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
- 自分のタスクのみに集中することも、ローカル・スキャンとチーム・ビューでプロジェクトのコードベース全体をサポートすることも可能

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
- パイプライン・スキャンから優先課題に即座にアクセスすることで、エンドツーエンドのセキュリティ標準を維持

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、その役割を通じて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 は他のブラック・ダック 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

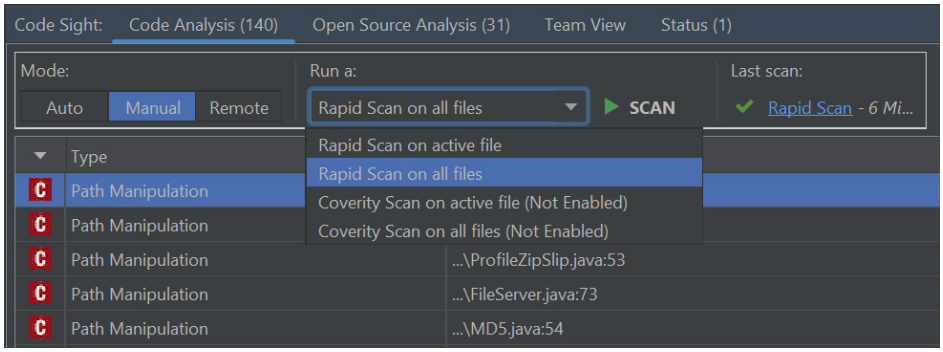
- コーディング中にソースコードを自動で解析し、問題を最も早い段階で検出
- プロジェクトのリスク評価データを開発チームのコントリビューター全員で共有できる Team View タブ
- 明確な修正ガイダンスと対話型のセキュア・コーディング・トレーニングにより、開発者全体のセキュリティ・スキルを標準化

よりスマートなサプライチェーン

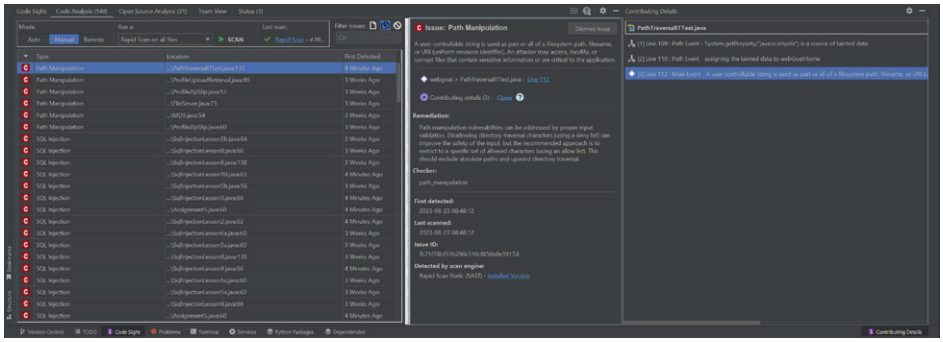
- 開発者がオープンソースを追加した時点で、直接または間接的な依存関係に存在する既知の脆弱性を特定
- 開発者によって見落とされる可能性のある問題、後の段階で検出される可能性のある問題、またはサードパーティのアセットがプロジェクトに組み込まれた後に発生する可能性のある問題に優先順位を付けて割り当てる
- 同じコンポーネントの脆弱性を含まないバージョン、またはより低リスクなバージョンが自動的に推奨されるため、開発者はよりスマートでセキュアな選択が可能

DevSecOps に適した柔軟性

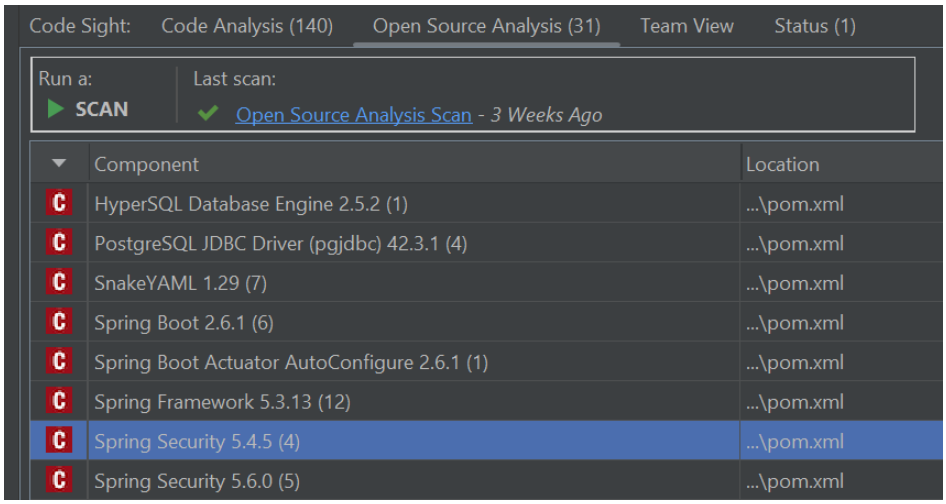
- 接続済みの Coverity®、Black Duck®、Software Risk Manager、Polaris プラットフォームのサーバーのポリシー違反アラートを一元的に提示
- セキュア開発のためのスタンドアロン・ソリューションとして、または接続済みのブラック・ダック AST ソリューションと組み合わせて導入が可能

