opentext™ | Cybersecurity

データシート

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

Fortify Static Code Analyzer (SCA) は、ソースコードにおける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て、詳しい修正方法を提供します。開発者は、一元管理されたソフトウェアセキュリティ管理を通じて迅速に問題を解決できます。

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 (SCA) 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

Fortify SCA 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 SCA はルールビルダーも備えているため、静的分析機能を拡張してカスタムルールを含めることもできます。分析結果は、確認するユーザーとタスクに合わせて複数の方法で表示できます。

Fortify Software Security Center (SSC) 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、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 / 動的アプリケーションセキュリティテスト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アクティビティのトラッキングおよび改善内容の測定が可能です。Fortify SSC により、組織全体のアプリケーションセキュリティ体制を正確に把握できます。中央に位置する Fortify SSC サーバーが、各種アプリケーションセキュリティテストアクティビティ (静的分析、動的分析、リアルタイム分析など) から結果を取得します。

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) を通じて開発者に提供します。また、不具合を手動または自動でバグ管理システム (OpenText™ ALM Octane、Jira、Azure DevOps Server、Bugzilla など) に送信することもできます。

統合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

- 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
    - 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実行

主なメリット

迅速で正確なスキャン

- 静的アプリケーションセキュリティテスト (SAST) により、コード関連の問題の大半を開発の初期段階で特定
- ソース、バイナリ、バイトコードの脆弱性を特定および解消
- Fortify SCA は、815 の固有カテゴリ、27 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出
- 真陽性率 100% の正確性 (OWASP 1.2b ベンチマーク)

CI/CD パイプラインにおけるセキュリティの自動化

- 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りリスクを軽減
- Fortify は CI/CD ツール (Jenkins、ALM Octane、Jira、Atlassian Bamboo、Azure DevOps、Eclipse、Microsoft Visual Studio など) と連携可能。Fortify の連携を参照してください。
- スキャン結果をリアルタイムでレビューして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の迅速な特定と共同作業による監査を実現

開発時間と開発コストを削減

- SDLC 内に組み込むことにより、開発時間と開発コストを 25% 削減可能。脆弱性を本番 / リリース後の段階で修正する場合は、ライフサイクル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。
- 脆弱性の検知件数は 2 倍、誤検知は最大 95% 削減 (出典：Mainstay Continuous Delivery of Business Value with Fortify by OpenText™ 2017)
- 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が実現

主な特長

- 幅広い言語をサポート
  - ABAP/BSP、ActionScript、Apex、ASP.NET、C# (.NET)、C/C++、Classic ASP (VBScript)、COBOL、ColdFusion CFML、Go 言語、HTML、Java (Android を含む)、JavaScript/AJAX、JSP、Kotlin、MXML (Flex)、Objective C/C++、PHP、PL/SQL、Python、Ruby、Swift、T-SQL、VB.NET、VBScript、Visual Basic、XML のサポート
  - サポート対象の言語の詳細は「Fortify ソフトウェアシステム要件」ドキュメントに記述されています。
- 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)
  - バグ管理システム統合により、セキュリティ問題を人の介在なしで修正可能
  - オープンソースとの統合：Sonatype、WhiteSource、Snyk、BlackDuck
  - 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により、CI/CD パイプラインを自動化
- チームの開発環境に合わせて導入できる柔軟なオプション
  - Fortify On Demand by OpenText™ は完全な SaaS ベース環境でのチーム作業が可能
  - Fortify Hosted は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するという SaaS とオンプレミスの優れた点を提供
  - Fortify On-Prem では Fortify ソリューションのすべての面を完全に制御することができます。
- Security Assistant は、コードの記述時にリアルタイムでセキュリティを分析し、開発者に結果を表示します。
  - スピードと効率を念頭に専用設計された構造 / 構成アナライザーを搭載した、高速のセキュリティフィードバックツールです。
  - Security Assistant は信頼度の高い検知結果 (すべて真陽性、または誤検知率が非常に低い結果のみ) を迅速に IDE (Microsoft Visual Studio、Eclipse、IntelliJ) に表示します。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。
- Fortify Audit Assistant by OpenText は、機械学習を通じて最も関連性の高い脆弱性を特定して優先度を設定することにより、手動監査の時間を短縮します。機械学習による自動化により、手動監査の時間短縮と静的アプリケーションセキュリティテストの ROI を改善できます。
  - 自動の監査結果を数分で提供
  - 監査官の負担を低減
  - 信頼度に基づいて問題の優先度を設定
  - すべてのプロジェクトで正確かつ一貫した結果を生成
  - DevOps のスピードに対応した監査結果：SCA をビルドサーバーやソースコード管理サーバーと連携して、スキャンの頻度を上げ、迅速に結果を取得可能
  - 詳細な手動検査が必要となる問題の数を削減
  - 関連する問題を特定し、誤検知を迅速に削除
  - 既存のリソースでアプリケーションセキュリティを強化
- ScanCentral では、ビルドサーバー上での軽量パッケージ化が可能です。また、今日の高い開発要件に対応するため、Fortify Software Security Center 内から、スケーラブルで一元管理された Fortify by OpenText™ スキャンインフラストラクチャを利用できます。

