AWS re:Inforce 2023 re:Cap
サービスアップデート

Takahiro Hiraga

Security Solutions Architect
AWS

自己紹介

名前：平賀 敬博（Hiraga Takahiro）

所属：セキュリティソリューションアーキテクト

経歴：

- SIer で金融系アプリケーション開発
- セキュリティ専業企業で Web アプリケーションのセキュリティ
- AWS におけるセキュリティ課題解決のサポート

好きな AWS サービス：
Amazon Key Management Service

アジェンダ

カテゴリ	新サービス・アップデート
ID およびアクセス管理	- Amazon Verified Permissions - AWS IAM Identity Center supports Google Workspace
検出	- Amazon Inspector code scanning - Amazon Inspector SBOM - Amazon CodeGuru Security - AWS Security Hub Automation Rules - Amazon GuardDuty Summary View - AWS CloudTrail Lake dashboard for top trends - Amazon ECR Basic Scan supports CVSS v3
ネットワークとアプリケーションの保護	- WAF Account Creation Fraud Prevention - Amazon EC2 Instance Connect Endpoint
データ保護	- AWS Payment Cryptography - AWS Database Encryption SDK
インシデントへの対応	- Amazon Detective finding groups - AWS DRS VPC configurations recovery
コンプライアンス	- AWS Audit Manager third-party risk assessment / CSV

ID およびアクセス管理

Amazon Verified Permissions を一般提供開始

一般利用開始

- カスタムアプリケーション向けのスケーラブルできめ細やかな認証およびアクセスコントロールを実現する新サービス
- アクセス制御はオープンソースとして公開しているポリシー言語の Cedar で定義

- アプリケーションロジックからアクセス制御を分離し、コードを変更する必要なく、パーミッションルールの変更と更新を一元管理し、運用を簡素化。アプリケーションリソースにパーミッションを実装する工数を大幅に削減
- 全リージョンで一般利用可能

ポリシーベースのアクセスコントロール

Fine-grained
リソースとユーザーの組み合わせによる
細かな制御

Real time
プリンシパルやリソースの現在の属性値
に基づくアクセス判断

Scalable
容易にメンテナンス可能なルール
アプリケーションからの独立性

User-managed access (UMA)
ユーザーによるアクセス管理

ポリシー

Role based

Attribute based

```
1  permit (
2      principal in Role::"SalesTeam",
3      action in [Action::"view", Action::"update"],
4      resource == Photo::"vacationPhoto94.jpg"
5  )
6  when {
       resource.accessLevel == "public" &&
       principal.location == "USA" &&
       context.request_client_ip == "222.222.222.222"
10 };
```

Amazon Verified Permissions の特徴

外部化
ポリシーベースの認可モデル

アプリケーション構築
動的でリアルタイムな認可

統合
アイデンティティプロバイダーとの同期

管理
きめ細かな権限設定

簡素化
監査や監視フローの簡素化が可能

分析
アプリケーションの権限を分析

一般利用開始

AWS IAM Identity Center が Google Workspace からのユーザ情報の自動プロビジョニングをサポート

- ユーザ情報の自動プロビジョニングが可能な外部の ID プロバイダー (IdP) として、Google Workspace が追加
- ユーザは、自らの Google Workspace ID を使用して AWS IAM Identity center ユーザーポータルから AWS コンソールに簡単にアクセス可能
- また、管理者は AWS Organizations を利用することで、組織から AWS へのアクセスを一元管理
- AWS IAM Identity Center が利用可能な全リージョンで一般利用可能

検出

一般利用開始

Amazon Inspector Code Scans for AWS Lambda を発表

- Lambda 関数・レイヤーのアプリケーションコードをスキャンして、インジェクションの脆弱性、データ漏洩、暗号化の欠如などのコードセキュリティの脆弱性を検出可能

- 脆弱性の名前、影響を受けるコードスニペット、脆弱性の修正提案など、実用的なセキュリティ検出結果を生成
- 東京を含む 10 リージョンで利用可能

Code Scan for AWS Lambda - Findings 例

脆弱性を含む箇所を明示的に指摘

修正方法

CWE-77,78,88 - OS command injection

Finding ID: arn:aws:inspector2:us-east-1:720849230328:finding/55322a3aaeb0b3c9d5ab85699a9d4045

Constructing operating system or shell commands with unsanitized user input can lead to inadvertently running malicious code.

Finding overview

AWS account ID	[redacted]
Severity	High
Type	Code Vulnerability
Detector name	OS command injection
Relevant CWE	CWE-77, CWE-78, CWE-88
Rule ID	Rule-52604
Detector tags	#injection, #security, #subprocess, #owasp-top10, #top25-cwes, #cwe-77, #cwe-78, #cwe-88, #python
Fix available	Yes
Created at	June 21, 2023 11:29 AM (UTC+09:00)

Vulnerability details

File path	lambda_function.py

Vulnerability location

```
18      address = request.args.get("address")
19      cmd = "ping -c 1 %s" % address
20      client = client.SSHClient()
21      client.connect("ssh.samplehost.com")
22      # Noncompliant: address argument is not sanitized.
23      client.exec_command(cmd)
24
25  def create_session_noncompliant():
26      import boto3
27      # Noncompliant: uses hardcoded secret access key.
28      ********** * ****************************************
```

Suggested remediation

Passing user-provided input to Python subprocess, OS, and command functions without validation or sanitization makes your code vulnerable to running arbitrary OS commands. To prevent this, implement input validation and use secure functions. For more information, see CWE-77, CWE-78 and CWE-88

脆弱性を含む箇所を明示的に指摘

修正方法

CWE-798 - Hardcoded credentials

Finding ID: arn:aws:inspector2:us-east-1:720849230328:finding/213435e3fb465b6d6bed5cf192a08fdf

Access credentials, such as passwords and access keys, should not be hardcoded in source code. Hardcoding credentials may cause leaks even after removing them. This is because version control systems might retain older versions of the code. Credentials should be stored securely and obtained from the runtime environment.

Finding overview

AWS account ID	[redacted]
Severity	Critical
Type	Code Vulnerability
Detector name	Hardcoded credentials
Relevant CWE	CWE-798
Rule ID	Rule-456991
Detector tags	#secrets, #security, #owasp-top10, #top25-cwes, #cwe-798, #python
Fix available	Yes
Created at	June 21, 2023 11:34 AM (UTC+09:00)

Vulnerability details

File path	lambda_function.py

Vulnerability location

```
23      client.exec_command(cmd)
24
25  def create_session_noncompliant():
26      import boto3
27      # Noncompliant: uses hardcoded secret access key.
28      ********** * ****************************************
29      boto3.session.Session(aws_secret_access_key=sample_key)
```

Suggested remediation

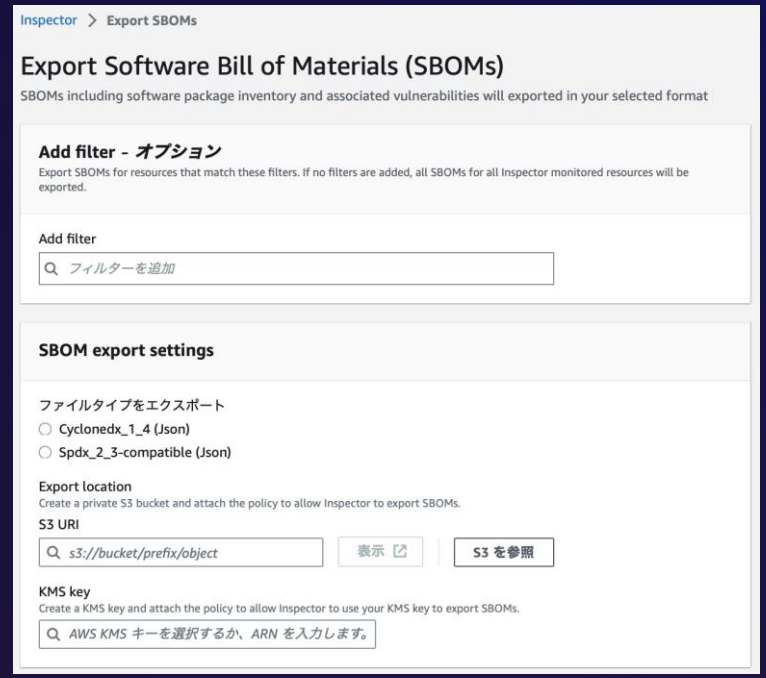
It appears your code contains a hardcoded AWS Secret Access Key ID. Hardcoded secrets or credentials can allow attackers to bypass authentication methods and perform malicious actions. We recommend revoking access to resources that use this access key and using IAM roles instead of hardcoded access keys for IAM users. If you must use IAM users, secure their secrets outside your code.

