Black Duck Binary Analysis

ソフトウェア・サプライチェーンに潜むセキュリティ、ライセンス、コード品質のリスクを管理

製品概要

Black Duck® Binary Analysis は、現代の複雑なソフトウェア・サプライチェーンにまつわるリスクの継続的管理に向けたソフトウェア・コンポジション解析（SCA）ソリューションです。商用アプリケーション、ベンダー支給のバイナリ、およびその他のサードパーティ・ソフトウェアのコンポジション（組成）を可視化することにより、調達、運用、開発チームを強力にサポートします。

リスクの現状

ビジネスを支える重要インフラにおけるイノベーションの加速と効率化を図るため、企業はさまざまなサプライヤからシステムやソフトウェアを調達しています。このように革新的なテクノロジーをサードパーティ・コンポーネントの形で入手していく中で、企業は複雑なソフトウェア・サプライチェーンへの依存を強めています。このアプローチには多くの利点がある一方で、セキュリティに関して以下のように多くの課題も存在します。

- **ソフトウェアのパッチワーク化：**現在のソフトウェアには無償のオープンソース・ソフトウェア（FOSS）、商用オフザシェルフ（COTS）コード、内製コンポーネントなど何らかのサードパーティ・コンポーネントが含まれていると言って過言ではありません。こうしたサードパーティ・コンポーネントには脆弱性が存在することもよくありますが、調達時にセキュリティが考慮されることはほとんどありません。
- **責任の所在の不明確化：**ソフトウェアやシステムを購入する際、セキュリティと堅牢性は上流で確保されているものと考えがちです。ソフトウェア・サプライチェーンを手放しで信用することはリスクを抱え込むことにつながります。
- **攻撃者にとって格好の標的：**脆弱なサードパーティ・ソフトウェアはサプライチェーン全体でセキュリティ上、攻撃を受けやすいポイントとなり、攻撃者に侵入の糸口を与えることになります。

主な特徴

ほとんどすべてのものをスキャン可能

Black Duck Binary Analysis はサードパーティおよびオープンソース・コンポーネントを追跡して完全なソフトウェア部品表（SBOM）を短時間で生成するほか、既知のセキュリティ脆弱性や関連するライセンス、コード品質のリスクを洗い出します。Black Duck Binary Analysis はソースコードではなくバイナリ・コードを解析するため、デスクトップおよびモバイル・アプリケーションから組み込みシステム・ファームウェアまで、事実上あらゆるソフトウェアをスキャンできます。

使いやすいダッシュボード

Black Duck Binary Analysis の対話型ダッシュボードには、コンポジションの概要およびスキャン済みソフトウェアの全体的な健全さに関する以下のサマリ情報が表示されます。

- **ソフトウェア部品表（SBOM）：**検出した各サードパーティ・コンポーネントについて、バージョン、ロケーション、ライセンス取得状況、既知の脆弱性など詳細な情報を提供します。SPDX や CycloneDX などの標準化された形式で SBOM をエクスポートします。
- **脆弱性評価：**先進の独自エンジンを使用して、検出した各脆弱性について NIST が管理する脆弱性情報データベース NVD（National Vulnerability Database）から CVE（Common Vulnerabilities and Exposures）番号や危険度などの詳細な関連情報を提示
- **オープンソース・ライセンス・レポート：**必要なライセンスを特定するだけでなく、ライセンス競合の可能性までを指摘し、ソフトウェアのライセンス違反を防止

セキュリティをさらに一歩進める

Black Duck Binary Analysis は、セキュリティ上の脆弱性以外にも以下のようなアタック・ベクターを特定することで、セキュリティをさらに強化します。

- **情報漏洩：**クリアテキストのパスワード、アクティブな AWS キー、開発者の資格情報、IP アドレスなど、アプリケーションに不用意に残された表層データを明らかにすることで、リスク計算をさらに強化します。
- **コンパイラ・スイッチ：**ソフトウェアをコンパイルする際に使用されているコンパイラのセキュリティ手法を特定し、残存リスクと潜在的なセキュリティ・ホールを評価します。
- **モバイルのパーミッション：**機密データのセキュリティやコンプライアンス要件に影響を与える可能性のあるモバイル・アプリケーションに必要な権限を特定します。

