レッドチームサービス

**人材、プロセス、テクノロジーが
確固たる目的を持った攻撃者による最重要資産へのアクセスを
効果的に防御しているかどうか評価します。**

MANDIANT
A FireEye® Company

機密情報の漏えいにつながる恐れのある複雑なセキュリティ脆弱性を事前に発見、解消します。

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、対応能力を向上
- セキュリティツールと手順を制御下にある攻撃シナリオでテスト
- 攻撃者に悪用される前に複雑な脆弱性を発見、解消
- 事実に基づくリスク分析の結果と改善策

MANDIANTが選ばれる理由

Mandiantは、インシデント対応専門のコンサルティング企業です。世界中の高度な攻撃グループへの対応を10年以上積み重ねた豊富な経験をベースに、世界各国の組織から厚い信頼を得ています。セキュリティ侵害発覚後の緊急事態における対応支援から、有事に備えた検知・対応・封じ込め体制の強化まで、インシデント・レスポンスに関する幅広いサポートを提供しています。レッドチームサービスの強みは、高度で持続的な標的型攻撃および攻撃者の行動パターンに関する豊富な専門知識です。現実の攻撃者と同じツール、戦術、手順（TTP）を用いて、事前に設定した目標の達成を目指します。

概要

レッドチームサービスは、「レッドチーム攻撃診断」と「レッドチーム攻撃演習」という2つのプランで構成されています。いずれも目的志向かつ現実的な診断で、お客様がご自身のビジネスにとって最重要と考える資産のみに焦点を当てています。

レッドチーム攻撃診断

レッドチーム攻撃診断は、お客様の環境における「制約なし」の現実的な攻撃シナリオで構成されています。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、（ビジネスに損害を与えずに）必要な方法を取り、攻撃者の行動パターンで擬似攻撃をします。これらの目標は、甚大なリスクとなり得る、ビジネスで最も重要な領域に焦点を当てています。

サンプル目標

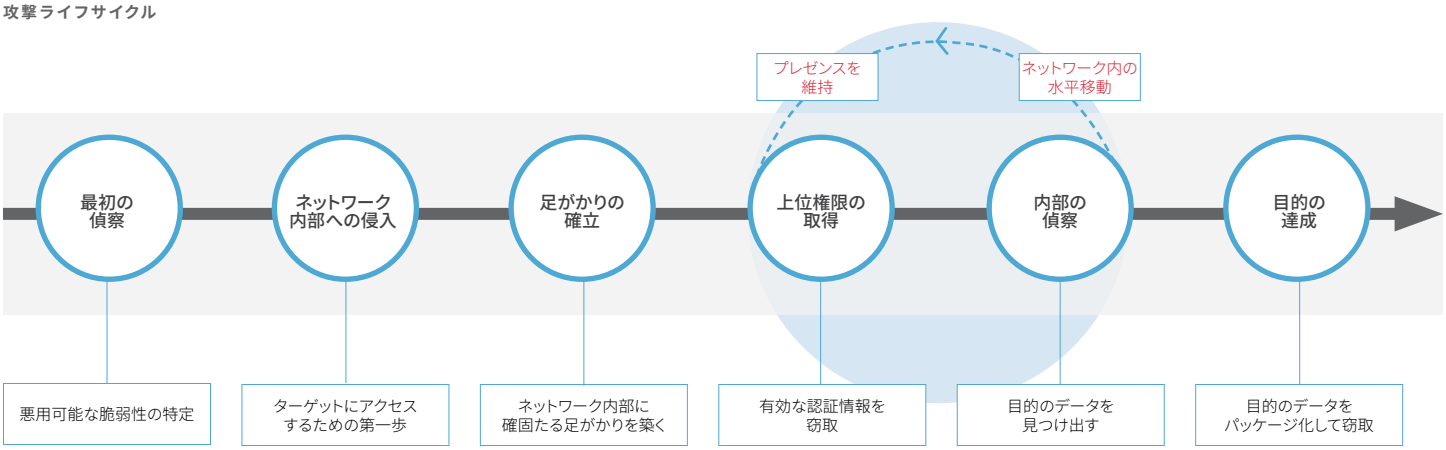
幹部または開発者のEメールを窃取する	ビジネスに重要なデータまたは機密データのある、セグメント化された環境に侵入する	IoTデバイス、医療機器、製造機器などの自動装置を乗っ取る

方法論

ホワイト・ボックス（専門知識あり）またはブラック・ボックス（専門知識なし）のどちらで進めるか、お客様と協議して判断したうえで開始します。Mandiantの業界に基づく今日インテリジェンスを活用し、ビジネスにとって重要であると見なされる領域における主要なリスクとなる3〜5つの目標をお客様のチームと共同で特定します。このプロセスは、これらのリスクの発生見込みを特定することを意図して行います。目標について合意したら、レッドチームは運用を開始します。レッドチームは、環境に侵入して内部偵察活動を試みます。アクセスに成功すると、実際の攻撃者が行

FireEye

攻撃ライフサイクル



うように、上位のアクセス権限への昇格やユニークなバックドアを複数配置することによって常駐化を試みます。その後、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。

レッドチーム攻撃演習

レッドチーム攻撃演習では、お客様組織のセキュリティ体制および社内セキュリティ・チームの両方を評価します。攻撃者がお客様の環境を侵害する前に、現実的なシナリオに基づいて評価を完了します。攻撃者に侵入されれば、メディアで望ましくない取り上げられ方をする可能性があります。

レッドチーム攻撃演習はレッドチーム攻撃診断に基づいており、社内セキュリティ・チームの防御、検知、対応能力にも焦点を当てています。インシデント・レスポンス担当は、診断中にレッドチームを検知できるようサポートし、アクティビティが検知された場合には適切な対応手法をアドバイスします。診断が完了すると、レッドチームのメンバーとお客様の社内チームに参加しているインシデント・レスポンス担当が、お客様の社内セキュリティ・チームと協力し、将来の攻撃に対する防御、検知、対応を向上させる計画を作成します。

方法論

レッドチーム攻撃演習の方法論とレッドチーム攻撃診断の方法論は基本的に同じですが、前者では、インシデント・レスポンス担当がお客様のセキュリティ・チームやセキュリティ・オペレーション・センター（SOC）と協力して、レッドチームのアクティビティを検知するという違いがあります。診断終了後、レッドチームとインシデント・レスポンス担当は、お客様の社内チームとともに改善策を作成します。レッドチーム攻撃診断と複雑な侵入に対応する当社の経験に基づき、お客様のセキュリティ体制を向上させるための防御、検知、対応を強化する方法について詳細に記載します。診断結果は、攻撃ライフサイクルにおけるセキュリティ体制の診断に基づいています。

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

Mandiantコンサルティング・サービスの詳細については、
以下のWebページをご覧ください。
www.FireEye.jp/services.html

〒101-0054 ファイア・アイ株式会社 Mandiantコンサルティング
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

www.FireEye.jp

FireEye