Learn more about the use of hardcoded credentials

Amazon Inspector SBOM Export を発表

一般利用開始

- Amazon Inspector で監視している
  全てのリソースについて、
  Software Bill of Materials (SBOM) を、
  S3 バケットに業界標準形式でエクスポート
- エクスポートされたデータには、
  リソースと関連する脆弱性情報を含むため、
  Amazon Athena または Amazon QuickSight
  を使用して、利用パッケージの脆弱性など、
  ソフトウェアサプライチェーンリスク傾向を
  分析可能
- 全リージョンで無料で利用可能



Software Bill of Materials 例（抜粋）

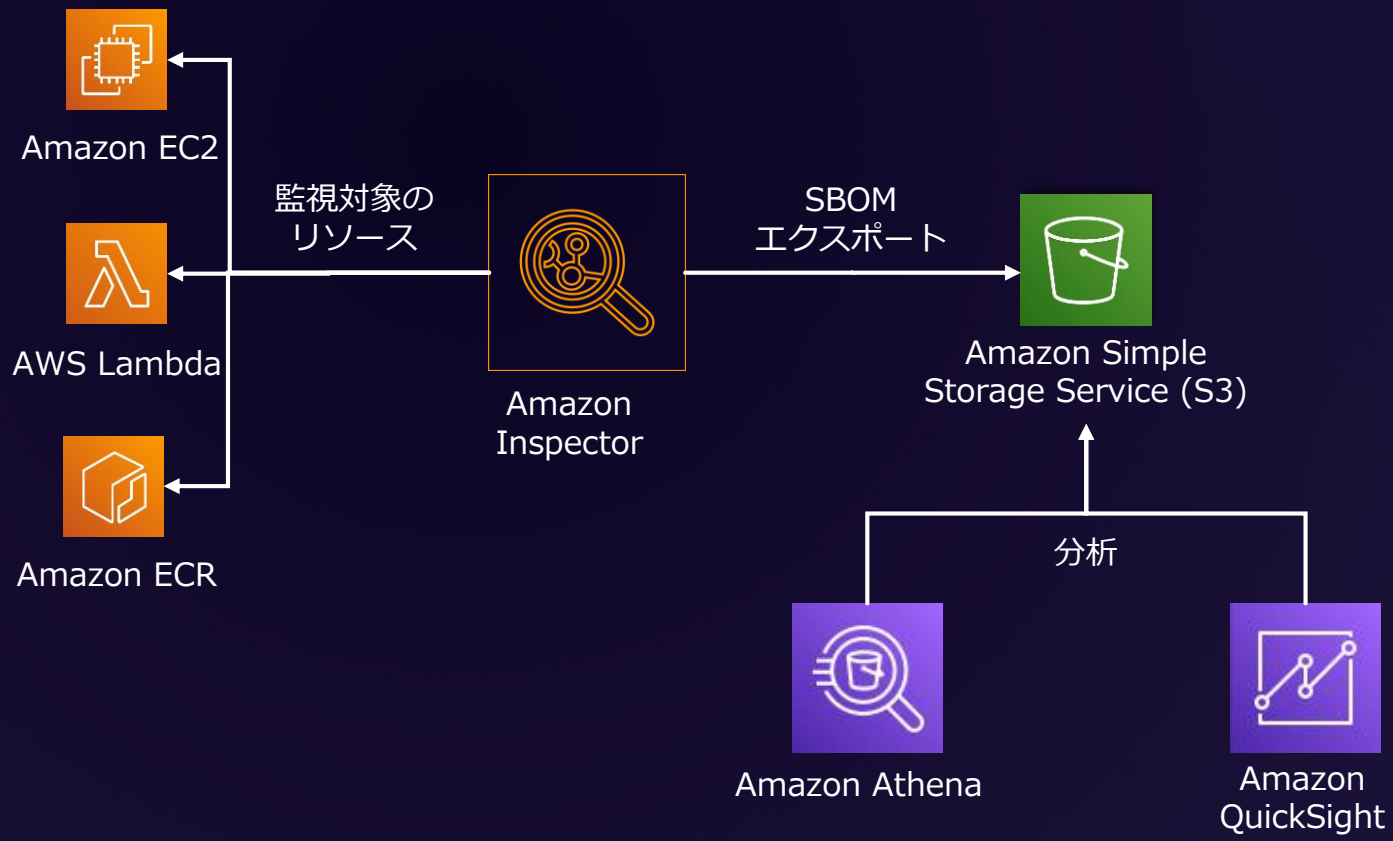
ソフトウェアパッケージの名称とバージョン

関連する脆弱性

```
{
        “name”: “python-jwt”, "versionInfo": "3.3.3",
        "downloadLocation": "NOASSERTION","sourceInfo": "NOASSERTION",
        "filesAnalyzed": false,
        "externalRefs": [
            {
                "referenceCategory": "PACKAGE-MANAGER",
                "referenceType": "purl",
                "referenceLocator": "pkg:pypi/python-jwt@3.3.3"
            },
            {
                "referenceCategory": "PACKAGE-MANAGER",
                "referenceType": "PYTHON",
                "referenceLocator": "python_jwt-3.3.3.dist-info/METADATA"
            },
            {
                "referenceCategory": "SECURITY",
                "referenceType": "vulnerability",
                "referenceLocator": "SNYK-PYTHON-PYTHONJWT-3017172"
            },
            {
                "referenceCategory": "SECURITY",
                "referenceType": "vulnerability",
                "referenceLocator": "CVE-2022-39227"
            }
        ],
        "SPDXID": "SPDXRef-Package-pypi-python-jwt-cc4a680f592426bfc7c1a16d368f5f73"
    }
```

Amazon Inspector SBOM Export の概要

Software Bill of Material (SBOM)
ソフトウェアコンポーネントやそれらの依存関係の情報も含めた、
機械処理可能な製品一覧リスト



- ✓ サポート SBOM フォーマット：
  CycloneDX and SPDX
- ✓ Organization 単位、リソース単位での
  エクスポートが可能
- ✓ Amazon Inspector でアクティブに監
  視されているすべてのリソースが対象
- ✓ 無料

