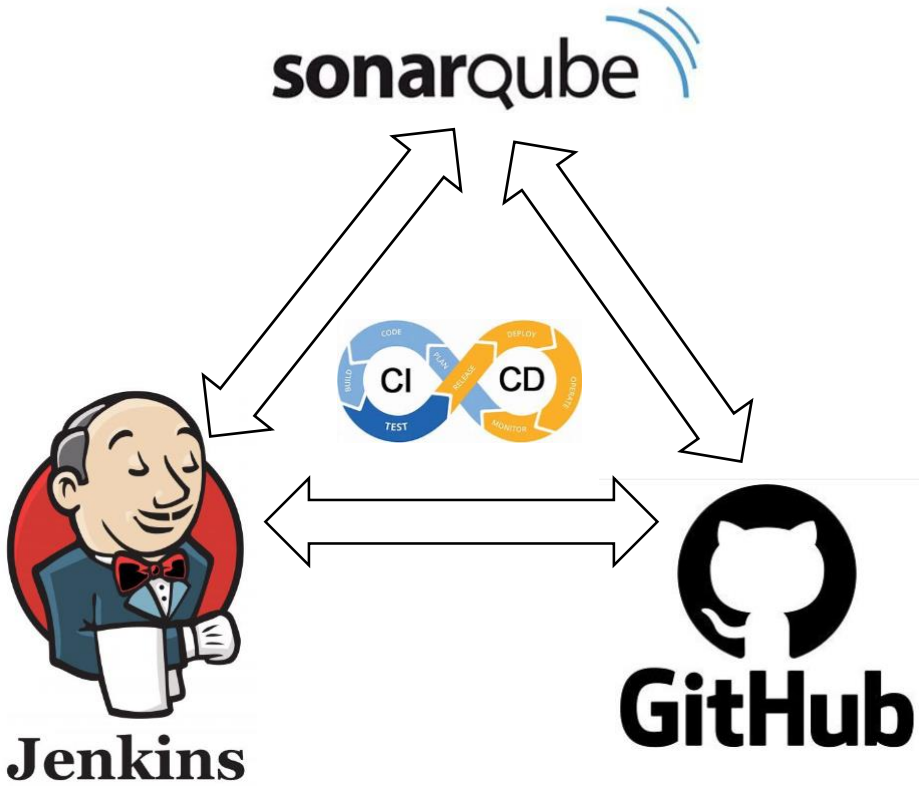
SonarQubeをCICDとの連携



https://github.com/sean-akatsuki/101.demo_sonarqube_cicd

AGENDA

1. 静的コード分析紹介
2. 静的解析とCICD現状
3. 今回研究目標について
4. SonarQube紹介
5. ツール、構築、展示、トラブルシューティング
6. そのた(Prototype展開＆GHASとの比較)

1.静的コード解析紹介

静的コード解析とは、コードを実行せずにコードの品質、信頼性、および、セキュリティの検証を行う作業、静的解析を行うと、アプリケーションの安全性とセキュリティを損なう可能性のあるバグとセキュリティの脆弱性を開発の早い段階で特定できます。静的解析は、テストケースの作成を行うことなく網羅的、かつ、短時間でコードの品質を確保する費用対効果の高いアプローチです。

