CloudShift

Stylez

株式会社スタイルズ

2022年1月18日

30分でわかる！
Amazon Inspectorで脆弱性診断

aws partner network

aws partner network Advanced Consulting Partner

RANCHER PARTNER NETWORK

ZABBIX CERTIFIED PARTNER

Nextcloud Gold partner

vmware PARTNER PROFESSIONAL SOLUTION PROVIDER

自己紹介

- 馬場 潤一（Junichi Baba）
- 株式会社スタイルズ
  - AWS上でのアプリ開発・インフラ構築
    チームリーダー
- 好きなAWSサービス
  - CloudFormation、Systems Manager、ECS(Fargate)

本日、お話しする内容

対象

- AWS上でサーバの脆弱性診断の実施を検討されている方
  （初級者向け：脆弱性診断がどういうものかあまり分からない方向け）
- Amazon Inspectorを導入しようか検討されている方

ゴール

- Amazon Inspectorはどのようなサービスなのかを理解する
- Amazon Inspectorの基本的な利用方法を理解する

脆弱性診断とは

脆弱性とは

➢ 脆弱性（ぜいじゃくせい）

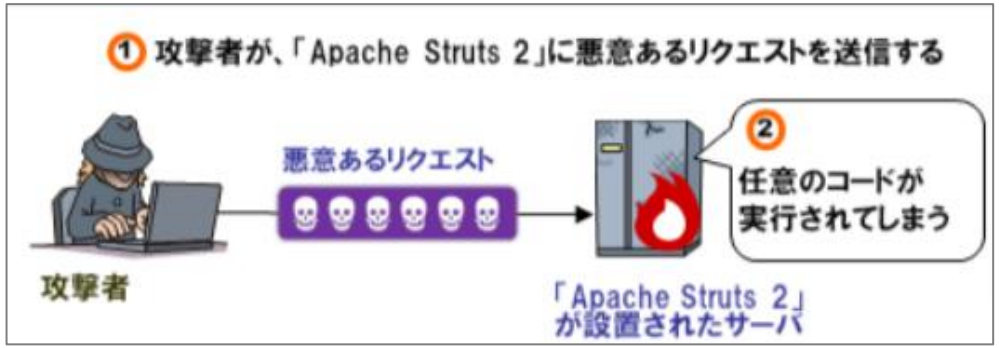
情報漏洩等

・OS、ミドルウェア、Webアプリケーション、ネットワークに潜むセキュリティ上の欠陥
・脆弱性のある部分に対して攻撃を仕掛けることで、本来できない操作が可能になってしまう

◆ 例：[CVE-2017-5638] Apache Struts2 に任意のコードが実行可能な脆弱性

・Javaのウェブアプリケーションを作成するためのソフトウェアフレームワーク
・ファイルアップロード処理に起因して、リモートで任意のコードが実行される脆弱性

[CVE-xxx] ：共通脆弱性識別子（CVE番号）



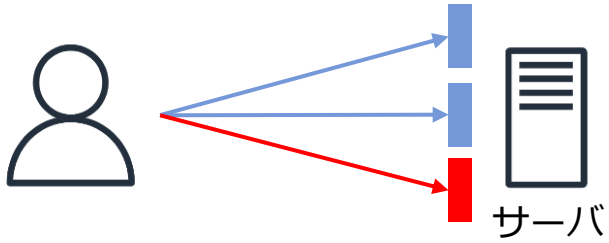
スタイルズ：レガシーJAVAをリニューアル
https://www.stylez.co.jp/java-renew/

