内部脅威検出

コードの内部に潜む見えない脅威とは?

ソフトウェアに対する最大の危険は目に見える脅威ではなく目に見えない脅威かもしれません。

ブラック・ダックが採用する画期的かつ体系的な手法では、コードがアクティブ化されて攻撃を仕掛けるか、またはデータを盗み出す前に、悪質である可能性のあるコードを無効化します。

コードを詳しく分析する

静的アプリケーションセキュリティテスト（SAST）とバイナリスキャンを組み合わせることで、正常に見えても実はセキュリティ侵害やシステムに損害を与えるような好ましくない結果をもたらすことを意図したあらゆるコードをソフトウェアシステムやスクリプトのどんな部分からでも発見します。

1. 理解

エキスパートによる顧客への聞き取り調査で SDLC と脆弱性管理計画を把握します。

2. 解析

独自ツールを利用した SAST によってバイナリコードまたはソースコードを解析し、要注意ポイントを特定します。また、手作業による解析を実施し、要注意ポイントに悪質である可能性のあるコードが含まれていないかについても調査します。

3. アドバイス

最後に悪質なコードが含まれている恐れのある要注意ポイントとそれぞれの危険度評価を付けて最終報告をまとめます。最終的に最善の解決方法を選択できるようアドバイスします。

発見可能な脅威

- バックドア
- 組織横断的な内部脅威アクター（悪意のある開発者）
- Rootkit のような動作
- 稼働中のバイナリ、設定、データ中の疑わしいパターン
- 時限爆弾
- トロイの木馬

内部脅威検出には以下のような機能があります

- 稼働中のバイナリ、設定、データ中の疑わしいパターンを発見します。
- 脆弱性を表す特徴がないため一般的なセキュリティツールでは発見できない悪質なコードを特定します。
- 組織横断的な内部脅威アクターを発見します（例えば、システム管理者、IT の運用、構成、変更管理、開発者など）。
- 悪質なコードの適切な管理方法および一般的な脆弱性修正戦略に関する専門家のアドバイスを利用できます。

常にリスクを排除する指針を示します

一番のメリットは、ただ結果を手渡せば終わりではないという点です。疑わしいポイントすべてに関して悪質なコードである確度とその理由を説明し、発見された悪質なコードを管理できるよう助言し、効果的な脆弱性修正戦略を提示します。

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