SYNOPSYS®

Black Duck
ソフトウェア・コンポジション解析

ソフトウェア・サプライチェーン全体でオープンソースを保護・管理

概要

Black Duck は、アプリケーションやコンテナおよび infrastructure-as-code (IaC) 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・コードの可視性を最大限に高め、ソフトウェア・サプライチェーン全体、およびアプリケーション・ライフサイクル全体にわたってサードパーティ・コードを管理します。

ソースコードとバイナリの両方をサポートした統合ソリューション

業界で唯一、オープンソースの広範なリスク管理と詳細なバイナリ解析機能を統合し、クラス最高の SCA ソリューションを実現した Black Duck は、オープンソースやその他のサードパーティ・ソフトウェアの使用に伴うリスクを最小限に抑えます。平均的なコードベースの 70% をオープンソースが占めるとも言われる現在、Black Duck を導入することで開発、運用、調達、セキュリティ・チームには以下の利点がもたらされます。

- 個々の脆弱性に関する詳細な対策の手引きと技術解説を提示しながら、ソフトウェア開発ライフサイクル（SDLC）の各ステージで**セキュリティ脆弱性を検知・修正します**。
- 2,750 種類以上のライセンスに対応した業界最大規模のオープンソース・ナレッジベースを使用し、アプリケーションで使用されているオープンソース（断片的利用を含む）が適用するライセンスを検出します。**ライセンス違反のリスクを解消し**、知的財産を保護します。
- 品質が不十分なオープンソース・コードに起因する運用リスクの指標を用いて、**開発コストの高騰とコード劣化を防止します**。
- 事実上すべてのソフトウェア、ファームウェア、IaC、ソースコードをスキャンして、**完全なソフトウェア部品表（SBOM）を生成**します。
- 生成した BOM に影響を与える**新たな脆弱性を自動で監視します**。カスタム・ポリシーやワークフロー・トリガーにより修正作業を迅速化し、リスク・エクスポージャーを減らします。

検出

- コード、バイナリ、コンテナに含まれるオープンソースを**特定します**
- 部分的に利用しているコンポーネントや変更されたコンポーネントも**検出します**
- DevOps との統合によりスキャンを**自動化します**

保護

- 既知の脆弱性とコンポーネントを**紐付けます**
- ライセンスおよびコンポーネントの品質に関するリスクを**特定します**
- 開発中およびリリース後に見つかった脆弱性も**監視します**

管理

- オープンソースの使用およびセキュリティに関するポリシーを**設定・適用します**
- DevOps との統合によりポリシーの適用を**自動化します**
- 修正作業に優先度を**割り当てて追跡します**

主な利点

解析の精度と効率が向上

宣言済みコンポーネント、ファイル固有のハッシュ値、ビルド中に解決された依存関係、オープンソース・コードの断片的利用を追跡する Black Duck 独自のマルチファクタ検出技術により、オープンソースの利用をこれまで以上に正確に特定し、完全な BOM を生成・検証します。Black Duck はこれらのスキャン手法を効率的な方法で適用し、SDLC のすべての段階と役割にセキュリティとコンプライアンスをもたらします。これには、IDE での Rapid Scan や、ビルドやビルド後の段階でより深い解析を行うための CI/CD やバイナリ・リポジトリ・ツールとの統合が含まれます。

脆弱性を短時間で検知・修正

Black Duck は、公開されている分類データ（NVD など）とサイバーセキュリティ・リサーチ・センター（CyRC）独自の詳細な解析結果の両方に基づいてオープンソースのセキュリティ・リスクを判定します。新しく見つかった脆弱性は NVD で公開される数週間前に通知されるため、対策実施の猶予期間を確保できます。また、シノプシス独自の強力な脆弱性データおよび Black Duck Security Advisory（BDSA）として以下の情報も提供されます。