画像引用：https://www.ipa.go.jp/security/ciadr/vul/20170308-struts.html

脆弱性診断とは

脆弱性診断

・システムに対し、攻撃につながる脆弱性がないかを確認するセキュリティテスト
・網羅的に確認をし、セキュリティリスクを発見することが目的

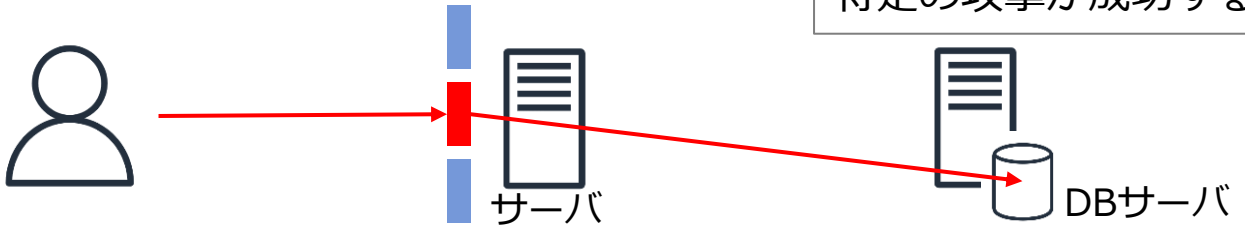


網羅的に攻撃のきっかけとなる入口を見つける

ペネトレーションテスト（侵入テスト）

・特定の攻撃シナリオを元に、どこまで被害を受けるかを確認するセキュリティテスト
・特定の攻撃に対する耐性を確認することが目的

特定の攻撃が成功するか確認



脆弱性診断の必要性

➢ 脆弱性診断はなぜ必要なのか

・攻撃されうる箇所を特定し、具体的な対策を講じるため

➢ 脆弱性診断の実施頻度

・頻度が多い方が望ましい（ただし費用と運用ルール次第）

いつ新たな脆弱性が発覚するかわからないため

・診断サービスを利用する場合、たいてい実施回数毎に費用がかかる

・発覚した脆弱性への対策は基本的に手動となる。
対策後に再チェックするケースが多い印象。

Amazon Inspector

Amazon Inspectorとは

➢ AWSが提供する脆弱性検出サービス

【コンテナイメージ】
Dockerを始めとするアプリ仮想化技術において、
アプリを動作させるための環境イメージ

- 2021年11月末にv2がリリース　New！
- EC2インスタンスとECRコンテナイメージを対象に脆弱性を検出、可視化
- インスタンス内のパッケージ情報を収集し、脆弱性に該当するかを判断

yumやaptで管理されていないプログラムは検知対象外

- EC2における検知はSSM（Systems Manager）エージェント＆IAMロールが必要

Amazon Linuxはプリインストール済
Inspector v1は専用エージェントが必要

Systems Manager の IAM インスタンスプロファイルを作成する
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/setup-instance-profile.html

Amazon Inspectorとは

スキャンのタイミング(EC2)

・Inspectorによりインスタンスが検出された
・新しいインスタンスを起動した
・既存のインスタンスに新しいソフトウェアがインストールされた
・Inspectorが新たなCVE情報を追加

