CrowdStrike Services

CROWDSTRIKE

レッドチーム/ブルーチーム演習

標的型攻撃から防御するために サイバーセキュリティチームの準備体制を整える

サイバー攻撃は絶えず進化

攻撃の戦術、技術、手順（TTP）は絶えず進化しており、すべての組織は、侵害を特定、阻止、防御する方法を理解する必要があります。多くの組織は、保護を任せている複雑なセキュリティツール群を抱えています。課題は、これらのツールとそれに実装されているポリシーと手順が効率的であり、現在の攻撃から防御できるかどうかを理解することです。

標的型攻撃から身を守るための訓練

CrowdStrike®レッドチーム/ブルーチーム演習は、その道の専門家から学ぶことで、サイバーセキュリティチームの準備体制を整えるのに役立ちます。レッドチーム（攻撃側）は攻撃者を模倣した演習でシステムを攻撃し、ブルーチーム(防御側)はチームによる環境内でのこの標的型攻撃からの防御対応を支援します。

この演習では、CrowdStrikeは2つのコンサルタントチームを配置します：実世界で攻撃者が取る手法を使用して環境を危険にさらすレッドチームと、既存のツールを使用してセキュリティ担当者と協力して悪意のあるアクティビティを特定し、評価、対応するインシデント対応者のブルーチームです。

主な利点

既存のセキュリティ製品の設定ミス、製品が網羅すべき範囲と実際の展開範囲のギャップを見つけ特定

セキュリティチームの脅威ハンティングの知識と全体的なインシデント対応プロセスを成熟させることに重点を置いたトレーニングを安全な環境で実施

セキュリティ担当者が、実際の脅威アクターの考え方と方法論、および環境内でのその活動を検出する方法を理解できる様に標的型攻撃のフェーズを実地検証

CrowdStrike Services

レッドチーム / ブルーチーム演習

主なサービス提供内容

キルチェーンに沿っての典型的な演習の流れ

積極的な偵察

レッドチームが外部に公開されているお客様のインフラストラクチャをスキャンして脆弱性を探します。一方、ブルーチームは、お客様の担当者が攻撃者の偵察を検知し、その対応として取りうる予防的措置を検討するための支援を行います。

配信、攻撃（エクスプロイト）

レッドチームは、見つかったアプリケーションやシステムの脆弱性を利用して、外部に公開されているインフラストラクチャへの侵害を試みます。この際、実世界の攻撃者が利用する戦術やソフトウェアを活用します。レッドチームが設計した侵入方法でアクセスできない場合、あるいはお客様が稼働中のインフラストラクチャへの侵入を避けたい場合は、お客様側の担当者が手動で攻撃を実行し、調査のための痕跡をのこします。ブルーチームはお客様のセキュリティ担当者とともに、このインシデントの判定を行います。ホストおよびネットワークの分析を行い、攻撃元、攻撃先、エクスプロイト手法、不正のプロセス、権限付きアクセスのレベルを特定します。

コマンド&コントロール

レッドチームのツールがその攻撃インフラストラクチャへの信号を発する間に、ブルーチームは、お客様のセキュリティ担当者がこのトラフィックを特定し、その他の侵害されうるポイントを探して、攻撃者のアクセスに関する包括的なイメージを得られるよう支援します。

オペレーション

レッドチームが権限を特権に昇格させ、脆弱性を列挙し、アクセス範囲を拡げて、お客様環境内でデータ抽出を模倣します。一方、ブルーチームはお客様の担当者とともに、これらの操作を追跡し、攻撃者の目的を評価します。これは、インシデント対応の中で最も難しい分析の一つです。攻撃者がお客様の環境への侵入のために使ったシステム、データ、手法を明らかにすることで、対応チームはそのインシデントによる組織的なリスクをより詳しく理解して、今後の攻撃者の活動を予測し、封じ込め・修復するための戦略を立てることができます。

実施後の振り返り

攻撃フェーズのすべてが完了した後、ブルーチームは引き続きお客様のセキュリティチームとともに、ホストおよびネットワークの分析を実施し、発生したイベントをつなぎ合わせてタイムラインとストーリーを構築します。その作業が完了したら、レッドチームが攻撃の一つひとつを詳細に説明し、この一連の攻撃についてお客様が完全に理解できるようにします。CrowdStrikeのコンサルタントも協力しながら、インシデント対応の行動を振り返り、得られた教訓や推奨される改善点について記録します。

CROWDSTRIKEが選ばれる理由

実際の標的型攻撃シナリオ：CrowdStrikeのレッドチームは、広範なペネトレーション・テストの経験と、今日の高度な攻撃で使用されるTTPについての深い理解を持っています。

サイバーキルチェーン・プロセス：CrowdStrikeのレッドチームは、サイバーキルチェーンの手順に従う標的型攻撃を模倣するために、攻撃者グループが使用する同じツールとテクニックを取り入れています。

高度な脅威インテリジェンス：CrowdStrikeのブルーチームは、特にお客様の属する業界を標的とする攻撃TTPへの洞察を提供します。この演習は、潜在的な脅威と、標的型攻撃から身を守る方法をよりよく理解するのに役立ちます。

CROWDSTRIKEのサービスについて

CROWDSTRIKEのサービスは、セキュリティインシデントの防御と対応に必要な保護策と専門知識を企業に提供します。CrowdStrikeのサービスチームは、クラウドベースのCrowdStrike Falcon®プラットフォームを活用して、次世代型のエンドポイント保護、サイバー脅威インテリジェンスの収集・報告、24時間365日のプロアクティブな脅威ハンティングを行うことにより、お客様がリアルタイムで攻撃者を特定、追跡、ブロックできるよう支援します。CrowdStrikeはその独自のアプローチで、不正なアクセスをただちに阻止して侵害の拡大を防ぎます。さらに、CrowdStrikeが提供するプロアクティブなサービスにより、組織は脅威を予測し、ネットワークのセキュリティ体制を整え、最終的には侵害を阻止できるようになります。

www.crowdstrike.jp/services/ で詳細をご覧ください。
Eメール: services@crowdstrike.com