Kaspersky Open Source Software Threats Data Feed

kaspersky bring on the future

ソフトウェアサプライチェーン攻撃

このタイプの攻撃では、サイバー犯罪者はソフトウェアベンダーのシステムやソフトウェア開発ツールを侵害し、顧客に配布する前のソフトウェアに悪意のあるコードやマルウェアを挿入します。

Kaspersky Open Source Software Threats Data Feed

サイバー脅威は常に進化し、ますます巧妙化しているため、それに対抗する企業のセキュリティの維持はより困難になっています。Kaspersky Open Source Software Threats Data Feedは、脅威と脆弱性に関する最新の情報を提供し、企業のネットワーク、エンドポイント、および重要なデータの保護を実現します。Kaspersky Open Source Software Threats Data Feedは、DevSecOpプロセスへの組み込みにより、使用されているオープンソースコンポーネントを監視し、内部に潜む脅威を検知することを目的として設計されています。

新しいアプローチでセキュリティを確保

ソフトウェア開発者の大半は、開発サイクルにオープンソースソフトウェアパッケージを含めており、これらのパッケージの健全性を信頼する傾向にあります。

サイバー脅威の件数と攻撃の深刻度が上昇し続ける中、ソフトウェア開発における従来のDevOpsの手法は、よりセキュリティを重視したアプローチ、いわゆるDevSecOpsへと移行し始めています。このアプローチは、初期の計画および設計段階から開発、テスト、そしてそれ以降の段階に至るまで、セキュリティ対策を実行することを提唱しています。この考え方は、開発サイクルで使用するすべてのオープンソースソフトウェアにも適用する必要があります。

Kasperskyは有用性が高いデータフィードを設計し、このセキュリティ最優先のアプローチをオープンソースソフトウェアに適用できるようにしました：それが、Kaspersky Open Source Software Threats Data Feedです。これはバイナリを使用しないテキストのみのデータセットで、オープンソースパッケージ内の既知の脅威と脆弱性をすべて明らかにします。

脅威の種別

Kaspersky Open Source Software Threats Data Feedは、次に挙げる種別の脅威を網羅しています：

特定の地域で機能が変更され、侵害されたパッケージ

クリプトマイナーやハッキングツールなど、危険な可能性があるソフトウェアを含むパッケージ

政治的なメッセージを含む侵害されたパッケージ

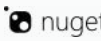
脆弱性があるパッケージ

悪意のあるコードが含まれるパッケージ

パッケージマネージャー











脆弱性アドバイザリ





フィードに含まれる内容

パッケージマネージャー

このフィードは、定期的にスキャンされたリポジトリのパッケージに関する情報を次のパッケージマネージャー*から提供します：Pypi、Npm、NuGet、Maven、Composer、Go、Rpm、Debian。

脆弱性アドバイザリ

あらゆるリポジトリに存在するすべてのパッケージが、次の脆弱性アドバイザリと自動的に照合されます：GitHub Security Advisory, CVE MITRE, Debian、セキュリティアドバイザリ、CentOS Security Alerts、RedHat Security Advisory（このアドバイザリへのリンクのみ提供）。

コンテキスト

パッケージのリストともに、次の有用なコンテキストも提供されます：

脆弱性に関するコンテキスト：

- エコシステムへの接続
- システムへの影響
- 脆弱なバージョンのリスト
- 脆弱なバージョンに関する自動化用CPE/PURL
- 脆弱性に対してパッチが適用された推奨バージョンのリスト
- OS バージョンのサポート（*nix パッケージの場合）
- 脆弱性関連のアドバイザリに対するリンク
- 現在出回っているエクスプロイトのハッシュ

悪意のあるパッケージ、または侵害されたパッケージの場合：

- エコシステムへの接続
- システムへの影響：マルウェアやハッキングツールなど
- 深刻度
- セキュリティが確保されていないパッケージのバージョン
- セキュリティが確保されていないパッケージのバージョンのハッシュ
- CWE（共通脆弱性タイプ一覧）：現時点ではマルウェアパッケージのみ

事業価値

下記を実現し、組織に大きな事業価値を供与します：

脅威の検知能力を改善

オープンソースソフトウェアに関連する最新のサイバー脅威と脆弱性に関するインテリジェンスをリアルタイムで提供します。これにより、組織の脅威の検知能力が向上し、想定される攻撃を被害の発生前に検知することができます。

