Black Duck

ソフトウェア・コンポジション解析

ソフトウェア・サプライチェーンによってもたらされるリスクを特定・管理

可視性を確立

- コード、バイナリ、および成果物に含まれるオープンソースを検出します
- SBOM からサードパーティ・コンポーネントをインポートします
- DevOps との統合によりスキャンを自動化します

リスクを管理

- 依存関係を既知の脆弱性や健全性の問題に対応付けます
- 悪意あるコンポーネントや機微な情報をスキャンします
- ライセンスのリスクおよび競合を特定します
- 重要度に基づいて修正の優先順位を決定します

信頼を構築

- リスク許容度および顧客からの要求事項に基づいてカスタム・ポリシーを定義します
- オープンソースとカスタムの依存関係を含む SBOM を生成します
- アプリケーション出荷前にサプライチェーンの脅威に対処します

概要

Black Duck® ソフトウェア・コンポジション解析（SCA）は、アプリケーションやコンテナなどあらゆるソフトウェア成果物やライブラリでオープンソースを使用した場合に発生するセキュリティ、ライセンス・コンプライアンス、コード品質のリスクを管理する包括的なソリューションです。Forrester 社によってソフトウェア・コンポジション解析（SCA）のリーダーとして認定された Black Duck は、サードパーティ依存関係の可視性を最大限に高め、ソフトウェア・サプライチェーンによってもたらされるリスクの管理を可能にします。

ソフトウェア・サプライチェーンの可視性を確立

商用アプリケーションを構成するコードのほとんどはサードパーティに由来しており、最終アプリケーションを頒布またはデプロイする企業が管理も監視もできない外部組織によって作成されています。Black Duck はさまざまな手法を組み合わせて依存関係を検出し、アプリケーションの構成を完全に可視化します。これにより、チームはリスクを効果的に評価および管理できるようになります。

- **依存関係解析：**パッケージ・マネージャーによって宣言された直接的および推移的依存関係を特定します。
- **バイナリ解析：**ファームウェアやコンテナ・イメージなど、ビルド済み成果物に存在する依存関係をソース・コードなしで検出します。
- **スニペット解析：**AI コーディング支援ツールが流用したコードなど、断片的なコードがどのオープンソース・プロジェクトに由来するものかを特定します。
- **CodePrint 解析：**パッケージ・マネージャーによって宣言されていなくても、ソース・ファイルおよびディレクトリに含まれる依存関係を特定します。
- **コンテナ・スキャン：**バイナリ解析と CodePrint 解析を組み合わせ、コンテナ・イメージに含まれるオープンソースの依存関係をレイヤーごとに特定します。
- **C/C++ スキャン：**パッケージ・マネージャーが存在しない場合でも、C/C++ アプリケーションで使用されているオープンソースの依存関係およびライブラリを正確に特定します。
- **AI Model Risk Insights：**シグネチャベースの解析手法を用いて、プロジェクトに統合されたオープンソースおよびサードパーティ製の AI・機械学習モデルを特定します。

リスクを特定・管理

特定したすべての依存関係について、Black Duck は関連するリスクを評価し、優先順位の高いものから修正できるよう支援します。

脆弱性

Black Duck Security Advisory（BDSA）は、Black Duck KnowledgeBase に基づいて既存および新たに公開されたオープンソース脆弱性について具体的な対策方法を示したアラートをいち早く提供します。これらのアラートには、以下の情報が含まれます。

- 重要なリスク指標、個々の脆弱性の技術解説、エクスプロイトの詳細
- CVSS スコアリングおよび CWE 分類データ
- 会社のリスク・プロファイルに一致するカスタム脆弱性リスク・スコアリング
- コンポーネント・レベルのアップグレードおよび対策の手引き、軽減要因、応急措置

BDSA は、人間による調査と AI を組み合わせることにより、Black Duck ユーザーに最も大きく影響すると考えられる脆弱性を発見・分析して報告します。このため、BDSA は一般的なセキュリティ・フィードよりも分析の完全性が高く、しかも脆弱性が公開されてから数時間後には発行されます。

ライセンスのリスク

Black Duck は、明示的に宣言されたライセンス、サブライセンス、および埋め込みライセンスを含め、依存関係と AI モデルによって使用されているライセンスを正確に特定します。そして、各ライセンスに関連する要求事項と制限事項の情報を抽出し、ライセンスの全文および著作権情報と一緒に分かりやすく表示してくれます。また、ほとんどすべてのオープンソース・ライセンスで必須とされている Notice ファイルも自動で生成できます。

Black Duck のライセンスに関する知見とスニペット解析の組み合わせは、AI コーディング・アシスタントの生産性のメリットを活用したい組織にとって最適なツールです。スニペット解析では、AI 生成コードを評価し、オープンソース・プロジェクトとの一致やライセンスの競合の有無を調べます。また、ライセンスで保護されたコードがビルドやソースコード管理システムに含まれないようにポリシーを定義することもできます。