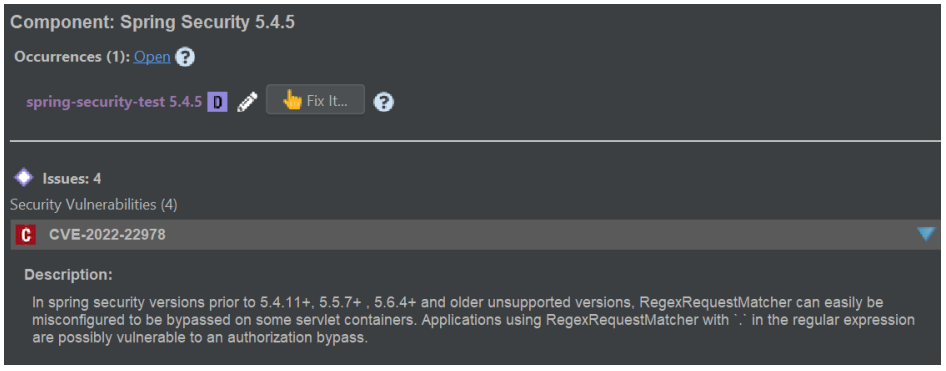


ソースコード・スキャンにおける解析の速度と深さのバランスを調整できる柔軟なオプション



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 によるブラック・ダック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 IDE プラグイン | 開発者ファーストまたはエンドツーエンドのセキュリティ

Code Sight はスタンドアロンのプラグインで、開発チームが開発の初期からセキュアなソフトウェアを作成するのを支援します。また、ブラック・ダックの AST ツール・スイートの IDE 拡張機能として利用することで、後段のパイプラインで実行されるセキュリティ・テストから優先すべき問題と修正ガイダンスが開発者に直接提示されます。

スタンドアロン版 Code Sight

スピードとセキュリティを両立した DevOps を必要とする開発チームに最適。

プロジェクトで使用しているコード、オープンソース、IaC テンプレートの品質およびセキュリティ上のリスクに関する情報を IDE 内で直接開発チームに提示。問題を後段にプッシュする前に修正することで、終盤での手戻りを防ぎます。

スタンドアロン版のすべての機能を利用可能な無料トライアルあり。

コード解析

- ✓ Rapid Scan Static
- x ~~フル・スキャン (Coverity SAST)~~

オープンソース解析

- ✓ Rapid Scan SCA

リスク・インサイト

- ✓ 脆弱性の深刻度、優先度、到達性の指標 (CVSS など)
- ✓ 安全でないコーディング作法 (CWE など)
- ✓ Black Duck Security Advisory
- ✓ リスクの深刻度、コード内の位置
- ✓ 修正ガイダンス

エンタープライズ機能

- x ~~複数のチーム / プロジェクトで検出されたセキュリティおよび品質上のリスクを表示~~
- x ~~セキュリティおよびライセンスに関するカスタム・ポリシー設定~~
- x ~~ポリシー通知 / 適用の自動化~~

スキャン設定

- ✓ 自動または手動スキャン
- ✓ 単一ファイル・スキャンまたはプロジェクト全体のスキャン

デプロイ形式

- ✓ 一般的な IDE のスタンドアロン IDE プラグインとして利用可能
- ✓ VS Code、Visual Studio、Eclipse、IntelliJ には無料トライアルあり

ブラック・ダック AST ツール向け Code Sight プラグイン

エンタープライズ環境でのライフサイクル全体にわたるアプリケーション・セキュリティに最適。

Black Duck、Coverity、Software Risk Manager、および Polaris Software Integrity Platform の完全なアプリケーション・セキュリティ機能を、既存のワークフローを妨げることなく拡張します。パイプライン・ベースのテストはこれまで通りセキュリティ・チームが管理しながら、開発者は IDE 内で直接リスクへの意識を高めることができます。

Coverity SAST、Black Duck SCA、Software Risk Manager、および Polaris Software Integrity Platform® に付属します。利用条件はソリューションにより異なります。

コード解析

- ✓ Rapid Scan Static
- ✓ フル・スキャン (Coverity SAST)

オープンソース解析

- ✓ Rapid Scan SCA

リスク・インサイト

- ✓ 脆弱性の深刻度、優先度、到達性の指標 (CVSS など)
- ✓ 安全でないコーディング作法 (CWE など)
- ✓ Black Duck Security Advisory
- ✓ リスクの深刻度、コード内の位置
- ✓ 修正ガイダンス

エンタープライズ機能

- ✓ 複数のチーム / プロジェクトで検出されたセキュリティおよび品質上のリスクを表示
- ✓ セキュリティおよびライセンスに関するカスタム・ポリシー設定
- ✓ ポリシー通知 / 適用の自動化

スキャン設定

- ✓ 自動または手動スキャン
- ✓ 単一ファイル・スキャンまたはプロジェクト全体のスキャン

デプロイ形式

- ✓ IDE プラグインとして利用可能。サポートされる IDE の一覧は Support matrix を参照。

Code Sight がサポートする言語およびフレームワークの最新情報は、Support matrix を参照してください。Coverity SAST、Black Duck SCA、Polaris® 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 2024.4.0 以降に関するものです。

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。
詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社
www.blackduck.com/jp

©2024 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2024 年 9 月