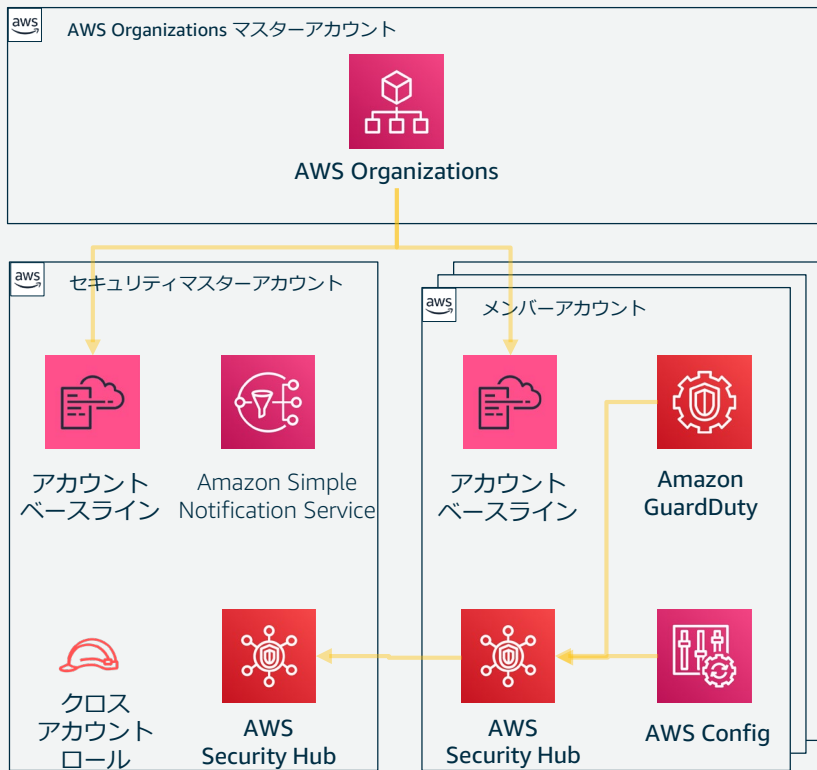
3. セキュリティ基準を
有効化する

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

Security Hub ×

概要
セキュリティ基準
インサイト
検出結果
統合
設定
最新機能

Security Hub > 設定

設定

アカウント | カスタムアクション | 使用 | 一般

メンバーアカウントの追加

このページを使用して、メンバーのアカウントを Security Hub に追加します。詳細はこちら

アカウントの入力

アカウントの追加 | リスト (.csv) のアップロード

アカウント ID

アカウント ID (12 桁) を入力します

E メールアドレス

アカウントの連絡先の E メール

追加するアカウント

アカウント ID



E メール



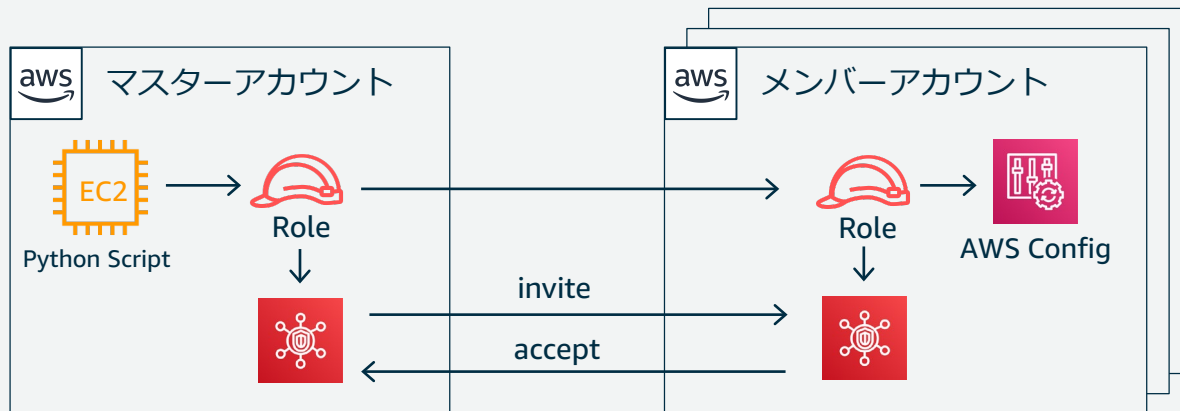
アカウントが追加されていません。

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
```



[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

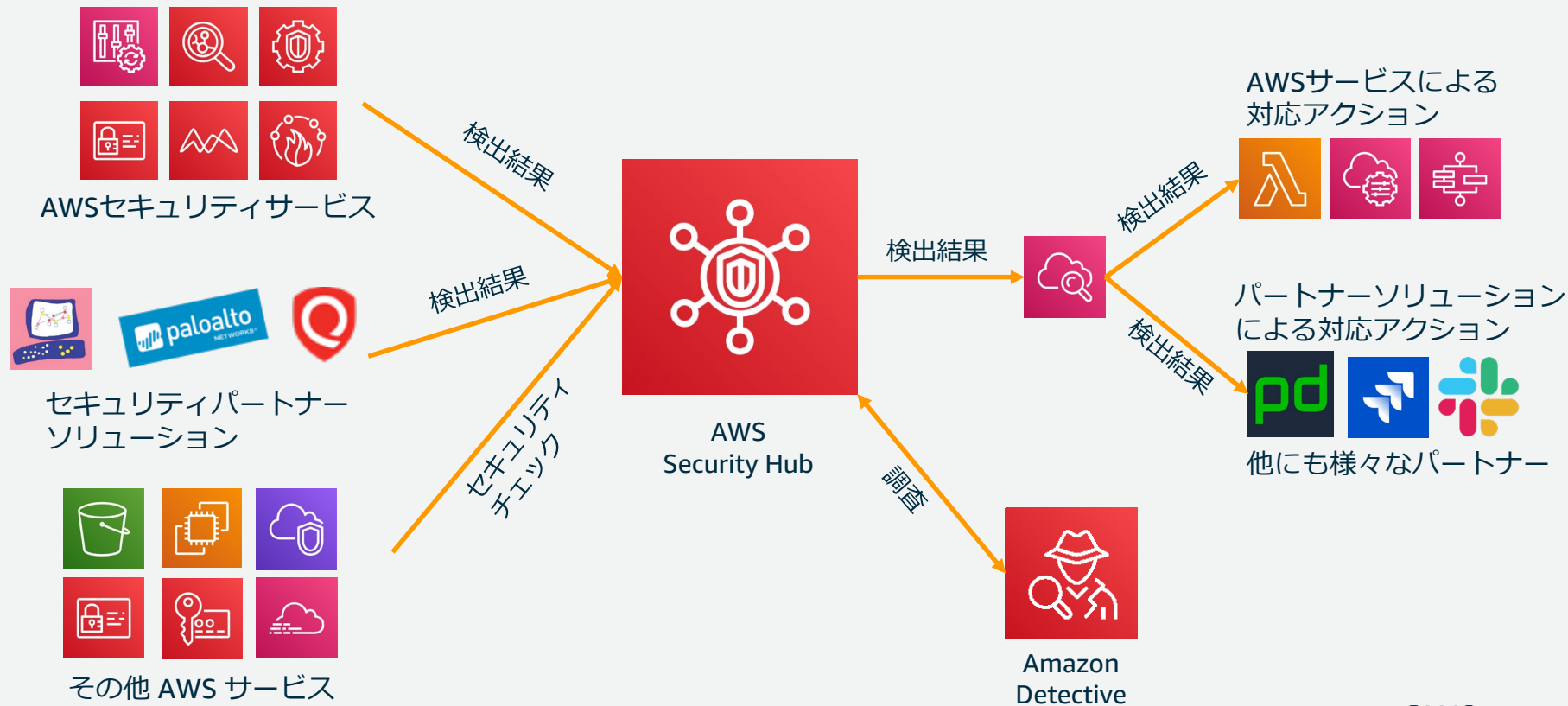
3. セキュリティ基準を
有効化する

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

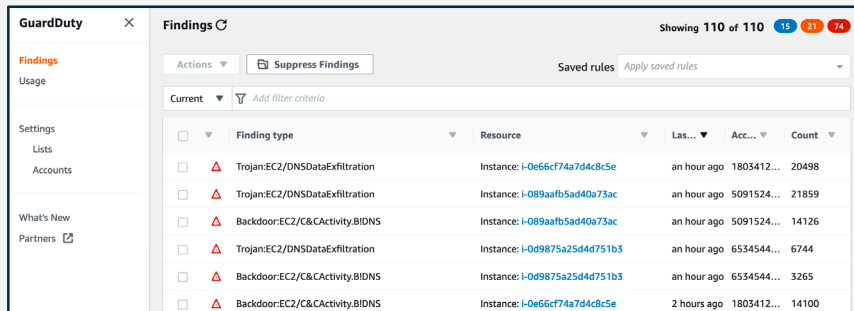


AWS セキュリティサービスとの統合

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



The screenshot shows the Amazon GuardDuty console interface. The main area displays a list of findings with columns for Finding type, Resource, Last updated, Accuracy, and Count. The findings listed are:

Finding type	Resource	Last updated	Accuracy	Count
Trojan:EC2/DNSDataExfiltration	Instance: i-0e66cf74a7d4c8c5e	an hour ago	1803412...	20498
Trojan:EC2/DNSDataExfiltration	Instance: i-089aafb5ad40a73ac	an hour ago	5091524...	21859
Backdoor:EC2/C&CActivity,BIDNS	Instance: i-089aafb5ad40a73ac	an hour ago	5091524...	14126
Trojan:EC2/DNSDataExfiltration	Instance: i-0d9875a25d4d751b3	an hour ago	6534544...	6744
Backdoor:EC2/C&CActivity,BIDNS	Instance: i-0d9875a25d4d751b3	an hour ago	6534544...	3265
Backdoor:EC2/C&CActivity,BIDNS	Instance: i-0e66cf74a7d4c8c5e	2 hours ago	1803412...	14100

Available AWS service integrations

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

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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

The screenshot displays the AWS Security Hub console interface. On the left, a sidebar menu includes 'GuardDuty', 'Findings', 'Usage', 'Settings', 'Lists', 'Accounts', 'What's New', and 'Partners'. The main content area is titled 'Findings' and shows a list of findings from Amazon Inspector. The findings are filtered by severity to 'High'. The table below shows the details of these findings.

Severity	Date	Finding	Target
High	05/15/2020 ...	Instance i-0ccef06e4bbd36da2 is vulnerable to CV...	WKSHP-Inspector...
High	05/15/2020 ...	Instance i-0ccef06e4bbd36da2 is vulnerable to CV...	WKSHP-Inspector...
High	05/15/2020 ...	Instance i-0ccef06e4bbd36da2 is vulnerable to CV...	WKSHP-Inspector...
High	05/15/2020 ...	Instance i-0ccef06e4bbd36da2 is vulnerable to CV...	WKSHP-Inspector...
High	05/15/2020 ...	Instance i-0ccef06e4bbd36da2 is vulnerable to CV...	WKSHP-Inspector...

Available AWS service integrations

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

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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

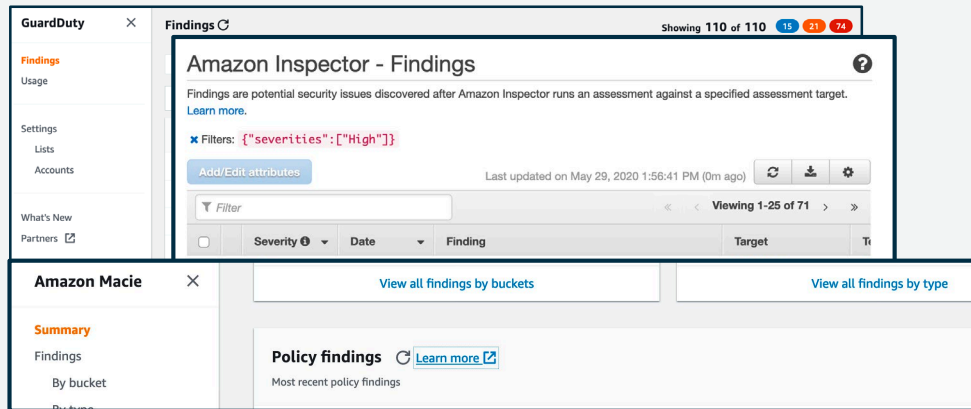
脅威検知に関する全ての検出結果

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>

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