コンポーネントの健全性

オープンソース・プロジェクトの健全性、履歴、コミュニティ・サポート、出所、評判を評価するための指標が Black Duck によって提供されるため、セキュリティ・リスクを未然に防止することが容易になります。これらのコンポーネント・メトリックは、放棄されたプロジェクトや悪意のあるパッケージを予防し、タイポスクワッティングや依存関係かく乱攻撃によって組み込まれたパッケージを識別するために必要な知見をチームに提供します。

AI で革新する

Black Duck SCA は、AI 生成コードと組み込み AI モデルに対する可視性とガバナンスを提供することで、開発チームが自信を持って AI を活用した革新を推進できるように支援します。プロジェクトに統合されたサードパーティ製の AI ／機械学習モデルを自動的に検出し、品質、ライセンス、コンプライアンス上のリスクを評価することが可能です。また、Black Duck SCA は AI 生成コードに対しても、従来のオープンソースと同等の厳格な評価を行い、生成ツールによって取り込まれたライセンス義務やライセンス制限の特定を支援します。この包括的な監督により、組織はコンプライアンスや対策を損なうことなく、AI 駆動型の開発を加速させることができます。

オープンソースのガバナンスを自動化

ライセンス・タイプ、脆弱性の重要度、オープンソース・コンポーネントのバージョンなどさまざまな基準に基づいてオープンソースのセキュリティと使用に関する独自のポリシーを設定できます。設定したポリシーは、自動ワークフロー・トリガー、通知、Jira または Azure との双方向の連携などの方法で適用でき、修正作業の開始と報告を迅速化できます。ポリシーを使用することで、開発チームがリスクのあるコンポーネントを使用するのを防ぐとともに、万一こうしたコンポーネントがリリース・ストリームに混入した場合でも、ビルドを停止することができます。

SBOM をアプリケーション・ライフサイクルに組み込む

Black Duck には以下の機能があります。

- サードパーティのソフトウェア部品表（SBOM）をインポートして依存関係を既知のコンポーネントに自動的にマップし、カスタムまたは商用のコンポーネントの依存関係に対応する新規コンポーネントを作成できます。
- オープンソース、カスタム、および商用の依存関係に加え、AI モデルをすべて含んだ SBOM を、顧客、業界、または各種規制の要求事項に適合するように SPDX または CycloneDX フォーマットでエクスポートできます。詳細情報の共有レベルは、そのまま使えるテンプレートを活用することで、利用者の指定に応じて適切に設定できます。
- SDLC ツールとの統合により、SBOM 生成を自動化するとともに、既存または新たに見つかったリスクについて SBOM の依存関係を継続的に監視できます。

Black Duck でサポートされる言語、パッケージ・マネージャー、および統合環境についての情報は、ブラック・ダックの web サイトでご確認ください。

ブラック・ダックについて

ブラック・ダックは、True Scale Application Security によって、モダン・ソフトウェアの経営レベルのリスクに対応し、規制された、AI を活用した世界におけるソフトウェアの信頼性を保証します。ブラック・ダックのソリューションは、セキュリティ、規制、ライセンスに関するリスクを排除しつつ、組織のスピード、精度、コンプライアンスのトレードオフから解放します。クラウドでもオンプレミスでも、コードが実行されるあらゆる場所でミッション・クリティカルなソフトウェアを保護するには、ブラック・ダックこそが選択肢となるのです。ブラック・ダックを活用することで、セキュリティ・リーダーはよりスマートな意思決定を行い、自信を持ってビジネス・イノベーションを推進することができます。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

BLACK DUCK®

Coverity

静的解析

主な長所

高い性能

新規コードや変更されたコードに存在する問題は、完全スキャンと同じ忠実度の高速な増分スキャンで特定します。このため、コミットやプルリクエストのたびにスキャンを容易に実行でき、開発スピードの低下を招きません。

大規模なエンタープライズ環境への対応

Coverity は数千人規模の開発チームで作成された数千万コード行のアプリケーションを含め、世界最大規模のアプリケーションで多くのスキャン実績があります。

拡張性

独自フレームワークやサポート対象外の言語も、簡単に作成可能なカスタム・チェッカーでサポートできます。

導入の柔軟性

Coverity はオンプレミスでもプライベート・クラウド環境でも動作します。このため、すべてのデータをネットワーク内に保持したまま最高の静的解析スキャンを実行できます。

最も包括的な静的解析

静的解析ツール Coverity® は市販の静的解析ソリューションの中で最も高い精度とスケーラビリティを備えており、開発者とセキュリティ・チームは大規模な環境でセキュリティと品質に優れたアプリケーションをデリバリできます。20 以上のプログラミング言語と 200 以上のフレームワークをサポートした Coverity は、各アプリケーションの詳細なモデルを構築してすべての依存関係とコンパイラを可視化することにより、世界最大規模のアプリケーションで多数のファイルやライブラリにまたがるような複雑な問題の特定も可能です。

