SYNOPSYS®

Seeker
インタラクティブ・アプリケーション・セキュリティ・テスト（IAST）

脆弱性を正確に特定・検証できる使いやすいエンタープライズ・クラスの IAST

概要

シノプシスのインタラクティブ・アプリケーション・セキュリティ・テスト（IAST）ソリューション Seeker は、Web アプリケーションのセキュリティ状態を最大限に可視化し、OWASP Top 10、PCI DSS、GDPR、CAPEC、CWE/SANS Top 25 などのコンプライアンス規格に照らし合わせて脆弱性トレンドを洗い出します。また、Seeker には機微なデータを特定し、これらが安全に取り扱われているかどうかを追跡する機能もあり、これらの情報が強力な暗号化で保護されていないログ・ファイルやデータベースに格納されるのを防ぐことができます。Seeker は CI/CD ワークフローにシームレスに統合できるため、継続的なアプリケーション・セキュリティ・テストと検証が実行できます。

一般的な IAST ソリューションにはセキュリティ脆弱性を特定する機能しかありませんが、Seeker は特定したセキュリティ脆弱性（XSS や SQL インジェクションなど）を検証し、悪用の可能性を判定する機能もあるため、リスク度に応じてどの順番に脆弱性を修正すればよいかがただちに分かります。Seeker は独自の特許技術により、数十万もの HTTP(S) リクエストを高速に処理して脆弱性を特定しながらも、誤検知はほぼゼロに抑えています。このため、セキュリティ・チームは本当に脅威となる検証済みセキュリティ脆弱性への対応を優先させることができ、生産性の飛躍的な向上とビジネス・リスクの軽減を図ることができます。Seeker を導入することは、Web アプリケーションへの自動ペネトレーション・テストを 24 時間体制で実行してくれる専属チームを持つのと同じ効果があります。

Seeker は実行中のアプリケーション内部にエージェントを配置するコード・インストルメンテーションの手法を採用しており、大規模なエンタープライズ環境におけるセキュリティ要件にもスケーラブルに対応します。また、面倒な設定なしに高精度な結果が得られるのも Seeker の特長です。脆弱性に関する詳細な解説、具体的な修正アドバイス、スタック・トレース情報を提示しながらどのコード行に脆弱性が存在するかを Seeker が指摘してくれるため、セキュリティの専門知識を持たない開発者にもご利用いただけます。

Seeker は Web アプリケーションに適用されるすべてのタイプのテストを常時監視し、自動 CI ビルド・サーバーおよびテスト・ツールとシームレスに統合します。Seeker はこれらのテスト（人手によるログイン・ページの QA や自動機能テストなど）を利用して、複数のセキュリティ・テストを自動で生成します。

Seeker には、シノプシスのソフトウェア・コンポジション解析（SCA）ソリューション Black Duck® Binary Analysis も付属しており、サードパーティおよびオープンソースのコンポーネント、既知の脆弱性、ライセンス・タイプ、およびその他の潜在的なリスクを洗い出すことができます。Seeker と Black Duck の解析結果は同じビューに表示され、最適なバグ追跡およびコラボレーション・システムへ自動的に送信できるため、通常の開発ワークフローの一環としてトリアージできます。

Seeker は 1 つのアプリケーションを構成する複数のマイクロサービスを一括評価できるため、マイクロサービス・ベースのアプリケーション開発に最適です。

Seeker はマイクロサービス間のデータの流れを解析し、関連性の無いアプリケーションの集合としてではなく、システム全体として解析します。データの流れは HTTP(S)、gRPC、共有データベースなどで追跡されます。

アプリケーションからコンポーネント、API に至るまで、主要なセキュリティ上の脆弱性を包括的に示すダッシュボード。

詳細なテスト・カバレッジとデータ・フローの追跡により、さまざまなソースからアプリに流入するデータ、システムのさまざまなコンポーネント間を流れるデータ、サードパーティ API やウェブサービスへの発信コールなどを速やかに可視化。テスト対象のシステムのアーキテクチャを表示します。