SYNOPSYS®

Code Sight

アプリケーションのセキュリティ上の不具合をコーディング中に検出して修正

開発者にとっての利点

直感的なワークフロー

- セキュリティの専門家でなくてもコードの弱点や脆弱なオープンソース依存ファイルを修正できる
- 問題のあるファイルはオープン、保存、編集時に自動アラートで通知。オンデマンドで手動による高速スキャンも可能
- インストールするだけですぐにセキュアなコードを作成できる

コード品質の改善

- ソースコード、オープンソース依存ファイル、API 呼び出し、暗号化、Infrastructure-as-Code（IaC）などに含まれる問題を指摘
- 明確なガイダンスにより問題の修正方法がすぐに分かると同時に、開発者のリスクへの意識とセキュリティ能力が向上
- Secure Code Warrior によるインタラクティブな開発者セキュリティ・トレーニングでセキュリティ・チャンピオンを育成

生産性の向上

- コードのチェックイン前に問題を解決できるため手戻りが減少
- IDEに最適化した高速スキャン機能により俊敏性を維持
- 下流テストの前に脆弱性の問題を取り除くことで、セキュリティ・チームのバックログを削減

概要

厳密に言えばセキュリティは必ずしも開発者の役割ではないかもしれませんが、開発者がプロジェクトや組織のセキュリティ・リスク態勢に直接影響を与えるのは事実です。このため、開発者がコーディングの段階でリスク評価データを確認し、誤ってプロジェクトに問題が混入した場合はその修正方法を理解できるようにする必要があります。

ただし、新しい手順やツールが増えてしまうと生産性に影響しかねないため、これらすべてを従来の開発ワークフローの一部として実行できることが求められます。

Code Sight™ は IDE プラグインのため、開発者は複数のツールを行き来する必要がなく、日々の開発業務をこなしながらアプリケーション・セキュリティの水準を高めることができます。静的アプリケーション・セキュリティ・テスト（SAST）とソフトウェア・コンポジション解析（SCA）を組み合わせた Code Sight は、以下の項目に対してリアルタイムにアラートを通知し、高い可視性をもたらします。

- コードに含まれるセキュリティ上の弱点（CWE）
- オープンソース依存ファイルに含まれる既知の脆弱性（CVE）
- Infrastructure-as-Code（IaC）の安全でない構成
- 秘密情報 / 機微なデータの潜在的な漏洩リスク
- 脆弱な API の使用

迅速な DevOps ワークフローおよび CI パイプライン向けに設計された Code Sight は、コードベース全体または変更されたプロジェクトのみをスキャンする自動化制御により、大規模なプロジェクトやファイル構造も極めて高速に解析できます。これにより、チームはコードのチェックイン前に不具合に対処でき、下流テストで初めて脆弱性が見つかった場合に比べ、手戻りのコストが削減されます。

Code Sight は他のシノプシス アプリケーション・セキュリティ・テスト（AST）ツールで検出された問題や関連するセキュリティ・ポリシー違反のアラートを開発チームに送ることにより、他の AST を補完し、その効果を高める役割を果たします。開発者が問題を迅速に修正できるように、Code Sight は詳細な修正ガイダンスを IDE 内に直接表示します。これには、推奨されるオープンソース・パッチ、コーディングのベストプラクティス、および Secure Code Warrior によるインタラクティブな開発者セキュリティ・トレーニングへのリンクなどが含まれます。

セキュリティ・チームにとっての利点

静的解析の前倒し

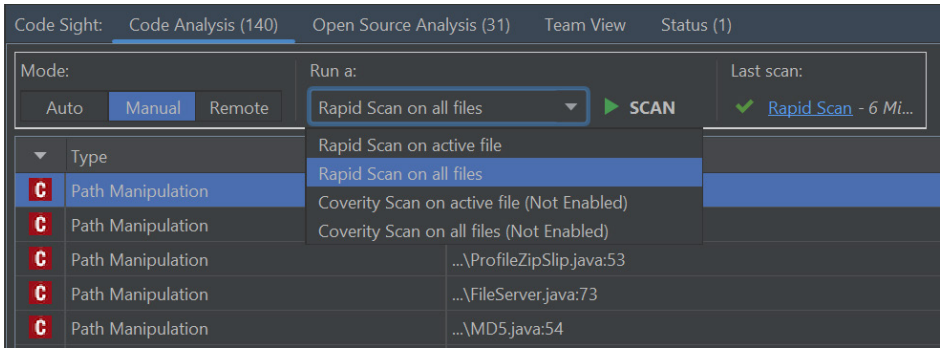
- コーディング中にソースコードを自動で解析し、問題を最も早い段階で検出
- プロジェクトのリスク評価データを開発チームのコントリビューター全員で共有できる Team View タブ
- 明確な修正ガイダンスとインタラクティブな開発者セキュリティ・トレーニングにより、主観に頼らないリスク認識とセキュリティ・スキルが身につく

