SYNOPSYS®

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・コンポーネント表（BoM）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。

- **ソフトウェアの部品表（BoM）：**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示
- **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 BoM 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。

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な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不具合を迅速に見つけて修正します。

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Email: sig-japan-sales@synopsys.com
TEL: 03-6746-3600 www.synopsys.com/jp/software

SYNOPSYS®
Silicon to Software™
©2020 Synopsys, Inc. All rights reserved. Synopsys は Synopsys, Inc. の米国およびその他の国における登録商標です。
Synopsys の商標に関しては、こちらをご覧ください。http://www.synopsys.com/copyright.html その他の会社名および商品名は各社の商標または登録商標です。
03/31/20.ds-bd-binaryanalysis-ja.