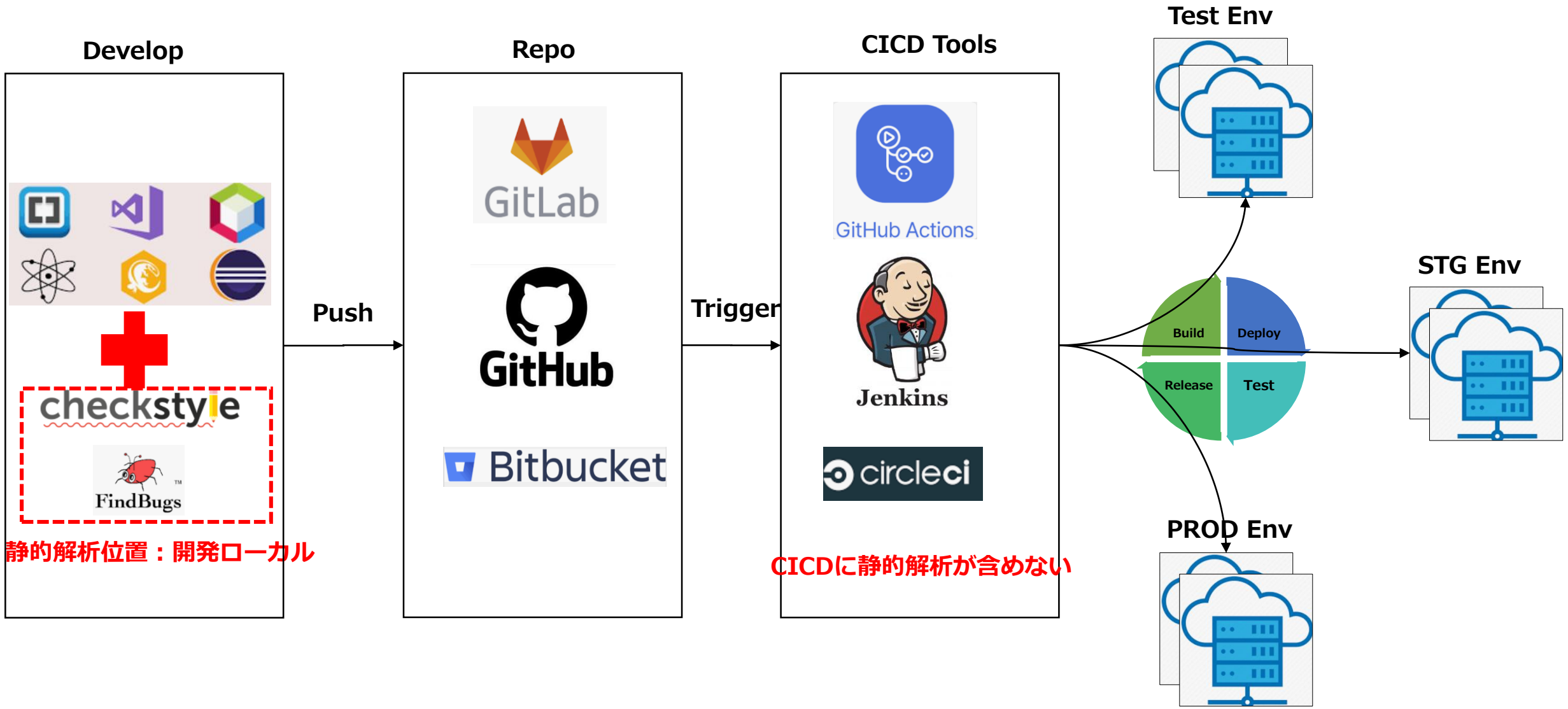
アプリケーションのセキュリティの分野では Static Application Security Testing (SAST) という用語が使われている。

利点
・エラー検出
・低コスト
・コーディング標準への準拠(コードの可読性や保守性が向上)

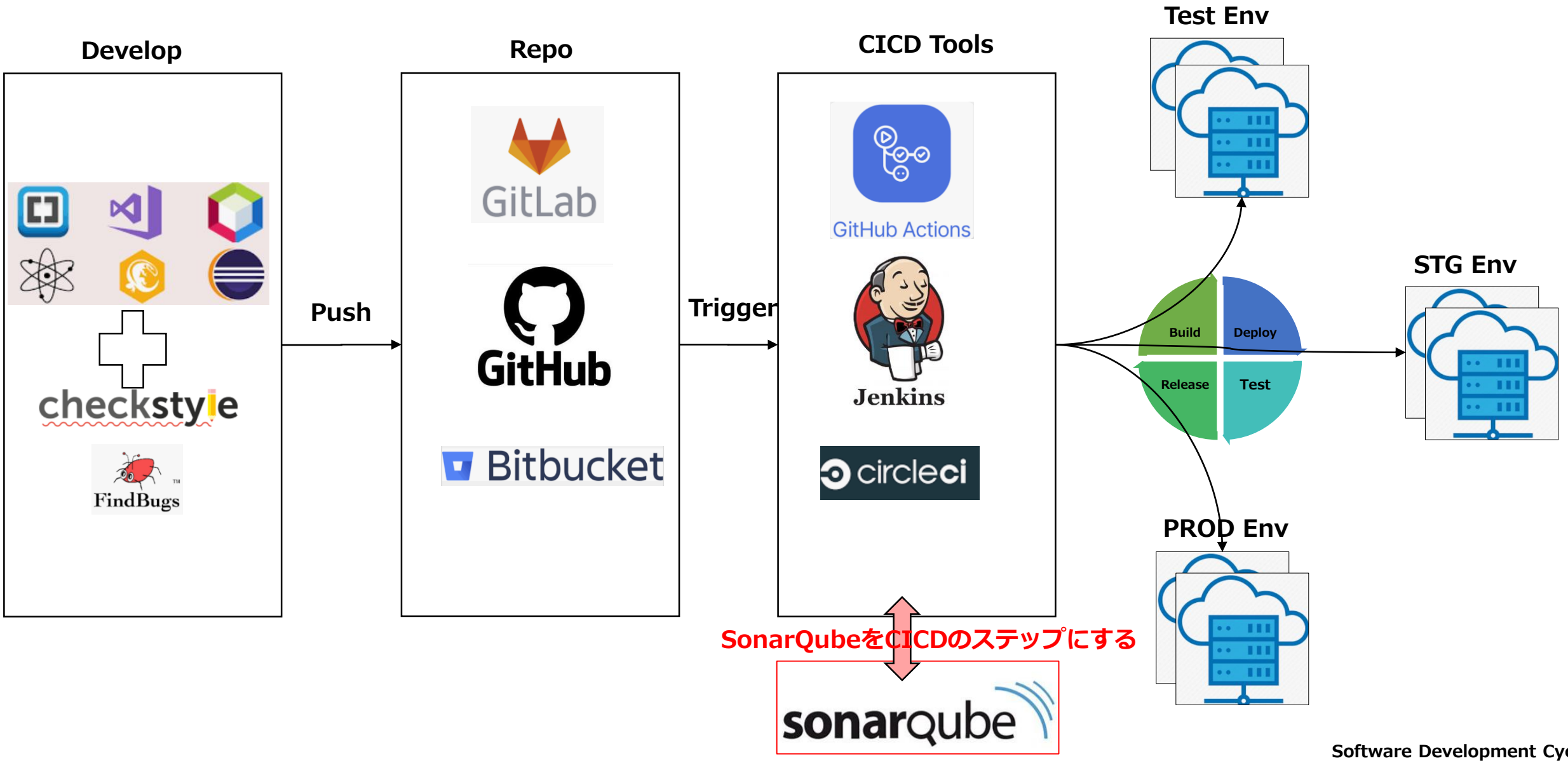
ツール
・anyWarp CodeDirector for C/C++
・PyChecker(Python)
・Sider(JavaScript,Php, Py)
・Checkstyle(Java)
・FindBugs(Java)
などなど