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

The screenshot displays the AWS Security Hub console interface. At the top, a 'Findings C' header indicates 'Showing 110 of 110' findings, with 15 high, 21 medium, and 74 low severity findings. The main content area is divided into three overlapping panels:

- Amazon Inspector - Findings:** Shows a list of findings with filters for severity (set to 'High'). A table header includes columns for Severity, Date, Finding, and Target.
- Amazon Macie:** Displays 'View all findings by buckets' and 'View all findings by type' options.
- Access Analyzer:** Shows details for an 'Active finding' from the 'AccountAnalyzer' zone of trust. It includes a table of active findings with columns: Finding ID, Resource, External principal, Condition, Shared through..., Access le..., and Upd.

Finding ID	Resource	External principal	Condition	Shared through...	Access le...	Upd
46a421b...	IAM Role Admin	AWS Account	-	-	Write	22 c

Available AWS service integrations

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

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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

The screenshot displays the AWS Security Hub console interface. It features a sidebar with navigation options like 'Findings', 'Settings', 'Lists', and 'Accounts'. The main content area shows a list of findings, with a detailed view for 'Amazon Inspector - Findings' and 'Access Analyzer' findings. The 'Access Analyzer' section includes a table of security policies.

Name	Policy type	Automatic remediation	Protected accounts	Noncompliant accounts	Pol...
ssh-deny-all-ip-policy	Security group - audit	⚠ Disabled	9	2	044:301:86a:
redundant-and-unused-security-group-audit-policy	Security group - usage	⚠ Disabled	9	3	db0:5ca-
Centralized-WAF-Rule	WAF	⚠ Disabled	9	1	bb9:a88

Available AWS service integrations

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

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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

The screenshot displays the AWS Security Hub console interface, showing a list of findings from various AWS services. The findings are categorized by severity and type, and are displayed in a table format. The table includes columns for the finding ID, the service name, the finding title, the severity level, and the target resource. The findings are sorted by severity, with high severity findings appearing first.

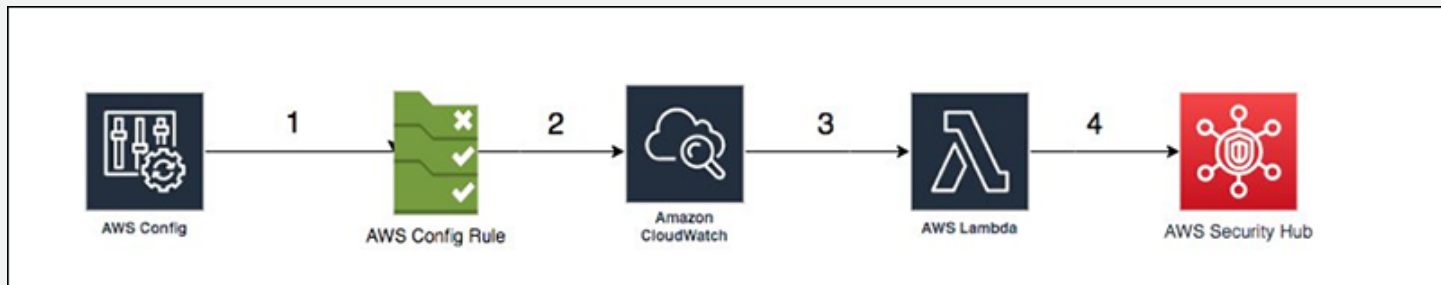
Severity	Date	Finding	Target
High	May 29, 2020 1:56:41 PM (0m ago)	Amazon Inspector - Findings	
High		Access Analyzer	
High		AWS Firewall Manager	
High		AWS Systems Manager Patch Manager	

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

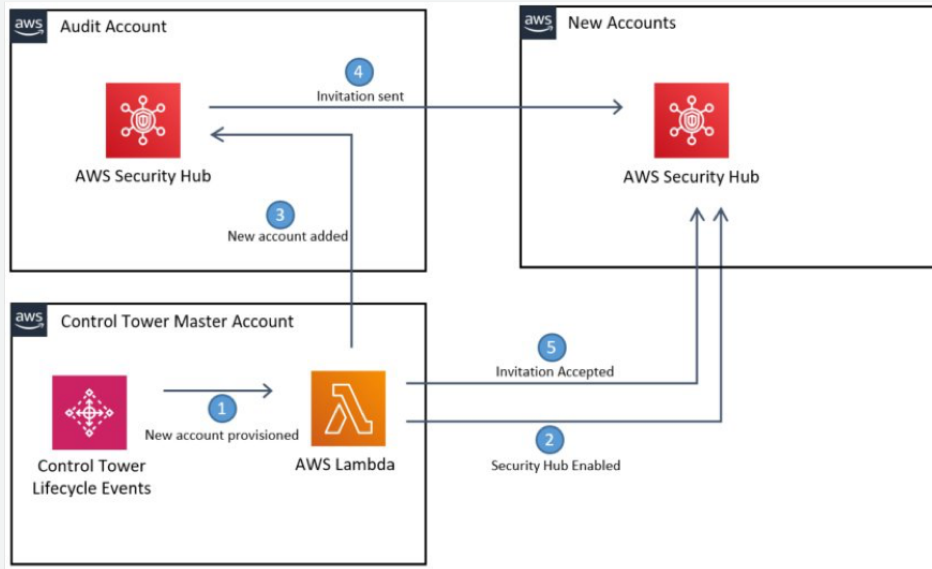


AWS Config ルールの評価結果を Security Hub にインポートする方法
<https://aws.amazon.com/jp/blogs/news/how-to-import-aws-config-rules-evaluations-findings-security-hub/>

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

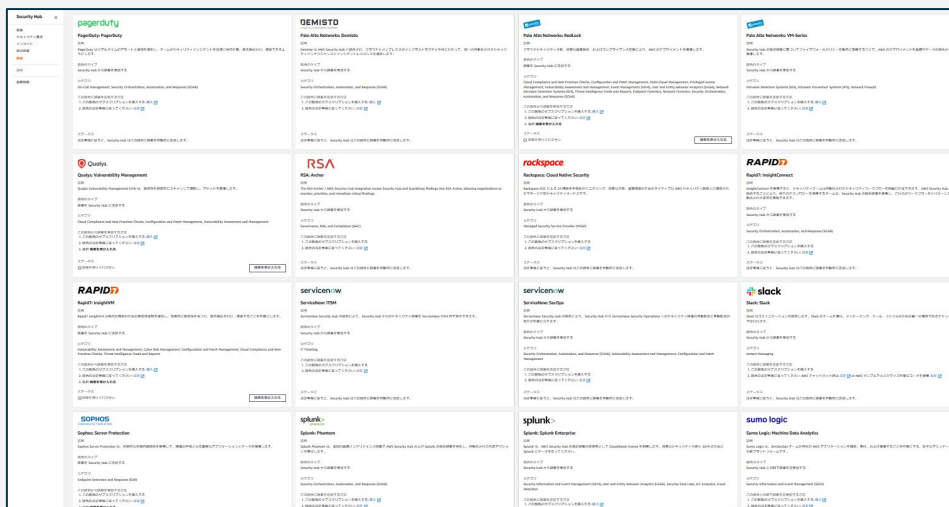
