SYNOPSYS®

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。

シノプシス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。

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の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を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欠陥を迅速に見つけて修正します。 業界をリードするツール、サービス、専門知識を組み合わせることで、SynopsysはDevSecOpsにおけるセキュリティと品質を最大化し、ソフトウェア開発のライフサイクル全体にわたって組織を支援します。

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

SYNOPSYS®
Silicon to Software™