開発ライフサイクル早期での高速スキャン

Coverity によるスキャンを SDLC の早期段階で実行することで、セキュリティと品質上の問題をいち早く特定できます。問題の修正は早ければ早いほど容易で、影響を最小に抑えることができます。

IDE 内でリアルタイムに動作

コーディング中に脆弱性やコード品質の問題を指摘してくれるため、問題のあるコードがリポジトリにチェックインされるのを防ぐことができます。

プルリクエストをトリガーとしてスキャンを実行

一般的なソースコード管理（SCM）システムに統合して、新規コードや変更されたコードに存在する問題を増分スキャンで特定できます。

CI/CD パイプラインでの自動化

修正されていないセキュリティや品質上の問題は、アプリケーションの完全スキャンで特定し、ポリシー違反が見つかった場合にはビルドを中断することもできます。

最高精度のスキャン結果

Coverity のスキャン結果は精度が高いため、開発者は誤検知のトリアージに時間を奪われることなく、実際の不具合の修正作業に専念できるなど、開発者の負担が軽減されます。

- **各アプリケーションの詳細なモデル**により、すべての依存関係とコンパイラ、データフローおよび制御フロー・パスを含め、アプリケーションの動作を可視化して重要な洞察を得ることができます。
- **20 以上のプログラミング言語と 200 以上のフレームワークを深く理解**し、コンテキストを考慮して誤検知と真の問題を区別します。
- **コンテキストを考慮した洞察**を最初のスキャン結果に適用することにより、各結果の妥当性を確認し、悪用の可能性を評価します。
- **設定可能なセキュリティおよび品質チェッカー**は、デフォルトでは精度優先にチューニングされていますが、ビジネスまたはアプリケーションのリスク・プロファイルに合わせた調整が可能です。

各種セキュリティおよび産業規格を幅広くカバー

Coverity はコードの品質問題の特定に関してクラス最高の精度を達成している他、セキュリティや安全に関する産業規格を最も包括的にサポートしています。これには以下のものが含まれます。

- **セキュリティ：**OWASP Top 10、SANS CWE Top 25、PCI DSS
- **安全：**MISRA®、CERT C/C++、CERT Java、DISA STIG、ISO 26262、ISO 23434、ISO/IEC TS 17961、AUTOSAR®、Hyundai Secure Coding Standards

レポートは PDF としてダウンロードでき、監査時に各標準に対する詳細なコンプライアンス記録を残しておくのに役立ちます。トレンド・レポートには、深刻度の時系列での推移や、優先度の高い問題に対する開発者やプロジェクト・チームごとの修正進捗情報などが表示され、さらに多くの洞察が得られます。

また、セーフティ・クリティカルなプロジェクトでは、ISO 26262 や DO-330 などの業界安全規格に適合するように Coverity が正しく設定されていることを Coverity Qualification Kit（Q-Kit）で確認できます。

主な特徴

- **簡単なオンボーディング** デスクトップ・アプリケーションの Point and Scan は、ユーザーがソースコードをポイントするだけでアプリケーションをオンボードすることができます。コマンドライン・インターフェイス（CLI）を好む開発チームには、Coverity CLI 機能で同様のオンボーディングが可能です。
- **開発ワークフローへの円滑な統合** Black Duck Bridge を使用すると、簡単かつ予測可能なアプローチを使用して Coverity を含むすべての Black Duck アプリケーション・セキュリティ・テスト・ソリューションを一般的な CI/CD ツールにコマンドライン・インターフェイスで統合できます。
- **リアルタイムでの不具合検出** IDE プラグインの Code Sight™ を使用すると、開発者はコーディング中に静的解析からの正確な洞察を得ることができます。検出された各問題について、その詳細説明、カテゴリ、深刻度、CWE データ、不具合の位置、詳細な修正ガイダンスなどが IDE 内で直接提示されます。
- **具体的な修正ガイダンス** 詳細なサジェスチョンやコンテキストに応じた e ラーニングにより、セキュリティの専門知識がない開発者でも問題の修正方法を容易に理解できます。
- **詳細なレポート** 業界で認知されているリスト、問題のタイプ、テクニカル・リスク指標に基づいた事前作成済みのレポートがダッシュボードに表示されるため、開発者はそれぞれの組織にとって最も重要な問題から優先的に対策をとることができます。CWE、標準規格の分類、優先リスト、リスク指標、パス、開発者ごとに問題を簡単にグループ化できるフィルター機能もあります。

