データシート

MANDIANT®
A FireEye® Company

レッドチーム・サービス

現実的な標的型攻撃から重要資産を保護する能力を診断

メリット

- 重要なデータがリスクにさらされているかどうか、および悪意のある攻撃者にどの程度容易にデータを窃取されてしまうかを認識
- 現実に即した「制約なし」の模擬攻撃でセキュリティ環境を診断
- 制御下にある現実に即した環境で、お客様の社内セキュリティ・チームのインシデントに対する防御、検知、対応能力をテスト
- 攻撃者に悪用される前に複雑なセキュリティの脆弱性を発見、解消
- 事実に基づくリスク分析とセキュリティ体制の強化に向けた提案

Mandiantが選ばれる理由

FireEyeのコンサルティング部門であるMandiantは、2004年の創業以来、サイバー・セキュリティとサイバー脅威インテリジェンスの最前線で活動を続けてきました。FireEyeのインシデント対応担当者は、世界各地で発生した数々の複雑なセキュリティ侵害事件を現場で経験しています。このため、新旧の攻撃グループや、絶え間なく変化する攻撃者のツール、戦術、手順を深く理解しています。

サービス概要

レッドチーム・サービスのエンゲージメントは、お客様の環境における現実的な「制約なし」の攻撃シナリオで構成されています。Mandiantのレッドチームは、チームとお客様で決めた目標を達成するために、非破壊的な方法を取り、攻撃者の行動パターンで擬似攻撃をします。レッドチームは、実際に最近発生したインシデント対応事例で確認されたTTPを使用して、現実の攻撃者の活発で複雑な攻撃手口を詳細に再現します。このため、活発な攻撃者のシナリオに対するお客様のセキュリティ・チームの検知、対応、封じ込め能力を診断できます。

サンプル目標		
幹部または開発者のEメールを窃取する	ビジネスに重要なデータまたは機密データのある、セグメント化された環境に侵入する	IoTデバイス、医療機器、製造機器などの自動装置を乗っ取る

方法論

レッドチーム・サービスは、レッドチームがお客様の環境に関してある程度の知識が必要か、または把握していなくてもかまわないかをお客様と協議して判断したうえで開始します。Mandiantは、業界で培った経験を活かして、お客様の基幹業務にとって最も大きなリスクと見なされる目標を明らかにします。

FireEye

レッドチーム・サービスの取り組みとしては、攻撃ライフサイクルの各段階に従います。

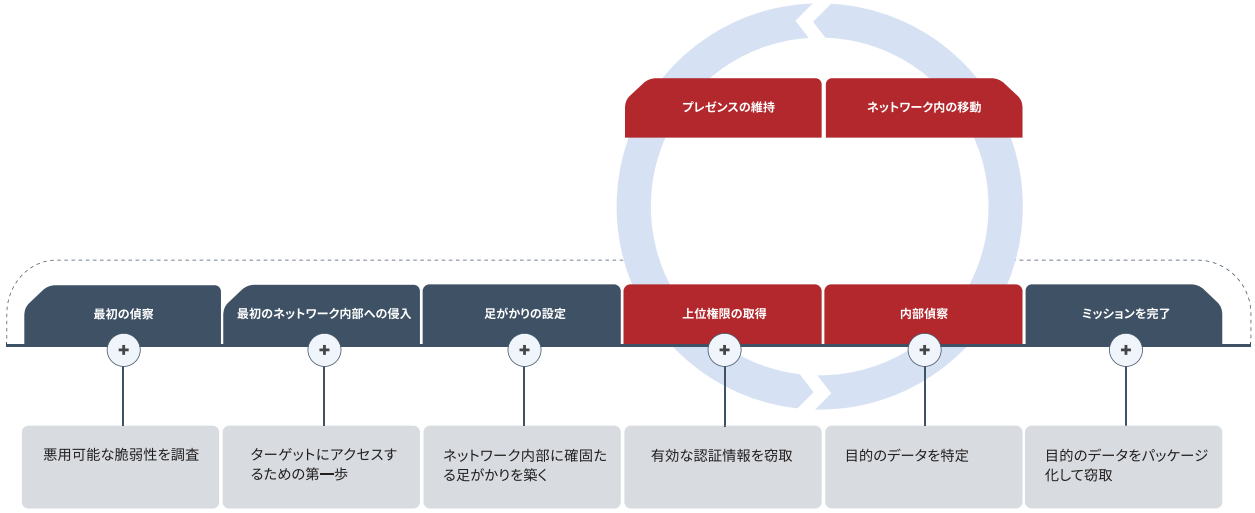

図1: 攻撃ライフサイクル

目標を設定したら、まずレッドチームは最初の偵察を実施します。Mandiantは、独自のインテリジェンス・リポジトリとオープンソース・インテリジェンス（OSINT）ツールおよび手法を組み合わせて、標的の環境の偵察活動を行います。

Mandiantは、脆弱性を悪用するか、ソーシャル・エンジニアリング攻撃を仕掛けて、標的の環境に最初にアクセスしようとします。Mandiantは、実際の攻撃者によって使用される手法を利用して、こうしたシステムへの特権アクセスを取得します。

アクセスに成功すると、実際の攻撃者が行うように、上位のアクセス権限への昇格やC&Cインフラストラクチャを配置することによってお客様の環境内で常駐化を試みます。

常駐化とC&Cシステムが環境内で確立された後、お客様のビジネスに影響しない方法を必要に応じて使い、目標を達成しようとします。

レッドチーム・サービスを選ぶ理由

レッドチーム・サービスは、以下の目的を実現しようとする組織に推奨されます。

- 検知および対応能力をテストする。セキュリティ・チームは現実のインシデントへの準備体制を整えますが、お客様は実際のリスクがない環境でセキュリティ・チームが適切に対応できることを確認する必要があります。
- 意識を高め、影響を示す。Mandiantのレッドチームは、現実の攻撃者を装って、インターネット上でのみ公開される情報を使用し、インターネットからお客様のネットワークを侵害しようとします。レッドチームがうまく関与することで、増加するセキュリティ予算の正当化と追加投資を必要とするギャップを把握することができます。

サービスの内容と特長

- 経営幹部や管理職向けの概要レポート
- 診断結果の再現に十分な情報を含む技術的な詳細レポート
- 事実に基づくリスク分析で、自社環境の問題を把握
- 短期的な改善に向けた戦術的な改善策
- 長期的な改善に向けた戦略的な改善策
- メディアを騒がす心配なしに、実際の攻撃に対応してきた貴重な経験

FireEyeの詳細については、**www.FireEye.jp**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03−4577−4401 |
Japan@fireeye.com

会社概要

FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデント対応といった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。FireEyeは「Forbes Global 2000」企業の45%以上を含む、世界67か国以上の6,600を超える組織で利用されています。

FireEye