WhiteHat Sentinel Source

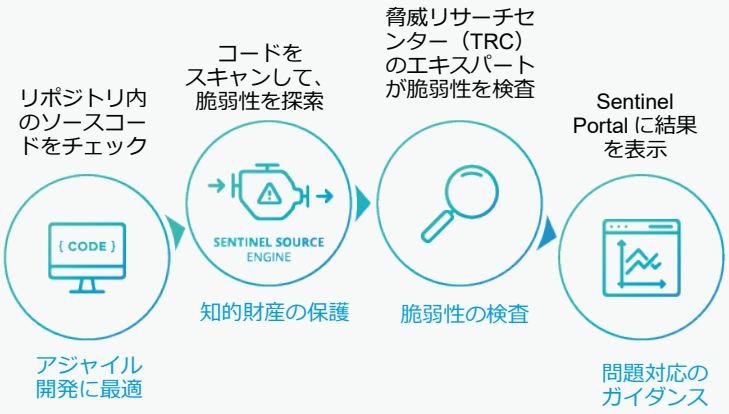
ソフトウェアの開発サイクルにセキュリティの要素を組み込む（DevSecOps）

特にアジャイル環境で顕著なように、ソフトウェアの開発スケジュールがタイトであると開発者は速いペースでコードを量産しなければならず、セキュリティのベストプラクティスを見失ってしまいます。現在、サイバー攻撃の拡大が大きな問題となっており、特に高い評価を受けている企業においても、顧客データの流出が発生しており、それが原因で、ブランドイメージが失墜し、収益が悪化する事態に陥っています。そのため、セキュリティを最優先に考え、アプリケーション開発のレベルでセキュリティを考慮することが欠かせません。侵害が発生してからセキュリティを「固めて」も意味ありません。

コード内に存在する最新の脆弱性を素早く特定して修復

WhiteHat の静的アプリケーションセキュリティテスト（SAST）サービスである Sentinel Source は、ソースコード全体をスキャンして脆弱性を特定し、脆弱性に関する詳しい説明と対応のアドバイスを提供します。特定の脆弱性を対象としてすぐに実装できるピンポイントの修正ソリューションも利用できます。Sentinel Source では次のことが可能です。

- 開発サイクルのどの時点でもコードを評価できます。部分的なコードの評価にも対応しています。
- 評価をスケジューリングして毎日実行することや、必要に応じて実行することが可能です。
- ソースコードは組織の環境内でスキャンできるため、知的財産を外部に持ち出す必要がありません。
- 脆弱性を特定、検査するルールパックを使用して、最新の攻撃に対応できます。
- 常時利用できる自動化されたクラウドベースのプラットフォームにより、組織のニーズに合わせたセキュリティのスケーリングが可能です。
- WhiteHat のコード行数計測ツール（WHLOC）を使用し、サポート対象のファイルタイプを持つアプリのサイズ（コード行数または MB）を簡単に探索、評価できます。



Sentinel Source での処理の流れ

Sentinel Source のエンジンは、セキュリティ上の問題を非常に素早く正確に特定することができます。スキャニングテクノロジーはソースコード言語ごとに最適化されているほか、これまでにないレベルでのスケーリングが可能です。

技術上の特長

評価、検査のできる脆弱性

Sentinel Source は以下のような 50 を超える観点から脆弱性を評価、検査できます。

- アプリケーションの構成の誤り
- 認証情報やセッションの予測
- ディレクトリのインデックス化
- 不十分な認証と承認
- 自動参照カウント
- リクエスト強要
- 情報の漏洩
- 不十分なトランスポート層の保護
- 不十分なバイナリの保護
- クロスサイトスクリプティング
- インジェクション攻撃
- プロセス間通信
- OS コマンディング
- 安全性に欠けた暗号化技術
- SQL インジェクション
- 暗号化関連の攻撃

対応している言語

Sentinel Source は、Web アプリケーションや Web サービス、デスクトップアプリケーション、モバイルアプリケーションで使用する以下のようなさまざまなコーディング言語に対応しています。

ソースコード

- Java
- C# (.NET)
- ASP.NET
- PHP
- JavaScript
- Node.js
- Objective-C (iOS)
- Android
- HTML5
- TypeScript
- Python

バイナリ

- Java
- C# (.NET)

さまざまなデリバリ手法

組織ごとにそのニーズは異なりますが、Sentinel Source では、さまざまなデリバリモデルを提供しており、顧客の現行のインフラストラクチャに柔軟に対応できます。Sentinel Source では、以下の環境にデリバリが可能です。

- オンプレミスの仮想マシンアプライアンス
- クラウドの仮想マシン

Sentinel Source を選択する理由

知的財産を組織の内部にとどめたままでテストを実施

Sentinel Source では、顧客の社内環境でソースコードをテストします。ソースコードやバイナリを別の場所にアップロードする必要はありません。

現実に即した実用性の高い確認済みの情報を入手可能。ほぼすべての誤検知を排除

脆弱性が疑われるすべての事象を WhiteHat の脅威リサーチセンター（TRC）が検査してグループ化するため、レポートが重複するのを避けられます。また、誤検知でないと確認できたバグや不具合だけに集中して修正作業に取り組めるので、余計な時間やコストをかけずに済みます。

セキュリティ上の問題の修正にかかる時間を短縮

WhiteHat のセキュリティエキスパートが提供する問題対応のガイダンスを利用すれば、リソースを最適なかたちで割り当てるべきポイントを問題の影響度や脅威の重大度に応じて容易に判断できるようになります。また、「Ask a Question」や「Directed Remediation」などの組み込みの機能により、セキュリティ上の問題の修正にかかる時間を短縮できます。

WhiteHat SECURITY.

NTT Security

NTT セキュリティ・ジャパン㈱ IoT 事業部
〒101-0021 東京都千代田区外神田 4-14-1 秋葉原 UDX
TEL: 050-3733-0919　E-mail: ntts.nsj-it-all@global.ntt