ちょっぴりDD

Amazon CodeGuru Securityの紹介

Masahiro Eguchi

ISV / SaaS SA
AWS Japan G.K

自己紹介

- 江口昌宏（えぐちまさひろ）
- 所属
  - ISV / SaaS SA
  - ソフトウェアベンダーや SaaS 事業者の支援
- 好きなAWSサービス
  AWS Lambda
- 最近買ったモノ
  ヒゲトリマー

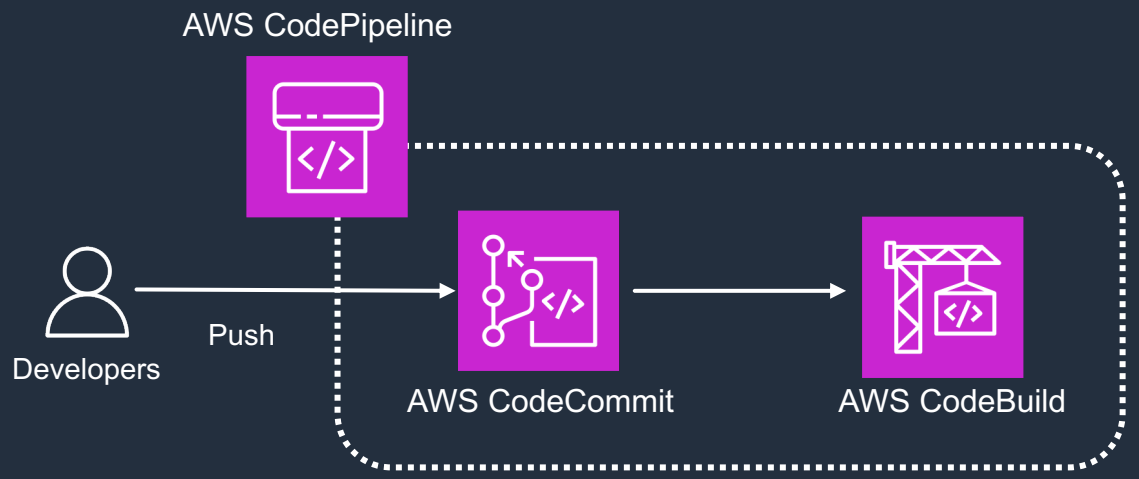
早速ですが
「デモ祭り」なので

デモの説明

Amazon CodeGuru Security

脆弱性を検知するサービス

デモ内容



- Amazon CodeGuruSecurity 専用の AWS CodeBuild プロジェクトを実行して脆弱性がどのように検出されるかデモでお伝えします
- CI/CDパイプラインへの組み込みについては後ほどお伝えします。
- デモ内では検出を目的とした、脆弱性が存在するコードを投影しています
- ソースコードの取り扱いについてはご注意ください。

CodeGuru

- セキュリティ
  - ダッシュボード
  - 統合
  - スキャン
  - 検出結果
  - フィードバックを送信
- プロファイラー
  - グループのプロファイリング
- レビュー担当者
  - CI ワークフロー
  - リポジトリ
  - コードレビュー
- BugBust
  - 開始方法
  - イベント
  - プレイヤーポータル

新着情報

ダッシュボード 情報

.pdf をダウンロード

検出結果の概要

最終更新日: September 1, 2023, 10:44 (UTC+09:00)

未解決の重要な検出結果

データは週ごとに比較されます。

未解決の検出結果の合計

0 ▼ 100% 前週から減少

重要な未解決の検出結果

0 ▼ 100% 前週から減少

重要度の分布

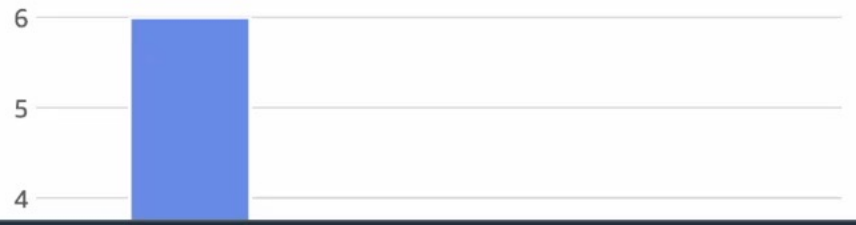
すべての未解決の検出結果における重要度の全体的な分布。

すべての検出結果を表示

脆弱性の評価

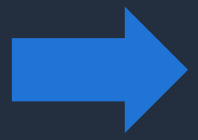
最も多くの検出結果を生成した脆弱性。

検出結果



Amazon CodeGuru Security とは

- 機械学習 (ML) と自動推論を組み合わせた静的アプリケーションセキュリティ検査 (SAST) ツールです。
- コードの脆弱性を特定し、特定された脆弱性を修正する方法に関する推奨事項を提示します。
- CI/CD パイプラインへの組み込みが可能で、アプリケーションの脆弱性検出に役立てることが可能です