AWS Control Tower ライフサイクルイベントによる AWS Security Hubの有効化

- 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



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



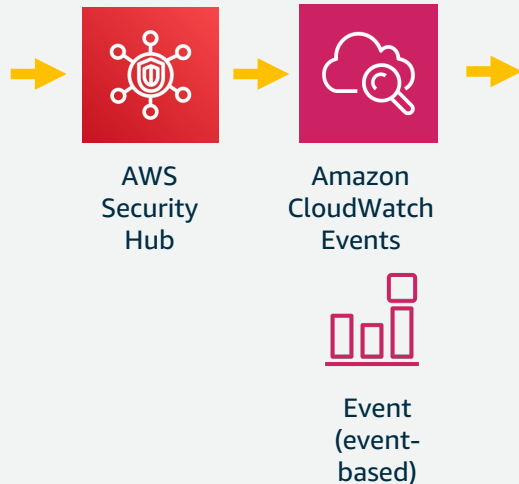
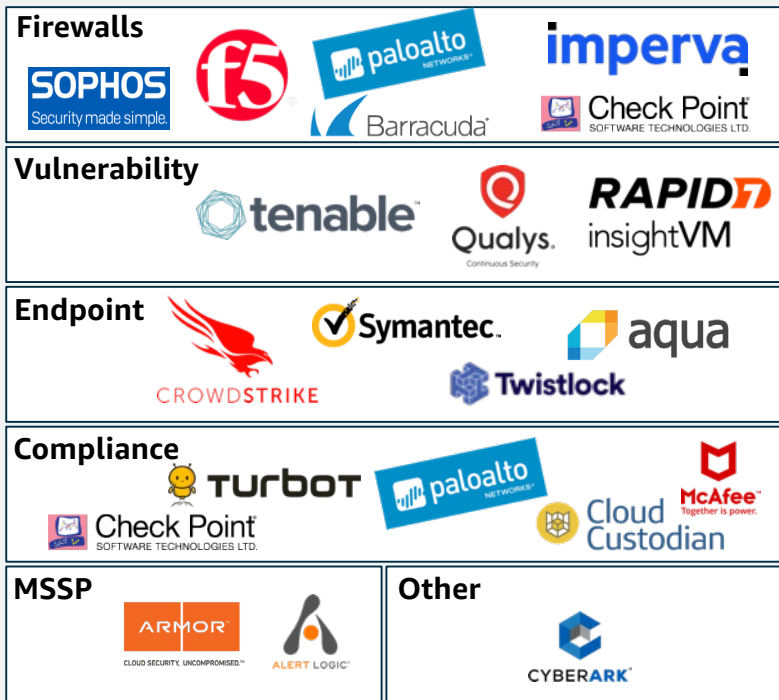
AWS Security Finding Format (ASFF)

<https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-findings-format.html>

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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

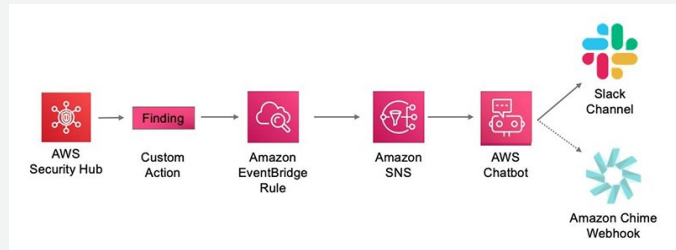


検出結果に基づいた対応アクション



[参考] パートナー製品との統合例

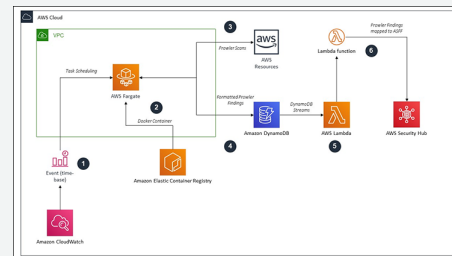
Slack との統合例



Enabling AWS Security Hub integration with AWS Chatbot

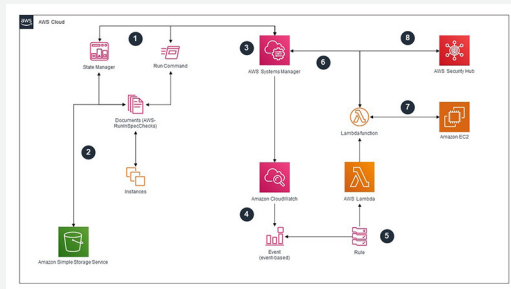
<https://aws.amazon.com/blogs/security/enabling-aws-security-hub-integration-with-aws-chatbot/>

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/>

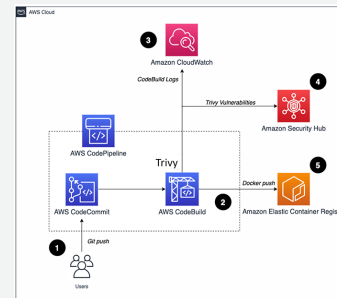
Chef InSpec との統合例



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/>

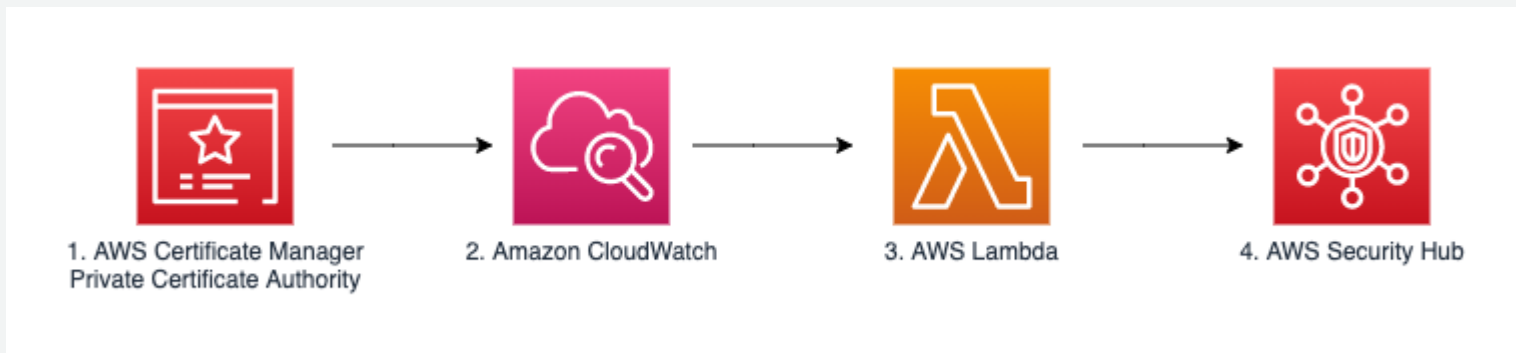
Trivy との統合例



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/>

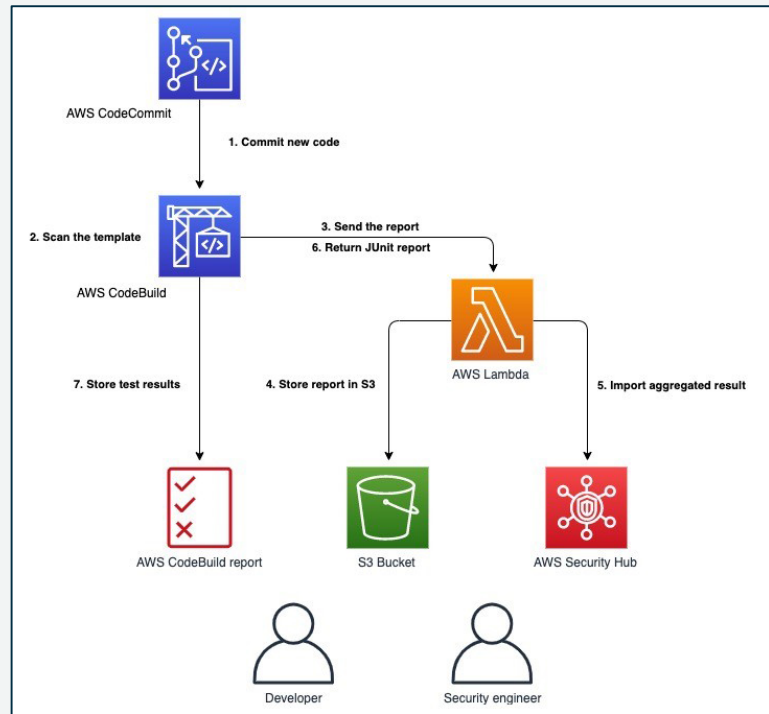
AWS Certificate Manager Private CA の監視

- 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



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/>

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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 > AWS Security Hub へようこそ

AWS Security Hub へようこそ

セキュリティ基準

AWS Security Hub を有効にすると、セキュリティチェックを実行する権限が付与されます。サービスにリンクされたロール (SLR) 以下のサービスがセキュリティチェックを実行するために使用されます: Amazon CloudWatch、Amazon SNS、AWS Config、AWS CloudTrail。

- AWS 基礎セキュリティのベストプラクティス v1.0.0 を有効化
- CIS AWS Foundations Benchmark v1.2.0 を有効化
- PCI DSS v3.2.1 を有効化

AWS 統合

Security Hub を有効にすると、以下から結果をインポートするアクセス許可が付与されます。

- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- AWS IAM アクセスアナライザー
- AWS Firewall Manager

キャンセル

Security Hub の有効化

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

Security Hub ×

概要

セキュリティ基準

インサイト

検出結果

統合

設定

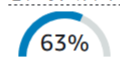
最新機能

Security Hub > 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

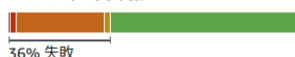
AWS 基礎セキュリティのベストプラクティス v1.0.0

概要

セキュリティスコア



115 of 322 チェック 失敗



すべて有効	失敗	不明	データなし	成功	無効
52	19	0	0	33	0

すべて有効 (52)

無効化

	ステータス ▼	重要度 ▼	ID ▼	タイトル ▼	チェックに失敗しました ▼
<input type="radio"/>	⊗ 失敗	■ 重要	IAM.6	ハードウェア MFA はルートユーザーに対して有効にする必要があります	1 / 1
<input type="radio"/>	⊗ 失敗	■ 高	EC2.8	EC2 インスタンスでは、Instance Metadata Service Version 2 (IMDSv2) を使用する必要があります	8 / 8
<input type="radio"/>	⊗ 失敗	■ 中	S3.5	S3 バケットでは Secure Socket Layer を使用するためのリクエストを求める必要があります	24 / 24
<input type="radio"/>	⊗ 失敗	■ 中	S3.4	S3 バケットでは、サーバー側の暗号化を有効にする必要があります	21 / 24
<input type="radio"/>	⊗ 失敗	■ 中	EC2.3	アタッチされた EBS ボリュームは、保管時に暗号化する必要があります	8 / 8
<input type="radio"/>	⊗ 失敗	■ 中	IAM.3	IAM ユーザーのアクセスキーは、90 日以内にローテーションする必要があります	7 / 7
<input type="radio"/>	⊗ 失敗	■ 中	SSM.1	EC2 インスタンスは、AWS Systems Manager で管理する必要があります	7 / 8
<input type="radio"/>	⊗ 失敗	■ 中	IAM.8	使用されていない IAM ユーザー認証情報は削除する必要があります	6 / 7
