

脅威検知 (THREAT DETECTION)

包括的な脅威検知分析でソフトウェアの完全性を確保

概要

近年、ソフトウェアのサプライチェーンにおける脆弱性が悪用され、改ざんやマルウェアの混入など、重要なビジネスソフトウェアが脅かされています。

Software Trust Manager Threat Detection (脅威検知) は、オープンソースソフトウェア、著作権ソフトウェア、コンテナ、リリースパッケージの脅威と脆弱性を高度かつ包括的に検知することで、ソフトウェアのサプライチェーンを保護します。

ReversingLabs を実装した Software Trust Manager Threat Detection (脅威検知) は、独自の再帰的バイナリ解析により、ソフトウェアオブジェクトの最下層をスキャンすることを可能にします。世界最大のマルウェア/安全なソフトのリポジトリを活用して、脅威を検知します。JAVA、.NET、Python、macOS、Linux、APK、Docker イメージなど4800以上のファイルタイプに対応しています。

また、Threat Detection (脅威検知) は、ソフトウェア構成の透明性を提供するために、新たな規制要件に準拠した包括的なソフトウェア部品表を生成します。

主な特長

- コンパイルされたソフトウェアにマルウェア、脆弱性、機密情報が含まれるリスクを低減
- 脅威の検知をソフトウェアのサプライチェーンに組み込むことで、コントロールを一元化
- 検知されたリスクの優先順位に基づき、ポリシーに基づいた「GO/NO GO」アプローチでソフトウェアのリリースを行うことで、ソフトウェアの信頼性を向上
- ソフトウェア部品表 (SBOM) に関する新たな規制要件に対応

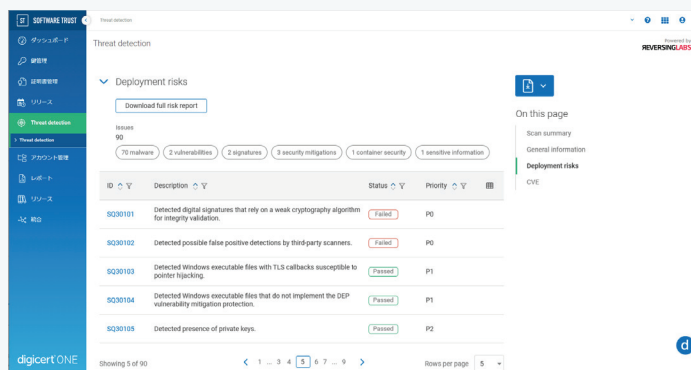
主な機能

ソフトウェアバイナリの脅威と脆弱性を検出する マルウェア、ソフトウェア改ざん、CVE検出、機密漏洩などの脆弱性を、サードパーティのオープンソースや商用コードを含むバイナリから検知します。

コード署名と同じワークフローで脅威をスキャン 安全なコード署名を行う前に、同じワークフローとプラットフォームを使いソフトウェアをスキャンすることで、改ざんの可能性を最小限に抑えます。

迅速かつ自動化された脅威検知
あらゆるDevOpsプラットフォームのCI/CDパイプラインに脅威検知を簡単に組み込むことができます。様々なプラットフォームやバイナリタイプで動作します。

複雑なソフトウェア構成の報告、分析 ソフトウェア部品表 (SBOM) およびリスク脆弱性報告書は、大統領令 EO14028、M-22-18などの新しい規制要件に対応するために利用できます。



Threat Detection (脅威検知) は、ソフトウェアバイナリをスキャンしてマルウェアなどの脆弱性が存在しないことを確認し、SBOMとリスク分析レポートを作成します。