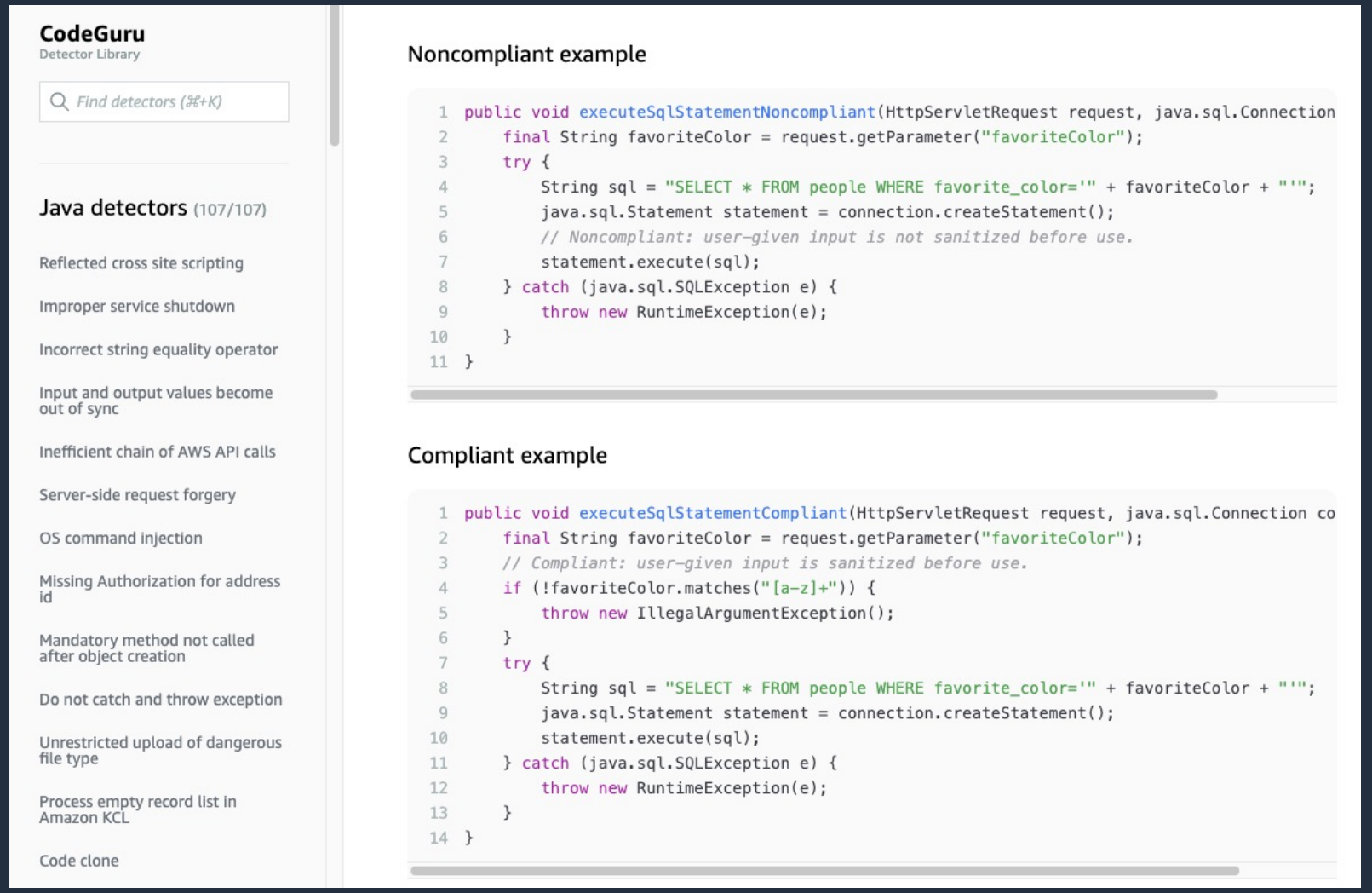
開発者や、プルリクエスト時のコードレビュワーが注意すべき「アプリケーションコードの脆弱性」を検出するのに役立ち、開発者やレビュワーの負担軽減となります。

