opentext™ | Cybersecurity

データシート

Fortify Static Code Analyzer：静的アプリケーションセキュリティテスト

ソースコードのセキュリティ脆弱性の根本原因を特定し、問題の重大度に基づいて優先度を設定し、問題の修正方法に関して詳細なガイダンスを参照します

静的テストによるコード品質の向上

静的アプリケーションセキュリティテスト (SAST) は、開発の初期段階 (修正コストが最も低い段階) でセキュリティ脆弱性を特定します。開発中にコードに問題が発生したとき直ちに開発者にフィードバックを提供することにより、アプリケーションのセキュリティリスクを軽減します。また、開発者は作業を進めながらセキュリティに関する情報を取得できるため、よりセキュアなソフトウェアを開発できます。

Fortify Static Code Analyzer by OpenText™ は、セキュアなコーディングルールに関する広範なナレッジベースと複数のアルゴリズムにより、アプリケーションのソースコードを分析し、悪用される可能性のある脆弱性を特定します。

あらゆる実行パスとデータパスを分析し、脆弱性を特定および修正します。

セキュリティの問題を早期に発見

Static Code Analyzer のコード処理はコンパイラーと似ています。ソースコードファイルを読み取り、セキュリティ分析用に強化された中間構造に変換します。この中間フォーマットを使用して、セキュリティ脆弱性を特定します。複数の専用アナライザーで構成された分析エンジンが、セキュアなコーディングルールを使用してコードベースを分析し、セキュアなコーディングプラクティスに対する違反の有無を調べます。

Fortify Software Security Center による結果の管理

Fortify Software Security Center (SSC) by OpenText™ は、組織のアプリケーションセキュリティプログラム全体を可視化してソフトウェアポートフォリオ全体のセキュリティ脆弱性を解決するための一元管理リポジトリです。静的 / 動的 / ソフトウェアコンポジション分析の結果を最適化するため、管理ダッシュボードとレポートにより修正作業の確認、監査、優先度設定、管理を行えるほか、ソフトウェアセキュリティテストのアクティビティのトラッキングと改善内容の測定を行うことが可能です。

Fortify SSC は、スキャン結果と評価結果の相関付けとトラッキングを経時的に行い、その情報を Fortify Audit Workbench by OpenText™ または IDE プラグイン (Fortify Plugin for Eclipse、Fortify Extension by OpenText™ for Visual Studio など) を通じて開発者が利用できるようにします。

また、手動または自動で、問題をバグ管理システム (OpenText™ ALM Octane、Jira、Azure DevOps Server、Bugzilla など) に送信することもできます。

- Audit Workbench
  - Smart View—ビジュアル表示により監査と修正を簡素化。
    - データフローの観点から複数の問題の関係性を素早く理解

インテグレーションエコシステムの内容：

- 柔軟な導入オプション：サービスとしての AppSec、オンプレミス、クラウド
- 統合開発環境 (IDE)：Eclipse、Visual Studio、JetBrains (IntelliJ を含む)
- CI/CD ツール：Jenkins、Bamboo、Visual Studio、Gradle、Make、Azure DevOps、GitHub、GitLab、Maven、MSBuild
- バグ管理システム：Bugzilla、Jira、ALM Octane
- オープンソースセキュリティ管理：Sonatype、Snyk、WhiteSource、BlackDuck
- コードリポジトリ：GitHub、Bitbucket
- Swaggerised API による無制限のカスタマイズ
- 開発者に便利な幅広い対応言語：
  - サポート対象：Java、Kotlin、Scala、C#、VB.NET、TypeScript、JavaScript、C/C++、Python、PHP、Go、COBOL、Swift、Objective C/C++、Salesforce Apex、Dart/Flutter、Bicep、Solidity、Ruby、SAP ABAP、PL/SQL、T-SQL、ColdFusion、ActionScript、Visual Basic 6、VBScript、Ruby、HTML、XML、JSON、YAML、HCL。サポート対象の言語の詳細については、Fortify ソフトウェアシステム要件に関するドキュメントに記載されています。
- CI/CD ツール (IDE、バグ管理システム、オープンソース) との統合
  - すべての主要 IDE をサポート：Eclipse、Visual Studio、JetBrains (IntelliJ を含む)
  - バグ管理システムの統合により、セキュリティの問題を透過的に修正可能
  - オープンソースセキュリティの統合：Sonatype、Debricked
  - Swagger をサポートする REST API、オープンソースの GitHub リポジトリ、および Bamboo、Azure DevOps、Jenkins 用のプラグインと拡張機能を組み合わせて、CI/CD パイプラインを自動化するツールとして利用

