データシート

FireEye Managed Defense

セキュリティの最前線で得られたインテリジェンスと専門知識を活用して水面下に潜む脅威を見つけ出し、迅速に対応

ハイライト

- **既存の投資を強化：** セキュリティ・オペレーション・センター（SOC）と統合可能なマネージド検知・対応機能
- **専門家のチーム全体による対応：** 数千名に及ぶ脅威アナリスト、マルウェア専門家、インシデント対応担当者、インテリジェンス・キュレーター、フォレンジック専門家が対応
- **体系的な探索：** アナリストはFireEyeの製品と専門知識を使用して、セキュリティ脅威に対する独自の探索手法を予防的に導入
- **リアルタイムで可視化：** カスタマイズ可能なポータルはコミュニケーション、レポート、コラボレーションのためのパイプ役であるだけでなく、コミュニティ・プロテクションのダッシュボード経由で現在のセキュリティ状況に関する知見を提供し、新たな脅威が確認された場合に対応
- **市場をリードする脅威インテリジェンス：** セキュリティ・アナリストが、マシン、被害者、攻撃者に関する最新のインテリジェンスに基づいてお客様の組織内に潜む脅威を速やかに発見し、詳細を解明
- **脅威解析担当マネージャ：** 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
- **24時間365日対応：** 米国（バージニア/カリフォルニア）、アイルランド、ドイツ、シンガポール、オーストラリア（シドニー）、日本を拠点とするSOCが24時間365日対応

セキュリティ脅威が深刻化の一途をたどっているにもかかわらず、多くの組織は重要資産を保護するためにいまだに事後対応的なテクノロジーベースのセキュリティソリューションに依存しています。確固たる動機を持つ攻撃者にテクノロジーだけで立ち向かうなど、もはや不可能な状況です。しかし、人材不足に加えて人件費の高騰により、多くの組織にとってセキュリティの専門家、特に水面下に潜む脅威の検出を専門とする専門家の獲得、採用、育成、長期の雇用は困難になっています。

一方、高度なサイバー攻撃に対処するためには、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です。

インテリジェンスに基づく検知と対応

FireEye Managed Defenseは、業界で高い評価を受けているサイバー・セキュリティの専門知識、FireEyeテクノロジー、攻撃者に関する比類のない知識を組み合わせ、セキュリティ侵害の影響を最小限に抑えるマネージド検知・対応（MDR）サービスです。

Managed Defenseを継続的に支えているのは、業界最大のグローバルなセキュリティ脅威インテリジェンス機能です。世界中で猛威を振るうサイバー攻撃の最前線で得られたマシン、キャンペーン、攻撃者、被害者に関する情報を活用します。この最前線からのインテリジェンスと専門知識により、検知の効果を高めながら、アナリストの探索・調査活動をガイドし、きわめて高度な攻撃も見つけ出します。サイバー攻撃に精通したFireEyeのセキュリティ・アナリストが、攻撃者の活動の包括的な評価とお客様の状況に合わせてカスタマイズされたインシデント対応の推奨事項、さらには脅威に対する理解、リスクの評価、効果的な対策の実施に必要なコンテキスト情報を提供します。

仕組み

FireEye Managed Defense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。

高度な専門知識を有するFireEyeの脅威アナリストは、攻撃者、被害者、マシンに関する脅威インテリジェンスを活用して、既知・未知の脅威の検知、調査、予防的な探索を行います。

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。

攻撃者を知る
高度化の一途をたどるセキュリティ脅威や標的型攻撃の動向に備え、対応するためには、攻撃者の動機、目的、特徴、手口を理解することが必要です。この理解は、最前線での経験から得た知識に基づいています。

Managed Defenseは、独自の調査手法を駆使して、侵入の痕跡を発見し、攻撃者の手口や能力レベルを把握、解析します。

経験豊富なアナリストは、中国のAPT攻撃（Advanced Persistent Threat：高度で持続的な標的型攻撃）グループやロシアの攻撃グループなど、国家レベルのグループを30以上含む1万6,000近くの攻撃者について業界有数の情報も活用しています。

アナリストは、攻撃者の行動についての知識をもとに、状況を速やかに把握して攻撃者の能力レベルを評価し、次の活動を予測して、効果的な対応計画を策定します。

図1： インテリジェンスに基づく検知

予防的な探索　　攻撃キャンペーンへの対応　　優先度の高いアラートの特定と検証

予防的な探索
FireEye Managed Defenseは予防的なアナリスト主導型のアプローチを採用しており、経験豊富なアナリストは不正な活動の痕跡を探索するときに攻撃者とその戦術、技術、手順（TTP）に関する知識と理解を組み合わせて対応します。Managed Defenseのアナリストは、絶え間なく進化を遂げ、手法を変えることで、検出を回避しながら標的のネットワークに足がかりを築こうとする攻撃者による新しいTTPの証拠を体系的に探索します。

