BLACKDUCK®

Coverity

静的解析

主な長所

高い性能

新規コードや変更されたコードに存在する問題は、完全スキャンと同じ忠実度の高速な増分スキャンで特定します。このため、コミットやプルリクエストのたびにスキャンを容易に実行でき、開発スピードの低下を招きません。

大規模なエンタープライズ環境への対応

Coverity は数千人規模の開発チームで作成された数千万コード行のアプリケーションを含め、世界最大規模のアプリケーションで多くのスキャン実績があります。

拡張性

独自フレームワークやサポート対象外の言語も、簡単に作成可能なカスタム・チェッカーでサポートできます。

導入の柔軟性

Coverity はオンプレミスでもプライベート・クラウド環境でも動作します。このため、すべてのデータをネットワーク内に保持したまま最高の静的解析スキャンを実行できます。

最も包括的な静的解析

静的解析ツール Coverity® は市販の静的解析ソリューションの中で最も高い精度とスケーラビリティを備えており、開発者とセキュリティ・チームは大規模な環境でセキュリティと品質に優れたアプリケーションをデリバリできます。20 以上のプログラミング言語と 200 以上のフレームワークをサポートした Coverity は、各アプリケーションの詳細なモデルを構築してすべての依存関係とコンパイラを可視化することにより、世界最大規模のアプリケーションで多数のファイルやライブラリにまたがるような複雑な問題の特定も可能です。

開発ライフサイクル早期での高速スキャン

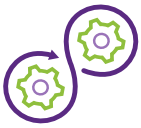
Coverity によるスキャンを SDLC の早期段階で実行することで、セキュリティと品質上の問題をいち早く特定できます。問題の修正は早ければ早いほど容易で、影響を最小に抑えることができます。

IDE 内でリアルタイムに動作

コーディング中に脆弱性やコード品質の問題を指摘してくれるため、問題のあるコードがリポジトリにチェックインされるのを防ぐことができます。

プルリクエストをトリガーとしてスキャンを実行

一般的なソースコード管理 (SCM) システムに統合して、新規コードや変更されたコードに存在する問題を増分スキャンで特定できます。



CI/CD パイプラインでの自動化

修正されていないセキュリティや品質上の問題は、アプリケーションの完全スキャンで特定し、ポリシー違反が見つかった場合にはビルドを中断することもできます。

最高精度のスキャン結果

Coverity のスキャン結果は精度が高いため、開発者は誤検知のトリアージに時間を奪われることなく、実際の不具合の修正作業に専念できるなど、開発者の負担が軽減されます。

- **各アプリケーションの詳細なモデル**により、すべての依存関係とコンパイラ、データフローおよび制御フロー・パスを含め、アプリケーションの動作を可視化して重要な洞察を得ることができます。
- **20 以上のプログラミング言語と 200 以上のフレームワークを深く理解**し、コンテキストを考慮して誤検知と真の問題を区別します。
- **コンテキストを考慮した洞察**を最初のスキャン結果に適用することにより、各結果の妥当性を確認し、悪用の可能性を評価します。
- **設定可能なセキュリティおよび品質チェッカー**は、デフォルトでは精度優先にチューニングされていますが、ビジネスまたはアプリケーションのリスク・プロファイルに合わせた調整が可能です。

各種セキュリティおよび産業規格を幅広くカバー

Coverity はコードの品質問題の特定に関してクラス最高の精度を達成している他、セキュリティや安全に関する産業規格を最も包括的にサポートしています。これには以下のものが含まれます。

- **セキュリティ：**OWASP Top 10、SANS CWE Top 25、PCI DSS
- **安全：**MISRA®、CERT C/C++、CERT Java、DISA STIG、ISO 26262、ISO 23434、ISO/IEC TS 17961、AUTOSAR®、Hyundai Secure Coding Standards

レポートは PDF としてダウンロードでき、監査時に各標準に対する詳細なコンプライアンス記録を残しておくのに役立ちます。トレンド・レポートには、深刻度の時系列での推移や、優先度の高い問題に対する開発者やプロジェクト・チームごとの修正進捗情報などが表示され、さらに多くの洞察が得られます。

また、セーフティ・クリティカルなプロジェクトでは、ISO 26262 や DO-330 などの業界安全規格に適合するように Coverity が正しく設定されていることを Coverity Qualification Kit (Q-Kit) で確認できます。

主な特徴

- **簡単なオンボーディング** デスクトップ・アプリケーションの Point and Scan は、ユーザーがソースコードをポイントするだけでアプリケーションをオンボードすることができます。コマンドライン・インターフェイス (CLI) を好む開発チームには、Coverity CLI 機能で同様のオンボーディングが可能です。
- **開発ワークフローへの円滑な統合** Black Duck Bridge を使用すると、簡単かつ予測可能なアプローチを使用して Coverity を含むすべての Black Duck アプリケーション・セキュリティ・テスト・ソリューションを一般的な CI/CD ツールにコマンドライン・インターフェイスで統合できます。
- **リアルタイムでの不具合検出** IDE プラグインの Code Sight™ を使用すると、開発者はコーディング中に静的解析からの正確な洞察を得ることができます。検出された各問題について、その詳細説明、カテゴリ、深刻度、CWE データ、不具合の位置、詳細な修正ガイダンスなどが IDE 内で直接提示されます。
- **具体的な修正ガイダンス** 詳細なサジェスチョンやコンテキストに応じた e ラーニングにより、セキュリティの専門知識がない開発者でも問題の修正方法を容易に理解できます。
- **詳細なレポート** 業界で認知されているリスト、問題のタイプ、テクニカル・リスク指標に基づいた事前作成済みのレポートがダッシュボードに表示されるため、開発者はそれぞれの組織にとって最も重要な問題から優先的に対策をとることができます。CWE、標準規格の分類、優先リスト、リスク指標、パス、開発者ごとに問題を簡単にグループ化できるフィルター機能もあります。

サポートされるテクノロジーの詳細な一覧は、Coverity Languages and Framework の web ページをご参照ください。

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