Inspector v1は定期的 or 手動で実施

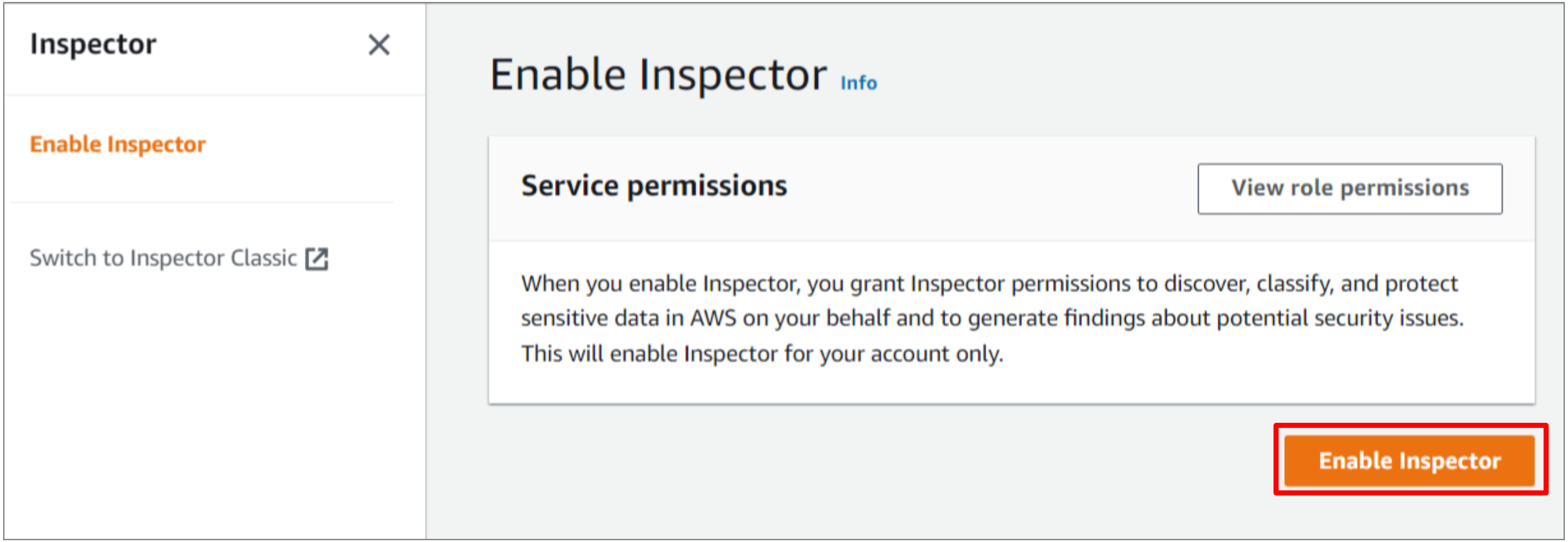
料金

【EC2】
・スキャンされたEC2インスタンス平均数 x $1.512

1ヵ月=720時間/1インスタンス として、