「Fortifyの導入により、分析できるコードの量が増え、分析作業の俊敏性や迅速性も大幅に向上しています。今では、当社のパイプラインは通常、脆弱性のエラーなしで私のところまで到達しています。そのようなエラーは開発プロセスにおいてあらかじめ検知済みであるからです」

Wilson González氏
DevOps マネージャー
Location World

お問い合わせ
www.opentext.com

. Smart View フィルターを適用して、最も効率的なポイントで問題のトリアージまたは修正を開始

迅速で正確なスキャンの実行

静的アプリケーションセキュリティテスト (SAST) では、コード関連の問題の大半が開発の初期段階で特定されるため、ソースコード、バイナリコード、バイトコードの脆弱性を特定して排除することができます。Fortify は、真陽性率 100% の正確性 (OWASP 1.2b ベンチマーク) をもって、1,627 の固有カテゴリ、33 以上のプログラミング言語、100 万以上の個別 API について脆弱性を検知します。

CI/CD パイプラインにおけるセキュリティの自動化

Fortify は、脆弱性に優先度を付けて最大の脅威となるものを特定することによってリスクを軽減し、CI/CD ツール (Jenkins、ALM Octane、Jira、Atlassian Bamboo、Azure DevOps、Eclipse、Microsoft Visual Studio など) と連携します (「Fortify インテグレーション」を参照)。スキャン結果をリアルタイムで確認できるとともに、推奨事項にアクセスし、コード行のナビゲーションにより脆弱性を迅速に特定し、共同作業による監査を実施できます。

開発時間の短縮とコストの削減

SDLC 内に組み込むことにより、開発時間と開発コストを 25% 削減できます。本番 / リリース後の段階で脆弱性を修正すると、ライフサイクルの初期段階で修正する場合と比べてコストが 30 倍かかります。Fortify を導入すると、開発者は作業を進めながら静的アプリケーションセキュリティテストに関する情報を取得できるため、セキュアなコーディングプラクティスを実現できます。

以下のように、チームの開発環境に合わせて柔軟に導入オプションを選択できます。

- Fortify On Demand by OpenText™：完全な SaaS ベース環境でのチーム作業が可能
- ホスティング型 Fortify：ユーザーデータを完全に管理できる分離された仮想環境で作業ができ、SaaS とオンプレミスの優れた点を提供
- Fortify On-Prem：他と比べ、最も柔軟に Fortify ソリューションを活用

セキュリティ分析と結果を開発者にリアルタイムで提供

Security Assistant は、スピードと効率を上げる目的で特別に設計された構造 / 構成アナライザーであり、高速のセキュリティフィードバックツールとして活用できます。信頼度の高い (すべて真陽性、または誤検知率が極めて低い) 検知結果のみが迅速に IDE (Microsoft Visual Studio、Eclipse、IntelliJ) に表示されます。

Security Assistant 搭載の Fortify on Demand は開発者の作業を支援する追加機能としての使用が想定されています。セキュリティ問題をより包括的に把握するためには、フル静的スキャンと組み合わせて使用します。Fortify Static Code Analyzer および Fortify on Demand 静的評価のユーザーは、追加のライセンスまたはコスト不要で Security Assistant を使用できます。

手作業での監査の時間を削減

Fortify Audit Assistant by OpenText™ は、機械学習を通じて組織と最も関連性の高い脆弱性を特定して優先度を設定するため、手作業による監査の時間が削減されます。機械学習を使用した自動化により、手作業での監査の時間が短縮され、静的アプリケーションセキュリティテストイニシアチブの ROI が向上します。Fortify Audit Assistant の機能は以下のとおりです。

- 自動の監査結果を数分で提供
- 監査担当者の負担を低減
- 信頼度に基づいて問題の優先度を設定
- プロジェクト全般にわたって正確かつ一貫した監査結果を生成
- DevOps の進捗に合わせて結果を提供
- 詳細な手動検査が必要とされる問題の件数を削減
- 関連する問題を特定し、誤検知を迅速に削減
- 既存のリソースによってアプリケーションセキュリティを拡張

一元管理されたスキャンインフラストラクチャの提供

ScanCentral は、ビルドサーバー上の軽量パッケージ化を可能にし、増大する昨今の開発ニーズに対応する一元管理されたスキャンインフラストラクチャを Fortify Software Security Center 内から利用できるようにします。オンプレミス、オンデマンド、ハイブリッドの各アプローチに対応できる、拡張性の高い製品です。ScanCentral は柔軟性に優れており、必要に応じてスキャンの範囲を調整できるほか、スキャンパフォーマンスの向上、高速スキャンを重視する調整、包括的で正確なスキャンを重視した調整、restful API/Swaggerised API に対応した調整ができます。

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。