サポートされるテクノロジーの詳細な一覧は、Coverity Languages and Framework の web ページをご参照ください。

ブラック・ダックについて

ブラック・ダックは、True Scale Application Security によって、モダン・ソフトウェアの経営レベルのリスクに対応し、規制された、AI を活用した世界におけるソフトウェアの信頼性を保証します。ブラック・ダックのソリューションは、セキュリティ、規制、ライセンスに関するリスクを排除しつつ、組織のスピード、精度、コンプライアンスのトレードオフから解放します。クラウドでもオンプレミスでも、コードが実行されるあらゆる場所でミッション・クリティカルなソフトウェアを保護するには、ブラック・ダックこそが選択肢となるのです。ブラック・ダックを活用することで、セキュリティ・リーダーはよりスマートな意思決定を行い、自信を持ってビジネス・イノベーションを推進することができます。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

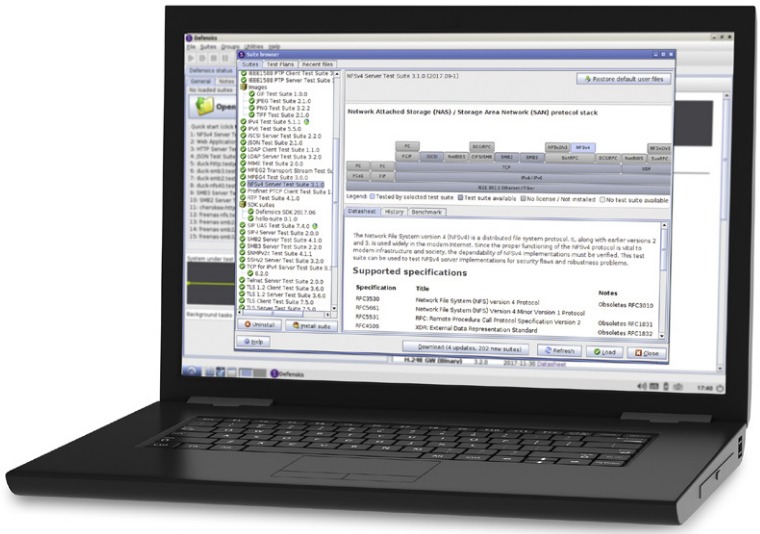
Defensics

ファジング・テスト

外部調達か内製かを問わず、
ビジネスを支える
ソフトウェアの脆弱性を
洗い出し、ソフトウェアの
堅牢性とシステムの
相互運用性を高めます。

概要

Defensics® ファジング・テストは、ソフトウェアのセキュリティ脆弱性を効果的かつ効率的に検出、修正する包括的かつ強力な自動ブラックボックス・ソリューションです。体系的かつインテリジェントなアプローチを取り入れたネガティブ・テストにより、市場投入スケジュールや運用コストに影響を与えることなく製品の革新性とソフトウェア・セキュリティを両立できます。

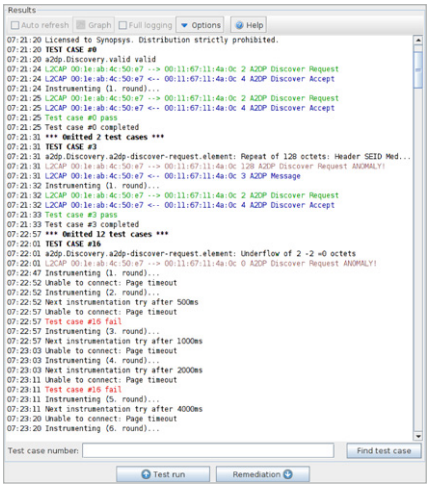


Defensics は論理的なユーザー・インターフェースを採用。画面の指示に従って手順を実行するだけで高度なファジング・テストを簡単に実行できます。

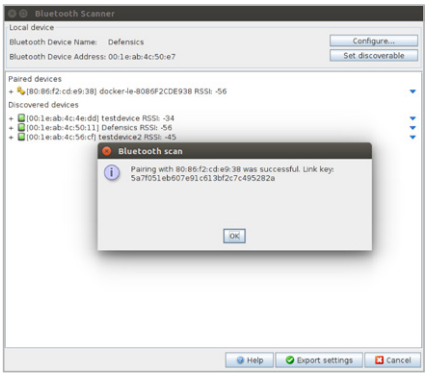
主な機能

インテリジェントなファジング・エンジン

Defensics エンジンにはインターフェース、プロトコル、ファイル・フォーマットなど入力タイプに関するナレッジが事前にプログラムされています。このため、入力タイプ内での通信を司る規則を深く理解し、その入力タイプに特有のセキュリティ脆弱性を突くような、ターゲットを絞り込んだテスト・ケースを送り込むことができます。このインテリジェントで体系的なアプローチによるファジング・テストにより、コストやセキュリティを犠牲にすることなくテスト時間を短縮できます。



Defensics のレポート。メッセージ・シーケンス・ログを利用して異常な応答の根本原因を突き止めることができます。



Defensics には Device Explorer などテスト・プロセス全体を自動化する機能が用意されており、ユーザーによる面倒な設定は不要です。

包括的なファジング・ソリューション

300 を超えるビルド済みのインテリジェントなテスト・スイートが用意されており、人手でテストを作成しなくてもすぐにファジング・テストを開始できます。テスト・スイートは、新しい入力タイプ、仕様、RFC を反映して常に更新されています。

