BLACKDUCK
BY SYNOPSYS

Black Duck
ソフトウェア・コンポジション解析
製品構成とモジュール

リスク察知能力と
管理能力を大きく向上し、
さまざまなニーズと
予算に対応する
柔軟な構成および
モジュール・オプション

概要

Black Duckソフトウェア・コンポジション解析（SCA）ソリューションは、2つの独創的な構成で提供されています――Standard Editionと、追加モジュールでソリューションが拡張されるProfessional Editionです。Standard Editionに任意のモジュールを追加して、個別のニーズに対応することもできます。このようなモジュール構成により、自社アプリケーションをとりまくリスク状況を鋭く察知し、オープンソースおよびサードパーティ・ソフトウェアの使用状況の管理を強化できるとともに、ニーズに合わせた柔軟な導入が可能です。Black Duckには、コンパイル済みのバイナリ・ファイルや実行可能ファイルを解析するSCAソリューションもあり、オープンソースの脆弱性とライセンスを検出し、機密データをリスクにさらす弱点を洗い出すことができます。

Black Duck Standard Edition

SDLCの一環として、オープンソースのリスクを特定し対策を計画

Black Duck Standard Editionでは、自社アプリケーションの一部として組み込まれているオープンソース・コンポーネントを可視化することによって、チームをサポートします。Black Duckのマルチファクタ・オープンソース検出テクノロジーは、SDLC（ソフトウェア開発ライフサイクル）のあらゆる段階に統合され、コードに含まれているオープンソースを自動的に検出します。ソフトウェア・プロジェクトのオープンソースの完全なBoM（部品表）を表示し、管理できるようになり、アプリケーションに影響を及ぼす既知の脆弱性、ライセンス、コード品質上のリスクに関する重要な情報を得られます。

- **マルチファクタ・オープンソース検出：**パッケージ・マネージャの宣言、ファイル・システムのスキャン、ビルド依存性解析の組み合わせにより、ターゲットのコードベースに含まれるすべてのオープンソース・コンポーネントのインベントリを自動的に作成します。結果は、包括的なBoMとして表示されます。
- **脆弱性のマッピング：**使用中のオープンソース・コンポーネントに付随するセキュリティ・リスクを特定します。米国の脆弱性データベース「NVD（National Vulnerability Database）」による詳細な脆弱性データとともに、対策を助けるパッチ・ガイダンスが得られます。
- **ライセンス・リスクの特定：**アプリケーションのコンポーネントに適用されるオープンソース・ライセンスを特定することにより、大切な知的財産を守り、訴訟問題を未然に防ぎます。ライセンス条項全文をレビューし、法律やコンプライアンスに違反する可能性のある箇所をハイライトします。
- **オペレーショナル・リスクの指標：**古いバージョンのコンポーネントや、プロジェクトやコミュニティの活動が停滞しているコンポーネントを特定して、開発チームによるサポートや対策にかかるコスト増大のリスクを低減します。

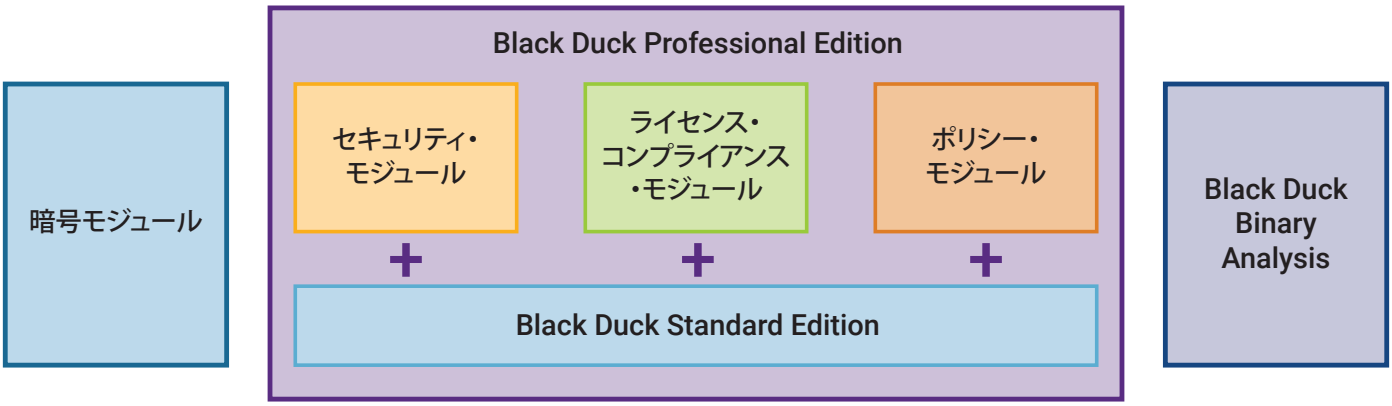
- **脆弱性のモニタリングとアラート：**インベントリ内のオープンソース・コンポーネントは、新しく報告された脆弱性に対して自動的にモニタリングされます。セキュリティ・チームや開発チームに瞬時にアラートを出すことで、迅速な対策を可能にします。
- **DevOps ツールとの統合：**本ツールは、CI/CD（継続的インテグレーション / 継続的デリバリ）ツール、パッケージ・マネージャ、IDE、コンテナ・プラットフォーム、コード・リポジトリ、課題トラッカー、アプリケーション・セキュリティ・スイートと統合可能であり、オープンソース検出を自動化し、重大なリスクについての有用な情報を、必要とするチームに必要なタイミングでお届けします。
- **Black Duck KnowledgeBase™：**オープンソース・プロジェクト、脆弱性、ライセンス・データの業界最大のデータベースにアクセスできます。15 年以上蓄積してきたデータ、NVD より 30% 多い脆弱性情報、2,500 超のユニーク・ライセンスに、貴社の BoM をマッピングできます。

