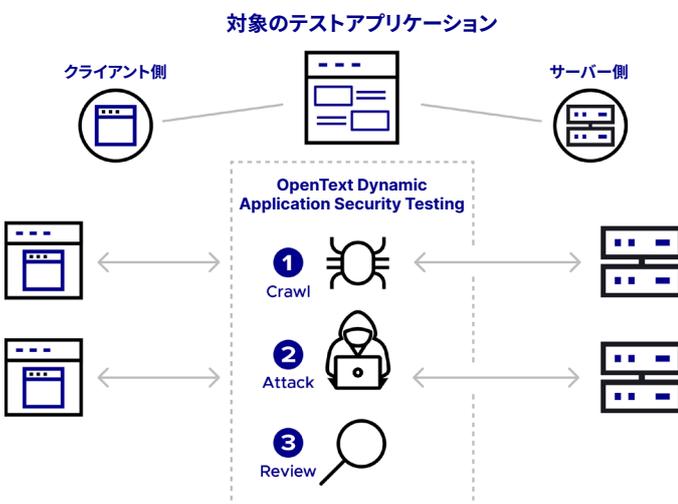


OpenText Dynamic Application Security Testing

OpenText Dynamic Application Security Testing は、導入済みの Web アプリケーションと Web サービスについてアプリケーションの脆弱性を特定するための動的アプリケーションセキュリティテスト (DAST) ツールです

OpenText™ Dynamic Application Security Testing は、包括的な脆弱性検出機能を備えた自動化された DAST ソリューションです。セキュリティ担当者や QA テスターによるセキュリティの脆弱性や設定の問題の特定を支援します。このソリューションでは、動作中のアプリケーションに対して外部からの実際のセキュリティ攻撃をシミュレートすることで、問題を特定し優先順位付けを行い、根本原因分析を可能にします。OpenText Dynamic Application Security Testing は統合に便利な多数の REST API を実装し、また、直感的な UI を使用した管理や完全な自動実行といった柔軟性も備えています。OpenText Dynamic Application Security Test での認証の定義は、静的か、動的か、マクロからトークンを取得するかどうかにかかわらず、単一の一貫性のある方法で行われます。

OpenText Dynamic Application Security Testing



主な機能

- Functional Application Security Testing (FAST)**
 IAST だけに限定する必要はありません。FAST は IAST と同じ機能テストをすべて実行して解析しますが、その後さらに探索を続けます。機能テストで見逃されたとしても、FAST は見逃しません。
- ハッカーレベルのインサイト**
 クライアント側のフレームワークやバージョン番号などの、更新されないと脆弱性となる可能性がある検出結果を確認できます。
- ワークフローマクロ用の HAR ファイル**
 OpenText Dynamic Application Security Testing ではワークフローのスキャンに HAR ファイルを使用でき、スキャン中に重要なコンテンツが保護されるようにします。
- エンタープライズアプリケーションのセキュリティリスクを管理**
 アプリケーション内の傾向をモニターし、最も重大な脆弱性から対処していくことで、DevOps のニーズを満たします。
- 柔軟な導入**
 オンプレミス、SaaS、サービスとしての AppSec を選択できる柔軟性により、迅速な開始と必要に応じた拡張が可能です。
- コンプライアンス管理**
 事前構成済みのポリシーとレポートにより、PCI DSS、DISA STIG、NIST 800-53、ISO 27K、OWASP、HIPAA を始めとする、Web アプリケーションセキュリティに関連するすべての主要なコンプライアンス規制に対応します。
- 水平スケーリングによる高速化**
 水平スケーリングでは、JavaScript の処理に焦点を当てた、OpenText Dynamic Application Security Testing の小さなバージョンを複数、Kubernetes を使用して作成します。これにより、スキャンを並行して実行できるようになり、高速化につながります。
- API スキャンによる精度向上**
 OpenText Dynamic Application Security Testing ではユーザーによる API スキャンの設定が可能のため、GraphQL、gRPC、SOAP、Postman、Swagger を使用してあらゆる認証シナリオに対応できます。また、ユーザーはペアレントトークンを ID プロバイダーから自動的にプルできます。
- クライアント側のソフトウェアコンポジション**
 クライアント側のソフトウェアコンポジション分析 (SCA) は、クライアント側のライブラリの CVE、オープンソースプロジェクトのヘルスデータ、エクスポート可能な CycloneDX SBOM を提供します。

製品の特長

統合による自動化

OpenText Dynamic Application Security Testing は、完全に自動化されたソリューションとして実行することで DevOps や拡張性のニーズを満たし、また、追加のオーバーヘッドを引き起こすことなく SDLC と統合できます。

- REST API は、統合の緊密化、スキャンの自動化、およびコンプライアンス要件の適合性チェックをサポートします。
- OpenText Application Lifecycle Management (ALM) や OpenText Application Quality Management、その他のセキュリティテストシステムと管理システムのための、事前構成済みの統合機能を活用できます。
- この強力な統合により、チームは既存のスクリプトやツールの再利用が可能になります。OpenText Dynamic Application Security Testing は、任意の Selenium スクリプトと簡単に統合できます。
- RESTful Web サービスのスキャン：WISwag コマンドラインツールを介して Swagger および OData 形式をサポートするため、OpenText Dynamic Application Security Testing を任意の DevOps パイプラインに適合させることができます。
- 基本設定：ScanCentral Admin は事前設定したスキャンテンプレートを提供可能なため、ユーザーはセキュリティに関する知識がなくてもアプリケーションをスキャンできます。