- 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、影響度解析
- CVSS 2/CVSS 3 スコアリングおよび CWE 分類データ
- CAPEC（Common Attack Pattern Enumeration and Classification）
- NVD では提供されない現状値
- 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
- 脆弱なコードがアプリケーションから呼び出されているかどうかを判断するための脆弱性影響分析
- 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
- 脆弱性は、深刻度、ソリューションの可用性、悪用可能性、CWE、到達可能性など、複数の重要なデータ・ポイントに基づいて優先的に修正されます

セキュリティおよび使用に関するポリシーを自動で適用

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 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。

ソースコードなしでもオープンソースのリスクを特定

Black Duck をツールキットに加えると、ソースコードがなくてもベンダから調達したバイナリを短時間で簡単に解析し、ソフトウェア・サプライチェーンに潜む弱点を特定できます。具体的な対策方法を示した詳細な指標データに基づいてテクノロジの調達と利用を決定できるため、リスクを未然に防止できます。Black Duck のインテリジェント・スキャン・クライアントはターゲット・ソフトウェアがソースかコンパイル済みバイナリかを自動的に判断し、サードパーティ・ソフトウェア・コンポーネント、関連するライセンス、およびアプリケーションに影響する既知の脆弱性をすべて特定してカタログを作成します。

Black Duck | ソース＆パッケージ・マネージャー・スキャニング

■ Black Duck only
✖ BDBA only

スキャニング

言語

- C
- C++
- C#
- Clojure
- Erlang ■
- Golang
- Groovy
- Java
- JavaScript ■
- Kotlin
- Node.js ■
- Objective-C
- Perl ■
- Python ■
- PHP ■
- R ■
- Ruby
- Scala
- Swift ■
- .NET Cloud technologies

パッケージ・マネージャー

- NuGet ■
- Hex ■
- Vndr ■
- Godep ■
- Dep ■
- Maven ■
- Gradle ■
- Npm ■
- CocoaPods ■
- Cpanm ■
- Conda ■
- Pear ■
- Composer ■
- Pip ■
- Packrat ■
- RubyGems ■
- SBT ■
- Bazel
- Cargo
- C/C++(CLang)
- GoLang
- Erlang/Hex
- Rebar
- Python
- Yarn
- Yocto
- Conan

BDBA パッケージ・マネージャー・サポート

- Linux ディストリビューション・パッケージ・マネージャー : データベースの情報を活用して、コンポーネント情報を抽出します。 .
- 残りの 4 つの方法は、Java バイトコードにのみ適用可能です。
  - pom：JAR ファイルの pom.xml または pom.properties ファイルから Java パッケージ、グループ名、およびバージョンを抽出します。
  - マニフェスト：JAR ファイルの MANIFEST.MF ファイルのエントリから Java パッケージ名とバージョンを抽出します。
  - jar-filename：jar-filename から Java パッケージ名とバージョンを抽出します。
  - hashsum：JAR ファイルの sha1 チェックサムを使用して、既知の Maven Central 登録済み Java プロジェクトから検索します。

バイナリ・フォーマット

- Native バイナリ
- Java バイナリ
- .NET バイナリ
- Go バイナリ

圧縮フォーマット

- Gzip (.gz)
- bzip2 (.bz2)
- LZMA (.lz)
- LZ4 (.lz4) ✖
- Compress (.Z)
- XZ (.xz)
- Pack200 (.jar)
- UPX (.exe)
- Snappy
- DEFLATE
- zStandard (.zst) ✖

アーカイブ・フォーマット

- ZIP (.zip,.jar,.apk およびその他の形式)
- XAR (.xar) ✖
- 7-Zip (.7z)
- ARJ (.arj)
- TAR (.tar)
- VM TAR (.tar) ✖
- cpio (.cpio)
- RAR (.rar)
- LZH (.lzh) ✖
- Electron archive (.asar) ✖
- DUMP

