3D マネージド・アプリケーション・セキュリティ・テストのサブスクリプション

Web テスト、モバイル・テスト、ソースコード・テスト、ネットワーク・テストのすべてのニーズを 1 つのサブスクリプションにバンドル

オンデマンドでセキュリティ・テストの専門知識を駆使し、ビジネスにとって重大な脆弱性を特定および利用することで、漏洩のリスクを低減

概要

今日のセキュリティ専門家やソフトウェア開発者は、アプリケーションのセキュリティを確保しながら、短時間で多くの仕事をこなす必要があります。リスクを軽減し、コンプライアンス要件に取り組むには、ソフトウェア・セキュリティ・イニシアティブにアプリケーション・セキュリティ・テストを組み込む必要があります。とはいえ、進化し続けるアプリケーション・ポートフォリオ全体にアプリケーション・セキュリティ・テストを効果的に適用するリソースやスキルがチームに不足している場合、どうすればよいでしょうか。

ブラック・ダックの 3D マネージド・アプリケーション・セキュリティ・テスト（AST）のサブスクリプションでは、1 つの年間サブスクリプションによる単一価格ですべての種類のマネージド AST を利用可能にすることで、リスク管理目標を達成するために必要なアプリケーションとネットワークのテストの範囲をカバーします。

主な利点

- **柔軟性。**リスクベースのテストをアプリケーション・ポートフォリオに適用します（ハイリスクのアプリケーションでのペネトレーション・テスト対ローリスクのアプリケーションでの DAST など）。さらに、テスト対象のアプリケーション、テストの種類、テストの深度を変更することができます。
- **カバレッジ。**リソースの制約によってテストできない可能性のあるアプリケーションおよびネットワークをテストします。
- **一貫性。**あらゆるアプリケーション、ネットワークで、いつでも同様の高品質のテスト結果が得られます。
- **実現のための支援。**テスト結果を段階的に検討し、お客様のニーズに最適な修正計画を開発する支援が得られます。
- **スケーラビリティ。**手動レビューに支障を来すことなく、アセスメント・センターを通じてスケーラブルなテストを提供します。
- **包括性。**結果の徹底的な分析と詳細なレポートを確認し、手動評価とツールベース評価の混合アプローチからすぐに実施可能な修正ガイダンスが得られます。

進化するテスト要件に迅速に対応

アプリケーションのセキュリティを確保するには、効率的なスケール変更と高速スキャンを可能にしてくれる、人、プロセス、テクノロジーを継続的に利用できる必要があります。ブラック・ダックの 3D マネージド AST のサブスクリプションでは、Web アプリケーション、モバイル・アプリケーション、外部ネットワークを、任意の深度、任意の回数でテストすることができます（一度に 1 テスト）。その結果、圧倒的な透明性、柔軟性、予測可能な費用でのクオリティに加えて、リスクを効果的に修正するために必要なデータが得られます。ブラック・ダックのアセスメント・センターでは、スキルやツールを備え、訓練を受けたセキュリティ・テストの専門家チームを、お客様が継続的に利用できるようにすることで、お客様のアプリケーションをいつでも分析することができます。テスト・ギャップを埋め、任意の深度でテストを実施し、迅速にスケール変更することで、需要の高いテスト期間に対処することができます。

5 つのタイプの評価を実施

3D マネージド AST のサブスクリプションは、複数のテスト・ツール、自動化されたスキャン、詳細な手動テストを組み合わせて、最も包括的なアプリケーション・セキュリティ評価を実施できるようにします。リスク・プロファイルおよびテスト要件の進化に伴い、テスト対象のアプリケーションまたは外部ネットワークのほか、評価の種類およびテストの深度を変更することができます（一度に 1 テスト）。一度に複数のアプリケーションをテストする必要がある場合は、サブスクリプションをもう 1 つ、または個別のマネージド・アプリケーション・セキュリティ・テストをご購入ください。

動的アプリケーション・セキュリティ・テスト（DAST）	ペネトレーション・テスト	静的アプリケーション・セキュリティ・テスト（SAST）	モバイル・アプリケーション・セキュリティ・テスト（MAST）	ネットワーク・セキュリティ・テスト
Web アプリケーションの実行中にソースコードを必要とせずにセキュリティの脆弱性を特定します。	脆弱性を見つけてそれらを利用しようとするビジネス・ロジックに焦点を当てた複数のテスト・ツールと徹底的な手動テストを使用して、DAST を拡張します。	体系的にスキャンし、徹底的な手動テストを適用して、ソースコード内の重大なソフトウェア・セキュリティの脆弱性に共通するものを特定して取り除きます。	従来の静的テスト技術と動的テスト技術を組み合わせて、iOS アプリケーション、Android アプリケーション、対応するバックエンド・コンポーネントにおけるセキュリティの脆弱性を検出します。	手動トリアージが可能な自動スキャンによって、外部ネットワークおよびシステム内の重大なセキュリティの脆弱性に共通するものを検出します。
ソフトウェア・コンポジション解析		**セキュア・デザイン・レビュー**		
ソースコードまたはバイナリコード上でコンポーネントレベルのスキャンを実行して、オープンソースの脆弱性、修正ガイダンス、ライセンス情報を含む部品表を生成します。また、専門家チームが結果のトリアージを実施して、誤検知を解消します。		アプリケーションのアーキテクチャ、デプロイメント、DevSecOps パイプラインのセキュリティを評価します。評価は、AppSec のベストプラクティスに基づきます。		

課題への取り組み

環境全体に新たに出現した脅威、動的なアプリケーション・ポートフォリオ、変化するビジネス要件には、変化に迅速に対応し、特定のリスク・プロファイルおよびテスト要件に適合する、アプリケーションのセキュリティ・テスト計画が求められます。3D マネージド AST のサブスクリプションでは以下を支援します。

- ソフトウェアの不具合によるリスクの測定、改良、管理
- （新たにセットアップ、更新、または廃棄されたアプリケーションによる）変化するアプリケーション・ポートフォリオへの取り組み
- PCI DSS や GDPR などのコンプライアンス要件への適合
- 対応を免れないイベントに対処するための組織内の専門知識やリソースの不足への取り組み
- 開発ワークフローに組み込まれたセキュリティ・テスト

すぐに実施可能なソリューションへの着目

ブラック・ダックは、お客様をバグのリストが残ったままにしておきません。各評価の最後に、ブラック・ダックの専門家が適切な開発チームやセキュリティ・チームとともにテスト結果の説明会を実施して、評価中に特定された各脆弱性のレビュー、質問への回答、すぐに実施可能な軽減ストラテジーおよび修正ストラテジーについての話し合いを行います。

ビジネス・ニーズに合わせたスケール変更

アプリケーション・ポートフォリオやテスト要件が増えても、費用は増えません。3D マネージド AST のサブスクリプションは、調達および予算計画をシンプルにする優れた方法です。

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

©2024 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2024 年 9 月