運用
(複雑・高度な ソフトウェア開発で活用)
・医療用ソフトウェア
・原子力関連のソフトウェア
・自動車機械ソフトウェア
・航空防衛

2.静的解析とCICD現状



3.今回研究目標



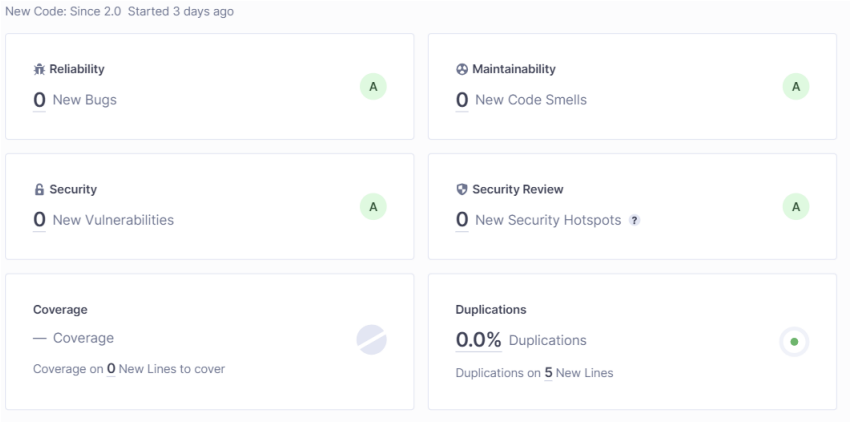
Software Development Cycle

4.SonarQube紹介

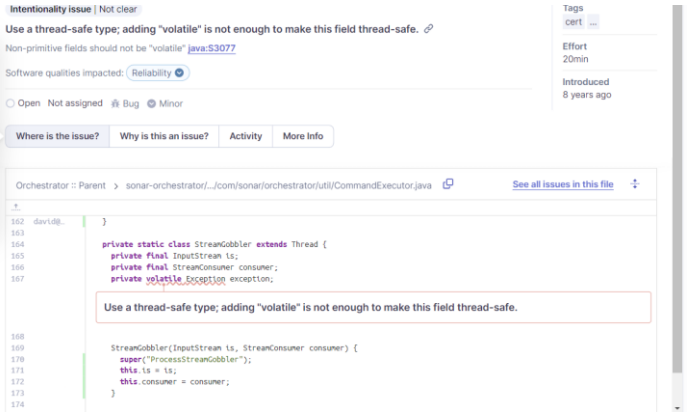
sonarqube
the code quality tool for better code

SonarQubeは、SonarSourceが開発したオープンソースのプラットフォームで、コード品質を継続的に検査し、30以上のプログラミング言語のバグやコードのにおいを検出するために、コードの静的分析による自動レビューを実行します。SonarQube は、重複コード、コーディング規約、単体テスト、コードカバレッジ、コードの複雑さ、コメント、バグ、およびセキュリティに関する推奨事項に関するレポートを提供します。