どのような内容の脆弱性を検査しているのか

- Java, Python, JavaScript コードのセキュリティ脆弱性を検出することが可能
- コードを改善するための推奨事項を提示
- ハードコードされた認証情報をスキャンできる
- OWASP の上位10件の脆弱性（アクセスコントール、インジェクション）
- CWEの上位25件の問題（クロスサイトスクリプティング、SQLインジェクション、OSコマンドインジェクション、CSRF …）
- ログインジェクション、シークレット、AWS API と SDK の安全な使用について検出

https://aws.amazon.com/jp/codeguru/features/
より

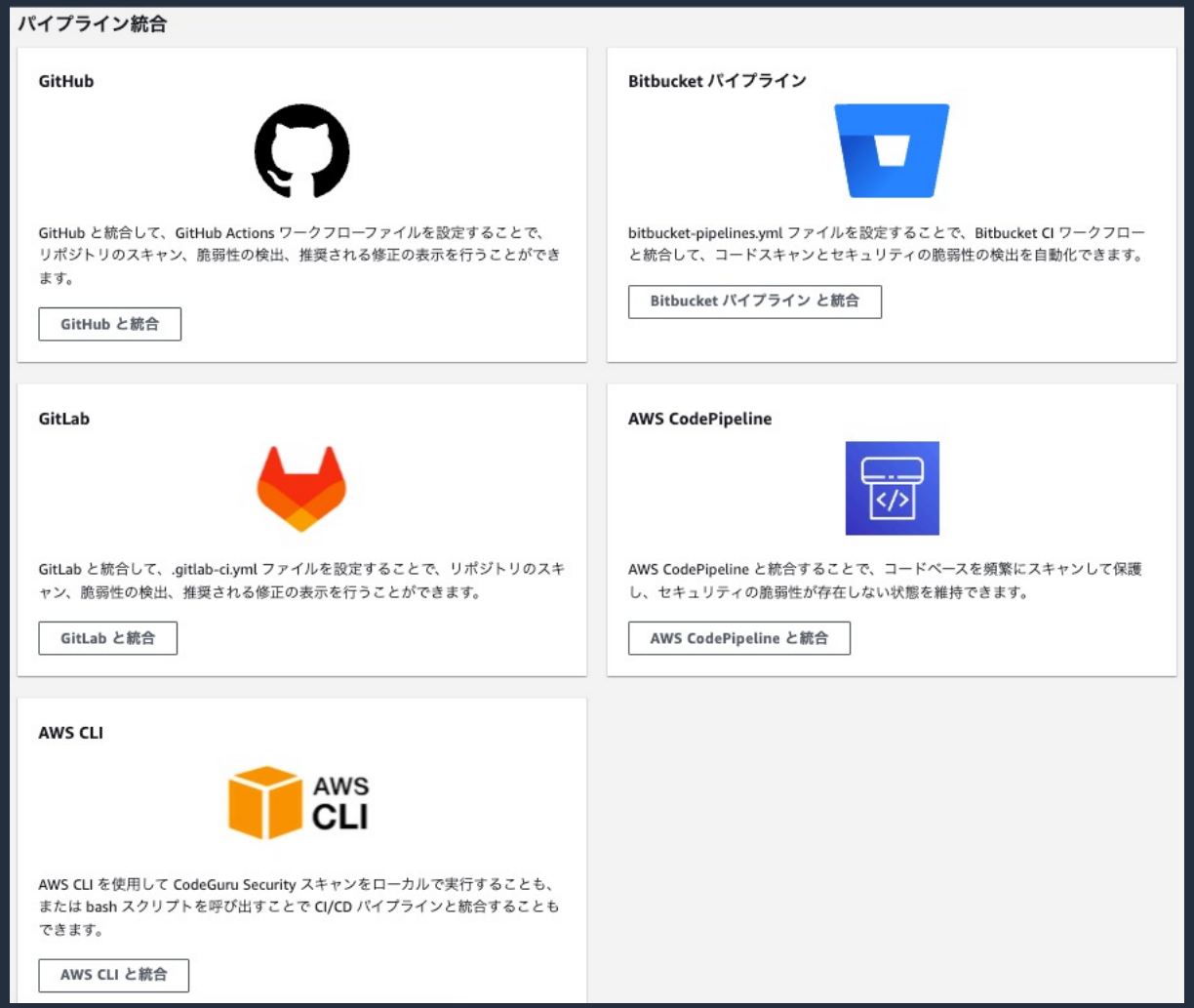
より具体的に



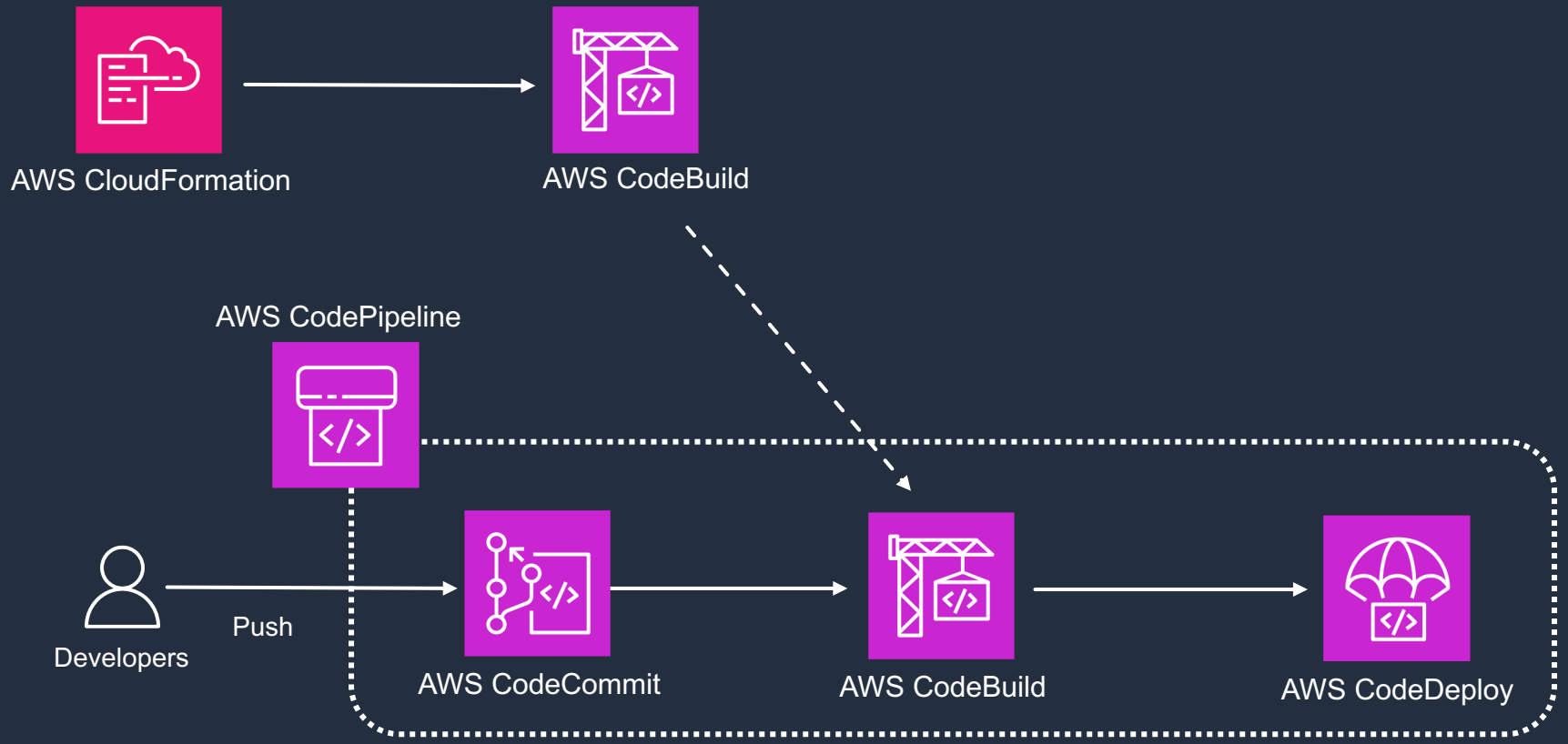
https://docs.aws.amazon.com/codeguru/detector-library/index.html