Amazon CodeGuru Security を発表

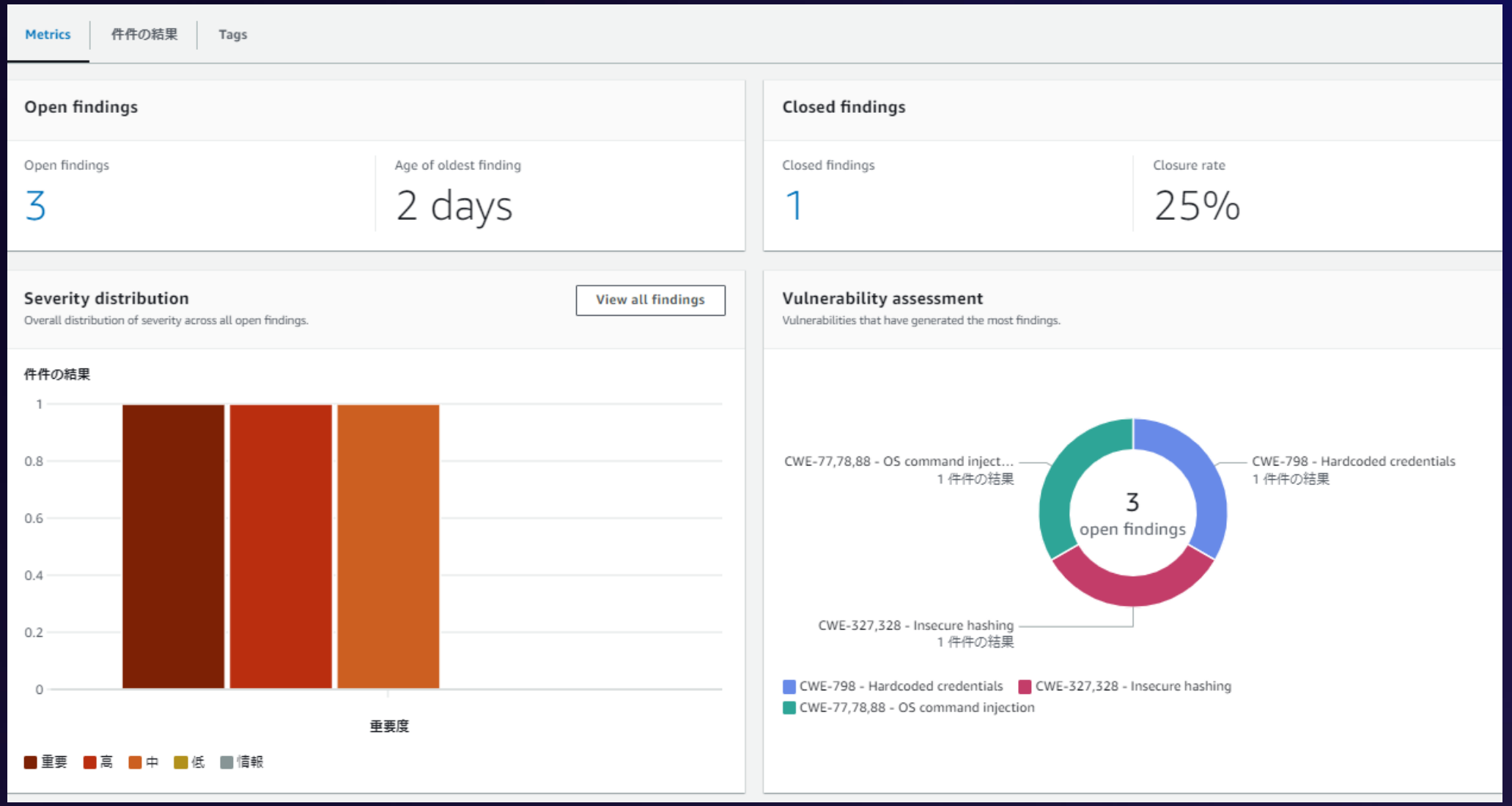
プレビュー

- 機械学習を使用して
コードの脆弱性を特定し、
修正方法のガイダンスを提供する
静的アプリケーションセキュリティ
テスト (SAST) ツール

- アプリケーションコードに対して、
詳細なセマンティック分析を実行する
ことにより、低い誤検知率で脆弱性を検出。
さらに特定の脆弱性にはパッチコードが生成されるので、
脆弱性を修正するために必要な労力を軽減可能

- 東京を含む 10 のリージョンのプレビューの利用可能

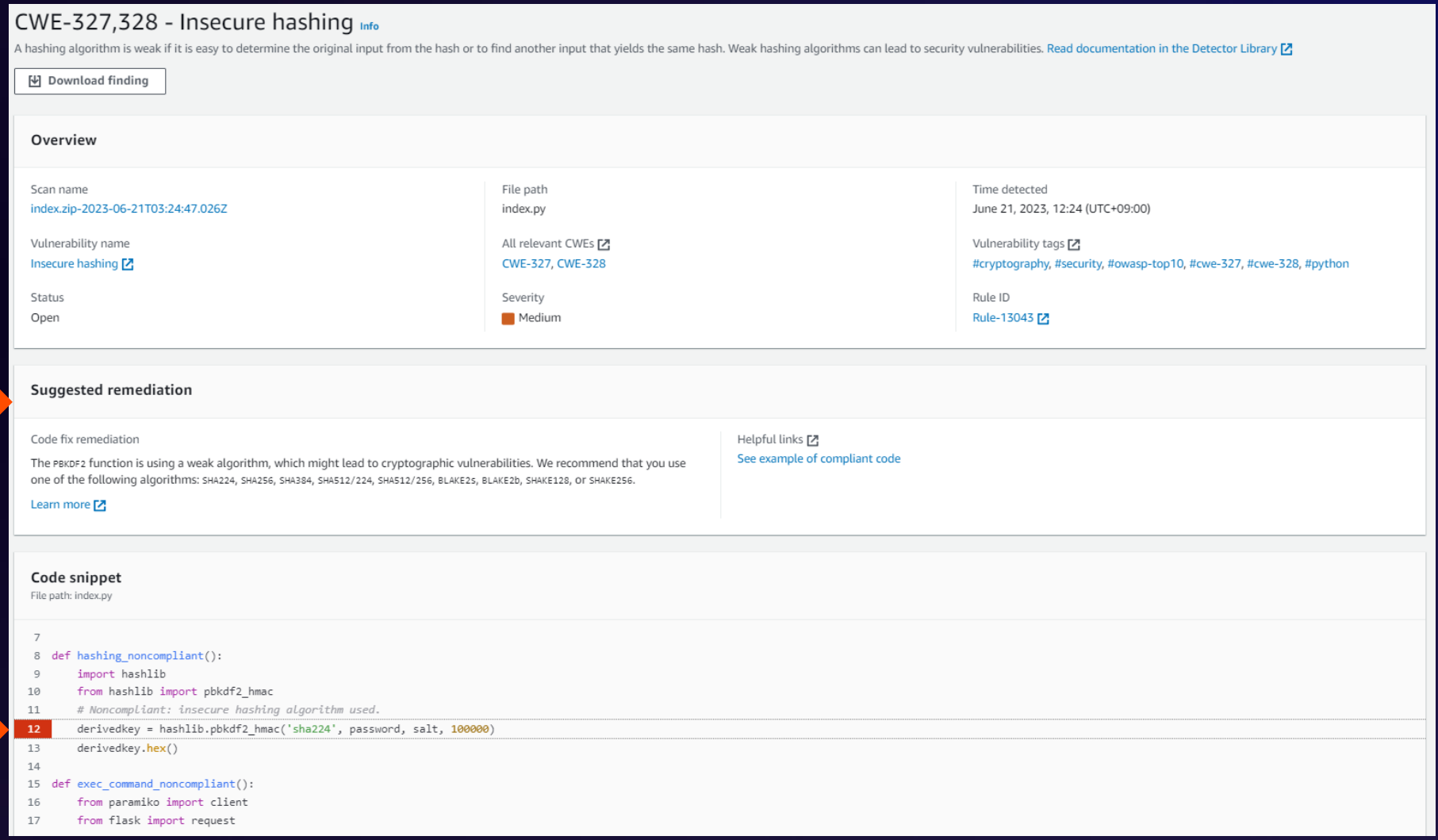
Amazon CodeGuru Security 結果例 (1)



Amazon CodeGuru Security 結果例 (2)