<input type="radio"/>	⊗ 失敗	■ 中	KMS.2	IAM プリンシパルには、すべての KMS キーで復号アクションを許可する IAM インラインポリシーがあってはなりません	5 / 77

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

The screenshot displays the AWS Security Hub interface. On the left, the 'Security Hub' sidebar is visible with the 'セキュリティ基準' (Security Standards) menu item highlighted. The main content area shows two security standards: 'AWS 基礎セキュリティのベストプラクティス v1.0.0' and 'PCI DSS v3.2.1'. A modal dialog is open in the foreground, titled 'PCI DSS v3.2.1 を有効化' (Enable PCI DSS v3.2.1). The dialog contains the following text:

この標準オンにすると、セキュリティ評価を実行できます。現在の料金およびサンプルシナリオについては、[AWS Security Hub の料金を参照してください](#)。

AWS Config は、標準を実行する各 AWS リージョンのすべてのリソースで有効化する必要があります。AWS Config は手動で有効化できるほか、[AWS CloudFormation StackSets サンプルテンプレート](#)にある「AWS Config を有効にする」AWS CloudFormation テンプレートを使用することも可能です。

AWS Config で記録される設定項目には、[AWS Config の料金](#)に従い、料金が発生します。これらの料金は Security Hub 料金に含まれておらず、別途請求となります。

At the bottom of the dialog, there are two buttons: 'キャンセル' (Cancel) and '有効化' (Enable).

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

検出結果 アクション ▼ ワークフローステータスを変更 ▼ インサイトを作成する

検出結果は、セキュリティ上の問題か、失敗したセキュリティチェックです。

< 1 ... >

<input type="checkbox"/>	重要度 ▼	ワークフローのステータス ▼	会社	製品	タイトル ▼	リソース ID	リソースタイプ	ステータス ▼	更新日時 ▼
<input type="checkbox"/>	● CRITICAL	NEW	AWS	Security Hub	PCI.IAM.4 Hardware MFA should be enabled for the root user		AwsAccount	FAILED	5時間前
<input type="checkbox"/>	● CRITICAL	NEW	AWS	Security Hub	IAM.6 Hardware MFA should be enabled for the root user		AwsAccount	FAILED	5時間前
<input type="checkbox"/>	● HIGH	NEW	AWS	Security Hub	4.1 Ensure no security groups allow ingress from 0.0.0.0/0 to port 22		AwsAccount	FAILED	5時間前
<input type="checkbox"/>	● HIGH	NEW	AWS	Security Hub	4.1 Ensure no security groups allow ingress from 0.0.0.0/0 to port 22		AwsEc2SecurityGroup	FAILED	5時間前
<input type="checkbox"/>	● HIGH	NEW	AWS	Security Hub	4.1 Ensure no security groups allow ingress from 0.0.0.0/0 to port 22		AwsEc2SecurityGroup	FAILED	5時間前

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

Security Hub > 検出結果

検出結果は、セキュリティ上の問題を、失敗したセキュリティチェックです。

アクション ▼ ワークフローステータスを変更 ▼ インサイトを作成する

ワークフローのステータス EQUALS NEW X | ワークフローのステータス EQUALS NOTIFIED X

レコードの状態 EQUALS ACTIVE X | フィルターの適用

重要度	ワークフローのステータス	会社	製品	タイトル
MEDIUM	NEW	AWS	Security Hub	PCI IAM.8 Password policies for IAM users should have strong configurations
LOW	NEW	Amazon	GuardDuty	API DescriptionStandardControls was invoked using root credentials.
MEDIUM	NEW	AWS	Security Hub	5.5.5 S3 buckets should require requests to use Secure Socket Layer
MEDIUM	NEW	AWS	Security Hub	5.5.5 S3 buckets should require requests to use Secure Socket Layer
MEDIUM	NEW	AWS	Security Hub	5.5.5 S3 buckets should require requests to use Secure Socket Layer
MEDIUM	NEW	AWS	Security Hub	5.5.5 S3 buckets should require requests to use Secure Socket Layer
MEDIUM	NEW	AWS	Security Hub	5.5.5 S3 buckets should require requests to use Secure Socket Layer
MEDIUM	NEW	AWS	Security Hub	5.5.5 S3 buckets should require requests to use Secure Socket Layer

