データシート

MANDIANT
A FireEye® Company

インシデント対応プロセス評価サービス

高度なサイバー攻撃に対するお客様組織の検知、対応、封じ込め能力を診断

サービスの内容と特長

- **第三者の目で診断：**
  お客様組織のセキュリティ監視およびインシデント対応体制を客観的に診断します。
- **ベスト・プラクティスと比較：**
  SOCの編成、セキュリティ監視体制の強化、脅威インテリジェンスの統合の方法など、インシデントレスポンスのベスト・プラクティスに照らして現状を評価します。
- **サイバー攻撃机上演習：**
  Mandiantのコンサルタントが過去に対応した実際のインシデントをベースにした、リアルタイムのサイバー演習を実施します。
- **優先すべき改善策を提案：**
  インシデント対応に最も費用対効果のある対策案として、ロードマップを作成します。

Mandiantの特長

FireEyeのコンサルティング部門であるMandiantは、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14年以上にわたり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。

概要

Mandiantのインシデント対応プロセス評価サービスでは、セキュリティ・オペレーション・センター（SOC）やインシデントレスポンス・チームの能力を含む、お客様組織のインシデント対応体制を業界のベスト・プラクティスに照らして評価し、改善の余地がある領域を特定します。

チームでのディスカッション、内部文書のレビュー、机上演習を組み合わせて、お客様組織の現在のセキュリティ・イベント監視体制、脅威インテリジェンスの活用状況、インシデント対応能力を総合的に調査し、今後に向けた詳細なロードマップと低コストで具体的な改善策を提案します。

インシデント対応体制のゼロからの構築、既存のプロセスの改善、支援テクノロジーの導入など、Mandiantの提案する実績ある方法により、高度で執拗な現実のサイバー攻撃への対策を強化することが可能です。

Mandiantのアプローチ

最初に、Mandiantのコンサルタントは、Mandiantの6つの主要能力モデルに基づいてお客様の現状を評価します。このモデルでは、インシデント対応能力を次の6つに分類しています。

ガバナンス
効果的なインシデントレスポンスの基盤となり、組織の主要目標の達成を後押しします。

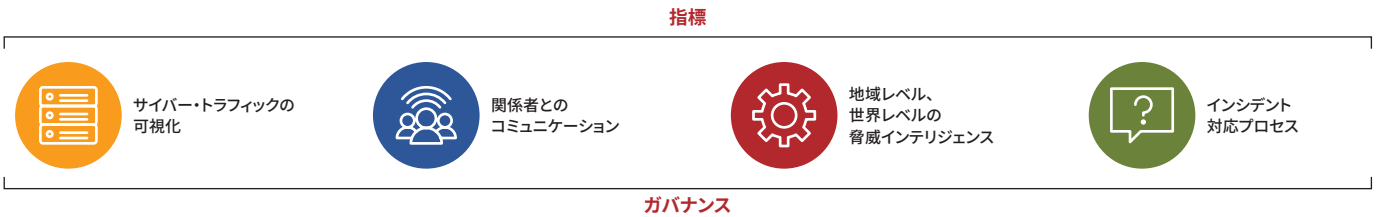
可視性
組織のビジネス・アーキテクチャ全体にわたり、漏れなく脅威を検知するための人材、プロセス、テクノロジーを指します。

コミュニケーション
インシデントレスポンスに関する情報を組織内外の主な関係者に伝達するためのプロセスを表します。

脅威インテリジェンス
攻撃者が用いるツール、戦術、手順（TTP）を把握、検知するための情報です。

対応
インシデントの検証と分類、重大度の判定、適切な対応策の決断を実施する方法を表します。

指標
インシデント対応能力の維持と改善に必要な測定基準と能力開発戦略を示します。



FireEye

次に、Mandiantの専門家が経験した日常的なシナリオに沿って、お客様のインシデント対応プログラムをテストします。最後に、より強固なサイバー・セキュリティ・プログラムを策定、改善、維持するための、お客様の組織にあったロードマップと詳細な改善策を提案します。

診断内容

Mandiantの専門家は、実績あるアプローチに基づいて、お客様組織のセキュリティ・プログラムを構成する次の領域を検証します。

コンプライアンス

インシデント対応計画は、該当する規制および法律の要件に対応しているか。

組織

人員の配置は的確か。各スタッフは、問題発生時の役割と責任を明確に理解しているか。

トレーニング

各スタッフは、効果的、効率的にインシデント対応を実施するためのトレーニングを受けているか。

検知

発生したインシデントを迅速に検知するための仕組みが整っているか。

プロセス

データ侵害の疑いがあるときに、素早く対応するためのプロセスが明確に規定されているか。

テクノロジー

インシデント対応を支援するためのハードウェアとソフトウェアが導入されているか。

Mandiantのプロセス

ステップ1

セキュリティ脅威の検知、対応、隔離能力を診断

Mandiantのコンサルタントが、お客様組織のSOCおよびインシデント対応に関する文書をレビューし、現在のプロセスを業界のベスト・プラクティスと比較して、お客様組織の基本的なパフォーマンスを把握します。また、お客様組織の担当者への詳細な聞き取り調査を実施して、お客様組織特有のプロセスを詳細に把握します。

ステップ2

サイバー攻撃机上演習でインシデント対応プロセスをテスト

システムに対する侵害、個人を特定可能な情報（PII）への不正アクセス、ポリシー違反、不適切なEメールなどのインシデント・シナリオに基づいて、インシデントの検知から解決に至るお客様組織のインシデント対応プロセス全体を評価します。

ステップ3

改善策と独自のロードマップを提案

文書のレビューや担当者への聞き取り調査、サイバー攻撃机上演習の結果に基づいて、最終的な報告書を作成し、プレゼンテーションを実施します。また、法律や規制要件、業界のベスト・プラクティスに照らしてお客様組織を評価します。これにより、お客様組織のSOCやインシデント対応体制の強み、改善の余地がある領域を示します。

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 | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com

FireEyeについて

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・レスポンスといった、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