「Fortify Static Code Analyzer のおかげで、以前よりずっと効率的に問題を特定、分析、解決できるようになりました」

Brenton Witonski 氏
シニアITセキュリティエンジニア
Acxiom

お問い合わせ
www.opentext.com

- 必要に応じてスキャンの範囲を柔軟に調整できます。
  - 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
- オンプレミス、オンデマンド、またはハイブリッドアプローチによる拡張性

アプリケーションのセキュリティ状態を正確に評価

Fortify は、ソフトウェアライフサイクル全体に対応する広範なソフトウェアセキュリティテスト製品群です。

- **Fortify Static Code Analyzer (SCA) による静的アプリケーションセキュリティテスト (SAST)：**開発の初期段階 (問題を最も容易に、低コストで修正できる段階) に脆弱性を特定し、問題の重大度に基づいて優先度を付けます。スキャン結果は Fortify SSC に保存されます。SCA の詳細はこちら: **www.microfocus.com/ja-jp/cyberres/application-security/static-code-analyzer**。
- **Dynamic Application Security Testing (DAST) by OpenText™ に対応した Fortify WebInspect：**実行中の Web アプリケーションおよび Web サービス内のセキュリティ脆弱性を特定し、優先度を付けます。インタラクティブアプリケーションセキュリティテスト (IAST) との統合により、より広い攻撃対象領域をカバーし、より多くの脆弱性を特定できます。スキャン結果は Fortify SSC に保存できます。
- **Fortify Software Security Center by OpenText™：**アプリケーションセキュリティプログラムを自動化できる AppSec プラットフォームです。管理、開発、セキュリティの各チームが連携してソフトウェアセキュリティアクティビティに優先度を付けて、トラッキング、検証、管理できます。
- **Fortify on Demand for Security as a Service:** 追加でリソースを割り当てることも、ソフトウェアをインストールして管理する必要もなく、ソフトウェアのセキュリティを簡単、柔軟、迅速、正確にテストできます。

システム要件

製品仕様とシステム要件の詳細については、**www.microfocus.com/documentation/fortify-static-code/**をご覧ください。

会社概要

Cybersecurity は、お客様のビジネスの運営と変革をお手伝いします。ソフトウェアにより、企業の構築、運用、セキュリティ対策、分析に欠かせないツールをご提供します。これらのツールは、既存のテクノロジーと新しいテクノロジーのギャップを解消するように設計されています。デジタル変革を目指すお客様のイノベーションを低リスクで迅速に実現します。

Fortify は、業界をリードするセキュリティ調査に基づき、ランタイムアプリケーションの監視および保護とともに、極めて包括的な静的および動的アプリケーションセキュリティテストテクノロジーを提供します。当ソリューションは社内に導入することもマネージドサービスとして導入することもできるため、今日の IT 組織の進化するニーズを満たす、拡張性に優れた機敏なソフトウェアセキュリティ保証プログラムを構築できます。

opentext™ | Cybersecurity

760-JA0015-005 | O | 12/23 | © 2023 Open Text