主な機能

Black Duck Binary Analysis はソースコードがなくてもシステムとソフトウェアを解析できるため、ソフトウェア・サプライチェーン全体でセキュリティ上、脆弱な箇所を短時間で簡単に見つけることができます。

- **ほとんどすべてのソフトウェア、ファームウェアを数分でスキャン**。デスクトップやモバイルのアプリケーション、組込みシステム・ファームウェア、仮想アプライアンスなど基本的にすべてのソフトウェアまたはファームウェアの内部を可視化できます。
- **ソースコード不要**。評価したいソフトウェアをアップロードするだけで Black Duck Binary Analysis が数分で完全なバイナリまたはランタイム解析を実行します。このブラックボックス手法は、攻撃者が実際に脆弱性検出に使用するアプローチを踏襲しています。
- **包括的な SBOM を作成**。すべてのサードパーティ・ソフトウェア・コンポーネントおよびライセンスを検出してカタログを作成します。
- **リスク・プロファイルの管理**。ソフトウェア・コンポーネントに存在する既知の脆弱性およびライセンス違反を検出し、ソフトウェアの健全性を診断します。テクノロジーの利用と調達に関して、現実的な評価指標を用いてデータに基づく意思決定が行えます。
- **「コード劣化」の問題に事前に対処**。過去にスキャン済みのソフトウェアに新たな脆弱性が見つかった場合、自動アラートでお知らせします。
- **選べる 2 つのご利用形態**。Black Duck Binary Analysis はクラウド型サービスとしても、オンプレミス型アプライアンスとしてもご利用いただけます。

Black Duck Binary Analysis | バイナリおよびパッケージ・マネージャー・スキャン

言語
- C
- C++
- C#
- Clojure
- CocoaPods
- Golang
- Groovy
- Java
- JavaScript
- Kotlin
- Objective-C
- Python
- Ruby
- Scala
- .NET Cloud technologies

パッケージ・マネージャー・サポート
- Npm
- Distro-package-manager: Leverages information from a Linux distribution package manager database to extract component information.
- The remaining four methods are only applicable to Java bytecode:
  - pom: Extracts the Java package, group name, and version from the pom.xml or pom.properties files in a JAR file.
  - manifest: extracts the Java package name and version from the entries in the MANIFEST.MF file in a JAR file.
  - jar-filename: Extracts the Java package name and version from the jar-filename.
  - hashsum: Uses the sha1 checksum of the JAR file to look it up from known Maven Central registered Java projects.

バイナリ・フォーマット
- Native binaries
- Java binaries
- .NET binaries
- Go binaries

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, and other derivatives)
- 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 installers (.dmg, .pkg)
- Unix shell file installers (.sh, .bin)
- Windows installers (.exe, .msi, .cab)
- vSphere Installation Bundle (.vib)
- Bitrock Installer
- Installer generator formats that are supported:
  - 7z, zip, rar self extracting .exe
  - MSI Installer
  - CAB Installer
  - InstallAnywhere
  - Install4J
  - InstallShield
  - InnoSetup
  - Wise Installer
  - Nullsoft Scriptable Install System (NSIS)
  - WiX Installer

ファームウェア・フォーマット
- Intel HEX
- SREC
- U-Boot
- Arris firmware
- Juniper firmware
- Kosmos firmware
- Android sparse file system
- Cisco firmware

ファイル・システム / ディスク・イメージ
- ISO 9660 / UDF (.iso)
- Windows Imaging
- ext2/3/4
- JFFS2
- UBIFS
- RomFS
- Microsoft Disk Image
- Macintosh HFS
- VMware VMDK (.vmdk, .ova)
- QEMU Copy-On-Write (.qcow2)
- VirtualBox VDI (.vdi)
- QNX—EFS, IFS
- NetBoot image (.nbi)
- FreeBSD UFS

コンテナ・フォーマット
- Docker

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