- 各テスト・スイートは、メッセージ・シーケンスを微調整してカスタマイズできます。データ・シーケンス・エディタを使用すると、デフォルトの定義済みテスト・スイートに含まれないコーナー・ケースも網羅できます。
- 更に拡張性が必要な場合は、テンプレート・ファザーを使用します。Universal Data Fuzzer（ファイル・フォーマット・テンプレート・ファザー）と SDK Express ヘルプは、ユーザーが用意したサンプル・ファイルをリバースエンジニアリングしてテスト・ケースを生成します。
- 独自 / カスタム入力タイプを使用する場合は Defensics SDK で専用のテスト・スイートを作成できます。Defensics SDK は一部のトランスポート層をサポートしており、インストルメンテーションが付属します。
- FuzzBox サポートでテストをスピードアップ。無線 LAN や IoT プロトコルのファジングが簡単になり、カスタム・ハードウェア上で直接テストを実行できます。
- 自動車、ICS、IoT、ネットワーク、通信の 5 つの新しい業種別ソリューション・バンドルから選択できます。業種別ソリューション・バンドルには、その業界市場に関連するプロトコルに加え、基本的なプロトコルが含まれています。

あらゆる開発ライフサイクルに適合

Defensics には、ほとんどすべてのテクノロジやプロセス環境への適合を可能にするワークフローが含まれます。伝統的な SDL であれ CI 開発ライフサイクルであれ、Defensics は早期段階で開発に組み込むことができるため、最小限のコストで脆弱性を捕捉して修正できます。独自の開発ライフサイクルを使用している場合は、ブラック・ダックの経験豊富なプロフェッショナル・サービス・チームがファジング・テスト・チェックポイントの特定からファジング・テストのメトリクス定義、ファジング・テスト成熟度プログラムの確立までをお手伝いします。

Defensics は開発プロセスに適合するだけでなく、周辺テクノロジとの連携も容易です。API およびデータ・エクスポート機能を利用してデータを共有することでレポート作成および解析の幅が広がるなど、Defensics を完全なプラグアンドプレイ方式で利用できます。

大量の詳細データを含むレポートにより効率的な修正をサポート

- **コンテキスト化されたログ：**Defensics とテスト対象システムの間のプロトコル・パスおよびメッセージ・シーケンスを詳細に記録した修正ログにより、各脆弱性のトリガと技術上の影響を容易に特定できます。
- **脆弱性マッピング：**Defensics には各脆弱性を CWE などの業界標準規格およびインジェクション・タイプにマッピングする機能があり、必要な情報をすぐに見つけて修正できます。
- **問題の再現：**Defensics では脆弱性トリガが 1 つのテスト・ケースにまで絞り込まれるため、問題を再現して正しく修正されているかどうかを検証できます。
- **修正パッケージ：**暗号化した修正パッケージを生成してソフトウェア・サプライヤに渡すことにより、サプライチェーン全体で安全かつ協調的な修正が可能です。

自動化によるスケーラブルなファジング・テスト

テスト・ターゲットのスキャンから接続先のレイヤ数の決定まで、Defensics には豊富な API が用意されており、あらゆるニーズに応じた柔軟でスケーラブルな自動化が可能です。

- 単一機器のテスト
- 毎回同じテスト・プランを実行できるように、繰り返し可能なオートメーションをセットアップ可能
- 最新のスケーラブルな仮想化技術によりテスト時間を短縮

Defensics | テスト・スイート・カタログ

Authentication（認証）、Authorization（許可）、Accounting（課金やユーザーのアクセス情報の収集）(AAA)
- Diameter クライアント / サーバー
- EAPOL サーバー
- Kerberos サーバー
- LDAPv3 クライアント / サーバー
- RADIUS クライアント / サーバー
- TACACS+ クライアント / サーバー
- MACsec サーバー

アプリケーション
- FIX
- JSON フォーマット
- Web アプリケーション
- WebSocket クライアント / サーバー
- XML SOAP クライアント / サーバー
- XML ファイル
- XMPP サーバー
- AMQP サーバー
- WAMP サーバー
- OWAMP サーバー
- TWAMP サーバー

自動車*
- CAN Bus
- CAN FD
- DoIP サーバー
- gPTP サーバー
- SOME/IP
- SRP サーバー

セルラー・コア
- BICC/M3UA
- GRE
- GTP Prime
- GTPv0
- PMIPv6 クライアント / サーバー
- SCTP クライアント / サーバー
- SMPP
- SMS (SMPP injection)
- SMS (file injection)
- MAP
- BSSAP
- BSSAP+
- CAP
- INAP
- ISUP
- MTP3/M2UA|M2PA
- TCAP/SCCP/M3UA
- SBI Client/Server

