データシート

MANDIANT®
A FireEye® Company

レッドチーム・セキュリティ・オペレーション

現実的な攻撃のシナリオに対する検知・対応を改善するために セキュリティ・チームをコーチング

メリット

- 検知および対応機能の状態を評価
- インシデント対応時に必要な適切な人材、プロセス、テクノロジーがすべて揃っていることを確認
- 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非破壊的な攻撃シナリオでテスト
- 対応時間の短縮と効率の向上
- 成熟したインシデント対応手順
- さまざまな攻撃シナリオへの対応策を確保

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

「パープルチーム・サービス」とも呼ばれるレッドチーム・セキュリティ・オペレーション（RTSO）では、ネットワーク内で発生する高度な標的型攻撃に対する社内セキュリティ・チームの防御、検知、対応、封じ込めの能力を評価します。 これは、攻撃者ライフサイクルの段階ごとに現実的な攻撃シナリオを使用するという方法で実現できます。

Mandiantのレッドチームは、この業種において最も活発な活動を見せている脅威グループを特定し、こうしたグループが使用するツール、戦術、手順（TTP）を用いてお客様の環境を模擬攻撃するためのシグネチャを作成します。作成されたシグネチャは、セキュリティ・チームが現実的なTTPを体験できるよう、RTSOシナリオに組み込まれます。

RTSOは、全体的な検知およびアラート機能の改善に役立ちます。RTSOは、ネットワーク・インフラストラクチャ内の脆弱性や不適切な設定を発見するためのものではありません。

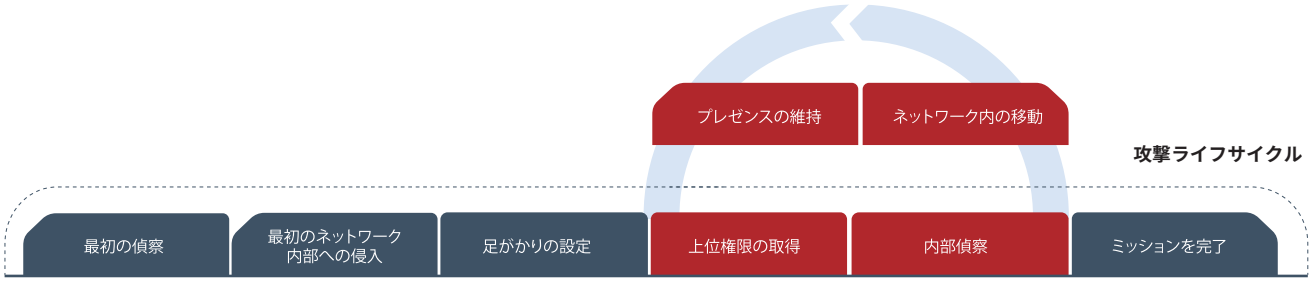
レッドチーム・セキュリティ・オペレーションと標準的なレッドチーム・サービス

	レッドチーム・セキュリティ・オペレーション	レッドチーム・サービス
目的	攻撃ライフサイクルの各段階における検知、防御、対応能力を評価する。	経営幹部のメールを窃取したり、重要なビジネス・データにアクセスしたりするなど、目的のはっきりしたサンプル対象を狙う。
差別化	Mandiantのインシデント対応担当者がお客様のセキュリティ・チームと連携し、その過程でコーチングも行う。	目的のはっきりした現実的な標的型攻撃をシミュレートする。Mandiantのチームは目標の達成に必要なすべての対策を実施する。
シミュレートされる攻撃	攻撃ライフサイクルの各段階で複数の攻撃グループをシミュレート可能。	合意した目標に向けて継続的に攻撃を実施する。
お客様のセキュリティ・チームの関与	Mandiantのインシデント対応担当者による観察とコーチングの下で攻撃シナリオに対応する。	Mandiantチームとの直接的な関与はない。レッドチームの攻撃の検知、防御、対応に向けて活動する。セキュリティ・チームに対して演習中であることをわからないように設定可能。

FireEye

方法論

レッドチーム・セキュリティ・オペレーションの方法論は、攻撃ライフサイクルの各段階に適用される段階的なシナリオに基づく演習です。



クライアント機能のサンプル評価

	最初の偵察	最初のネットワーク内部への侵入	足がかりの設定	上位権限の取得	内部偵察	ネットワーク内の移動	プレゼンスの維持	ミッションを完了
検知	—	✓	✓	✓	✗	✗	✗	✓
無力化	✓	✓	✓	✓	✗	✓	✗	✗
対応	✗	✓	✗	✗	✗	✗	✗	✗

図1：Mandiantのレッドチームは、攻撃ライフサイクルの各段階においてクライアントのセキュリティ・チームの能力をテストします。

これらの段階には、偵察、最初の侵害、足がかりの設定、権限の昇格、内部偵察、目的の達成が含まれます。この評価には、お客様の社内セキュリティ・チームまたはセキュリティ・オペレーション・センター（SOC）と協力して、レッドチームによって実行される各シナリオを検知するインシデント対応担当者が含まれます。

各段階で、不正な活動が検知された場合、Mandiantは社内セキュリティ・チームと協力して、検知に対する対応が適切であり、継続的なメリットを得られるような手順が整っていることを確認します。不正な活動が検知されなかった場合、レッドチームはMandiantのインシデント対応コンサルタントと協力して、次回のシミュレーション時に既存の検知テクノロジーをより適切に利用するか、技術的な改善が必要な領域を特定します。

セキュリティ・チームがレッドチームの活動を検知して対応すると、インシデント対応コンサルタントは実行中のインシデント対応のプロセスと手順を監視し、検知と応答時間の向上を促進します。Mandiantのコンサルタントは、既存のログを検証して、レッドチームの活動を検知するのに十分かどうかも判断します。

内容

- 経営幹部や管理職向けの概要レポート
- 実施した各シナリオに対する十分な情報を含む技術的な詳細レポート
- 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
- 大規模な侵害に対応してきた長年の経験を持つセキュリティ担当者と直接連携できる貴重な体験

レッドチーム・セキュリティ・オペレーションを選ぶ理由

RTSOは、セキュリティ・チームの能力、プロセス、テクノロジーを評価および開発して、攻撃ライフサイクルの各段階において標的型攻撃を検知、防御、対応したいと考えている組織に推奨されます。

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