WhiteHat Sentinel Dynamic

最新のシステム、従来のシステムを問わずにWebフレームワークやWebアプリケーションのセキュリティを維持

現代の組織では、さまざまなWebアプリケーションを展開しています。外部の環境と接する企業Webサイトやカスタマーポータル、ショッピングサイト、あるいは、組織内部に配置されているHRポータルにアクセスするためのログインページなどでも、Webアプリケーションが稼働しています。どこからでもアクセスできるこれらのビジネスクリティカルなWebアプリケーションは今、ハッカーの標的となりやすく、彼らはアプリケーション内の脆弱性を狙った攻撃を仕掛けてバックエンドの企業データベースにアクセスします。

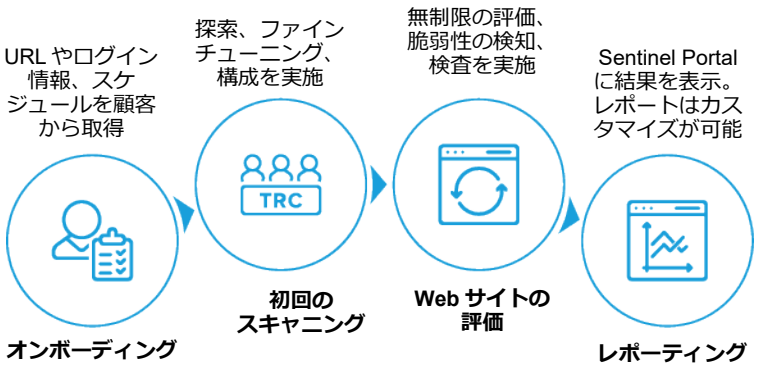
Sentinel Dynamic

WhiteHat Sentinel Dynamicは拡張性の高いWebセキュリティプログラムを素早く導入できるサービスとしてのソフトウェア（SaaS）プラットフォームです。顧客が保有しているWebサイトの数やサイトで変更が発生する頻度に関係なく、需要の変動に合わせたスケーリングが可能です。脆弱性の評価はピットクルースタイルで行います。これにより、高い効率と広範な脆弱性への対応をこれまでにないレベルで実現します。WhiteHatでは、攻撃者の観点から脆弱性を特定するため、それらを狙った攻撃を受ける前に修正を施すことが可能です。

- クラウドベースのプラットフォームにより、ハードウェアを新たに用意したりスキャニングソフトウェアをインストールしたりする必要がありません。
- 無制限かつ継続的な評価を同時に行うことができます。
- Webアプリケーションに加えられたコードの変更を自動的に検知、評価します。
- SIEMやバグ追跡システム、WAFなどと連携するためのオープンAPIが用意されています。
- どの環境にもスケーラブルに対応し、数千のWebサイトを同時に評価します。
- WhiteHatの脅威リサーチセンター（TRC）のセキュリティエキスパートがすべての脆弱性を検査するため、ほぼすべての誤検知が排除されます。

人工知能と機械学習の活用

WhiteHat Sentinel Dynamicでは、機械学習とセキュリティエキスパートのノウハウを融合し、最も精度の高いアプリケーションセキュリティテストプラットフォームを実現して、本番環境のアプリケーションのセキュリティを確保します。高度なトレーニングを受けたTRCのセキュリティエキスパートが何年もかけて貴重なデータを収集しており、これらのデータを使って、AIと機械学習を組み合わせた独自のモデルを開発しています。TRCによる確認を加えた評価の結果が、短期間で自動的に顧客に提供されるため、攻撃が強まるおそれがあるなかで、問題を早期に把握でき、素早い対応が可能になります。



Sentinel Dynamic での処理の流れ

Sentinel Dynamicでは、自動化されたSentinel Scannerと世界最大規模のセキュリティのエキスパートチームを組み合わせ、検査により誤検知がほぼゼロの脆弱性情報と、実用性の高いレポートを提供します。

SENTINEL PE
Premium Edition

- マルチステップのフォームを持ち、コンプライアンス要件の厳しい、ミッションクリティカルで恒久的なWebサイト向けのエディションです。
- SEの機能すべてを利用でき、ビジネスロジックテストが可能です。

SENTINEL SE
Standard Edition

- 必ずしもミッションクリティカルではない恒久的なWebサイト向けのエディションです。
- BEの機能すべてを利用でき、マルチステップやログインに関する問題を検出できるテストが可能です。

SENTINEL BE
Baseline Edition

- 重要度の高くないベーシックなWebサイト向けの基本的なソリューションです。
- 自動化されたスキャニングと脆弱性検査のソリューションを「お手頃な価格」でご利用いただけます。リスクの高くないマーケティングタイプのWebサイトに最適です。