コア IP
- DHCP/BOOTP クライアント / サーバー
- DHCPv6 クライアント / サーバー
- DNS クライアント / サーバー
- FTP クライアント / サーバー
- HTTP クライアント / サーバー
- HTTP/2 クライアント / サーバー
- HTTP/3 サーバー
- ICAP サーバー
- IPv4 パッケージ
  - ARP クライアント / サーバー
  - ICMP
  - IGMP
  - IPv4
  - TCP for IPv4 クライアント / サーバー
- IPv6 パッケージ
  - ICMPv6
  - IPv6
  - TCP for IPv6 クライアント / サーバー
- SOCKS クライアント / サーバー
- マルチキャスト DNS
- PPP over L2TP クライアント
- PPPoE

電子メール
- IMAP4 クライアント / サーバー
- MIME
- POP3 サーバー
- SMTP クライアント / サーバー

汎用
- SDK Express
- Universal ASN.1 BER
- Universal Fuzzer

ICS*
- 60870-5-104 (iec104) クライアント / サーバー
- 61850/Goose/SV
- 61850/MMS クライアント / サーバー
- BACNET
- CIP サーバー
- COAP サーバー
- DNP3 クライアント / サーバー
- MQTT クライアント / サーバー
- Modbus マスター
- Modbus PLC
- OPC UA サーバー
- Profinet DCP
- Profinet PTCP クライアント / サーバー
- DLMS/COSEM クライアント / サーバー
- ISASecure テスト・ソリューション

IoT*
- Thread
- BT
- Wi-Fi AP
- gRPC
- Zigbee

リンク・マネジメント
- LACP (802.3ad)
- STP/RSTP/MSTP/ESTP

メディア
- アーカイブ・パッケージ
  - GZIP
  - JAR
  - ZIP
- オーディオ・パッケージ
  - MP3
  - MPEG4 (M4A/MP4)
  - OGG
  - WAV
  - Windows Media (WMA/WMV)
- イメージ・パッケージ
  - GIF
  - JPEG
  - PNG
  - TIFF
- ビデオ・パッケージ
  - H.264 ファイル・スイート
  - H.264 RTP フォーマット
  - MPEG2-TS
  - MPEG4 (M4A/MP4)
  - OGG
  - Windows Media (WMA/WMV)

医療
- DICOM サーバー
- HL7v2 サーバー
- FHIR クライアント / サーバー

広域イーサネット
- BFD
- CFM (802.1ag, Y.1731)
- E-LMI (MEF-16)
- イーサネット (802.3, 802.1Q)
- GARP (802.1D)
- LLDP (802.1AB)
- OAM (802.3ah)
- PBB-TE サーバー
- Synchronous Ethernet (ESMC)

ネットワーク*
- BGP
- SNMP
- IPv4/IPv6
- SIP
- Metro Ethernet

PKI（公開鍵基盤）
- CMPv2 クライアント / サーバー
- CSR

遠隔管理
- CWMP (TR-69) ACS
- CWMP (TR-69) CPE
- IPMI サーバー
- Netconf
- PCP サーバー
- SNMP trap
- SNMPv2c サーバー
- SNMPv3 サーバー
- SSHv1 サーバー
- SSHv2 サーバー
- Syslog
- TFTP サーバー
- Telnet サーバー

ルーティング
- BGP4+ クライアント / サーバー
- IS-IS
- LDP
- MPLS サーバー
- MSDP
- OSPFv2
- OSPFv3
- Openflow コントローラ
- Openflow スイッチ
- PIM-SM/DM
- RIP
- RIPng
- RSVP
- TRILL サーバー
- VRRP
- COPS クライアント / サーバー

* Defensics と同時に購入可能な業種別ソリューション

ストレージ
- CIFS/SMB サーバー
- DCE/RPC サーバー
- NFSv3 サーバー
- NFSv4.0/4.1 サーバー
- Netbios サーバー
- DNNG
- SMBv2 クライアント / サーバー MP
- SMBv3 クライアント / サーバー
- SunRPC サーバー
- iSCSI クライアント / サーバー

通信*
- 5G
- SMS
- Pre-5G
- O-RAN A1-P
- O-RAN-EI

時刻同期
- IEEE1588 PTP クライアント / サーバー
- NTP クライアント / サーバー

ユニバーサル・プラグ・アンド・プレイ
- UPnP パッケージ
  - UPnP マルチキャスト・イベント
  - UPnP SOAP
  - UPnP SSDP コントロール・ポイント
  - UPnP SSDP デバイス

VoIP
- H.323 クライアント / サーバー
- H.248 GW バイナリ / テキスト
- H.248 MGC バイナリ / テキスト
- MGCP サーバー
- MSRP サーバー
- RTP/RTCP/SRTP
- RTSP クライアント / サーバー
- SIP UAC
- SIP UAS (+TT)
- SIP-I サーバー
- STUN クライアント / サーバー
- TURN クライアント / サーバー
- SigComp サーバー