スキャンが有効である稼働時間数の合計

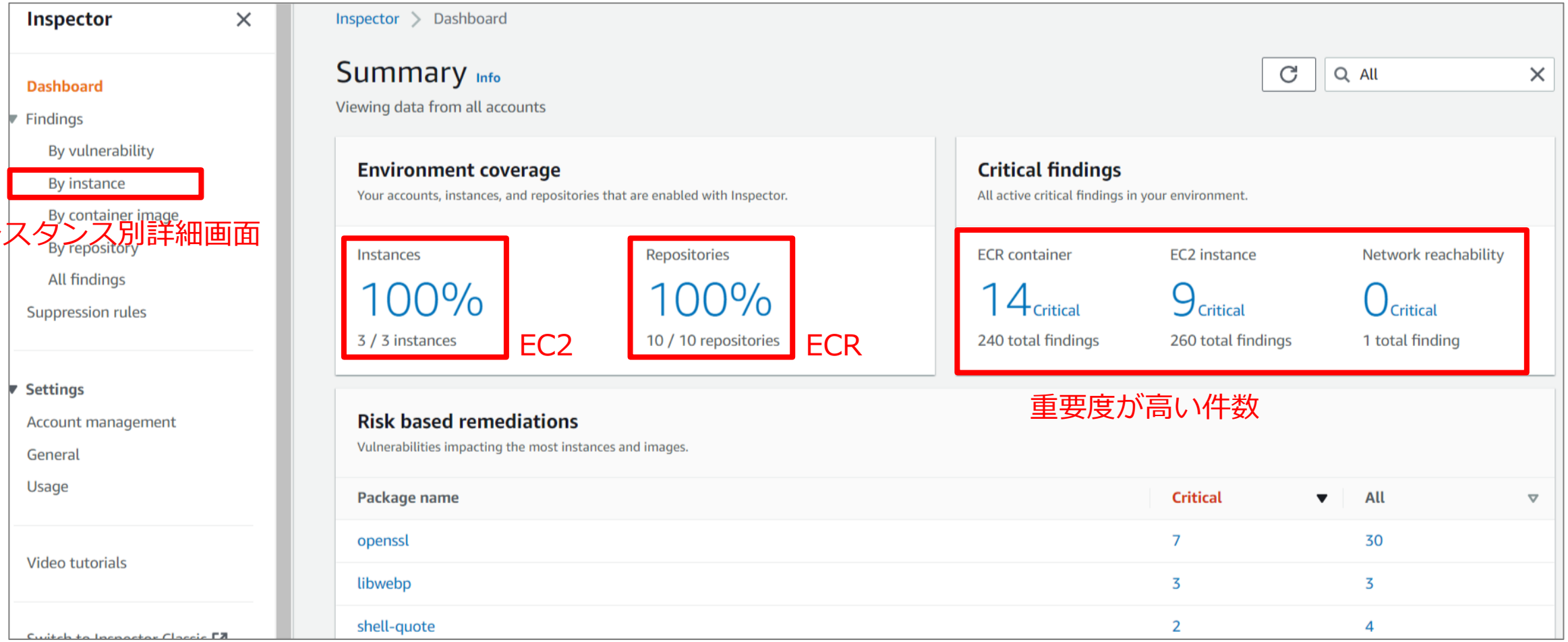
【ECR】
・スキャンされたコンテナイメージ数 x $0.11
・自動再スキャン回数 x $0.01