インストール・フォーマット

- Red Hat RPM (.rpm)
- Debian package (.deb)
- Mac インストーラ (.dmg, .pkg)
- Unix シェル・ファイル・インストーラ (.sh, .bin)
- Windows インストーラ (.exe, .msi, .cab)
- vSphere インストレーション・バンドル (.vib) ✖
- Bitrock インストーラ ✖
- 対応しているインストール・ジェネレータ・フォーマット :
  - 7z, zip, rar self extracting .exe ✖
  - MSI インストーラ ✖
  - CAB インストーラ ✖
  - InstallAnywhere ✖
  - Install4J ✖
  - InstallShield ✖
  - InnoSetup ✖
  - Wise インストーラ ✖
  - Nullsoft Scriptable Install System (NSIS) ✖
  - WiX インストーラ ✖

ファームウェア・フォーマット

- Intel HEX ✖
- SREC ✖
- U-Boot ✖
- Arris ファームウェア ✖
- Juniper ファームウェア ✖
- Kosmos ファームウェア ✖
- Android sparse ファイルシステム ✖
- Cisco ファームウェア ✖

ファイル・システム / ディスク・イメージ

- ISO 9660 / UDF (.iso) ✖
- Windows イメージング ✖
- ext2/3/4 ✖
- JFFS2 ✖
- UBIFS ✖
- RomFS ✖
- Microsoft ディスク・イメージ ✖
- Macintosh HFS ✖
- VMware VMDK (.vmdk, .ova) ✖
- QEMU コピー・オン・ライト (.qcow2) ✖
- VirtualBox VDI (.vdi) ✖
- QNX—EFS, IFS ✖
- NetBoot イメージ (.nbi) ✖
- FreeBSD UFS ✖

コンテナ・フォーマット

- Docker

対応する IaC ファイル・フォーマット

- HCL (Terraform)
- HTML
- JSON
- JSX
- TOML
- TSX
- Vue
- XML
- YAML

Black Duck | 統合

クラウド・テクノロジー

クラウド・プラットフォーム

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Pivotal Cloud Foundry

コンテナ・プラットフォーム

- Docker
- OpenShift
- Pivotal Cloud Foundry
- Kubernetes Package managers

データベース

- PostgreSQL

DevOps ツール

IDE

- Eclipse
- Visual Studio IDE
- IntelliJ IDEA
- WebStorm
- PyCharm
- RubyMine
- PhpStorm
- VS Code
- Android Studio

CI ツール

- Jenkins
- TeamCity
- Bamboo
- Team Foundation Server
- Travis CI
- CircleCI
- GitLab CI
- Visual Studio Team Services
- Concourse CI
- AWS CodeBuild
- Codeship
- Azure DevOps
- GitHub Actions
- OpenShift

ワークフローと通知

- Jira
- Slack
- Email
- SPDX
- Azure Boards
- Microsoft Teams

バイナリおよびソース・リポジトリ

- Artifactory
- Nexus

アプリケーション・セキュリティ・スイート

- IBM AppScan
- Micro Focus Fortify
- SonarQube
- ThreadFix
- Cybric
- Code Dx
- Fortify
- ZeroNorth

シノプシスの特色

シノプシスがご提供する統合型ソリューションは、ソフトウェア開発とデリバリのあり方を根底から変革し、ビジネス・リスクに対処しながらイノベーションを加速することを可能にします。シノプシスのソリューションにより、開発者はスピードを落とすことなくセキュアなコードを作成することができます。開発およびDevSecOps チームはスピードを犠牲にすることなく、開発パイプライン内でテストを自動化できます。セキュリティ・チームは先手を打ったリスク管理が可能となり、組織にとって最も重要な問題の修正に集中できます。シノプシスは業界随一のノウハウを活かし、最適なセキュリティ・イニシアティブの立案と実行をご支援します。信頼性の高いソフトウェアの構築に必要なものをワンストップでご提供できるのは、シノプシスだけです。

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
〒 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@synopsys.com