修正方法

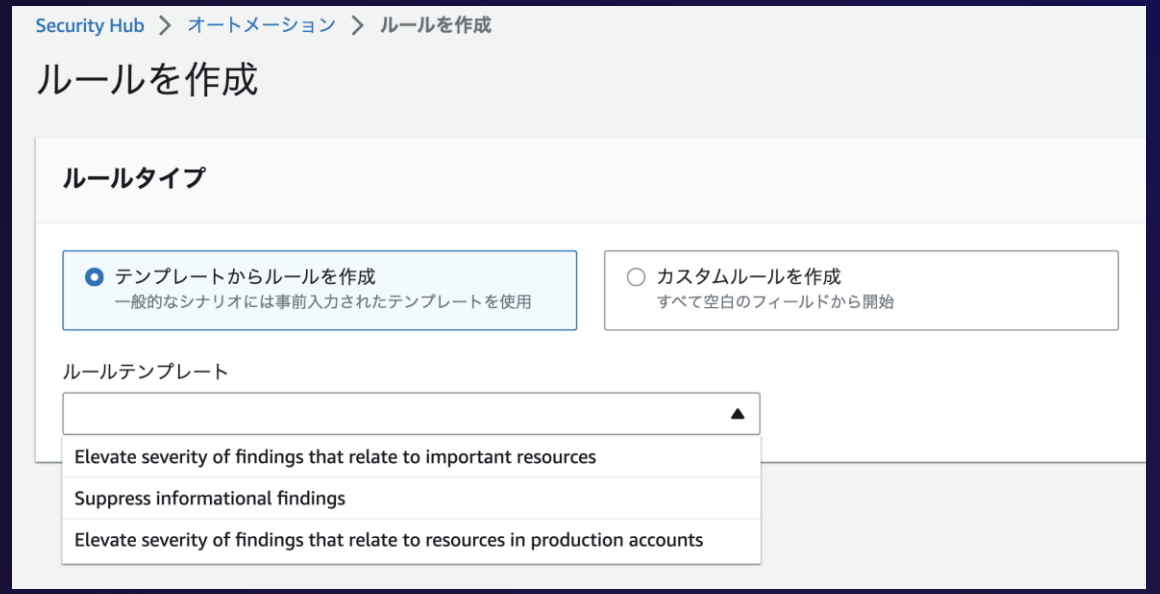
脆弱性を含む箇所を明示的に指摘



AWS Security Hub automation rules を発表

一般利用開始

- AWS Security Hub にニアリアルタイムで検出結果を自動的に更新または抑制する自動化ルール機能が追加
- 自動化ルールを使用することで、検出結果のさまざまなフィールドの自動的な更新、検出結果の抑制、検出結果の重大度、ワークフローステータスの更新、メモの追加、が実現可能
- 大量の検出結果に対する
  重要度の低い検出結果の抑制、
  環境に応じた重要度の変更、
  などの対応を通じて、
  検出結果の確認、
  インシデント対応の効率化を支援

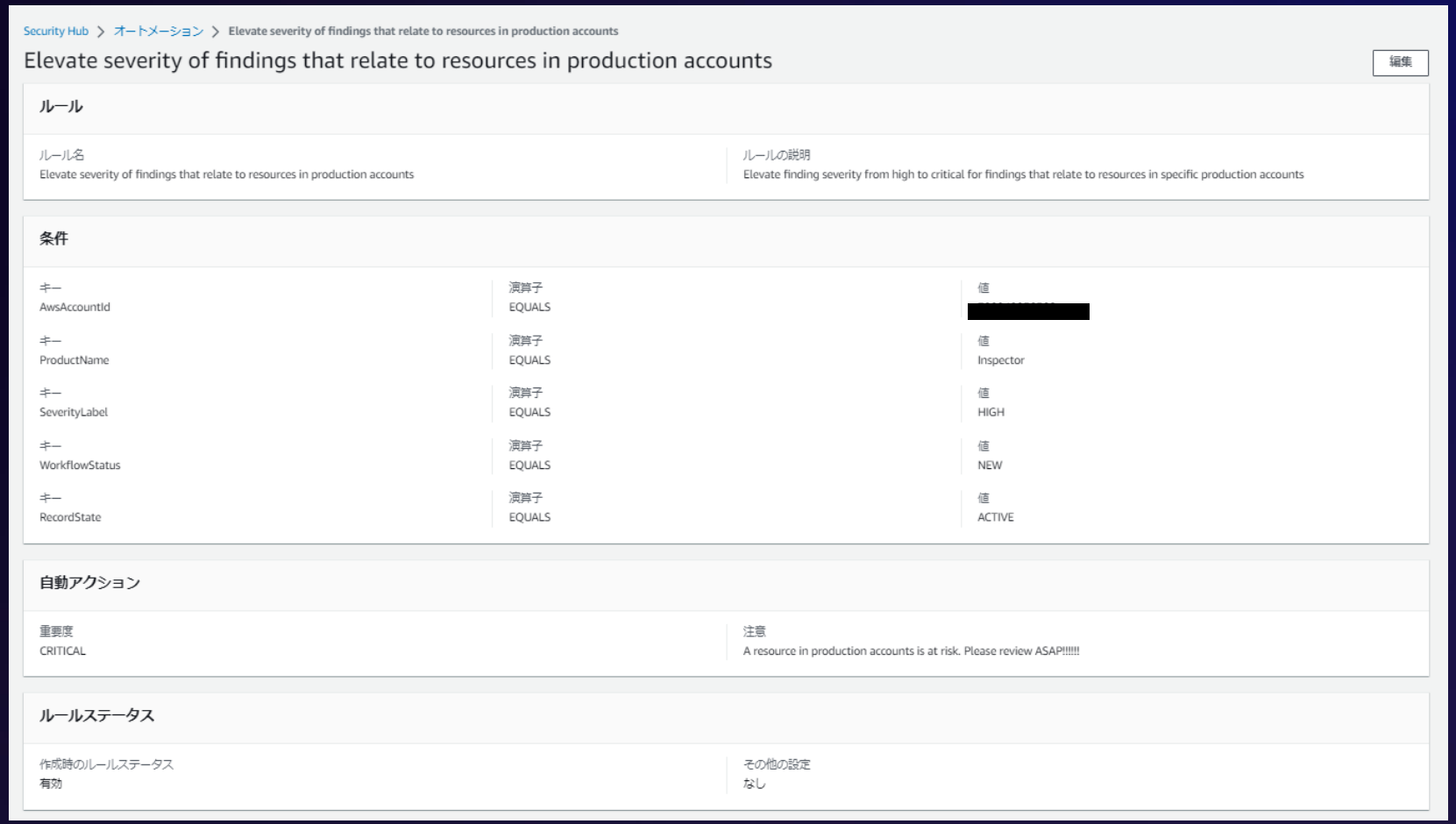


AWS Security Hub automation rules 結果例 (1)