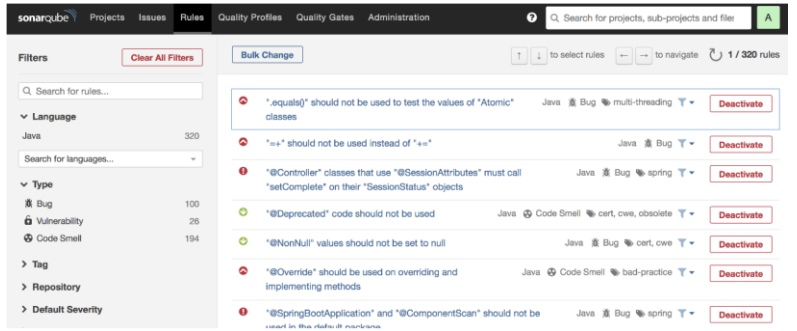
SonarQube は、Maven、Ant、Gradle、MSBuild および継続的インテグレーション ツール (Atlassian Bamboo、Jenkins、Hudson など) との完全に自動化された分析と統合を提供します。



結果レポート



バグ/脆弱性箇所提示



ルールカスタマイズ

4.SonarQube紹介

sonarqube
the code quality tool for better code

Sonar製品一覧

Sonarlint : SonarQube は、プラグインを使用して拡張できます。SonarLint プラグインを介して、Eclipse、Visual Studio、Visual Studio Code、IntelliJ IDEA 開発環境、および LDAP、Active Directory、GitHub などの外部ツールと統合されます。

SonarQube(Self-Managed) : オンプレミスで構築、四つのEdition

- Community Edition-Free and Open Source
- Developer Edition
- Enterprise Edition
- Data Center Edition

SonarCloud : SonarQube As A Service、簡易にクラウドDevopsプラットホームとCICDワークフローに統合できる

四つのEdition間機能差別↓

All of the following features:	Community Edition plus:	Developer Edition plus:	Enterprise edition plus:
Static code analysis for 19 languages: Java, C#, JavaScript, TypeScript, CloudFormation, Terraform, Docker, Kubernetes, Kotlin, Ruby, Go, Scala, Flex, Python, PHP, HTML, CSS, XML, VB.NET and Azure Resource Manager	Support for C, C++, Obj-C, Swift, ABAP, T-SQL and PL/SQL	Support for Apex, COBOL, PL/I, RPG and VB6	Component redundancy
Detect Bugs & basic Vulnerabilities	Detection of advanced vulnerabilities including Injection Flaws in Java, C#, PHP, Python, JavaScript, TypeScript	Portfolio Management & PDF Executive Reports	Data resiliency
Review Security Hotspots	Detection of advanced bugs causing runtime errors and crashes in Python & Java	Project PDF reports	Horizontal scalability
Track Code Smells & fix your Technical Debt	Analysis of feature and maintenance branches	Security Reports	
Code Quality Metrics & History	Pull request analysis and decoration in the following DevOps platforms: GitHub, Bitbucket, Azure DevOps and GitLab	Regulatory Reports to record state & quality of release	
CI/CD integration		Project Transfer	
Extensible, with 50+ community plugins		Parallel processing of analysis reports	

5.ツール、構築、展示、トラブルシューティング

1. ツール

2. 構築手順

https://github.com/sean-akatsuki/101.demo_sonarqube_cicd/blob/main/EnvSetup.md

3. 効果展示

別途展示

4. トラブルシューティング

SonarQubeのコード解析機能ElasticSearchの稼働で大量のメモリを使用する、構築手順をご参考ください。

6.そのた

1. ソリューション向かって本自由研究をプロトタイプとしての展開

Jenkins → GitHub Action, Circle CI, Jira
GitHub → Bitbucket, Gitlab
SonarQube → GitHub Advanced Security

2. SonarQubeとGitHub Advanced Security(CodeQL)の比較

Tool	統合	分析能力と精度	言語サポートと互換性	パフォーマンスと拡張性	適用シナリオ
SonarQube	・サーバーへのインストールと構成 ・Jenkins や Azure DevOps などの CI/CD パイプラインとの統合を提供	・広範な静的コード分析機能 ・幅広い事前定義されたルール ・選択したルールセットとコードベースの品質に依存	強	・大規模なコードベースではコンピューターに分散するオプションが用意される	・大規模なコードベースと複雑なプロジェクト ・保守性とコードの健全性の向上
GHAS CodeSQL	・他のツールやプラットフォームに統合 ・GitHubとのシームレスな統合	・高度なセマンティック コード分析 ・開発者の習熟度に依存	弱	・クエリの複雑さとコードベースのサイズに依存	・高度なセキュリティ分析と脆弱性検出 ・詳細なセマンティックコード分析