データシート

MANDIANT®
A FireEye® Company

サイバー攻撃演習

シナリオに基づく攻撃演習で、組織のインシデント対応計画を診断

メリット

- 書面上の対応計画と実際の行動のギャップを把握
- 実際のインシデント対応のベスト・プラクティスに基づく改善策を提案
- 侵入行為を伴わず、短時間で効率的に実施できる机上演習

「セキュリティ・インシデントに効率的・効果的に対応できる体制作りは、当社のビジネスにとってきわめて重要です。机上演習は、意思決定の是非を検証し、ディスカッションによる検討が可能になるので、非常に有意義でした」

-CISO、国際的なテクノロジー・ディストリビュータ

Mandiantが選ばれる理由

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。Mandiant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戦術、手法、手順を深く理解しています。

Mandiantの専門知識を活用するサイバー攻撃演習は、実環境での経験に即した個別のシナリオ用インジェクトを提供し、ビジネスおよび技術面の主要なリスク領域をカバーするように考案されています。

概要

サイバー攻撃演習では、戦略的・技術的なインシデント対応という経営幹部の視点から、サイバー危機に対処する上でのお客様組織のプロセス、ツール、能力の有効性を診断します。演習中は、Mandiantのコンサルタントが実環境での経験に即した複数のシナリオ用インジェクトを机上で実施。組織の行動やその意思決定の経過を観察します。

FireEye

サービスの内容と特長

経営幹部向けの説明資料 [PPT]

- 対面演習の概要:
  - インシデント対応計画(IRP)、コミュニケーション計画、上申計画に基づく演習参加者の行動などを解説
  - 演習で得られた教訓
  - 戦略的な推奨事項

サイバー攻撃演習の事後検証レポート [PDF]

- イベントの流れ
  - すべてのインジェクト
  - 関係者/参加者の対応
- 各ステップにおける、戦略的なインシデント対応の診断結果と推奨される改善案
  - 検知
  - 対応
  - 封じ込め
  - 復旧

アプローチ

Mandiantのコンサルタントはまず、お客様組織のリスク特性や作業環境、特に懸念される領域について把握します。続いて、お客様組織の主要関係者を対象にオンサイトで演習を開始。Mandiantのインシデント対応活動で確認された攻撃者の行動パターンや技法、戦術に基づいてシナリオ用インジェクトを調整、投入します。演習の間、参加者の行動や判断が事前に定められた計画や手順、Mandiantが提唱するインシデント対応のベスト・プラクティスに沿っているかどうかを確認します。

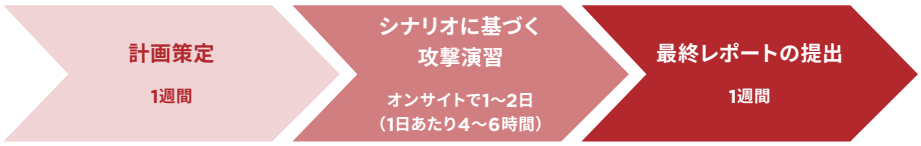
演習終了後、確認された事項をコンサルタントが対面で簡単に説明します。そして後日、演習の流れと、検知・対応・封じ込め・復旧というセキュリティ侵害対策の各ステップにおける参加者の行動をまとめた事後検証レポートを提出します。

サイバー攻撃演習の手順

ステップ1:
計画策定:シナリオとインジェクトの作成

ステップ2:
サイバー攻撃演習:インジェクトを調整したシナリオの実施と、その対応の診断

ステップ3:
レポートの作成と提出:診断結果を共有し、専用の作業ロードマップを作成



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