PCI IAM.8 Password policies for IAM users should have strong configurations

Finding ID: amonawssecurityhubap-northeast-1:238589436340:subscription:pci-dss/v3.2.1/PCI IAM.8/finding/h456b5cb-804c-4648-9902-d9c39a60303a

MEDIUM

This AWS control checks whether the account password policy for IAM users uses the following minimum PCI DSS configurations: RequireUppercaseCharacters: Require at least one uppercase character in password. (Default = true) RequireLowercaseCharacters: Require at least one lowercase character in password. (Default = true) RequireNumbers: Require at least one number in password. (Default = true) MinimumPasswordLength: Password minimum length. (Default = 7 or longer) PasswordReusePrevention: Number of passwords before allowing reuse. (Default = 4) MaxPasswordAge: Number of days before password expiration. (Default = 90)

ルール

ワークフローのステータス: 新規

レコードの状態: ACTIVE

AWS アカウント ID: 238589436340	重要度 (オリジナル): 40
重要度 (正規化済み): 40	ステータス: FAILED
作成時刻: 2020-07-28T06:26:56.987Z	更新日時: 2020-07-28T06:26:56.987Z
製品名: Security Hub	重要度レベル: MEDIUM
会社名: AWS	

種類および関連検出結果

改善

For directions on how to fix this issue, please consult the AWS Security Hub PCI DSS documentation.

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

3. 最も多くの検出結果を生み出している AMI

Security Hub マネージド型インサイト



インサイト: 3. 最も多くの検出結果を生み出している AMI

Security Hub マネージド型インサイト

アクション ▼

ワークフローのステータス ▼

インサイトを作成する

リソースタイプ 次と同じ: AwsEc2Instance × ワークフローのステータス 次と同じ: NEW × ワークフローのステータス 次と同じ: NOTIFIED ×
レコードの状態 次と同じ: ACTIVE × グループ化条件: ResourceAwsEc2InstanceImageld × フィルターの追加

EC2 インスタンスのイメージ ID	検出結果
ami-	181
ami-	16
ami-	7
ami-	7
ami-	4
ami-	4
ami-	4
ami-	4
ami-	2

AWS Security Hub のインサイト

https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-insights.html

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



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

検出結果

検出結果は、セキュリティ上の問題か、失敗したセキュリティチェックです。

アクション ▼ ワークフローステータスを変更 ▼ **インサイトを作成する**

Q ステータス EQUALS FAILED X グループ化条件: ResourceType X | フィルターの追加

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)

The screenshot shows the AWS Security Center console. On the left, there is a navigation menu with options like '概要', 'セキュリティ基準', 'インサイト', '検出結果', '統合', '設定', and '最新機能'. The main area is titled '検出結果' and contains a search bar with the filter 'ワークフローのステータス EQUALS NOTIFIED'. Below the search bar, there is a table of findings. The table has columns for '重要度', 'ワークフローのステータス', '会社', '製品', and 'タイトル'. The first row shows a finding with a 'MEDIUM' severity, 'NEW' status, 'AWS' company, 'Security Hub' product, and a title about PCI IAM password policies.

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

The screenshot shows the AWS Security Center console with two custom filters applied: 'ワークフローのステータス EQUALS NEW' and 'ワークフローのステータス EQUALS NOTIFIED'. A dropdown menu is open, showing options for 'グループ化' and 'グループ化条件'.

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

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

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