主な利点

脆弱性をすばやく早期に検出

OpenText Dynamic Application Security Testing は、アプリケーションに合わせて調整、最適化できるため、SDLC の脆弱性をより早く簡単に見つけることができます。エージェントテクノロジーでスキャンを強化することで、攻撃への対応範囲を拡大し、より多くの種類の脆弱性を検出します。

- OpenText Dynamic Application Security Testing は動的テストとランタイム分析を統合することで、検出結果と範囲を拡充します。アプリをより詳細に探索し、攻撃対応範囲を拡大し、エクスプロイトを発見することによって、動的テストのみを実行するよりも脆弱性を効果的に特定できます。

高度なテクノロジーによる優先度設定：

- ポリシーマネージャーにより、高速化できるように調整されたカスタムポリシーを実行します。
- 探索と監査を同時に実行します。
- 重複排除：アプリの異なる部分に存在する同一クラス / 機能のスキャンを回避することで、送信される攻撃の数を減らします。
- 冗長ページ検出によりスキャン時間を短縮します。
- 開発者にコード行の詳細とスタック追跡情報が提供されるため、脆弱性を迅速に修正できます。
- OpenText Dynamic Application Security Testing は二要素認証 (2FA) 環境でもスキャンを継続します。

自動化とエージェントテクノロジーで時間を節約

- 冗長ページ検出、自動マクロ生成、増分スキャン、コンテナ化によるデリバリーなどの機能により、時間とリソースを節約します。
- スキャンプロセスを最適化し、速度を上げ、精度を向上させます。

最新のフレームワークと Web テクノロジーの探索

OpenText Dynamic Application Security Testing は最新のフレームワークと Web テクノロジーを探索し、あらゆる脆弱性クラスを包括的に監査します。

- HTML5、JSON、AJAX、JavaScript、HTTP2 などの最新の Web テクノロジーをサポートします。
- 「アウトオブバンド」型または OAST で検出される、新しいクラスの脆弱性をテストします。パブリック OAST サーバーを使用すると、OpenText Dynamic Application Security Testing は Log4Shell などの OAST で検出可能な脆弱性を検出できます。
- 次の一般的なフレームワークをサポートするシングルページアプリケーション (SPA) 検出：Angular、AngularJS、React、GWT、Vue、Dojo、Backbone。
- モバイルに最適化された Web サイトや、ネイティブの Web サービス呼び出しもテストできます。
- OpenText Dynamic Application Security Testing は、自動マクロ生成、マクロ検証、修正検証などの機能を提供し、小規模なチームでも大規模に脆弱性を検出して修正できます。
- Linux バージョンの OpenText Dynamic Application Security Testing と ScanCentral DAST を API を介して実行します。

企業の AppSec リスクを ScanCentral DAST で管理

修正と管理の概要を確認できるレポートにより、組織全体のアプリケーションセキュリティリスクを管理できます。傾向をモニターし、アプリケーション内の脆弱性に対応できます。全社規模の AppSec プログラムを作成してリスクプロファイルの可視性をダッシュボードやレポートを通じて管理、活用することで、修正、追跡指標、傾向、進捗を確認できます。ScanCentral DAST を、何十万回ものスキャンを実行するオーケストレーションプラットフォームとして使用することで、AppSec 専門家の少人数チームでも組織全体を管理できます。

- **ScanCentral DAST の可視化**：ScanCentral DAST で DAST の脆弱性を確認して優先順位付けします。
- **ユーザーとドメインの制限**：DAST ユーザーの集中管理は複雑です。ユーザーとドメインを制限することで、管理者はルールを設定して、ScanCentral DAST をセルフサービスモデルで使用する際のスキャンの質を確保できます。
- **PostGresSQL**：MS SQL はデータベースのための高価な選択肢ですが、PostGresSQL は ScanCentral DAST インストール時のもう一つの選択肢であり、速度と品質を諦める必要もありません。

- ScanCentral DAST を Kubernetes と統合してセンサーをスケールアップすると、コスト節約とスキャン実行ごとの新しい環境の確保が可能です。
- ScanCentral 資格情報管理：時間を節約し、すべてのパスワードを 1 か所で更新します。
- ScanCentral DAST リポジトリとの統合：実行時にリポジトリからスキャン設定アーティファクトをプルするため、設定内容を更新する必要はありません。

OpenText Core Application Security について

OpenText Core Application Security は広範な製品スイートを提供し、開発者と AppSec 専門家に包括的なセキュリティと可視性をもたらします。SDLC のどの段階でもあらゆるツールと自動統合し、また、オンプレミス、クラウドホスト、サービス型で利用可能な堅牢な機能セットを提供します。

OpenText について

OpenText は、エンタープライズ向けのセキュリティおよびコンプライアンスソリューションのリーディングプロバイダーとして、ハイブリッド環境におけるリスクを軽減し、高度な脅威からも企業を保護します。市場をリードする OpenText 製品を基盤とする Security Intelligence Platform は、他に類のない最新の相関分析、アプリケーション保護、データセキュリティを提供し、現在のハイブリッド IT インフラストラクチャを高度なサイバー脅威から保護します。

詳細はこちら：[アプリケーションセキュリティ](#)