- 検出結果の重大度を変更するルール

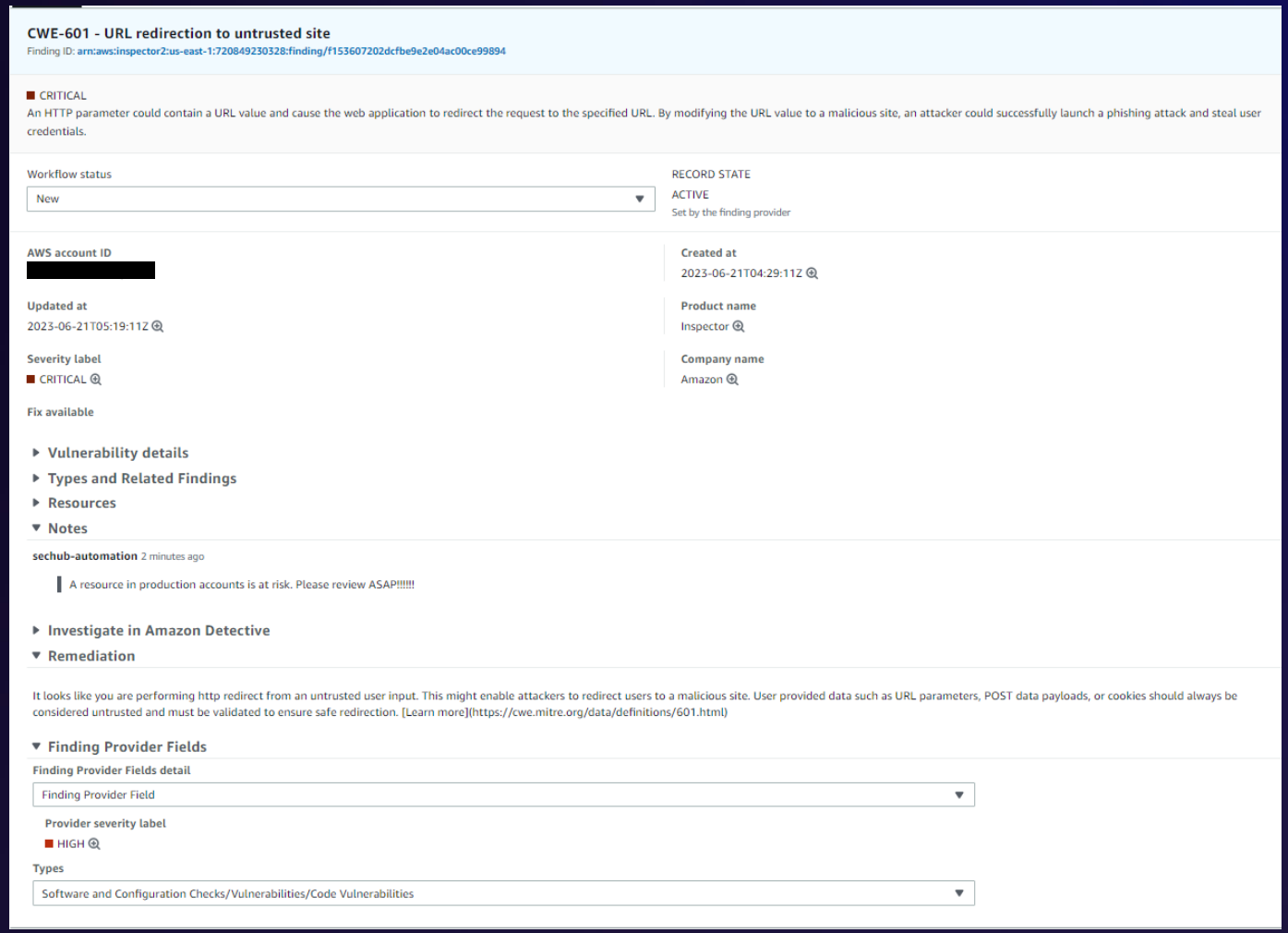
ルールの実行条件

実行される
アクション



AWS Security Hub automation rules 結果例 (2)

