マネージド・モバイル・アプリケーション・セキュリティ・テスト（MAST）

モバイル・アプリケーション・エコシステム全体で重大なセキュリティ脆弱性を特定および除去し、データ漏洩のリスクを軽減する MAST をオンデマンドで

概要

現在のセキュリティ・プロフェッショナルおよびソフトウェア開発者は多面的な役割を負うようになっており、アプリケーション・セキュリティ以外にも多くの業務で多忙をきわめています。モバイル・アプリケーション・セキュリティ・テスト（MAST）はアプリケーション・セキュリティ・テストを構成する必須要素の 1 つですが、ポートフォリオ全体に MAST を効果的に適用しようとすると、それなりのリソースとスキルが必要です。ブラック・ダックのマネージド MAST をご利用いただくと、クライアント・サイド・コード、サーバ・サイド・コード、サードパーティ製ライブラリの解析を簡単に導入し、モバイル・アプリケーションに潜むセキュリティ脆弱性をソースコードなしで体系的に見つけ出して修正できます。

主な利点

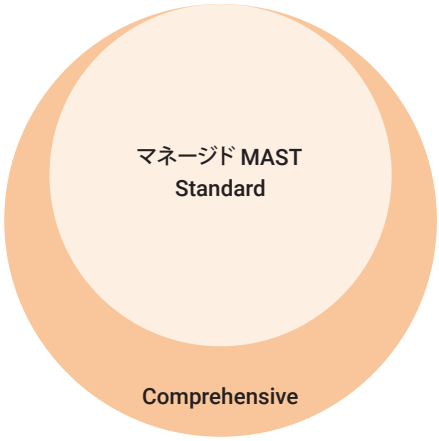
- **柔軟性：**使いやすいオンデマンドのポータルでサービスを管理できます。テストのスケジュール設定、テスト深度の選択、そして業務要件の変化や脅威の進化に応じた変更も簡単に行えます。
- **カバレッジ：**リソース不足でモバイル・アプリケーションを十分にテストできないという悩みを解消します。
- **一貫性：**あらゆるモバイル・アプリケーションについて、いつでも高品質な MAST 結果を得ることができます。
- **支援：**テスト結果を丁寧にご説明し、ご要望に応じた最適な対策プラン作りを支援します。
- **スケーラビリティ：**ブラック・ダックのアセスメント・センターを通じて、マニュアル・レビューの質を低下させることなく、スケーラブルな MAST を実施できます。
- **包括性：**徹底した結果解析、詳細なレポートの作成、実践的な対策指針など、マニュアル・ベースの評価とツール・ベースの評価を併用します。

規模の変更にもスピーディに対応できるリソースをご用意

アプリケーションのセキュリティを維持するには、あらゆる規模のテストを効率良くスピーディに実施できる必要があり、そのためにはそれを支えるスタッフ、プロセス、テクノロジにいつでもアクセスできることが重要です。ブラック・ダックのマネージド MAST は、柔軟でスケーラブル、そして低コストのテストを通じ、お客様のリスク・マネージメントの目標達成に必要なアプリケーション・テスト・カバレッジを実現します。ブラック・ダックのアセスメント・センターでは、お客様のモバイル・アプリケーション解析にふさわしいスキル、ツール、規律を備えたセキュリティ・テスト専門家のチームをいつでもご利用いただけます。これにより、テストの不備を解消し、任意の深度でテストを実施できるほか、大量のテストが必要な期間にもスケーラブルに対応できます。

変化への対応

モバイルを取り巻く環境は目まぐるしく変化しています。モバイル・オペレーティング・システムのアップデート、新しいモバイル・アプリケーション開発フレームワークの登場、新しい攻撃の発見などのたびに新しいセキュリティ問題が発生し、アプリケーションが影響を受ける可能性があります。



モバイルの代表的なリスク

- 脆弱なサーバ・サイド管理
- 安全でないデータ・ストレージ
- 不十分なトランスポート層保護
- 意図しないデータ漏洩
- 認可・認証の不備
- 暗号手法の不備
- クライアント・サイド・インジェクション
- 信頼できない入力によるセキュリティ決定
- 不適切なセッション・ハンドリング
- バイナリ保護の不足

2 つのテスト深度を選べるマネージド MAST

マネージド MAST では、モバイル環境専用に設計したアプリケーション・セキュリティ・テスト・スイートを使用して、動作中のモバイル・アプリケーションに潜むソフトウェア・セキュリティ脆弱性を一般的なものから重大なものまで特定します。独自技術に基づく静的解析ツールと動的解析ツールを組み合わせて使用するため、別々に適用したのでは見つからない脆弱性も正確かつ効率よく特定できます。マネージド MAST は 2 つの深度をご用意しており、アプリケーションのリスク・プロファイルに合わせて最適なテスト・レベルをお選びいただけます。

マネージド MAST–Standard

モバイル機器で動作するアプリケーション・バイナリに自動解析とマニュアル解析を組み合わせて適用することにより、自動解析だけでは見つからない脆弱性を特定します。認証と認可の問題、クライアント側の信頼の問題、セキュリティ設定のミス、クロスプラットフォーム開発フレームワークの問題などを検知できます。また、マニュアル・レビューによる誤検知の特定、およびお客様とのミーティングによるテスト結果のご説明も実施します。

マネージド MAST–Comprehensive

マネージド MAST–Standard のサービス内容に加え、マニュアル解析をより手厚く適用することにより、モバイル機器で動作するアプリケーション・バイナリだけでなく、対応するサーバ・サイド機能に潜む脆弱性も見つけます。サーバ・サイド脆弱性の例としては、セッション管理、暗号化の問題、認証と認可の問題、その他の一般的な Web サービスの脆弱性などがあります。また、マニュアル・レビューによる誤検知の特定、およびお客様とのミーティングによるテスト結果のご説明も実施します。

問題の解決までをしっかりサポート

ブラック・ダックのマネージド・サービスは、見つかった問題を報告して終わりではありません。毎回のテスト実施後に、ブラック・ダックのエキスパートがご担当の開発 / セキュリティ・チームとミーティングを実施し、テストで見つかった個々の脆弱性をレビューし、お客様のチームからのご質問に答え、実践的な軽減・修正戦略について話し合います。

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