アナリストによって作成および使用される独自の探索手法は、Managed Defenseを導入した他のお客様、FireEye傘下のMandiantでのコンサルティング事例、およびFireEye iSIGHTインテリジェンス機能から得られたインテリジェンスに基づいて随時更新および変更されています。

攻撃キャンペーンへの対応
Managed Defenseを導入したお客様は、FireEyeがサイバー攻撃の最前線で6,300件を超えるお客様のセキュリティを守ることで取得した知識と経験からメリットが得られます。

お客様の業種や地域、利用テクノロジーに類似する組織への攻撃が確認された場合、または攻撃者の手口に変化が見られた場合は、直ちにお客様のネットワークで予防的な調査を開始し、攻撃活動を示唆する証拠の有無を確認します。この時点で侵害が確認されなくても、一定の根拠のもとに、標的として狙われている可能性があると考えられる場合には、その攻撃を無力化するための対応策を提案します。

優先度の高いアラートの特定と検証
FireEye Managed Defenseのアナリストは、他の製品から大量に発生するが無関係の場合が多いアラートによるノイズを排除して、最も影響の大きい脅威に焦点を合わせ、重要なアラートに集中することによってチームの時間と労力を節約します。FireEyeのアナリストとインシデント対応担当者の知識を結集すれば、従来型のセキュリティ対策では対処できなかった脅威も含め、最も影響が大きそうな脅威を特定するなどのメリットが得られます。

Managed Defenseを選ぶ理由

経験
年間10万時間を超える重大なセキュリティ侵害のIR経験を活用

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

地域別のサポート
世界に7か所のSOCを配置。地域別の技術担当エンゲージメント・マネージャが毎日24時間体制で対応

適応型検知
攻撃側のTTP（戦術、技術、手順）を詳細に分析して攻撃者の手口と行動の検知に注力

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駆使した独自のテクノロジー・スタック

- 1日あたり500億回以上の仮想マシンによる解析結果
- 1日あたり40万種類のマルウェアを処理
- 1,600万台の情報収集センサーを世界中に配置
- 豊富なコンテキスト情報でセンサー・データをサポート
- FireEyeのエコシステムを60分ごとに更新

図2： 経験に基づく対応

インシデントの影響範囲の特定

迅速な対応

効果的な復旧策を提案

インシデントの影響範囲の特定
調査中、Managed Defenseのアナリストは、FireEyeのインテリジェンスを総動員して全アラートを検証し、ネットワーク・トラフィックやエンドポイントを検査してセキュリティ侵害の範囲を特定します。さらに、該当するすべてのイベントを総合的に分析して、「キル・チェーン」と呼ばれる攻撃活動のステップ全体の流れを把握します。アナリストは、年間10万時間以上に及ぶインシデント対応の経験で培われたFireEye独自の手法とインテリジェンスを使用して、インシデントの影響範囲を正確に把握します。

迅速な対応
より深刻な攻撃に対しては、Managed Defenseのアナリストは、マルウェアやインテリジェンス、インシデント対応を担当する各チームの専門家を増員し、トリアージされたイベントの詳細解析を実施し、環境全体を調査して、侵害の全体像を把握する場合があります。

効果的な復旧策を提案
調査を行って診断結果を出したら、Managed Defenseのアナリストはお客様のチームによる対応を支援するために、効果的な復旧策を提案します。

可能性としてはほとんどありませんが、大規模なインシデント対応が必要な場合は、フォレンジック分析の専門知識を持つFireEyeのインシデント対応担当者により、インシデントの迅速な解決と、正確で速やかな情報開示に向けた影響評価の支援を実施することもできます。

アドバイスと知見
Managed Defenseを利用するお客様は、安全なポータルにアクセスすることができます。このポータルを通じて、お客様はコミュニケーション、コラボレーション、レポートおよびインテリジェンスへのアクセスが可能です。お客様には日々の連絡先として脅威評価マネージャ（TAM）も割り当てられます。TAMは、インシデント対応とフォレンジックの専門知識を持ち合わせた熟練専門家で、セキュリティ対策の強化に役立つ戦略的な推奨事項を提供します。

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

DS.FMD.JA-JP-032018

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