- 検出結果の重大度を変更した、検出結果の例



追加されたメモ

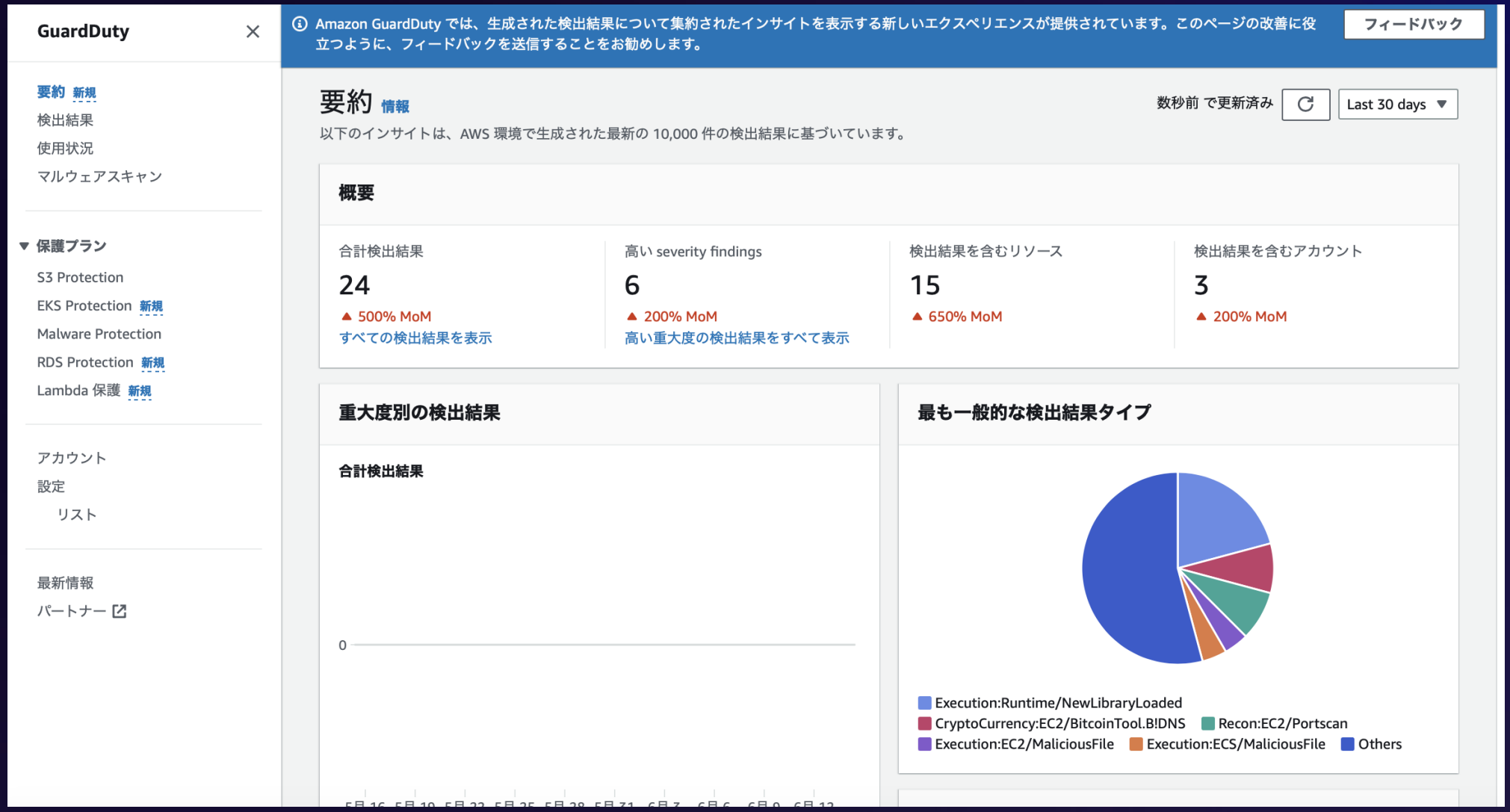
元の重大度

一般利用開始

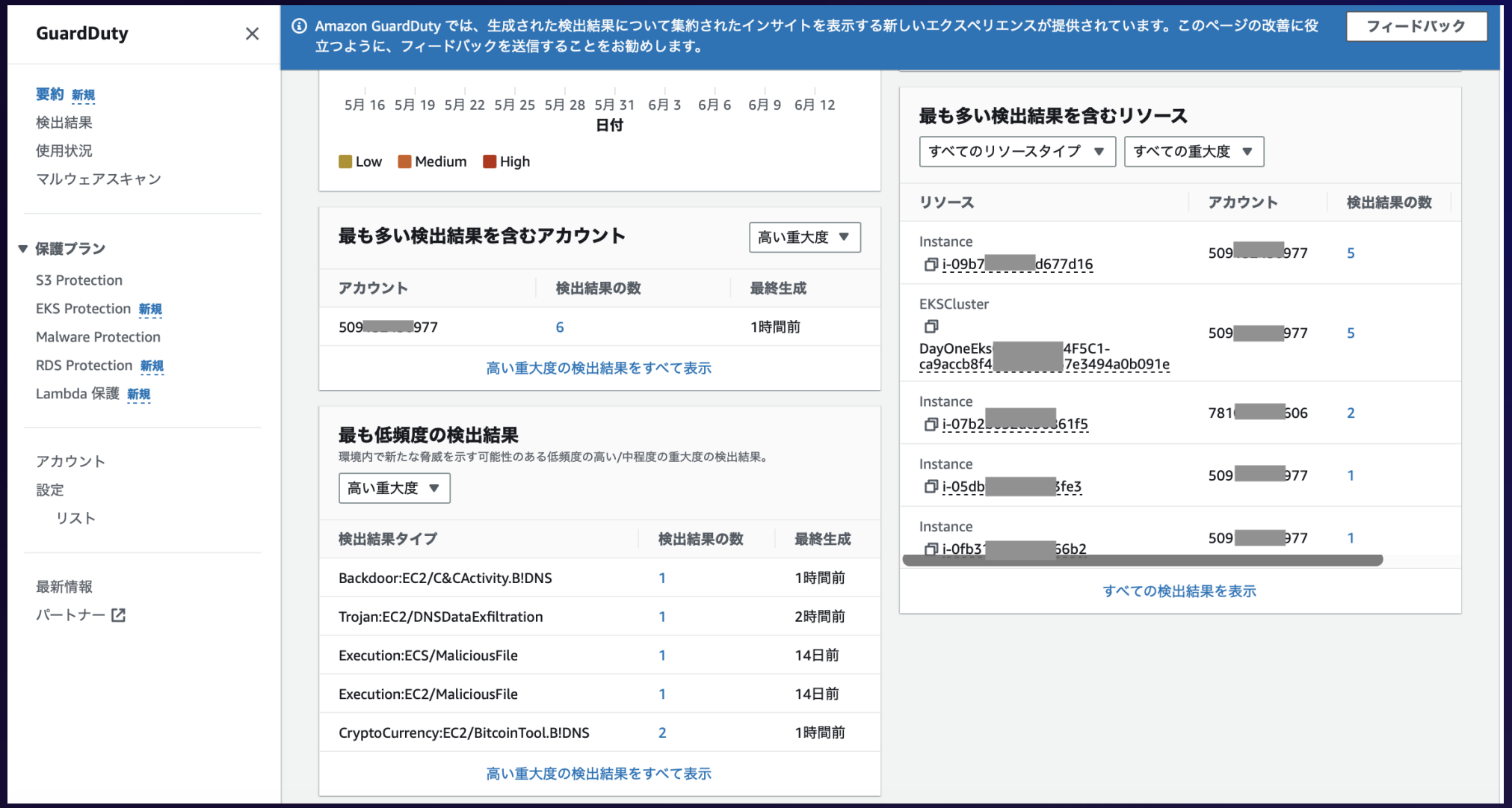
Amazon GuardDuty Findings Summary View の発表

- Amazon GuardDuty コンソールに要約が追加
- 要約では、時間の経過に伴う検出結果の傾向、重大度および検出結果の種類別の内訳等を表示
- 組織全体からの調査結果が統合され、最も大きな影響を受けたアカウントのより迅速な特定をサポート
- Amazon GuardDuty を利用可能な全リージョンで一般利用開始

Findings Summary View (1)



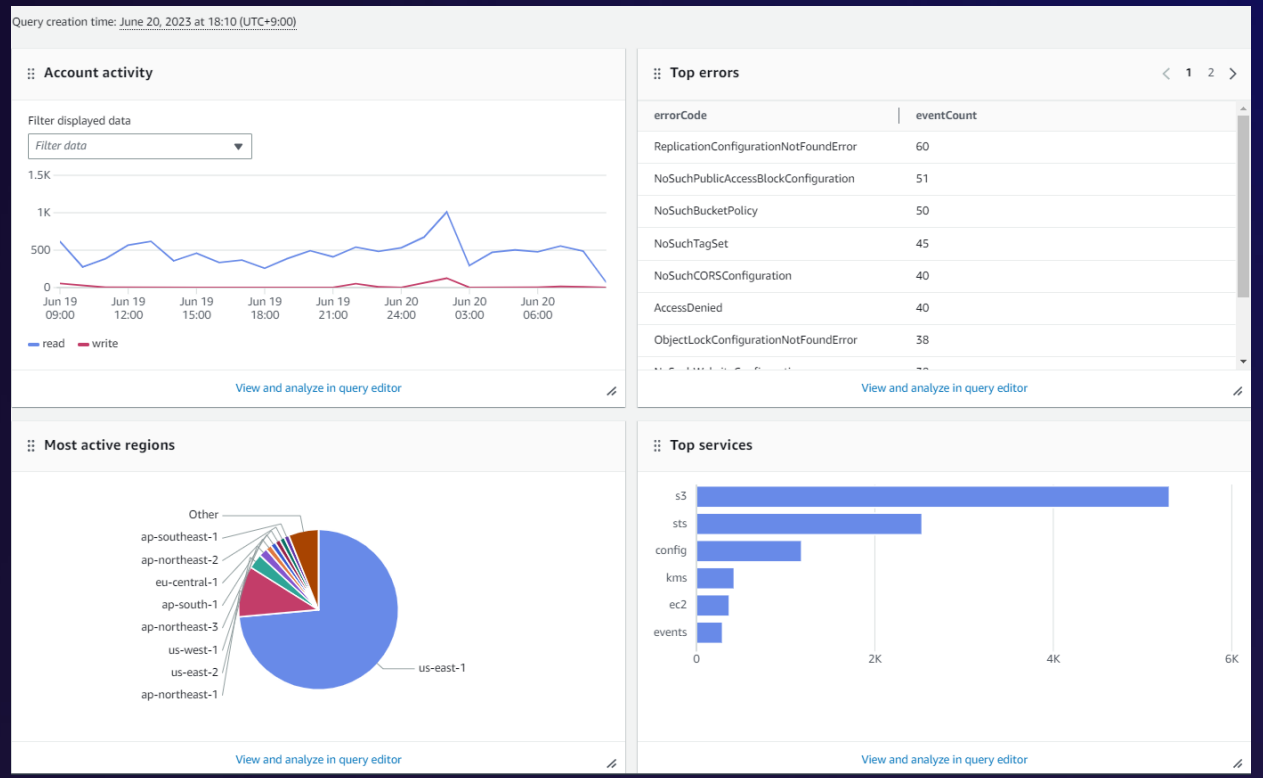
Findings Summary View (2)



AWS CloudTrail Lake で トップトレンド可視化ダッシュボードを発表

一般利用開始

- 事前に定義されたクエリを用いて、CloudTrail イベントのトレンドを視覚的にダッシュボードで把握可能
- 傾向分析が容易となり、アカウントの異常動作検知などの分析をサポート
- CloudTrail Lake が利用可能な全リージョンで一般利用開始



一般利用開始

Amazon Elastic Container Registry (ECR) ベーシックスキャンで CVSS v3 をサポート

- CVSS v3 の情報を利用した、脆弱性の重大度判断
- 環境条件を加味した評価により、よりシステムの実態に即した重大度評価が可能
- 全リージョンで一般利用可能


```
"imageScanFindings": {
"findings": [
        {
          "attributes": [
            {
              "value": "5.5",
              "key": "CVSS3_SCORE"
            },
            {
              "value": "9.4.0-1ubuntu1~20.04.1",
              "key": "package_version"
            },
            {
              "value": "gcc-9",
              "key": "package_name"
            },
            {
              "value": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N",
              "key": "CVSS3_VECTOR"
            },
            {
              "value": "AV:L/AC:L/Au:N/C:P/I:N/A:N",
              "key": "CVSS2_VECTOR"
            },
            {
              "value": "2.1",
              "key": "CVSS2_SCORE"
            }
          ],
          "severity": "MEDIUM",
          "uri": "http://people.ubuntu.com/~ubuntu-security/cve/CVE-2020-13844",
          "name": "CVE-2020-13844"
}
```