Amazon Inspectorの有効化



v1はスキャン対象設定を行う必要があったが、
v2は有効化のみでスキャンが開始される。

有効化後のダッシュボード画面



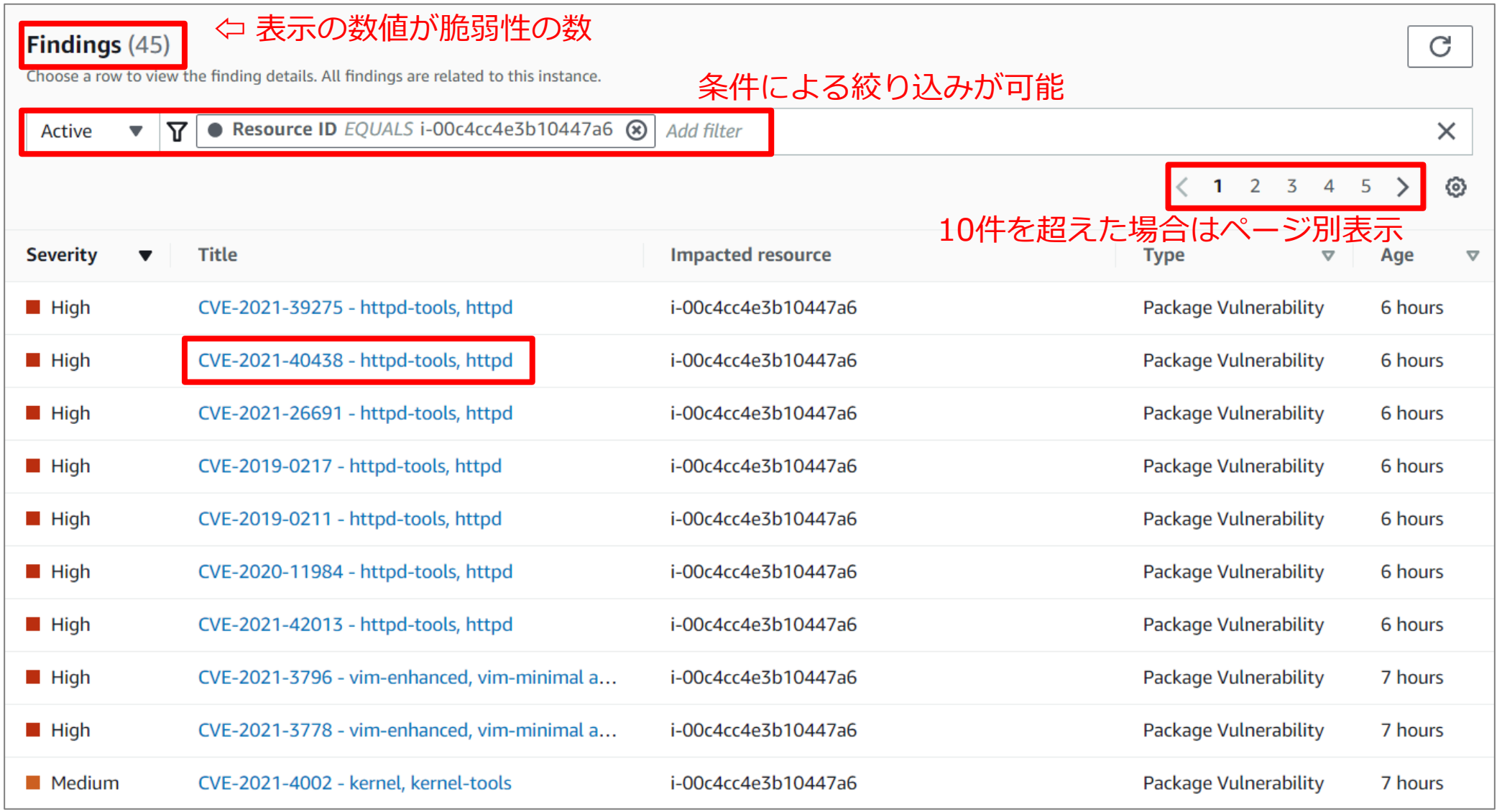
インスタンス別表示画面

① 2年前に利用した後、停止していたインスタンス

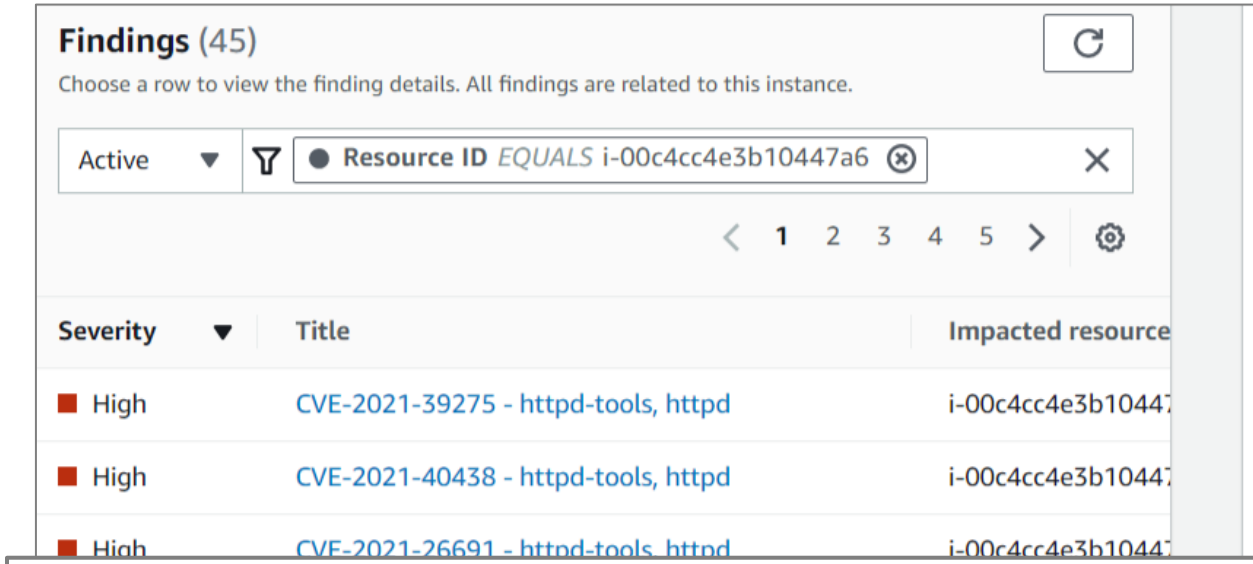
② 最新のAmazon Linux2の素の状態

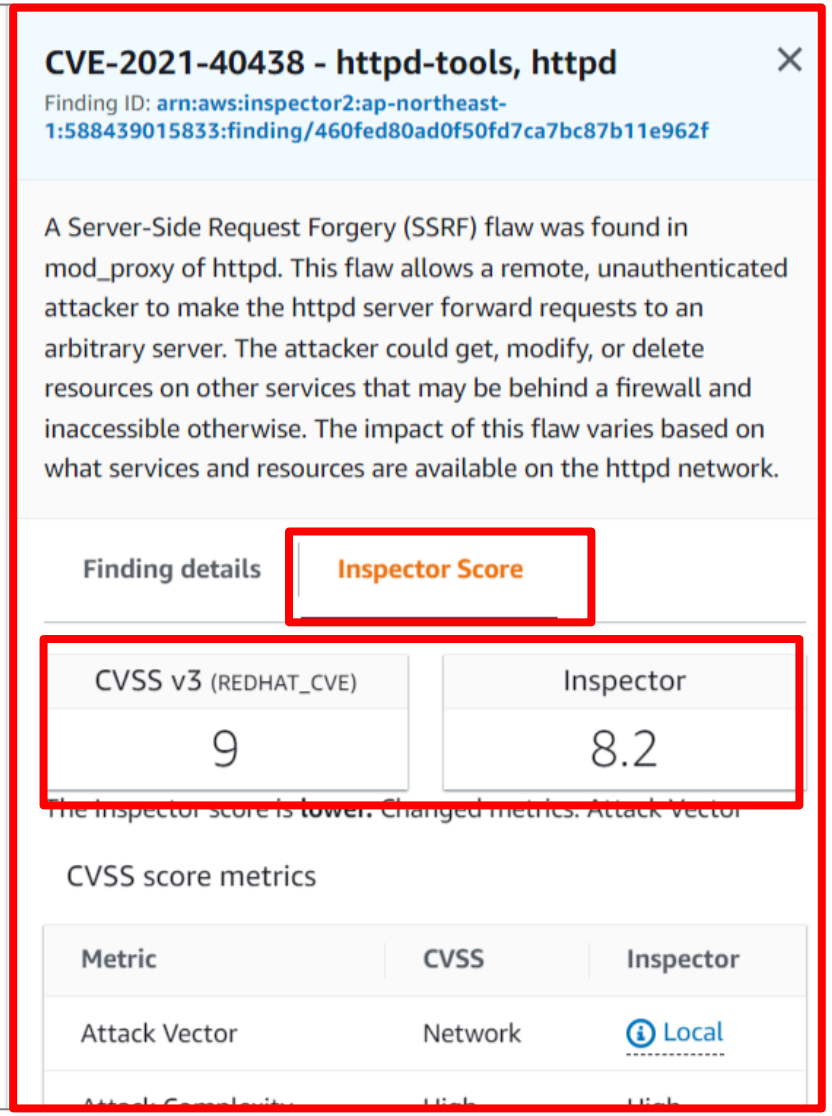
③ 最新のAmazon Linux2に少し古いhttpd(Apache)をインストール

特定EC2インスタンスの詳細画面



特定CVEの詳細画面





■ 10段階評価
- 10に近いほど深刻度が高い

■ CVSS v3
- 共通脆弱性評価システム（世界で標準的に利用）
- 深刻度を定量的に評価したスコア

■ Inspector
- ネットワーク到達可能性、悪用可能性、CVEを加味したスコア

特定CVEの詳細画面

Remediation

Red Hat has investigated whether a possible mitigation exists for this issue, and has not been able to identify a practical example. Please update the affected package as soon as possible.

改善
Red Hat は、この問題に対して可能な緩和策が存在するかどうかを調査しましたが、
実用的な例を特定することはできませんでした。
できるだけ早く該当するパッケージを更新してください。

