データシート

MANDIANT®
A FireEye® Company

侵害調査サービス

ネットワークにおける
進行中・過去の攻撃活動を特定

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戦術、手法、手順を深く理解しています。

メリット

- 進行中または過去のセキュリティ侵害の証拠の発見に特化し、環境を包括的に分析
- システム的なリスクと漏えいに関する情報を提供
- セキュリティ対策の問題を特定
- 組織の能力を向上させ、今後のインシデントに効果的に対応するための推奨事項を提案
- オンプレミスまたはクラウドホスト・テクノロジーの導入に柔軟に対応

サイバー・セキュリティの現状を見る限り、セキュリティ侵害の発生を完全に防ぐことは不可能です。

ケビン・マンディア（Kevin Mandia）
FireEye CEO

Mandiant侵害診断サービスは、高度な攻撃者による侵入に対応してきた豊富な経験、業界をリードする脅威インテリジェンス、およびFireEyeテクノロジーを組み合わせ、以下を診断します。

- 組織内における進行中または過去の侵入を特定
- セキュリティ・アーキテクチャの弱点、脆弱性、不適切な使用またはポリシー違反、およびシステム・セキュリティの設定ミスを特定し、リスクを評価
- 組織の能力を強化し、今後のインシデントに効果的に対応

侵害診断の必要性

ニュースで報じられる大規模なデータ侵害は、世界的に行われている侵入行為のごく一部に過ぎません。組織が侵害を受けているかどうかを認識し、リスクを軽減する方法を特定することは、メディアの見出しを飾るようなデータ侵害から組織を守るために重要です。

Mandiantのアプローチ

侵入に対する豊富な経験と業界をリードする脅威情報をFireEyeテクノロジーのモジュール・スタックと組み合わせ、ビジネス目標に応じた評価の全体像を迅速かつ効率的に提供します。この評価では、過去または進行中の攻撃活動の証拠を特定するほか、以下の情報を提供します。

脅威インテリジェンスに基づくコンテキスト情報
攻撃者とその動機を特定し、組織が標的にされているかどうかを認識できるようにします。

リスクの特定
パッチやセキュリティ・ソフトウェアの欠落など、セキュリティ・アーキテクチャと構成に関する脆弱性を特定します。

将来的な調査の提供
組織のセキュリティ・チームが侵入に十分に対応できる戦略的オプションを推奨します。

FireEye

Mandiantのコンサルタントは FireEyeテクノロジーを使用して、エンドポイントの検索、ネットワーク・トラフィックの監視、Eメールの検査を行います。また、他のセキュリティ・ソリューションからのログを解析して攻撃活動の証拠を特定します。さらに、シグネチャ・マッチングに依存しないデータ解析手法を使用して、未知の攻撃を発見します。顧客はそれぞれの環境に適したテクノロジーの組み合わせを選択します。

- エンドポイント検査：FireEyeエンドポイント・セキュリティ・エージェントは、マルウェアをはじめとする攻撃、手法、および手順をリアルタイムで検知し、Windows、macOS、およびLinuxのエンドポイントを調査します。Mandiantは、オンプレミスとクラウドの両環境に柔軟に対応します。
- ネットワーク検査：FireEyeネットワーク・セキュリティ・センサーを企業内の戦略的な監視位置に設置し、マルウェアのC&C通信、不正なリモート・アクセス、およびデータの窃取などのセキュリティ侵害を検知します。
- Eメール検査：オンプレミスまたはクラウドのFireEye Eメール監視は、インバウンドおよびアウトバウンドのEメールをパッシブに検査するように構成できます。添付ファイルを動的に検査することで、Mandiantの専門家は他のシグネチャベースの製品より早く、侵入攻撃を特定できます。
- ログ検査：Mandiantコンサルタントは複数のテクノロジーを活用し、アプリケーションおよびインフラストラクチャのログを確認し、不正な活動を特定します。

エンドポイント検査

- 疑わしいまたは不正な活動に対するリアルタイム・アラート機能
- FireEyeエージェントに組み込まれたアンチウイルスエンジンを使用し、一般的なマルウェアを検知
- 複数のプラットフォームにまたがるオペレーティング・システムをサポート
  - Windows
  - macOS
  - Linux
- 高度なマルウェアの存在を示唆する異常値を識別

ネットワーク検査

- カスタム検知シグネチャとフル・パケット・キャプチャの組み合わせ
- 攻撃者のC&Cトラフィックの自動検知とデコード

Eメール検査

- 攻撃者が使用した標的型のフィッシング攻撃を検知し、復旧プロセス後に環境へのアクセスを回復
- シグネチャ・マッチングに依存しないMulti-Vector Virtual Execution™(MVX)エンジンを使用し、多様なオペレーティング・システム、アプリケーション、Webブラウザの組み合わせに対して、Eメールに含まれる添付ファイルやURLがどのように動作するかを解析
- Microsoft WindowsおよびmacOSオペレーティング・システム・イメージでの解析をサポート
- パスワードで保護/暗号化された添付ファイルに埋め込まれた脅威を解析

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