ネットワークとアプリケーションの保護

一般利用開始

AWS WAF Fraud Control Account Creation Fraud Prevention を発表

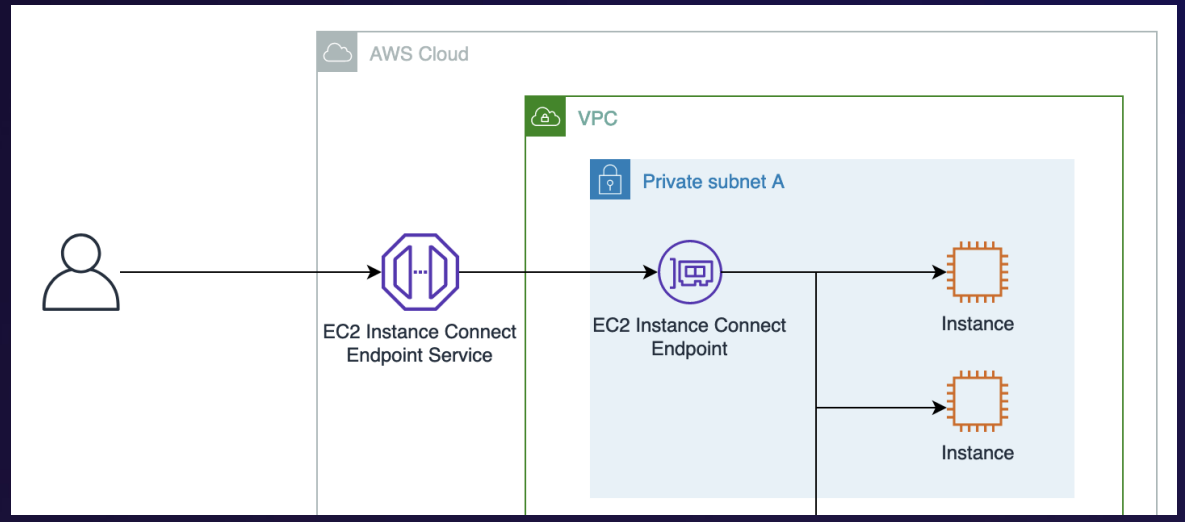
- 不正なアカウント作成を検出、ブロック
- プロモーションやサインアップボーナスの悪用、正規ユーザーへのなりすまし、フィッシング攻撃などのアカウントの悪用を自動的にブロック
- 東京・大阪を含む 22 のリージョンで利用可能
- 6月14日より Account Takeover Prevention 機能を含む Fraud Control について、サブスクリプションと一律単価から、段階的料金体系に変更

Requests	Request fee per Thousand analysis	Captcha	Challenge
First 10k	Free	Free	Free
Up to 2M	$1.00	Free	Free
Next 3M	$0.70	Free	Free
Next 10M	$0.40	Free	Free
Next 15M	$0.20	Free	Free
Over 30M	$0.05	Free	Free

一般利用開始

Amazon EC2 Instance Connect Endpoint (EIC Endpoint) を発表

- パブリック IP アドレスを使用せずに
  EC2 インスタンスに SSH および RDP 接続が可能
- インターネットゲートウェイとグローバル IP アドレスが不要となり、
  リモート接続のための要塞ホストの導入や維持のコストを削減可能
- IAM ベースのアクセス制御と
  セキュリティグループなど NW 制御を組合せた制御や、
  AWS CloudTrail を用いた監査
- 全リージョンで一般利用開始



データ保護

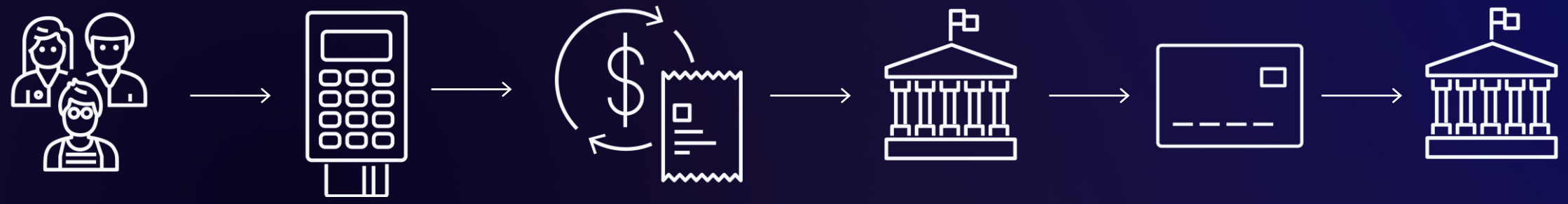
AWS Payment Cryptography の発表

一般利用開始

- 決済トランザクション処理に必要な
  暗号処理を行うための決済 HSM と
  暗号鍵管理機能を提供するマネージドサービス

- オンプレミスの決済 HSM 管理が不要となり、
  決算暗号処理の自動スケーリング、
  サードパーティ間の安全な鍵交換の自動化を実現
- 関連する PCI SSC の要件に適合
- 米国東部 (バージニア北部) と米国西部 (オレゴン) で一般利用可能

AWS Payment Cryptography ユースケース



Customers | Merchant | Payment gateway | Acquirers | Card network | Issuers

Not in scope

Issuer processor and card networks on roadmap

AWS Payment Cryptography

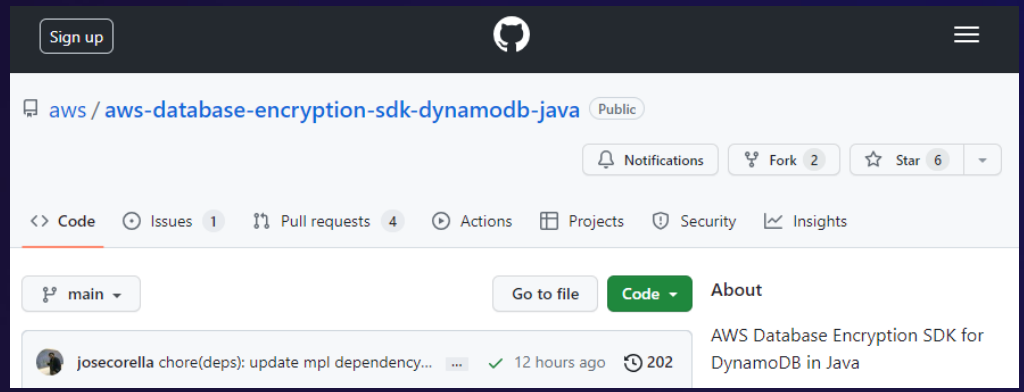
AWS Payment Cryptography のユースケース

- 機密データの暗号化と復号、内容の検証
- PIN の取り扱い (PCI PIN, DUKPT, BDK)
- データ復号 (PCI P2PE)
- MAC の生成と検証

AWS Database Encryption SDK の発表

プレビュー

- Amazon DynamoDB におけるクライアントサイド暗号化を容易に実現するためのソフトウェアライブラリのセット
- DynamoDB テーブル保存前の属性値単位の暗号化が簡易に実現可能
  また、暗号化データの属性値検索を実現
- AWS Key Management Service と統合し暗号鍵の制御を実現
- 全リージョンでプレビューの利用が可能



