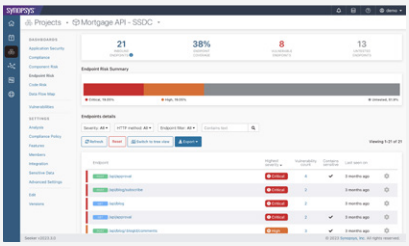
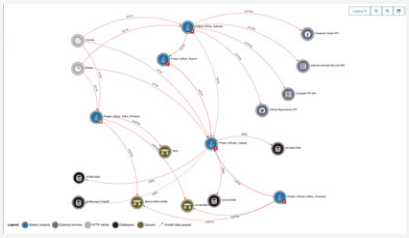
Seeker

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



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。

概要

ブラック・ダック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、ブラック・ダックのソフトウェア・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。

迅速かつ実用的な結果をリアルタイムで継続的に提供

包括的な解析結果には、脆弱性への対処に必要なすべての情報が含まれます。

- リスクに関する明確な解説
- 実行時のメモリー値およびコンテキスト
- 技術的な説明
- 脆弱性が見つかったコード行
- コンテキストを考慮した具体的な修正ガイダンス

データフローおよび悪意により挿入されたパラメータ（動的 SQL 連結など）の影響は、複数の詳細なペインに表示されます。この結果には、検出された脆弱性が自動検証によって悪用可能と判定されたか、誤検知として削除されたかも表示されます。

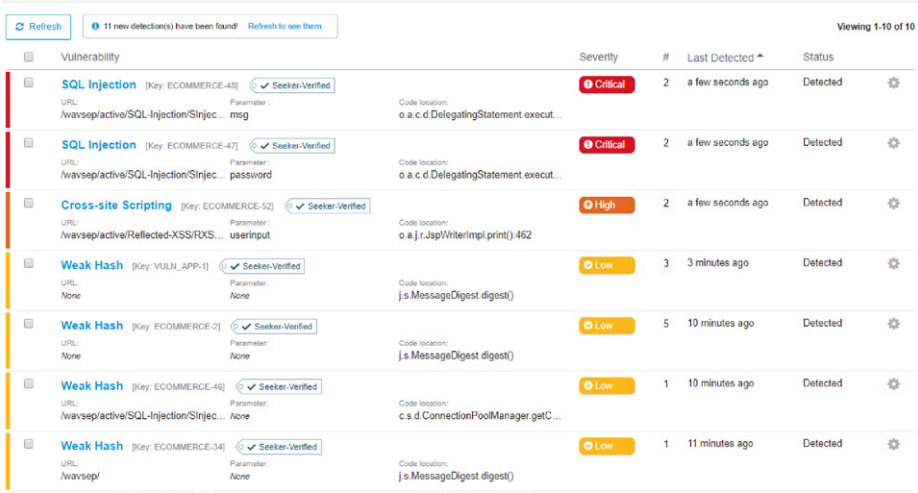
Seeker は Black Duck Binary Analysis と SCA を統合しています。アプリケーションのバイナリをコンポジション解析に送信するだけで、解析結果が Seeker のダッシュボードにアップロードされます。

アクティブな検証機能を備えた唯一のエンタープライズ・スケールの IAST ソリューション

Seeker 独自のアクティブ検証機能は数十万もの HTTP(S) リクエストを処理し、検出した脆弱性から誤検知をすばやく削除して提示するため、ユーザーが誤検知を目にすることはほとんどありません。更にテスト・カバレッジを高めるため、Seeker にはパラメータ特定機能があります。これは、使われていないパラメータを検出し、悪意のある値を用いてこれらを再テストする機能で、アプリケーションのアタック・サーフェス（攻撃対象領域）、隠れパラメータ、バックドアをより広範に調査できます。

これには以下の利点があります。

- セキュリティ・チームと開発チーム双方の生産性が飛躍的に向上。
- 少ないリソースでダイナミック・アプリケーション・セキュリティ・テスト（DAST）や人手によるペネトレーション・テストが実行でき、全体的なコストが削減。