```
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"
  }
}
```

[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 **概要** 特徴 料金 開始方法 よくある質問

Amazon Detective

セキュリティデータを分析および視覚化して、潜在的なセキュリティ問題の根本原因を迅速に把握する

[Amazon Detective の無料トライアルを開始する](#)

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っても便利です。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 Black Belt Online Seminar] Amazon Detective
https://d1.awsstatic.com/webinars/jp/pdf/services/20200715_AWSBlackBelt2020_AmazonDetective.pdf

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



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

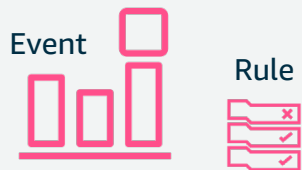
4. セキュリティ検出結果
を取り扱う

5. 対応を自動化する

6. コスト管理をする

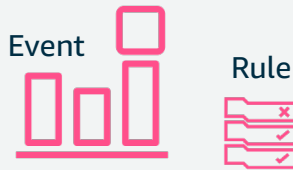
カスタムアクションによる自動化の開始

Security Hub
カスタムアクション



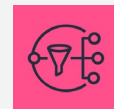
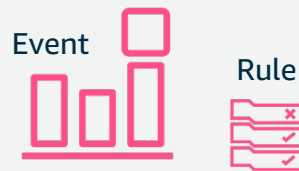
Lambda Function

Security Hub
カスタムアクション



Amazon Kinesis
Data Streams

Security Hub
カスタムアクション



Amazon Simple
Notification
Service



AWS Systems
Manager
Run command

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

The screenshot shows the AWS Security Hub console interface. On the left is a navigation menu with options like '概要', 'セキュリティ基準', 'インサイト', '検出結果', '統合', '設定', and '最新機能'. The '設定' (Settings) option is selected. The main content area is titled '設定' (Settings) and has tabs for 'アカウント', 'カスタムアクション', '使用', and '一般'. The 'カスタムアクション' (Custom Action) tab is active. Below the tabs, there's a section titled 'カスタムアクション' with a description: 'カスタムアクションを作成し、選択したインサイトと検出結果を Amazon CloudWatch Events に送信するように AWS Security Hub を設定します。' (Create a custom action and configure AWS Security Hub to send selected insights and detection results to Amazon CloudWatch Events). There are two buttons: '削除' (Delete) and 'カスタムアクションを作成する' (Create Custom Action). Below this is a table with columns: 'アクション名' (Action Name), '説明' (Description), and 'カスタムアクション ARN' (Custom Action ARN). The table contains one entry: 'SendToEmail' with description 'SendToEmail' and ARN 'arn:aws:securityhub:ap-northeast-1:123456789012:action/custom/SendToEmail'. There is a radio button to the left of the entry and an '更新' (Update) button to the right.

Security Hub ×

Security Hub > 設定

設定

アカウント | **カスタムアクション** | 使用 | 一般

カスタムアクション

カスタムアクションを作成し、選択したインサイトと検出結果を Amazon CloudWatch Events に送信するように AWS Security Hub を設定します。

削除 **カスタムアクションを作成する**

	アクション名	説明	カスタムアクション ARN	
<input type="radio"/>	SendToEmail	SendToEmail	arn:aws:securityhub:ap-northeast-1:123456789012:action/custom/SendToEmail	更新

ここではメール通知用のカスタムアクションを想定

Security Hub カスタムアクション作成 2

CloudWatch Events ルール作成画面

CloudWatch
ダッシュボード
アラーム
アラーム
不足
OK
請求
イベント
ルール
イベントバス
ログ
インサイト
メトリクス
Top-N
お気に入り

ステップ 1: ルールの作成

AWS 環境で発生するイベントに基づいてターゲットを呼び出すためのルールを作成します。

イベントソース

イベントパターンを構築またはカスタマイズするか、スケジュールを設定してターゲットを呼び出します。

イベントパターン ⓘ スケジュール ⓘ

カスタムイベントパターンの構築