インシデントへの対応

Findings Groups for Amazon Detective を拡張

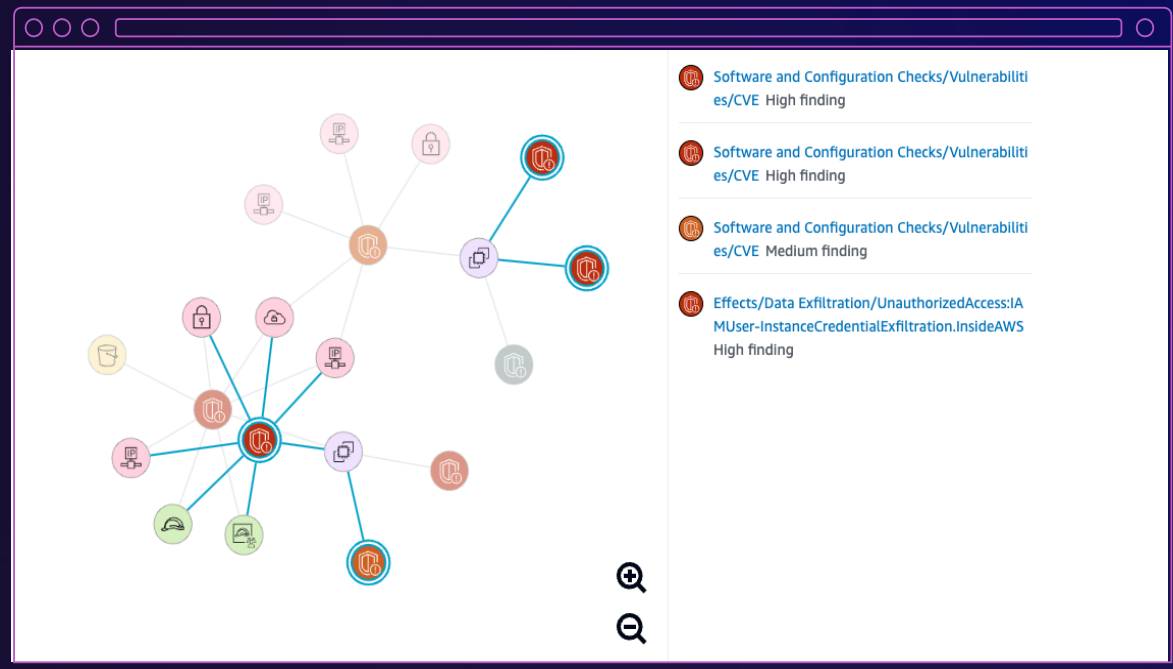
一般利用開始

- Amazon Detective は、Amazon Inspector のネットワーク到達可能性とソフトウェアの脆弱性の検出結果を含めるように検出結果グループを拡張

- Amazon GuardDuty で検出した脅威に加え、脆弱性情報も含まれるため、EC2 インスタンスで検出された脅威の原因が脆弱性かどうかといった調査を迅速に実現
- Amazon Detective を利用可能な全てのリージョンで利用可能

Amazon Detective - Findings groups の例

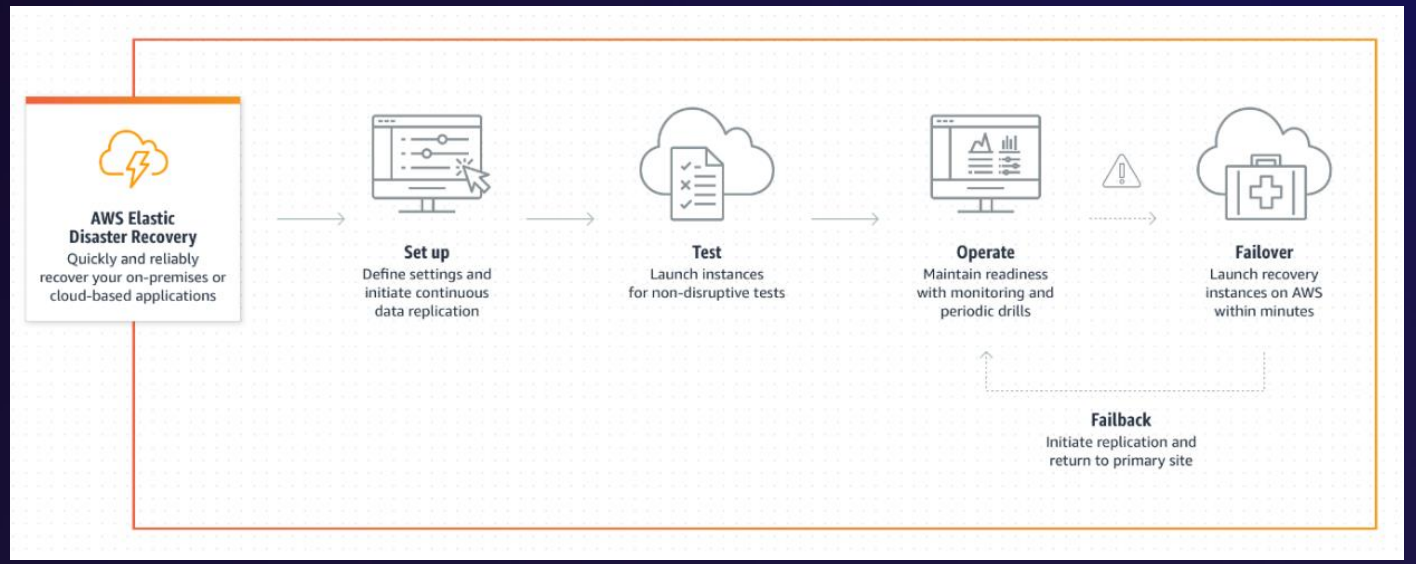
- 1 つのセキュリティイベントによって影響を受けた、全てのリソースの検出結果を可視化
- 全ての詳細情報、コンテキスト、アクティビティ履歴を一元化し、根本原因特定をサポート
- Amazon Inspector の検出結果を取り込み、ソフトウェア脆弱性や意図しないネットワーク露呈を Amazon GuardDuty や AWS リソースと関連付けて表示



一般利用開始

AWS Elastic Disaster Recovery (DRS) が VPC configurations recover を追加

- セキュリティグループ、NACL といったネットワーク構成に対応
- さらに、AWS DRS 関連のアクセス権限を一元的に設定、監視できる Trusted Account 機能を追加
- 迅速な復旧を実現し、データ損失のリスクを軽減
- 東京、大阪を含む各リージョンで一般利用可能



コンプライアンス

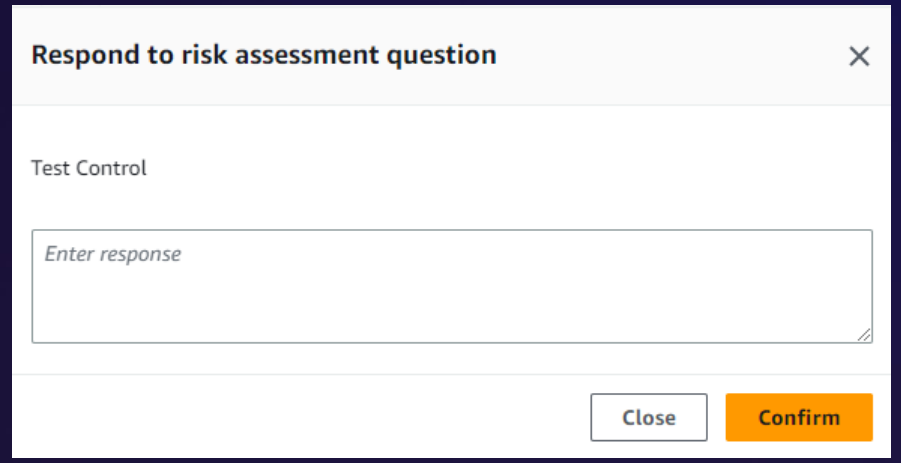
一般利用開始

AWS Audit Manager
第三者リスクアセスメントと CSV 出力をサポート

- 第三者による固有のリスク評価（質問票など）に対して、
テキストによる回答、エビデンス収集をサポート
全てのエビデンスは、エビデンスファインダーを通じて、
CSV ファイルとしてエクスポートが可能に

- カスタマイズされた質問を利用した、組織固有のリスク評価を実現
エクスポートによって、リスク評価やエビデンスの
関係各所への連携が可能

- AWS Audit Manager が利用可能な
全リージョンで一般利用可能



まとめ

まとめ

カテゴリ	新サービス・アップデート
ID およびアクセス管理	- Amazon Verified Permissions - AWS IAM Identity Center supports Google Workspace
検出	- Amazon Inspector code scanning - Amazon Inspector SBOM - Amazon CodeGuru Security - AWS Security Hub Automation Rules - Amazon GuardDuty Summary View - AWS CloudTrail Lake dashboard for top trends - Amazon ECR Basic Scan supports CVSS v3
ネットワークとアプリケーションの保護	- WAF Account Creation Fraud Prevention - Amazon EC2 Instance Connect Endpoint
データ保護	- AWS Payment Cryptography - AWS Database Encryption SDK
インシデントへの対応	- Amazon Detective finding groups - AWS DRS VPC configurations recovery
コンプライアンス	- AWS Audit Manager third-party risk assessment / CSV

Thank you!