導入から運用までが簡単

Seeker は、主にソフトウェア開発ライフサイクル（SDLC）の統合テスト /QA ステージでソフトウェア開発ライフサイクル（SDLC）の運用展開の直前まで、インストルメンテーション手法とランタイム解析を使用して、Web アプリケーションのセキュリティ脆弱性を常時監視、検出、検証します。アプリケーションはオンプレミス、マイクロサービス・ベース、またはクラウド・ベースのものを対象にできます。Seeker は最新のアプリケーション開発メソドロジーとテクノロジーをサポートしています。アプリケーション・コードが動作する各ティアまたはノード（Docker コンテナ、仮想マシン、クラウド・インスタンスなど）にエージェントを導入するだけで、動作中のアプリケーションで実行されるすべてのアクションを追跡できます。解析結果はすぐに取得でき、特別なスキャンは必要ありません。

Seeker はコードを 1 行ずつ解析し、データフローとランタイム・コード実行の相関をリアルタイムに取得するだけでなく、アプリケーション層およびコンポーネントに含まれる機密データを含むコードやマイクロサービス、API の呼び出しの相互作用も調査します。このテクノロジーは、他のテクノロジーでは検出できない複雑な脆弱性やロジックの欠陥を含め、クリティカルなデータに対して本当に脅威となる脆弱性を特定します。

Seeker と e ラーニングの統合は、開発者と DevOps チームに臨機応変なヘルプとトレーニングを提供します。それによって脆弱性に関する深い理解を得て、リアルタイムに修正することが可能になります。

導入後、即活用が可能な Seeker

- **CI/CD ワークフローにシームレスに適合。**ネイティブ統合と Web API により、オンプレミス、クラウド・ベース、マイクロサービス・ベース、コンテナ・ベース開発に使用している既存のツールとシームレスに統合します。
- **短時間で簡単にデプロイ可能。**Seeker のリアルタイム解析は、導入直後から誤検知がほぼゼロに抑えられます。
  - 面倒な設定や調整が不要で、すぐに高精度な結果を取得可能
  - Web サイトのログイン資格情報や特別なスキャンが不要
  - 入力バリデーション・ライブラリとカスタム関数を考慮したアクティブ検証により、入力をサニタイズ（SQL インジェクション脆弱性など）
  - 大規模なエンタープライズ環境にもスケーラブルに対応
- **あらゆるタイプのテスト手法に適合。**Seeker には非介入型のパッシブ監視機能もあり、既存のテスト・オートメーション、手動または機能テスト、自動 web クローラーなどと組み合わせて利用できます。

アプリとマイクロサービスの API でディスカバリー、トラッキング、データフロー・マップによる詳細なテスト・カバレッジ

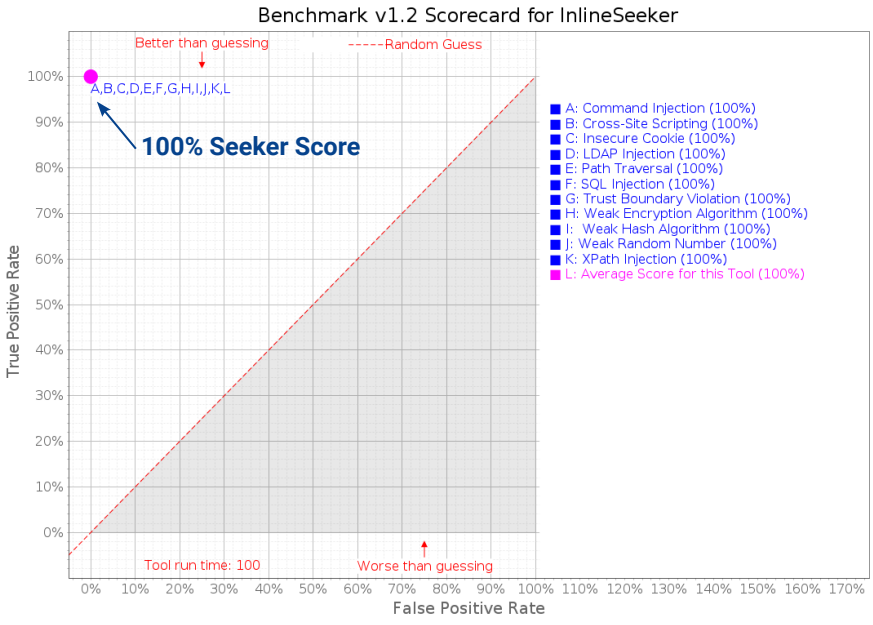
自動化された URL マッピング、API ディスカバリー、エンドポイント追跡により、Web アプリのテスト・カバレッジの範囲を包括的に把握することができます。Seeker は、何がテスト済みで何がテストされていないかをグラフィカルに表示し、効果的なテイント解析を支援する視覚的なデータ・フロー・マッピングも提供します。同じアプリケーションの異なるバージョン間でカバレッジの違いを容易に比較できます。

