MANDIANT

データシート

サイバー攻撃机上演習

シナリオに基づく攻撃演習でサイバー・インシデント対応を評価する

メリット

- 実際の行動と比較して、書面上の対応計画と期待される対応のギャップを把握
- 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。サイバー攻撃机上演習は、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、世界各地で発生する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TTP（Tactics、Techniques、Procedures）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机上演習は、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

サイバー攻撃机上演習では、戦略的かつ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。演習中は毎回、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。

アプローチ

サイバー攻撃机上演習を開始する前に、Mandiantの専門家はまず、組織の脅威プロファイル、運用環境、特に懸念される領域を理解するための作業を行います。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の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の専門家が特定した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。

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

サイバー攻撃机上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
  - インシデント対応
  - 封じ込め
  - 復旧

サービス・トラック

技術担当者向けのインシデント対応と**経営幹部向けの危機管理**という、2種類のサイバー攻撃机上演習を提供します。ベスト・プラクティスとしては、各演習を毎年行います。これは個別に行うことも、総合演習の一環として行うこともできます。

技術担当者向けのインシデント対応の演習は、セキュリティ・チームの管理者や担当者の対応プロセスの能力を診断します。

経営幹部向けの危機管理演習は、危機対応戦略の有効性をテストしたいと考える経営幹部に適しています。

ワークショップの後、組織に対して直接ブリーフィングを行い、演習の内容と対応をステップごとにまとめた事後検証レポートを提供します。

表1：サービス・トラック比較

サービス・トラック	技術担当者向け	経営幹部向け
目的	高度な攻撃の検知、対応、封じ込めを実施するため、組織の技術的な対応能力を診断、解析します。	高度な攻撃を受けた際の組織の危機管理能力を、経営幹部の視点から診断、解析します。
実施タイミング	**計画：**1週間（オフサイト） **シナリオに基づく攻撃演習：**1～2日（オンサイト） **最終レポート：**1週間	**計画：**1週間（オフサイト） **シナリオに基づく攻撃演習：**1～2日（オンサイト） **最終レポート：**1週間
対象参加者	• サイバー・セキュリティ・インシデント対応チーム（CSIRT） • セキュリティ・マネージャー • 技術担当スタッフ（ネットワーク、サーバー、Eメールなどの担当者）	• 最高情報セキュリティ責任者（CISO） • 一般の経営幹部 • 広報およびコミュニケーション担当者 • 法務責任者
重点エリア	• ネットワーク上のホストを隔離するタイミング • システムの初期化のタイミング • アナリストが定義済みIRP、コミュニケーション計画、エスカレーション・マトリックスを把握しておく方法 • サードパーティ・ベンダーに依頼するタイミングと方法	• 恐喝や身代金の要求に従うタイミング • 封じ込め戦術の影響を考慮した意思決定 • 規制当局や主な関係者に対する、侵害の開示規定 • 顧客への通知のベスト・プラクティス • メディア対応のベスト・プラクティス
納品方法	オンサイトでのシナリオ・ロール・プレイ	オンサイトでのシナリオ・ロール・プレイ

詳しくは**www.Mandiant.jp/consulting**をご覧ください。

マンディアント株式会社
〒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@mandiant.com

Mandiantについて

2004年の設立以来、Mandiantは世界中の企業・組織を進化するサイバー脅威から保護しています。数十年におよぶ最前線からの知見と経験、インテリジェンスをSaaSソリューションとして実際の運用に適用しやすい形で提供することで、お客様のサイバー防御態勢の強化と革新を支援します。