ソリューション・ブリーフ

FireEye Managed Defense for Endpoint Security

影響の強いサイバー攻撃に対する専門家主導の保護

ハイライト

- **迅速な脅威封じ込め：**
  検知およびインシデント対応を統合し、インシデント対応を迅速に行うため、エンドポイントを迅速に検出、調査、および封じ込め
- **最先端の脅威インテリジェンス：**
  最先端の検知技術を活用し、優れた脅威研究者によるサポート
- **「アラート」ではなく「具体的な対策」を提示：**
  アナリストは、重大な脅威を徹底的に調査し、詳細な調査報告を提供することで、効果的かつ迅速な対応を実現
- **Managed Defenseコンサルタント：**
  お客様の主要な連絡窓口の役割を務めるセキュリティ専門家として、マルウェア・サンプルの解析や詳細なフォレンジック分析、オンサイトのインシデント対応などの追加サポートを提供

2018年にサイバー攻撃の被害を受けたと報告された企業は、全体の78%に上りました。組織は、サイバー攻撃への効果的な対策を予防的に行う必要がありますが、ほとんどの組織は、最も価値のある資産を保護するために、事後対応的な技術ベースのセキュリティ・ソリューションに未だに依存しています。

サイバー攻撃に対処するためには、最前線の経験から培われた最新の脅威インテリジェンスを活用した、アナリストによる予防的なアプローチでネットワークとエンドポイントを常時監視する信頼性の高いパートナーが必要となります。ここで必要となるのがFireEye Managed Defense for Endpoint Securityです。

エキスパート主導の検知と対応

FireEye Managed Defense for Endpoint Securityを使用すると、企業は、業界をリードするエンドポイント・セキュリティと管理された検知および対応を使用して、エンタープライズセキュリティプログラムの有効性を向上できます。

FireEye Managed Defense for Endpoint Securityは、FireEyeの技術の結集に、FireEye Mandiantの最前線の専門知識、業界トップの脅威インテリジェンスとFireEyeエンドポイント・セキュリティを組み合わせた、マネージド検知・対応（MDR）サービスです。これらの機能により、セキュリティ・チームを強化し、高度なスキルを備えた攻撃者さえも捉える検知および調査活動を促進します。

Managed Defenseアナリストは、セキュリティ・オペレーションセンターと連携して、カスタマイズされたインシデント対応の推奨事項と併せて、攻撃者活動の詳細な検討を行い、最終的な行動をとるために必要なコンテキストを提供します。

大まかな流れ

FireEye Managed Defense for Endpoint Securityは、独自のテクノロジー・スタックを利用して、ICSやクラウド・インフラストラクチャを含む企業全体をリアルタイムで可視化します。

セキュリティ侵害の証拠や痕跡が発見された場合は、その事実をすぐさまお客様に通知。お客様は安全なポータルを介して最新の知見を確認でき、その一方でアナリストがインシデントの調査を進めます。

お客様はまた、脅威のコンテキスト情報と復旧のための推奨事項がまとめられた概要レポートも入手できるため、インシデントに効果的に対応し、攻撃者の目的達成を阻止することが可能です。

選び抜かれた機能

- 製品による検知：
  リアルタイム検知エンジン、Exploit Guard
- アナリスト主導の検知：
  webshell検知（Webベースのバックドア、アップロード・ツール、およびサーバー上のコマンドシェルを識別）
- エンドポイントのハンティングと調査データ収集：
  メモリからのプロセス・リスト、レジストリ・ハイブ・リスト、サービス・リスト、ポート・リスト、スケジュールされたタスク、イベント・ログ、Windowsサービス、プリフェッチ入力
- Managed Defenseポータルを介して封じ込めをワンクリックで実施

Managed Defenseを選ぶ理由

経験
年間10万時間以上を重大なセキュリティ侵害への対処に費やしているMandiantインシデント対応チームの経験を活用

迅速な検知
Managed Defenseが調査と対応に要する時間の中央値は67分

優れたコスト・パフォーマンス
組織内でセキュリティ能力を開発し維持するには、多くの時間、費用、リソースが必要

インテリジェンス
インテリジェンス150人以上の専門アナリストが収集に協力している国家レベルのインテリジェンスを活用

強力な防御機能
FireEyeのテクノロジーとインテリジェンスを統合した独自のテクノロジー・スタック

- FireEye製品による検知件数は1億5,000万件
- Managed Defenseに取り込まれたアラートの件数は2,200万件
- アナリストによる調査件数は17万件
- 優先度の高い脅威の91%をラピッド・レスポンスなしで解決
- ラピッド・レスポンスの98%のインシデントをフル・インシデントレスポンスなしで解決

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

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™