アクティブ検証は、OpenAPI/Swagger および Graph-QL ベースのアプリケーションのカバレッジを高めるために、リクエストのシーケンスを自動的に生成します。

機密データおよびシークレットのトラッキング

Seeker は、機密データとシークレットのトラッキング機能においても業界をリードしています。この機能は、ユーザーが「Sensitive」と指定した情報（クレジットカード番号、トークン、パスワードなど）が、暗号化されていないログやデータベース、ファイルに保存されていないかを常時監視します。これにより、PCI DSS のデータ暗号化コンプライアンスに関するセクションや、GDPR（EU 一般データ保護規則）などの業界標準規格・規制へのコンプライアンスが容易になります。しかも、人手による検査に比べて生産性が飛躍的に向上し、時間、コスト、リソースも節約されます。

OWASP ベンチマークで最高スコアを達成



Seeker | 技術スペック

対応言語

- ASP.NET
- C#
- Clojure
- ColdFusion
- Go
- Gosu
- Groovy
- Java
- JavaScript (Node.js)
- Kotlin
- PHP
- Python
- Scala (Lift を含む)
- VB.NET

対応プラットフォーム

- Java
  - すべての Java EE サーバー
  - GlassFish
  - Red Hat JBoss Enterprise Application Platform
  - Red Hat JBoss Web Server
  - Tomcat
  - WebLogic
  - WebSphere
- .NET Framework
  - IIS
  - WCF
  - OWIN
  - SharePoint
- .NET Core
- Node.js
- PHP

ランタイム / フレームワーク

- .NET/CLR
  - ASP.NET MVC
  - Enterprise Library
  - Entity Framework
  - NHibernate
  - Ninject
  - NVelocity
  - OWASP ESAPI
  - SharePoint
  - Spring.NET
  - Telerik
  - Unity
- GO
  - Chi
  - Echo
  - Gin
  - Net/http
- Java/JVM
  - Enterprise JavaBeans (EJB)
  - Grails
  - GWT
  - Hibernate
  - Ktor
  - Micronaut
  - OWASP ESAPI
  - Play
  - Ring
  - Seam
  - Spring/Spring Boot
  - Struts
  - Vaadin
  - Velocity
  - Vert.x
- Java Runtime:
  - AdoptOpenJDK
  - Amazon Corretto
  - Eclipse OpenJ9
  - IBM
  - Oracle HotSpot
  - OpenJDK
  - Red Hat OpenJDK
- Node.js
  - Express
  - Fastify
  - Hapi
  - Koa
- PHP
  - Laravel
  - Symfony
- Python
  - Django
  - Flask

テクノロジー

- データベース
  - NoSQL DB
    - Cassandra
    - Couchbase
    - DynamoDB
    - HBase
    - MongoDB
- Relational/SQL
  - DB2
  - HSQLDB
  - MS SQL
  - MySQL
  - PostgreSQL
  - SQLite
  - Oracle
- アプリケーション・タイプ
  - Ajax
  - JSON
  - マイクロサービス
  - モバイル (HTTP/S)
  - RESTful
  - SPA (Single Page Application)
  - Web (HTML5 を含む)
  - Web API
  - Web サービス
- プロセス間通信
  - HTTP(S)
  - gRPC
  - Kafka
  - Apache Dubbo
  - RabbitMQ
  - JMS
  - データベース・テーブル

クラウド・プラットフォーム

- Azure PaaS/Azure Function
- AWS
- AWS Lambda
- Google Cloud
- Tanzu (PCF)

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社
www.blackduck.com/jp