Black Duck

ソフトウェア・コンポジション解析

ソフトウェア・サプライチェーンによってもたらされるリスクを特定・管理

可視性を確立

- コード、バイナリ、および成果物に含まれるオープンソースを検出します
- SBOM からサードパーティ・コンポーネントをインポートします
- DevOps との統合によりスキャンを自動化します

リスクを管理

- 依存関係を既知の脆弱性や健全性の問題に対応付けます
- 悪意あるコンポーネントや機微な情報をスキャンします
- ライセンスのリスクおよび競合を特定します
- 重要度に基づいて修正の優先順位を決定します

信頼を構築

- リスク許容度および顧客からの要求事項に基づいてカスタム・ポリシーを定義します
- オープンソースとカスタムの依存関係を含む SBOM を生成します
- アプリケーション出荷前にサプライチェーンの脅威に対処します

概要

Black Duck は、アプリケーションやコンテナなどあらゆるソフトウェア成果物やライブラリでオープンソースを使用した場合に発生するセキュリティ、ライセンス・コンプライアンス、コード品質のリスクを管理する包括的なソリューションです。Forrester 社によってソフトウェア・コンポジション解析（SCA）のリーダーとして認定された Black Duck は、サードパーティ依存関係の可視性を最大限に高め、ソフトウェア・サプライチェーンによってもたらされるリスクの管理を可能にします。

ソフトウェア・サプライチェーンの可視性を確立

商用アプリケーションを構成するコードのほとんどはサードパーティに由来しており、最終アプリケーションを頒布またはデプロイする企業が管理も監視もできない外部組織によって作成されています。Black Duck はさまざまな手法を組み合わせて依存関係を検出し、アプリケーションの構成を完全に可視化します。これにより、チームはリスクを効果的に評価および管理できるようになります。

- **依存関係解析：**パッケージ・マネージャーによって宣言された直接的および推移的依存関係を特定します。
- **バイナリ解析：**ファームウェアやコンテナ・イメージなど、ビルド済み成果物に存在する依存関係をソース・コードなしで検出します。
- **スニペット解析：**AI コーディング支援ツールが流用したコードなど、断片的なコードがどのオープンソース・プロジェクトに由来するものかを特定します。
- **CodePrint 解析：**パッケージ・マネージャーによって宣言されていなくても、ソース・ファイルおよびディレクトリに含まれる依存関係を特定します。
- **コンテナ・スキャン：**バイナリ解析と CodePrint 解析を組み合わせ、コンテナ・イメージに含まれるオープンソースの依存関係をレイヤーごとに特定します。
- **C/C++ スキャン：**パッケージ・マネージャーが存在しない場合でも、C/C++ アプリケーションで使用されているオープンソースの依存関係およびライブラリを正確に特定します。

リスクを特定・管理

特定したすべての依存関係について、Black Duck は関連するリスクを評価し、優先順位の高いものから修正できるよう支援します。

脆弱性

Black Duck Security Advisory（BDSA）は、Black Duck KnowledgeBase に基づいて既存および新たに公開されたオープンソース脆弱性について具体的な対策方法を示したアラートをいち早く提供します。これらのアラートには、以下の情報が含まれます。

- 重要なリスク指標、個々の脆弱性の技術解説、エクスプロイトの詳細
- CVSS スコアリングおよび CWE 分類データ

- 会社のリスク・プロファイルに一致するカスタム脆弱性リスク・スコアリング
- コンポーネント・レベルのアップグレードおよび対策の手引き、軽減要因、応急措置

BDSA は、人間による調査と AI を組み合わせることにより、Black Duck ユーザーに最も大きく影響すると考えられる脆弱性を発見・分析して報告します。このため、BDSA は一般的なセキュリティ・フィードよりも分析の完全性が高く、しかも脆弱性が公開されてから数時間後には発行されます。

ライセンスのリスク

Black Duck は、明示的に宣言されたライセンス、サブライセンス、および埋め込みライセンスを含め、アプリケーションの依存関係によって使用されているライセンスを正確に特定します。そして、各ライセンスに関連する要求事項と制限事項の情報を抽出し、ライセンスの全文および著作権情報と一緒に分かりやすく表示してくれます。また、ほとんどすべてのオープンソース・ライセンスで必須とされている Notice ファイルも自動で生成できます。

コンポーネントの健全性

オープンソース・プロジェクトの健全性、履歴、コミュニティ・サポート、出所、評判を評価するための指標が Black Duck によって提供されるため、セキュリティ・リスクを未然に防止することが容易になります。

マルウェア

Black Duck では、既知の脆弱性にとどまらず、より広範なリスク評価が可能です。ソフトウェア成果物のビルド後解析により、不審なファイル、潜在的に迷惑なアプリケーション（PUA）、プロテストウェア、不審なファイル構造などのマルウェアの存在を検出できます。

オープンソースのガバナンスを自動化

ライセンス・タイプ、脆弱性の重要度、オープンソース・コンポーネントのバージョンなどさまざまな基準に基づいてオープンソースのセキュリティと使用に関する独自のポリシーを設定できます。設定したポリシーは、自動ワークフロー・トリガー、通知、Jira または Azure との双方向の連携などの方法で適用でき、修正作業の開始と報告を迅速化できます。ポリシーを使用することで、開発チームがリスクのあるコンポーネントを使用するのを防ぐとともに、万一こうしたコンポーネントがリリース・ストリームに混入した場合でも、ビルドを停止することができます。

SBOM をアプリケーション・ライフサイクルに組み込む

Black Duck には以下の機能があります。

- サードパーティのソフトウェア部品表（SBOM）をインポートして依存関係を既知のコンポーネントに自動的にマップし、カスタムまたは商用のコンポーネントの依存関係に対応する新規コンポーネントを作成できます。
- オープンソース、カスタム、および商用の依存関係をすべて含んだ SBOM を、顧客、業界、または各種規制の要求事項に適合するように SPDX または CycloneDX フォーマットでエクスポートできます。詳細情報の共有レベルは、そのまま使えるテンプレートを活用することで、利用者の指定に応じて適切に設定できます。
- SDLC ツールとの統合により、SBOM 生成を自動化するとともに、既存または新たに見つかったリスクについて SBOM の依存関係を継続的に監視できます。

Black Duck でサポートされる言語、パッケージ・マネージャー、および統合環境についての情報は、ブラック・ダックの web サイトでご確認ください。

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