CodeGuru Security ダッシュボード

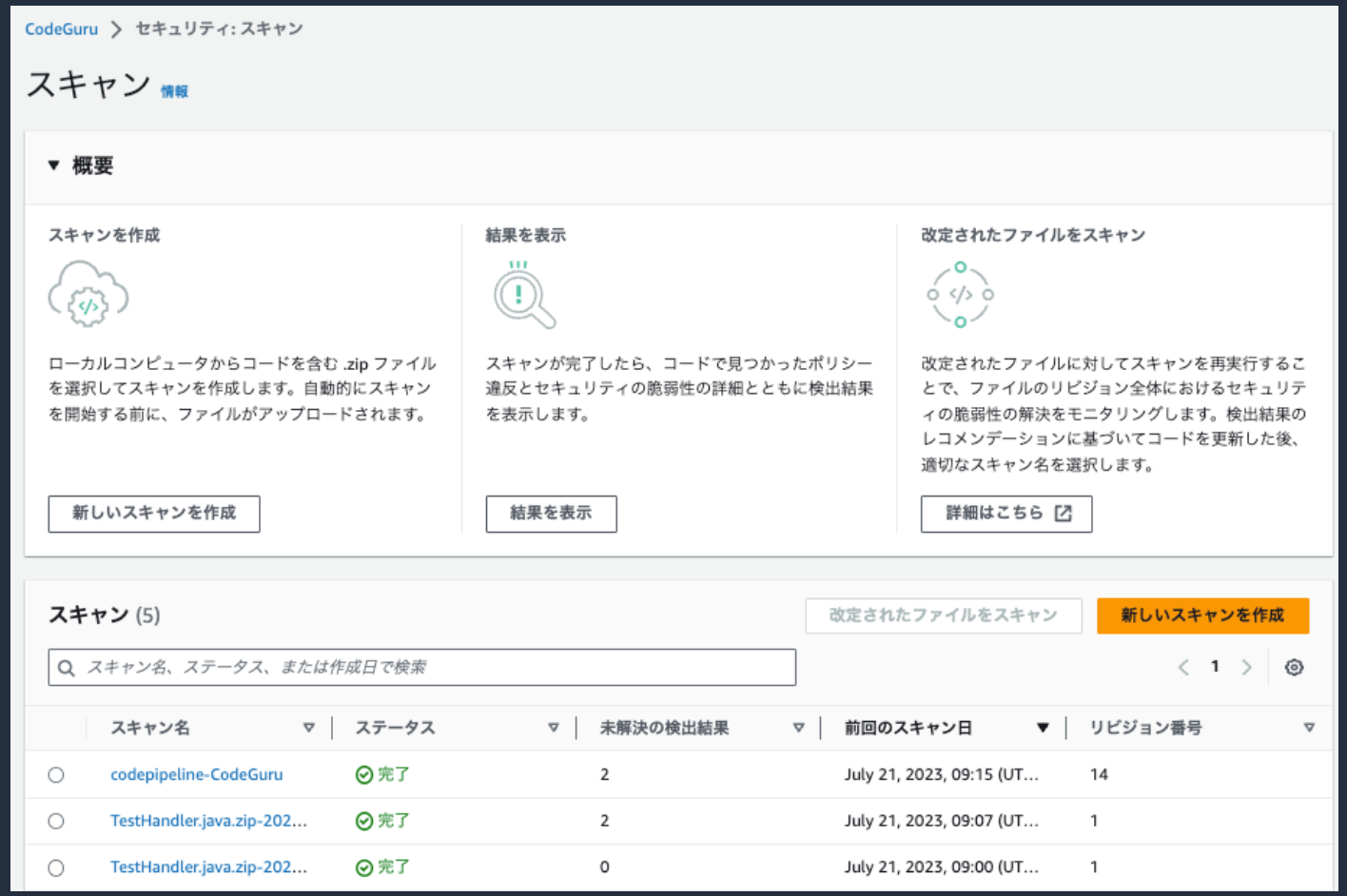
パイプライン統合



AWS CodePipelineとの統合



ファイルアップロードでのスキャンにも対応



まとめ

- ✓ Amazon CodeGuru Security
  - ✓ アプリケーションコードの脆弱性を検出するツール
  - ✓ CI/CDパイプラインへの組み込み等も可能
  - ✓ 活用することで開発者、レビュワーの負担軽減につながる
  - ✓ Amazon CodeGuru Securityの画面から検出された脆弱性の一覧を確認できるのでセキュリティ担当者にとっても活用可能
  - ✓ 2023年9月現在はパプリックプレビュー中につき無料で利用可能
  - ✓ 2023年9月現在の対応言語は Java, JavaScript, Python の3つ

Thank you!