```
{
  "source": [
    "aws.securityhub"
  ],
  "resources": [
    "arn:aws:securityhub:ap-northeast-1:XXXXXXXXXXXX:action/custom/
    /SendToEmail"
  ]
}
```

ターゲット

イベントがイベントパターンに一致するか、スケジュールがトリガーされたときに呼び出すターゲットを選択します。

SNS トピック

トピック* MyTopic

▶ 入力の設定

➕ ターゲットの追加*

Security Hub カスタムアクションARNを指定

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

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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



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

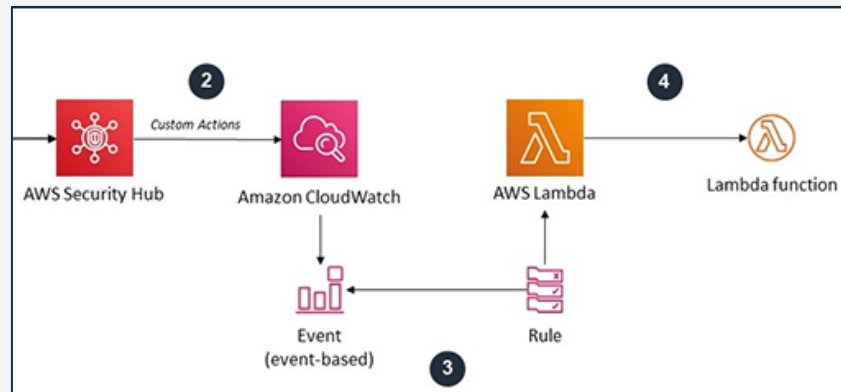
The screenshot shows the AWS Security Hub console interface. On the left is a navigation sidebar with options like '概要', 'セキュリティ基準', 'インサイト', '検出結果', '統合', '設定', and '最新機能'. The main content area is titled 'Security Hub > 検出結果'. It displays a '検出結果' (Detection Result) section with a message: '検出結果は、セキュリティ上の問題か、失敗したセキュリティチェックです。' (The detection result is a security issue or a failed security check). Below this are three buttons: 'アクション' (Action), 'ワークフローステータスを変更' (Change workflow status), and 'インサイトを作成する' (Create insight). The 'アクション' dropdown menu is open, showing 'SendToEmail' as the selected option. A filter bar at the top of the table shows 'レコードの状態 EQUALS ACTIVE' with a search icon and a close button. Below the filter is a table with columns: '重要度' (Severity), 'ワークフローのステータス' (Workflow status), '会社' (Company), '製品' (Product), 'タイトル' (Title), and 'リソース ID' (Resource ID). The table contains one row with a checked checkbox, 'MEDIUM' severity, 'NEW' status, 'AWS' company, 'Security Hub' product, and a title about IAM password policies. The resource ID is partially visible as 'AWS::Account:'.

重要度	ワークフローのステータス	会社	製品	タイトル	リソース ID
<input checked="" type="checkbox"/>	NEW	AWS	Security Hub	PCI.IAM.8 Password policies for IAM users should have strong configurations	AWS::Account: [REDACTED]

[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”

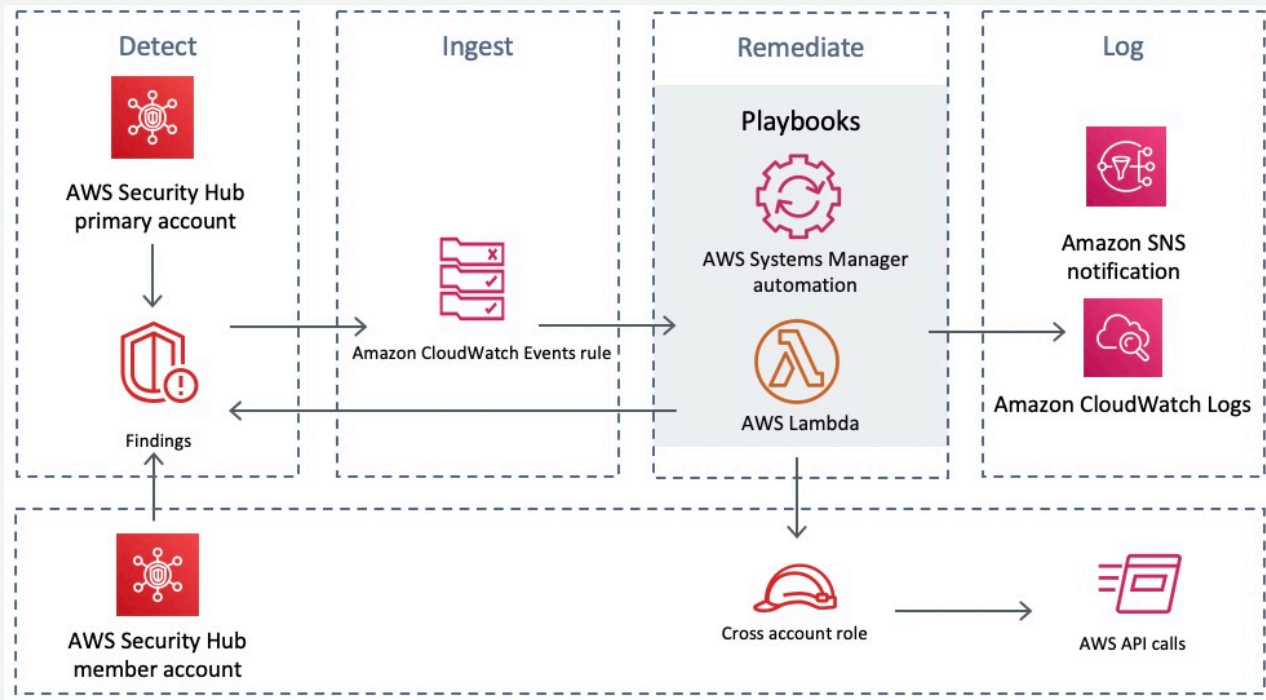


AWS Security Hubによる自動対応と修復

<https://aws.amazon.com/jp/blogs/news/automated-response-and-remediation-with-aws-security-hub/>

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

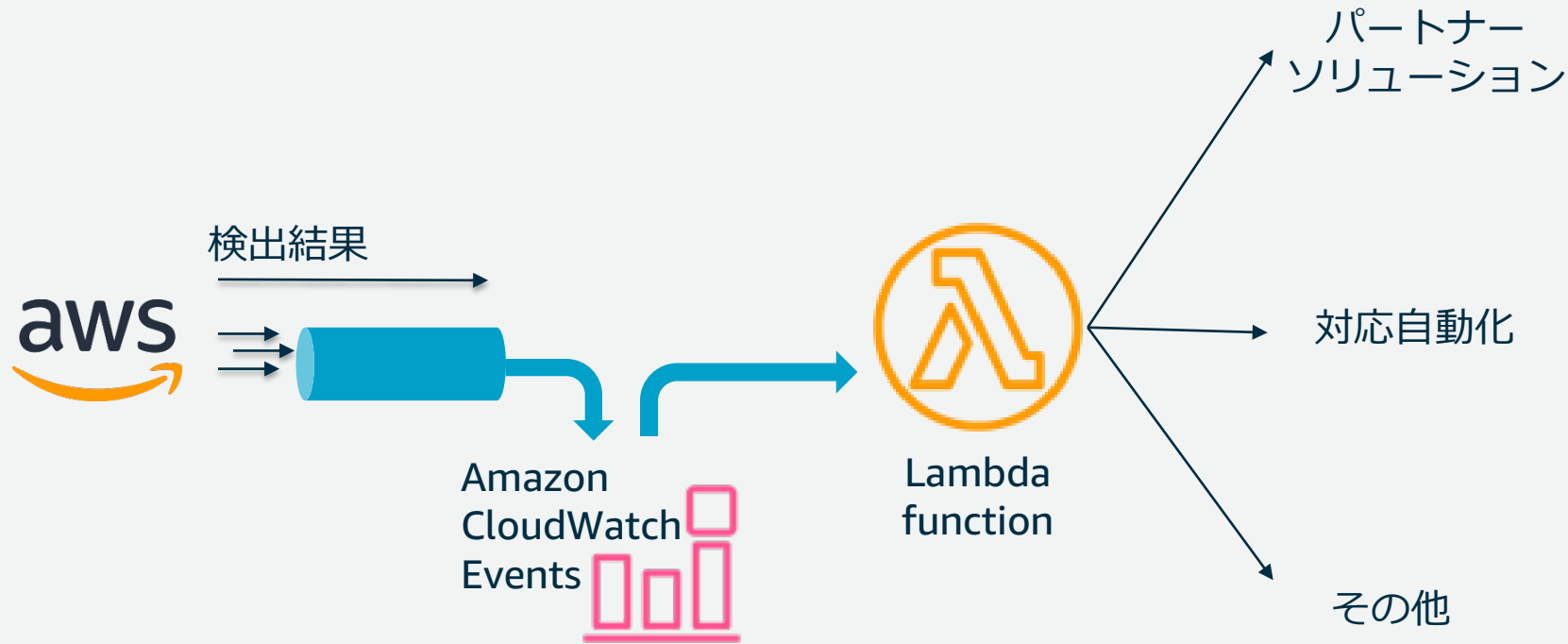
自動対応と修正ソリューション



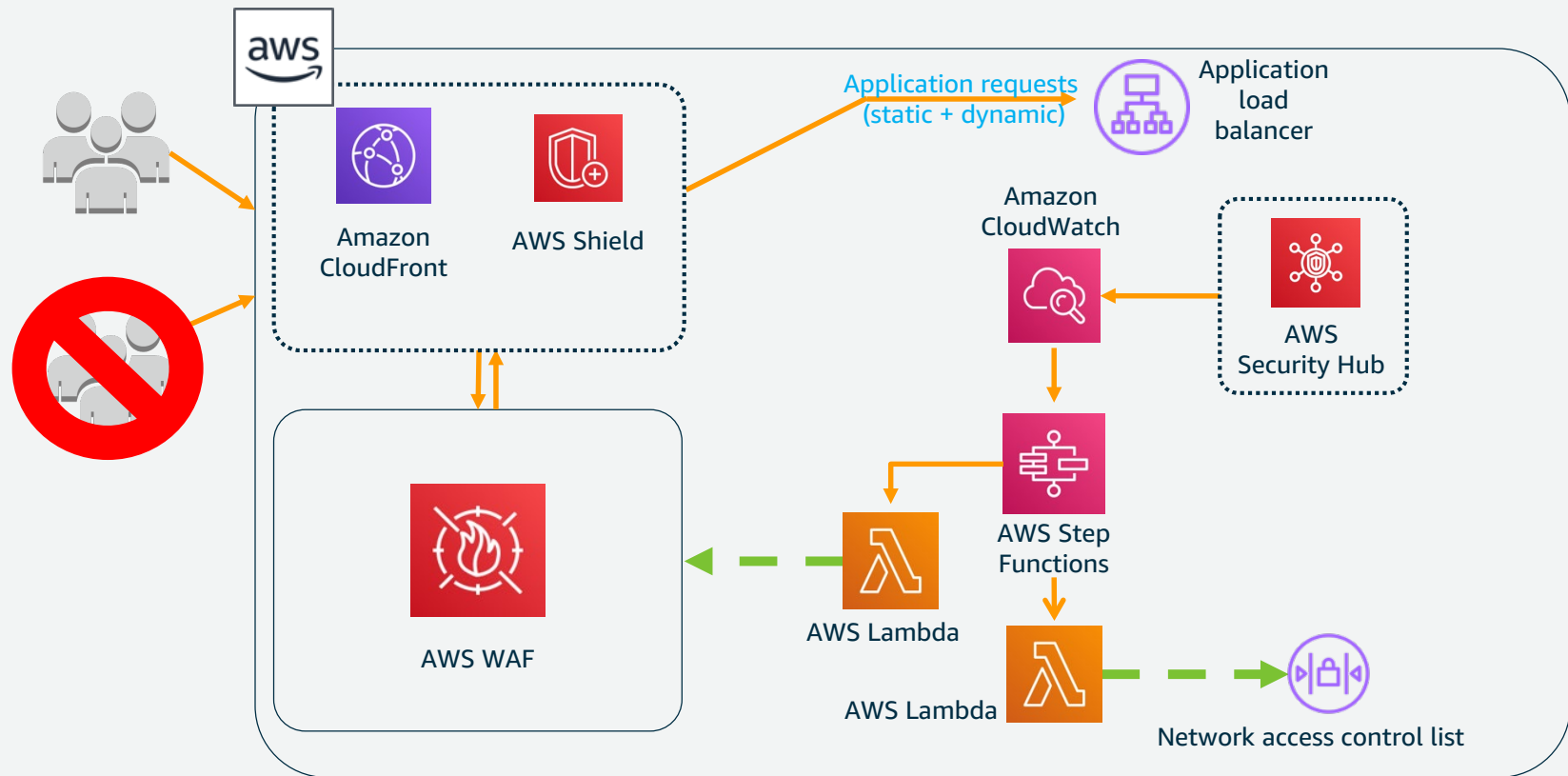
以下の典型的な使い方を示すテンプレートを提供するソリューション (下URL参照)

- 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

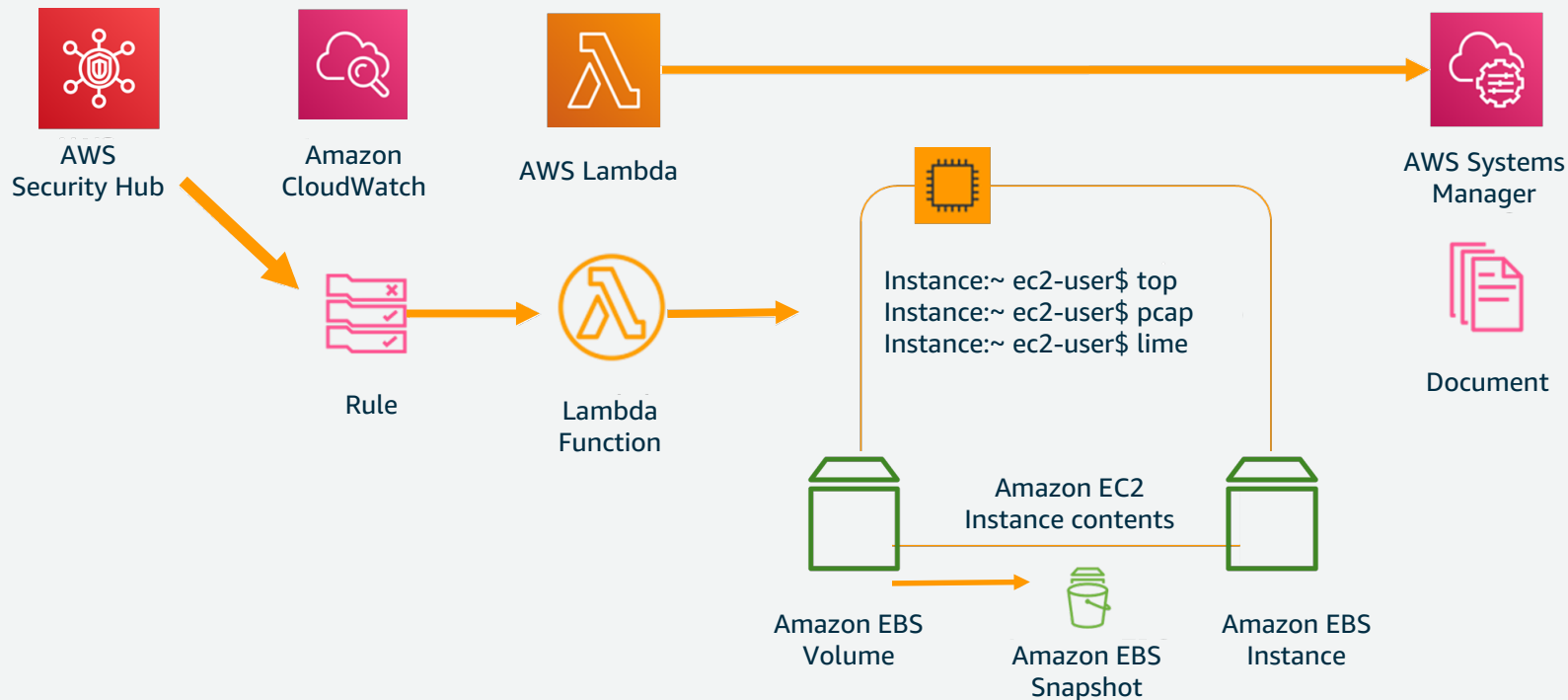
インシデントレスポンスの自動化