評価、検査のできる脆弱性

Sentinel Dynamic は、以下のような多数の観点から脆弱性を評価、検査できます。

* ご請求いただければ、製品ラインごとの互換性リストをすぐにご用意いたします。

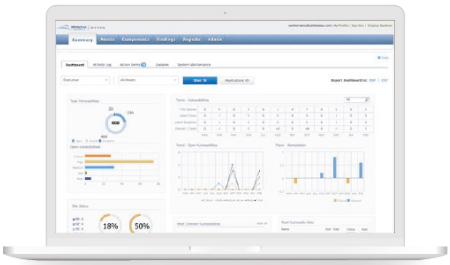
技術的な脆弱性 - WASC の脅威分類 2.0

- アプリケーションの構成の誤り
- ディレクトリ・インデックス
- HTTP スマグリング
- 不適切な入力処理
- 不十分なトランスポート層の保護
- OS コマンディング
- リモートファイルインクルージョン
- SQL インジェクション
- XML 外部実体攻撃
- XQuery インジェクション
- コンテンツスプーフィング
- フィンガープリンティング
- HTTP レスポンススプリッティング
- 不適切な出力処理
- メールコマンドインジェクション
- パストラバーサル
- ルーティングの迂回
- SSL インジェクション
- インジェクション
- クロスサイトスクリプティング
- フォーマット文字列攻撃
- ファイルシステムの不適切なアクセス権限
- 情報の漏洩
- Null バイトインジェクション
- 予測可能なリソースロケーション
- サーバーの構成の誤り
- URL リダイレクタの悪用
- XPath インジェクション

技術的な脆弱性 - OWASP トップ 10

- A1：インジェクション
- A2：認証の不備
- A3：機微な情報の露出
- A4：XML 外部エンティティ参照 （XXE）
- A5：アクセス制御の不備
- A6：不適切なセキュリティ設定
- A7：クロスサイトスクリプティング （XSS）
- A8：安全でないデシリアライゼーション
- A9：既知の脆弱性のあるコンポーネントの使用
- A10：不十分なロギングとモニタリング

柔軟なレポート形式に対応するエンタープライズクラスのレポート機能



Sentinel のユーザーインターフェースで提供されるレポートを活用すれば、セキュリティプログラムのパフォーマンスを把握でき、セキュリティポスチャを強化することが可能になります。また、高度な分析機能により、問題対応の完了の割合や問題の修正に要した時間、脆弱性の古さなど、トレンドや主要な統計値を監視します。さらに、トレンド分析の機能では、リアルタイムのデータと履歴データを追跡することによって、リスクエクスポージャーの変化を継続的に測定するほか、最もセキュリティが強固な Web サイトと最も脆弱なサイトを一目で把握できるようにします。

Sentinel Dynamic がほかのサービスと一線を画す理由

継続的な評価を行う手法

Sentinel Dynamic では、完全に継続的な評価を行っており、Web サイトが進化していくなかで、サイトのスキャンを常時実施しています。Web アプリケーションに加えられたコードの変更を自動的に検知、評価する仕組みや、新たな脆弱性が見つかったときにアラートで知らせる機能、脆弱性の再テストで一からのテストを不要にする機能により、リスクの評価が「絶えず」行われています。

本番環境に影響を与えない仕組み

Sentinel Dynamic は本番環境の Web サイトに一切影響を与えません。そのため、Sentinel Dynamic によりサイトのパフォーマンスが低下することはありません。Sentinel Dynamic では、害の生じないライブコードのインジェクションを行い、データの整合性を維持します。また、スキャンのカスタムチューニングにより、フルスキャンを行ってもサイトのパフォーマンスに影響が生じないようになっています。

PCI コンプライアンス

Sentinel Dynamicのサービスでは、検査を加えた脆弱性評価を内部のWebサイトと外部に公開しているWebサイトを対象に継続して実施しているため、PCI DSS 3.1 の要件を超えるコンプライアンスが実現しています。また、Sentinel PE のサービスでは、PCI DSS で求められているビジネスロジックの評価や侵入テストに対応しています。さらに、Sentinel と WAF との連携により、脆弱性を修正するための仮想パッチを作成できるほか、監査に合格するうえで必要なレポートも提供されます。

完全に自動化されたシングルページアプリケーション（SPA）のスキャニング

Sentinel Dynamic では、従来のアプリケーションに加え、シングルページのアプリケーションもスキャンできます。独自のテクノロジーにより、SPA サイトのスキャニングとテストを完全に自動化しています。スキャナーは Web サイトのアプリケーションをブラウザにロードし、ユーザーがするのと全く同じようにアプリケーションを操作します。処理において本番環境に影響を与えることはありません。従来のスキャニングツールが見逃すような脆弱性も見つけ出します。

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