VPN
- DTLS クライアント / サーバー
- IKEv2 クライアント / サーバー
- IPSec
- ISAKMP/IKEv1 クライアント / サーバー
- L2TPv2/v3 クライアント / サーバー
- OCSP クライアント / サーバー
- SCEP
- SSTP
- TLS/SSL クライアント / サーバー
- X.509v3 認証
- VXLAN

無線
- Zigbee パッケージ
  - FuzzBox Zigbee APS
  - FuzzBox Zigbee MAC
  - FuzzBox Zigbee NWK
- Thread パッケージ
  - FuzzBox Thread 6LoWPAN
  - FuzzBox Thread MAC
- Bluetooth LE パッケージ
  - ATT クライアント / サーバー
  - アドバタイズ
  - HOGP ホスト
  - Health
  - L2CAP サーバー
  - LL ペリフェラル
  - プロファイル
  - SMP クライアント / サーバー
- Bluetooth パッケージ
  - A2DP
  - AVRCP
  - BNEP
  - HFP AG/Unit
  - HSP AG/Unit
  - L2CAP
  - MAP クライアント
  - OBEX- サーバー
  - PBAP クライアント
  - RFCOMM
  - SDP
- Wi-Fi AP パッケージ
  - 802.11 WLAN AP
  - 802.11 WPA AP
  - 802.11 WPA3 AP
- Wi-Fi クライアント・パッケージ
  - 802.11 WLAN クライアント
  - 802.11 WPA クライアント
  - 802.11 WPA3 クライアント

5G テクノロジー
- GTPv2-C クライアント / サーバー
- S1AP/NAS クライアント / サーバー
- GTPv1 クライアント / サーバー
- E1AP クライアント / サーバー
- NGAP/NAS クライアント / サーバー
- X2AP クライアント / サーバー
- XnAP クライアント / サーバー
- PFCP クライアント / サーバー
- F1AP クライアント / サーバー

テスト・スイートのすべてのリストはこちらからご確認ください。
https://www.blackduck.com/ja-jp/fuzz-testing.html

モニタリング / エンジン機能

インストルメンテーション
- 有効ケース
- Syslog
- エージェント
- SNMP
- テスト実行ごとのカスタム・スクリプト

SafeGuard チェッカー
- アンプ攻撃
- 認証バイパス
- ブラインド LDAP インジェクション
- ブラインド SQL インジェクション
- 証明書の妥当性検査
- RRSIG レコードの署名者名の圧縮
- クロスサイト・リクエスト・フォージェリ
- クロスサイト・スクリプティング
- ECDH 公開鍵認証
- 有効ケースに比べ過剰なクッキー
- Heartbleed
- 情報漏洩
- 不十分な乱数性
- LDAP インジェクション
- 不正な形式の HTTP
- リモート実行
- SQL インジェクション
- SMP の安全でないペアリング・パラメータ
- 予期しないデータ
- 保護されていない認証情報
- 弱い暗号

各種アノマリ
- ASN.1/BER アノマリ
- 認証情報アノマリ
- ディープ・パケット・インスペクション
- EICAR アンチウイルス・テスト・ファイル
- GTUBE（Generic Test for Unsolicited Bulk Email）
- 制御プレーン・インジェクション・アノマリ
- 整数アノマリ
- ネットワーク・アドレス・アノマリ
- オーバーフロー・アノマリ
- アンダーフロー・アノマリ

注：テスト・スイートは頻繁に追加されます。最新のリストについてはお問い合わせください。

* Defensics と同時に購入可能な業種別ソリューション

ブラック・ダックについて

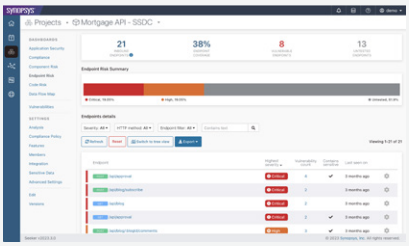
ブラック・ダックは、True Scale Application Security によって、モダン・ソフトウェアの経営レベルのリスクに対応し、規制された、AI を活用した世界におけるソフトウェアの信頼性を保証します。ブラック・ダックのソリューションは、セキュリティ、規制、ライセンスに関するリスクを排除しつつ、組織のスピード、精度、コンプライアンスのトレードオフから解放します。クラウドでもオンプレミスでも、コードが実行されるあらゆる場所でミッション・クリティカルなソフトウェアを保護するには、ブラック・ダックこそが選択肢となるのです。ブラック・ダックを活用することで、セキュリティ・リーダーはよりスマートな意思決定を行い、自信を持ってビジネス・イノベーションを推進することができます。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