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

The screenshot shows the 'Security Hub' settings page, specifically the 'Usage' tab. The page displays usage statistics for the current billing period (28/31 days) and provides a cost estimate of \$4.95. The usage is broken down by product name and type, with the most significant cost being from the Security Hub security checks.

製品名	使用タイプ	項目	月別予測項目
Amazon: GuardDuty	検出結果	639	707
Amazon: Inspector	検出結果	20	22
AWS: Firewall Manager	検出結果	1	1
セキュリティ基準	セキュリティチェック	4,472	4,952
本請求期間内の予測コスト合計			\$4.95

料金 (USD)
1 アカウント、1 リージョンあたり、1 か月あたり

セキュリティチェック	料金 (USD)
最初の 100,000	0.0010 USD/チェック
100,001~500,000	0.0008 USD/チェック
500,001 以上	0.0005 USD/チェック

検出結果取り込みイベント
既存の結果の更新の取り込みが含まれています。Security Hub セキュリティチェックの検出結果取り込みは無料でご利用いただけます。

検出結果取り込みイベント	料金 (USD)
最初の 10,000	無料
10,001 以上	0.00003 USD/検出結果

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

[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

▶ 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

▶ 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

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

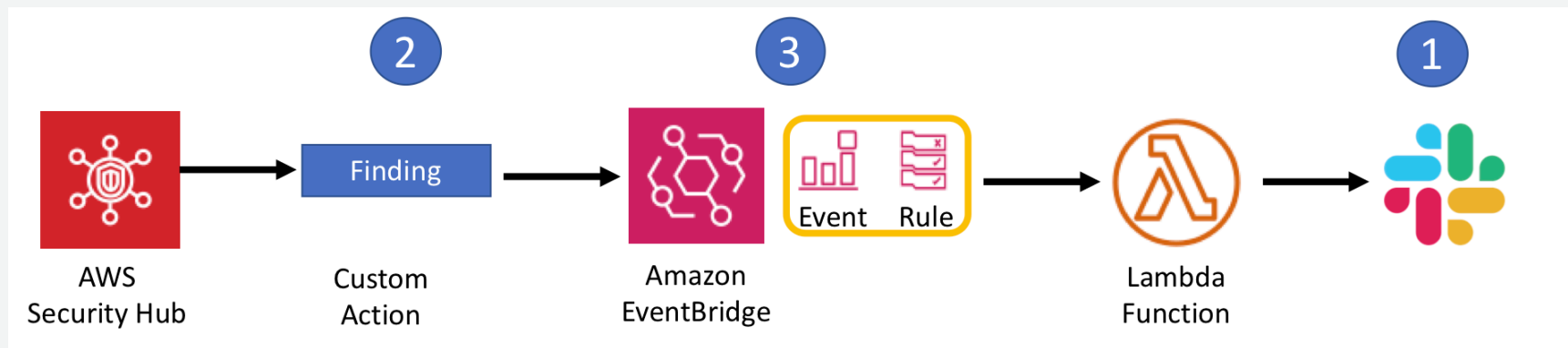
- カスタムアクションを定義し、対応を自動化する

- 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

[参考] AWS Security Hub ワークショップ

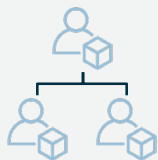
- レベル：中級
- 想定時間：2-3時間
- 事前準備：AWSアカウント、IAM管理ユーザー

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を用いて対応するサンプル(下URL参照)



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



The screenshot shows the AWS Japanese website header with the logo, navigation links for '日本語' and 'アカウント', and a 'サインイン' button. Below the header is a navigation bar with links for '製品', 'ソリューション', '料金', 'ドキュメント', '学習', 'パートナー', 'AWS Marketplace', and 'その他'. The main content area features the title 'AWS クラウドサービス活用資料集トップ' and a paragraph of introductory text. At the bottom, there are four buttons: 'AWS Webinar お申込', 'AWS 初心者向け', '業種・ソリューション別資料', and 'サービス別資料'.

aws

日本担当チームへお問い合わせ サポート 日本語 ▼ アカウント ▼ [コンソールにサインイン](#)

製品 ソリューション 料金 ドキュメント 学習 パートナー AWS Marketplace その他 🔍

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

[AWS Webinar お申込 »](#) [AWS 初心者向け »](#) [業種・ソリューション別資料 »](#) [サービス別資料 »](#)

<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

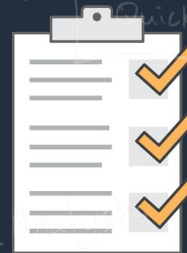
(<https://aws.amazon.com/jp/about-aws/events/>)

AWS イベント

で[検索]



AWS Well-Architected



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>

