BLACKDUCK®

レッドチーム

組織の現実の攻撃に対する耐性を評価する

脆弱性はそれ自体では小さく見えても、まとまって攻撃経路を形成すると大規模な損害を引き起こす可能性があります。ブラック・ダックのレッドチーム（模擬攻撃チーム）は、現実の敵がシステムを攻撃する方法やシステムが攻撃にどの程度耐えられるかをモデル化します。システムのセキュリティ評価だけでなく、ブラック・ダックのレッドチーム・プロフェッショナル・サービスでは、お客様の組織のインシデント対応手順もテストします。レッドチームによる演習が完了すると、定義された一連の資産を攻撃する特定の脅威アクターに対応する組織のセキュリティ体制に対する理解が向上し、重点的に取り組むべき改善ポイントが分かります。

悪用可能なセキュリティ・ホールを探し出す

ブラック・ダックのレッドチームは、別々に見えたり、複数の領域にまたがった脆弱性をつなぎ合わせ、さまざまな複雑な攻撃手法を駆使して、組織のアタック・サーフェス全体で悪用可能なセキュリティ・ホールを即座に特定します。これには、システム、ソフトウェア、人員の間の関係も含まれます。探し出すリスク領域には以下のようなものがあります。

- 従業員のワークステーションやネットワーク共有上にある個人識別可能情報（PII）、プライマリ・アカウント番号（PAN）、保護されるべき医療情報（PHI）
- ログファイルに記録された機密データ
- レポーティング・ダッシュボードのマスクされていないデータ
- ソースコード中の暗号鍵

組織として攻撃への準備はできていますか

ブラック・ダックの攻撃プロセスは、一見別々に見える脆弱性をつなぎ合わせ、アプリケーション、ネットワーク、チームの挙動を総体的にとらえます。各レッドチームの評価は、体系的かつ反復可能な方法論的手法を採用し、以下の 6 つの基本的手順で構成されます。

1. 目標設定

レッドチームの攻撃対象となる特定の目標または資産を設定します。

2. 偵察

レッドチームによってネットワークサービス、Web アプリケーション、従業員ポータルが洗い出されます。

3. ペネトレーション・テスト

アプリケーションとネットワークに関するペネトレーション・テストを実施し、脆弱性を明らかにします。（例えば、クロスサイトスクリプティング）

言い古された質問に答える。自社のリスクとは何か。

セキュリティに対して
どこに時間と予算、労力を
重点的にかけるべきかを
レッドチームが明らかに
します。

4. ソーシャル・エンジニアリング

レッドチームは、一般的な人的操作手法（メールや電話によるフィッシングなど）を利用し、「人的な脆弱性」（無意識のうちに自社の機密情報を漏らす人）を見つけ出します。

5. エクスプロイトとエスカレート

発見した脆弱性の１つを使ってネットワーク内部へ侵入します。これは、物理的な設備への攻撃だったり、ビジネスプロセスの改ざんの場合もあります。例えば、追従侵入や従業員や業者へのなりすましによって実際の職場に侵入します。

6. 目標達成

レッドチームが機密性の高い企業資産へのアクセスに成功します。

7. 修正

各評価の最後に、適切な組織のステークホルダーとともに、診断中に発見された脆弱性のレビューを行い、各脆弱性に関する質問に回答し、リスク緩和や修正に関する戦略のディスカッションをします。

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