よりスマートなサプライチェーン

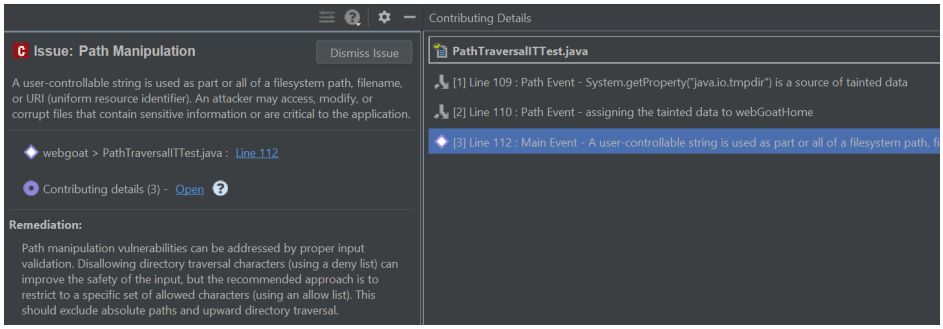
- 開発者がオープンソースを追加した時点で、直接または間接的な依存関係に存在する既知の脆弱性を特定
- 脆弱性の説明、CVE 詳細情報、その他の深刻度情報が表示されるため、修正の優先順位付けが容易
- 同じコンポーネントの脆弱性を含まないバージョン、またはより低リスクなバージョンが自動的に推奨されるため、開発者はよりスマートでセキュアな選択が可能

DevSecOps に適した柔軟性

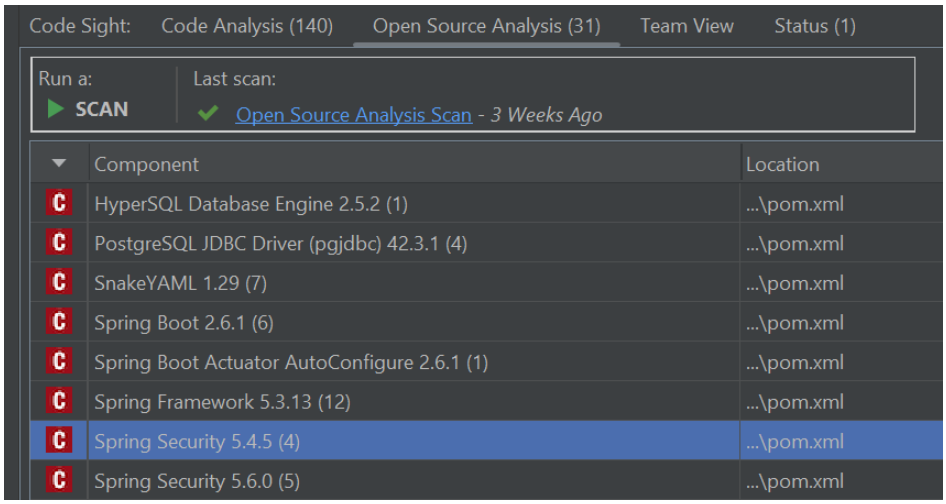
- 接続済みの Coverity® および Black Duck® サーバーのポリシー違反アラートを一元的に提示
- セキュア開発のためのスタンドアロン・ソリューションとして、または接続済みのシノプシス AST ソリューション（Coverity SAST、Polaris Software Integrity Platform®、Software Risk Manager など）と組み合わせて導入が可能



ソースコード・スキャンにおける解析の速度と深さのバランスを調整できる柔軟なオプション



迅速なコード解析（SAST）、詳細な改善ガイダンス、および Secure Code Warrior によるシノプシス開発者セキュリティ・トレーニングへのリンク



迅速なオープンソース解析（SCA）により脆弱性の詳細と修正の提案を表示

Code Sight Standard Edition | 技術スペック

Code Sight Standard Edition は、幅広い技術に対応しています。主な対応環境は以下の通りです。

IDE と言語

IDE

- Eclipse
- IntelliJ
- Visual Studio Code
- Visual Studio

言語

- Java
- JavaScript
- TypeScript

IaC プラットフォームとファイル・フォーマット

プラットフォーム

- AWS CloudFormation
- ELK
- Helm
- Kubernetes
- Terraform

ファイル・フォーマット

- HCL (Terraform)
- HTML
- JSON
- JSX
- Properties
- TOML
- TSX
- Vue
- XML
- YAML

Code Sight のコード解析およびオープンソース解析エンジンがサポートする言語とフレームワークの最新リストについては、Synopsys Community site にアクセスしてください。Coverity® SAST、Black Duck® SCA、Polaris Software Integrity Platform®、または Software Risk Manager 用の Code Sight エクステンションを使用する場合は、追加のテクニカル・サポートをご利用いただけます。

本データシートの内容は、Code Sight リリース 2023.9.0 以降に関するものです。

SYNOPSYS®

シノプシスの特色

シノプシスがご提供する統合型ソリューションは、ソフトウェア開発とデリバリのあり方を根底から変革し、ビジネス・リスクに対処しながらイノベーションを加速することを可能にします。シノプシスのソリューションにより、開発者はスピードを落とすことなくセキュアなコードを作成することができます。開発およびDevSecOps チームはスピードを犠牲にすることなく、開発パイプライン内でテストを自動化できます。セキュリティ・チームは先手を打ったリスク管理が可能となり、組織にとって最も重要な問題の修正に集中できます。シノプシスは業界随一のノウハウを活かし、最適なセキュリティ・イニシアティブの立案と実行をご支援します。信頼性の高いソフトウェアの構築に必要なものをワンストップでご提供できるのは、シノプシスだけです。
詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社
ソフトウェア インテグリティ グループ
〒 158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス
TEL: 03-6746-3600
Email: sig-japan@synopsys.com
www.synopsys.com/jp/software