⇨ yum update http といったコマンドを実行し対処

アップデートにより、システムが想定通りの挙動をしなくなる可能性もあるので、
事前に動作検証の実施を推奨。

ケースによりコメント内容は様々。
設定値レベルの対処を推奨されるケースや対処自体が記載されないケースもある。

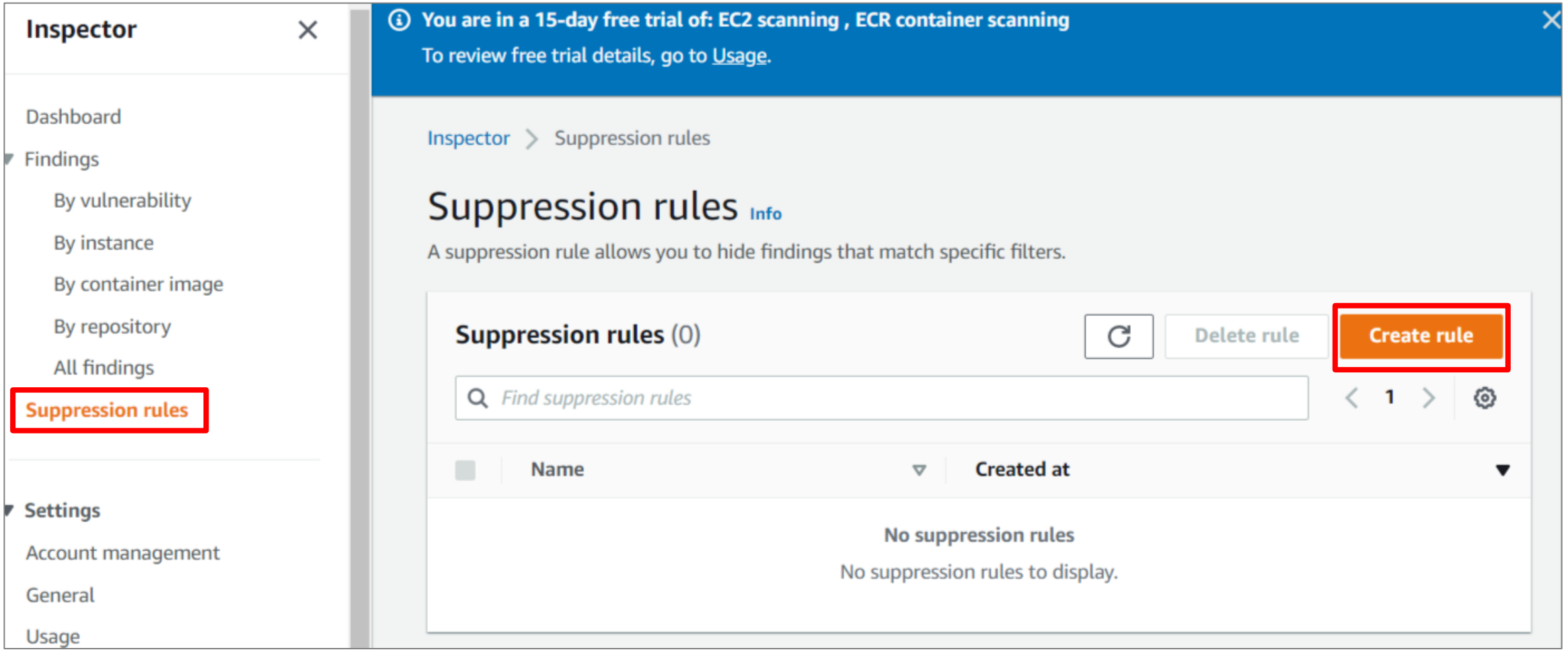
表示の抑制

➢ 検出された脆弱性全てを対応しないといけないということではない

・ソフトウェアとしては脆弱性が存在するが、設定値や構成次第では無害となる場合。
・ポリシー上、重要度が高いものだけ対応したい。

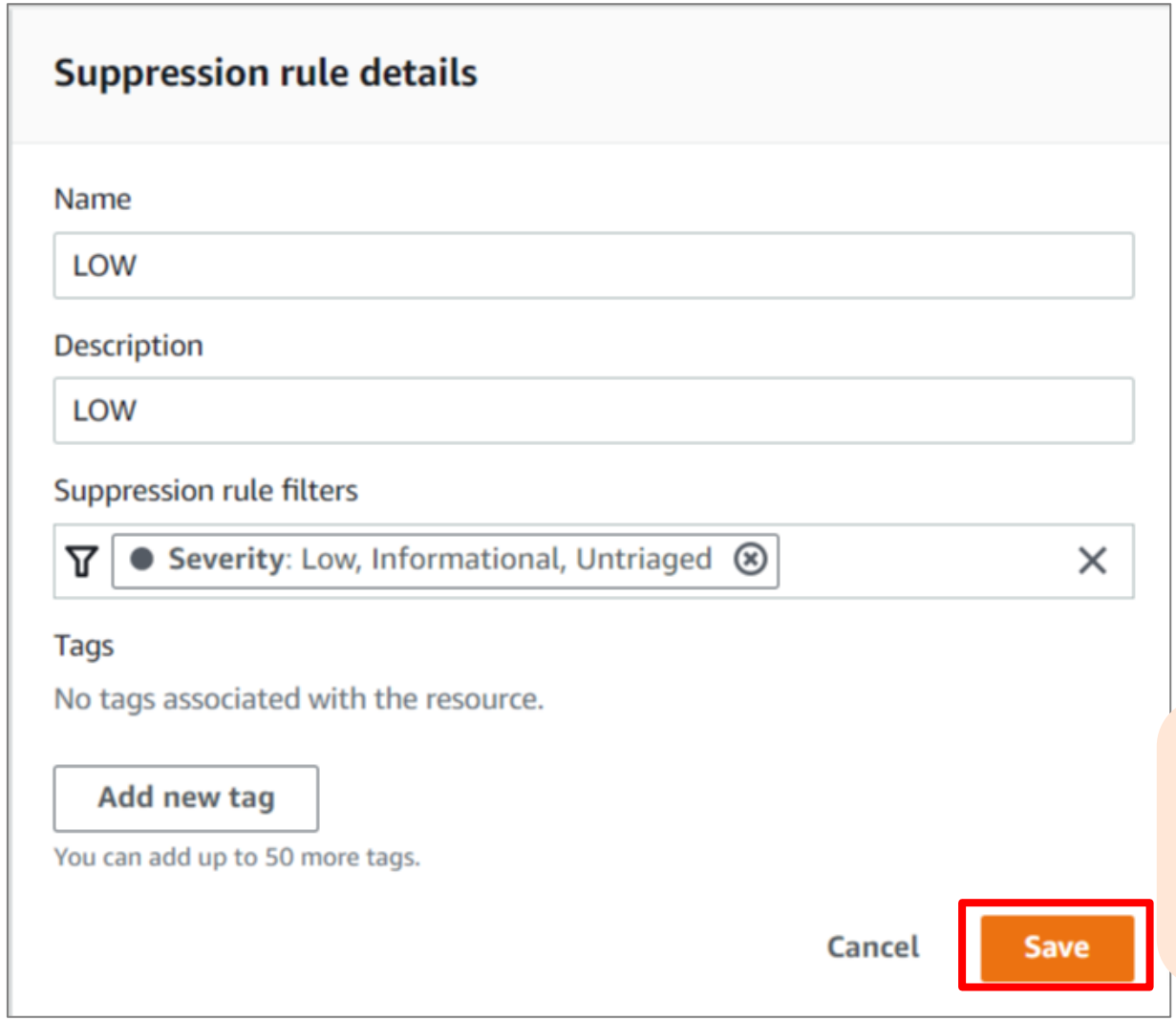
一覧から対応不要な脆弱性情報を非表示にしたい。

表示の抑制



表示抑制ルールの管理画面

表示の抑制



重要度Low(低)を除外するルール

Name：LOW
（ルール表示上の名称、任意の文字列で良い）

Description：LOW
（ルール表示上の名称、任意の文字列で良い）

Suppression rule filters：Severity：Low

重要度以外にも様々な条件で指定可能。
- 件名
- CVE番号
- パッケージ名
- スコア　　Etc…

表示の抑制


Findings (45)
Choose a row to view the finding details. All findings are related to this instance.
Active
Resource ID EQUALS i-00c4cc4e3b10447a6
Add filter
Findings (38)
重要度Low以下の表示抑制により、件数が減った
Choose a row to view the finding details. All findings are related to this instance.
Active
Resource ID EQUALS i-00c4cc4e3b10447a6
Add filter

まとめ

まとめ

脆弱性診断とは

- 脆弱性とはOSやアプリケーション等に潜むセキュリティ上の欠陥
- 脆弱性診断とはシステムに対して脆弱性があるかどうか網羅的に確認するテスト
- 高頻度で再確認をした方が望ましいが、費用や運用に合わせて実施するとよい

Amazon Inspector

- サービスの有効化
- 検出された脆弱性の確認方法
- 表示の抑制方法

実績豊富なエンジニア集団の技術と開発ツールで「開発期間/コスト削減」「品質向上」を実現

株式会社スタイルズ

https://www.stylez.co.jp

東京都千代田区神田小川町1-2　風雲堂ビル6階

Tel:03-5244-4111

オープンソースソフトウェア推進