

脅威モデリング

アプリケーションの 設計に潜む弱点を 洗い出します

脅威モデリングは、危害を生じうるタイプの脅威エージェントを特定するとともに、悪意あるハッカーの視点に立ち、ハッカーがどれだけの損害を与えることができるかを明らかにします。一般的に列挙されている攻撃以外に、新種の攻撃やその他の手法では考慮されることのない攻撃まで視野を広げて考えます。

回避すべき 4 つのセキュリティ・シンクホール

脅威モデリングでは、以下のものを特定してアタック・サーフェス全体を定義します。

- **一般的な攻撃では判断できない脅威**
すべてのシステムにとって、一般的な攻撃が必ずしもリスクになるわけではありません。脅威モデルは、個々のシステム構成に特有の攻撃を特定します。
- **脅威エージェントがアーキテクチャのどこに存在するか**
脅威エージェントの場所、動機、スキル、能力をモデル化し、潜在的な攻撃者がシステム・アーキテクチャのどの部分に存在するかを特定します。
- **トップ N リスト、攻撃者、最悪シナリオ**
脅威モデルを作成・更新し、アプリケーションに関する内部および外部の攻撃者に対して常に先手を打ったフレームワークを維持します。
- **追加の保護が必要なコンポーネント**
資産、脅威エージェント、セキュリティ対策を明らかにし、どのコンポーネントが最も攻撃の標的になりやすいかを突き止めます。

組織のニーズに合わせてアプローチを調整

リスク・プロファイルとリスク許容度は組織ごとに異なるため、組織のニーズと予算に合わせてアプローチを調整します。シノプシスの全体的な視野に立った脅威モデリング・アプローチは、2 つの基本的なステップで構成されます。

1. システムの主要なソフトウェア・コンポーネント、セキュリティ対策、資産、信頼境界線のレビューを実施します。
2. 次に、既存の対抗策に対するこれらの脅威をモデル化し、潜在的な結果を評価します。

ハッカーを食い止める 最良の方法は、 ハッカーの視点で 考えること

脅威モデリングの6つの利点

セキュリティに真剣に取り組み、以下の目標を達成しようとするなら、脅威モデリングが最も効果的な手段です。

- ・ コード実装前の SDLC の早期段階で問題を検出する
- ・ 従来のテスト手法やコード・レビューでは見落としがちな設計上の欠陥を特定する
- ・ その他の手法では考慮されることのない新種の攻撃を評価する
- ・ テストとコード・レビューの対象を絞り込むことにより、テスト予算を最大化する
- ・ 要件定義プロセスの穴を特定する
- ・ ソフトウェアのリリース前に問題を修正することにより、コードの修正を防ぎ、コストを削減する

脅威モデルには以下のものが含まれます。

- ・ リスクに基づいて優先順位付けした資産
- ・ 発現可能性に基づいて優先順位付けした脅威
- ・ 最も可能性の高い攻撃
- ・ 成功または失敗が予想される現在の対抗策
- ・ 脅威を軽減するための緩和策

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・グループが提供する統合型ソリューションは、ソフトウェア開発とデリバリのあり方を根底から変革し、ビジネス・リスクに対処しながらイノベーションを加速することを可能にします。業界をリードするシノプシスのソフトウェアセキュリティ製品のポートフォリオおよびサービスは、世界で最も包括的であるだけでなく、サードパーティおよびオープンソース・ツールとの連携も可能であり、組織は既存の資産を活用しながら最適なセキュリティ・プログラムを構築することができます。信頼性の高いソフトウェアの構築に必要なものをワンストップでご提供できるのは、シノプシスだけです。

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

©2022 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。2022年9月