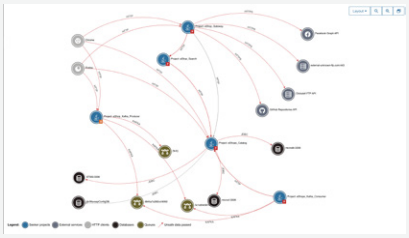
Seeker

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。

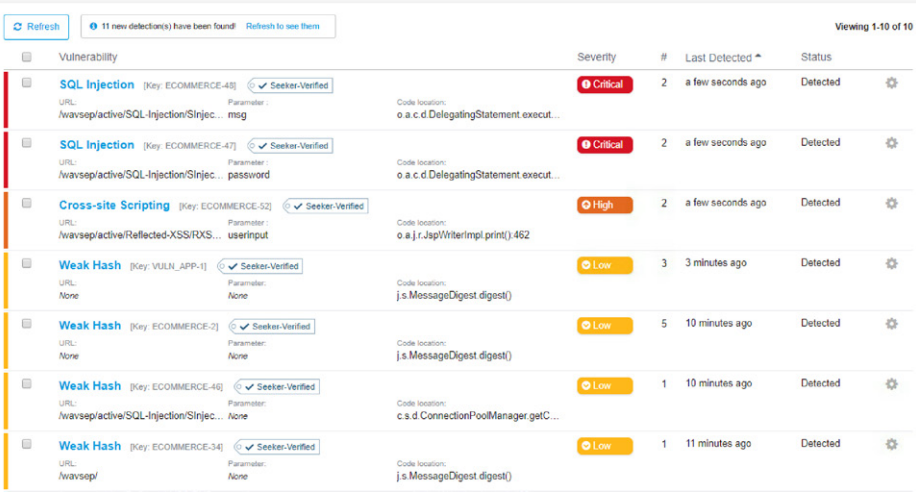
Seeker は Black Duck Binary Analysis と SCA を統合しています。アプリケーションのバイナリをコンポジション解析に送信するだけで、解析結果が Seeker のダッシュボードにアップロードされます。

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

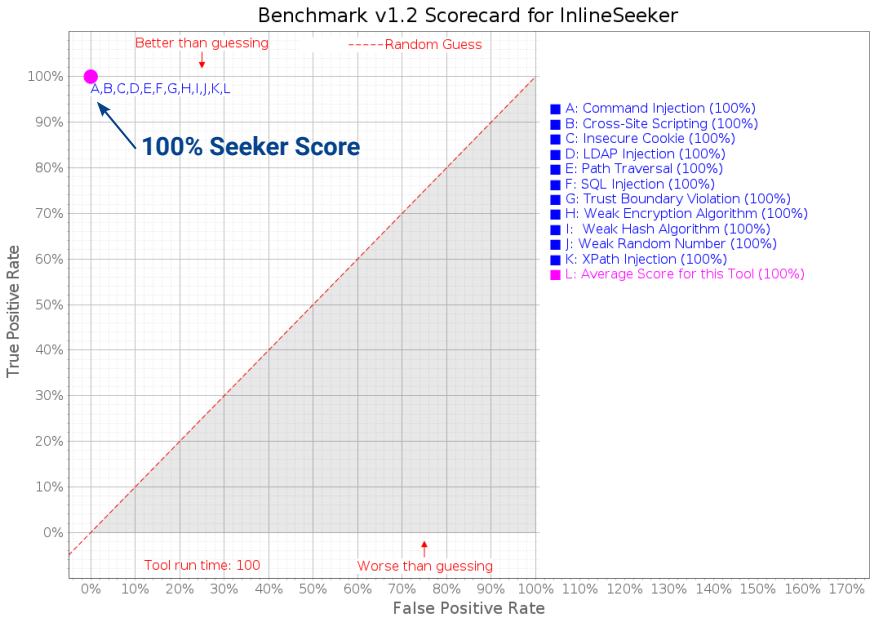
自動化された URL マッピング、API ディスカバリー、エンドポイント追跡により、Web アプリのテスト・カバレッジの範囲を包括的に把握することができます。Seeker は、何がテスト済みで何がテストされていないかをグラフィカルに表示し、効果的なテイント解析を支援する視覚的なデータ・フロー・マッピングも提供します。同じアプリケーションの異なるバージョン間でカバレッジの違いを容易に比較できます。

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、True Scale Application Security によって、モダン・ソフトウェアの経営レベルのリスクに対応し、規制された、AI を活用した世界におけるソフトウェアの信頼性を保証します。ブラック・ダックのソリューションは、セキュリティ、規制、ライセンスに関するリスクを排除しつつ、組織のスピード、精度、コンプライアンスのトレードオフから解放します。クラウドでもオンプレミスでも、コードが実行されるあらゆる場所でミッション・クリティカルなソフトウェアを保護するには、ブラック・ダックこそが選択肢となるのです。ブラック・ダックを活用することで、セキュリティ・リーダーはよりスマートな意思決定を行い、自信を持ってビジネス・イノベーションを推進することができます。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