Black Duck Professional Edition

SDLC の一環として、オープンソースのリスクおよび使用状況を管理

Black Duck Professional Edition は、自社アプリケーションやコンテナ内のオープンソース・ソフトウェアによるリスクを完全管理するために必要なツール群により、チームをサポートします。Professional Edition には、Standard Edition の機能に加え、セキュリティ・モジュール、ライセンス・コンプライアンス・モジュール、ポリシー・モジュールが同梱されています。

Black Duck のポートフォリオ：



Black Duck モジュールの概要

Black Duck には、オープンソース・リスク管理機能をさらに強化する、各種のアドオン・モジュールが用意されています。これらのモジュールを活用することで、開発者、エンジニア、セキュリティ、DevOps のチームは、それぞれが一番必要なタイミングで、強力な管理機能と有用な情報を得ることができるようになります。任意のモジュールを Standard Edition に追加して導入できます。また、セキュリティ・モジュール、ライセンス・コンプライアンス・モジュール、ポリシー・モジュールは、Professional Edition に含まれています。

セキュリティ・モジュール

より充実した脆弱性データ（Black Duck Security Advisories）と、シノプシスのリサーチセンター「Synopsys Center for Open Source Research and Innovation（COSRI）」が収集・管理する Black Duck 独自の脆弱性データにアクセスできるようになり、自社アプリケーションに影響を及ぼすオープンソースのセキュリティ・リスクをさらに鋭敏に察知できるようになります。Black Duck のセキュリティ・モジュールには、次のようなメリットがあります。

- 新たな脆弱性を早期に通知（最短で NVD の 3 週間前）、1 次ソースから BoM まで 4 時間以内
- /7%MBDL%VDL
- 総合的な技術情報と脆弱性プロファイル
- エクスプロイトの情報（出現時期、現象、利用可能な修正）
- 攻撃のインジケータ

- アップグレード、パッチ、対策の手引、ベンダのアップグレード情報
- 回避策、軽減要因、応急措置
- 影響解析と影響を受けたプロジェクト
- 完全な CVSS 2.0/3.0 スコアリング
- CWE 分類
- CAPEC（Common Attack Pattern Enumeration and Classification）

ライセンス・コンプライアンス・モジュール

ライセンス義務および帰属表示要件について有用な情報を提供することにより、大切な知的財産を守り、オープンソース・ライセンスのコンプライアンス違反のリスクを軽減します。Black Duck のライセンス・コンプライアンス・モジュールには、次のようなメリットがあります。

- 宣言されているライセンスだけではなく、適用されるすべてのライセンスを特定・解析
- プロジェクト単位またはリリース単位で、カスタマイズ可能なオープンソース・ソフトウェア通知レポートを自動生成
- 有名なオープンソース・ライセンスの全文を収録

Black Duck ライセンス・コンプライアンス・モジュールは、オープンソース・コードのスニペット解析をサポートしています。これは、オープンソース・コンポーネントから派生しており、同じライセンス義務が適用される短いコードのまとまりを特定する機能です。スニペット解析機能には、次のようなメリットがあります。

- 一致したコード・スニペットがコンポーネント・ソースで強調表示され、オープンソース BoM の精度が上がり、完成度が高まる
- コードベース全体をスキャンすることも、変更されたファイルのみのデルタスキャンを使用した解析も可能
- ライセンスのリスク、一致したコンポーネント・バージョンのリリース・データ、および普及状況に応じて、一致した箇所を評価して優先順位を付ける
- 一致したコンポーネント名とバージョン、コンポーネント・ライセンス、パス、コンポーネント・ファイルに一致したスキャン済みコードの割合（%）、リリース日付など重要なスニペット・データをレビュー
- 一括編集機能により、潜在的な一致箇所をまとめて確認、フラグ、または無視に設定