インシデントレスポンスの強化

組織が脅威に迅速かつ効果的に対応できるよう、有用性が高い情報を提供します。これにより、インシデントの影響を最小限に抑え、インシデントレスポンスに必要な時間とリソースを削減することができます。

セキュリティ態勢の強化

組織が使用するオープンソース製品に関連する最新のセキュリティ脅威と脆弱性に関する情報を提供します。この情報は、組織が脆弱性を迅速に特定し、是正処置を講じる際に役立ち、サイバー犯罪者による脆弱性攻撃のリスクを低減します。

セキュリティリスクの低減

組織がオープンソースソフトウェアを使用することに伴うセキュリティリスクを低減します。これにより、組織の重要なデータ、知的財産、および評判を保護することができます。

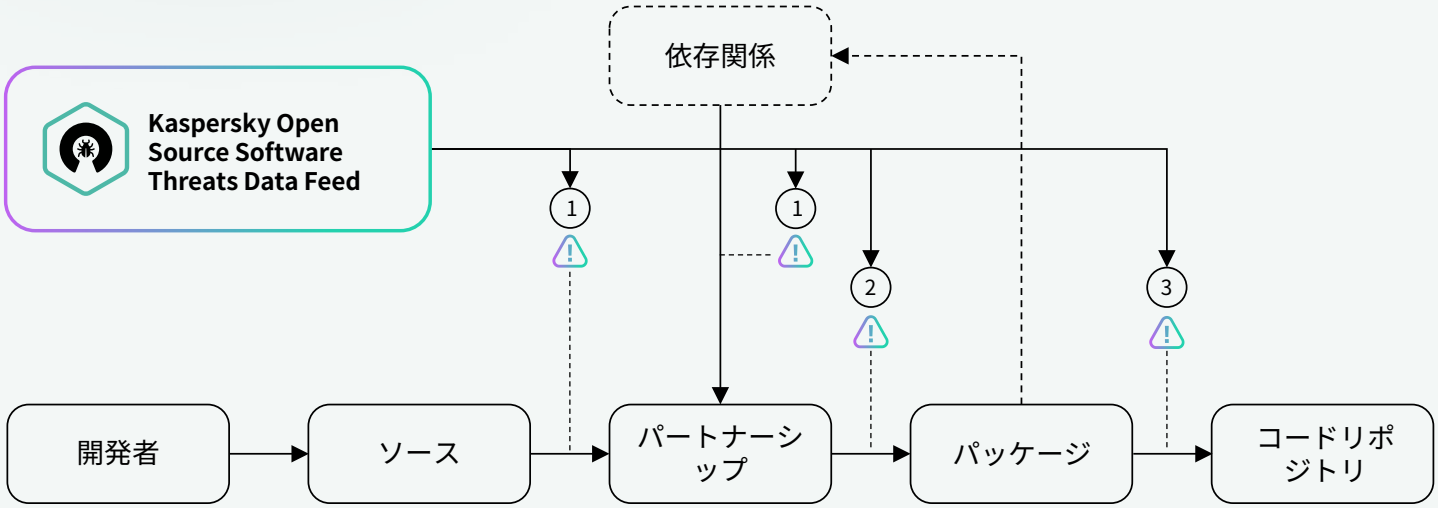
時間とリソースの節約

組織がオープンソースソフトウェアに関連する最新のセキュリティ脅威と脆弱性に関する情報を入手するための、費用対効果に優れた効率的な方法を提供します。これにより、組織は独自の脅威インテリジェンスシステムの構築と維持にかかる時間と費用を削減できます。

フィードはJSON形式で提供されます。

ユースケース

Kaspersky Open Source Software Threats Data Feedの推奨するユースケースは次の通りです：1つまたは複数のパラメータに基づいて、開発で使用するパッケージと、フィードからのパッケージの識別子（パッケージ名、パッケージバージョンなど）を照合します。



統合ポイント

1

オープンソース開発者がリポジトリからパッケージをダウンロードする段階（統合ポイント - リポジトリのプロキシ）。

2

ソースコードの開発者によるコンパイルの段階（問題の起こりうる依存パッケージのチェックも含む）（統合ポイント - 組み立てライン）。

3

ソースコードをリポジトリに公開する段階（統合ポイント - 公開メカニズム）

問題のあるパッケージを検知した場合に推奨される対応は、組織が採用したポリシーに従って行動することです（開発者への通知、リスク処理、ブロックなど）。

Kaspersky Threat Intelligence

詳細はこちら

www.kaspersky.co.jp

#kaspersky
#bringonthefuture