ポリシー・モジュール

SDLC 全体を通して、リスクを管理、軽減します。安全でコンプライアンスに準拠した方法でオープンソースを利用するために、ポリシーを定義します。ポリシー違反は自動的に通知されるようになり、実行と対策が高速化されます。Black Duck のポリシー・モジュールには、次のようなメリットがあります。

- 重要なプロジェクト属性（コンポーネント、バージョン、脆弱性指標、ライセンスの詳細など）に基づいて、ポリシーを定義可能
- Black Duck アプリケーション内でポリシー違反トラッキング情報のクリア設定
- DevOps ツールとの統合、CI/CD およびビルド・ツール / パッケージ・マネージャによる自動実行
- Jira および課題トラッキング・ワークフローとの双方向の統合
- ブラックリストとホワイトリストの両方のポリシーをサポート

暗号モジュール

アプリケーションに含まれるオープンソース・コンポーネントの暗号アルゴリズムをトラッキングし、弱い暗号や旧式化したハッシュ・メカニズムを特定することによって、データ・セキュリティ・イニシアチブと暗号輸出規制の遵守をサポートします。Black Duck の暗号モジュールには、次のようなメリットがあります。

- 各オープンソース・コンポーネント・バージョンに含まれる暗号アルゴリズムを特定
- 詳細な暗号データ（鍵の長さ、送信者、ライセンス、特許情報など）
- 弱い暗号化を指摘

Black Duck Binary Analysis

サードパーティのライブラリおよび実行可能ファイルに潜むオープンソースのリスクを特定し、対策を計画

現代のソフトウェアは、オープンソース・ソフトウェア、商用コード、内製コンポーネントを組み合わせたパッチワークと化しています。複雑なソフトウェア・サプライチェーン全体の責任の所在は曖昧なままにされがちですが、その傾向は大きなリスクをはらんでいます。自社アプリケーションの中に脆弱なオープンソース・コンポーネントがあると、サプライチェーンにほころびが生じ、攻撃者に侵入の糸口を与えることになります。コードベースに含まれるソフトウェア・ライブラリ、実行可能ファイル、ベンダ提供バイナリに潜む未対策のリスクを特定するため、対策を講じましょう。Black Duck Binary Analysis には、次のようなメリットがあります。

- ソース・コードがなくても、事実上すべてのコンパイル済みソフトウェア、ファームウェア、モバイル・アプリケーション、インストーラー・フォーマットを解析可能
- 脆弱なオープンソース・コンポーネントの詳細な BoM を作成（バージョン、場所、ライセンス、既知の脆弱性を含む）
- CVSS 2.0 および 3.0 指標を含む NVD からのデータを使用して、対策のために脆弱性のリスクをランク付け
- 脆弱性の詳細情報にアクセス、ベンダ・アドバイザリやパッチなどへのリンクを提供
- スキャン済みソフトウェアに新しい脆弱性が見つかると、自動的にアラート
- オープンソースのライセンス宣言およびコンプライアンス違反の潜在的リスクを特定
- REST API を利用して、重要なリスク軽減および対策タスクを高速化／自動化可能
- ソフトウェア・パッケージに含まれている機密データ（公開鍵、秘密鍵、URL、IP アドレス、メールアドレスなど）の意図しない漏洩が発生する可能性がある箇所を発見
- Android アプリや iOS アプリのバイナリ・コードの中に設定されているパーミッション情報を提供
- エクスプロイト対策なしでコンパイルされたコンポーネントや、危険な実行構成を含むコンポーネントを特定

シノプシスの特色

シノプシスのソフトウェア インテグリティ グループは、企業が安全で高品質のソフトウェアを構築し、リスクを最小限に抑えながらスピードと生産性の最大化に貢献します。シノプシスは、アプリケーション・セキュリティのリーダーであり、静的解析、ソフトウェア・コンポジション解析、動的解析ソリューションを提供しており、独自のコード、オープンソース・コンポーネント、およびアプリケーションの動作における脆弱性や欠陥を迅速に見つけて修正します。業界をリードするツール、サービス、専門知識を組み合わせることで、シノプシスは DevSecOps におけるセキュリティと品質を最大化し、ソフトウェア開発のライフサイクル全体にわたって組織を支援します。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社 ソフトウェア インテグリティ グループ
〒 158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス
TEL: 03-6746-3600
Email: sig-japan-sales@synopsys.com
www.synopsys.com/jp/software

SYNOPSYS®
Silicon to Software™

09/25/18.bd-modules-ds.