データシート

Advanced Intelligence Access

カスタマイズされた解析と、業界トップレベルの脅威データとインテリジェンスへのアクセス

ハイライト

- FireEyeのテレメトリーと脅威データにアクセスすることで、より的確な判断を行い、競争力を強化
- 生データ、ドラフト解析、痕跡、ブログが含まれており、未知の脅威に対する早期の対応を実現
- インテリジェンスのサイクルの全段階をカスタマイズすることにより、焦点を絞った対策と具体的な成果を実現
- オンサイトのインテリジェンス・インテグレーターが、組織のニーズや要件の変更に合わせて解析や成果物を柔軟に調整

昨今のサイバー攻撃者はますます巧妙になり、その攻撃は予測困難で、しかも執拗です。防御側の組織がこのような攻撃を検知して対処し、より効果的なビジネス判断やセキュリティに関する意思決定を行うためには、敵を知ることが欠かせません。つまり、攻撃者の思考、手口、目的を理解することが重要なのです。最先端のサイバー・セキュリティ組織には、生の脅威データにアクセスする能力と、そのデータを目的の遂行に関連のある具体的で実用的なインテリジェンスへと変換する能力とを備える必要があります。

FireEye Advanced Intelligence Accessサービスでは、FireEyeの生の脅威データ、解析ツール、最終的なインテリジェンスに即座にアクセスできるので、組織は具体的な脅威プロファイルとセキュリティ上の目標に合わせてカスタマイズした、脅威インテリジェンスを生成できるようになります。このアクセスは、組織のセキュリティ部門の延長として位置づけられた、専任のFireEyeインテリジェンス・インテグレーターを介して提供されます。脅威に関するコンテキスト情報、攻撃者が用いる戦術、技術、手順（TTP）についての可視性を向上し、また実用的な知見を提供することによって、競争力の優位性を獲得します。

Advanced Intelligence Accessは、FireEyeのデータ、知識、専門知識を最大限に活用する手段を提供します。

FireEyeの生の脅威データとセキュリティ・データ

Advanced Intelligence Accessは、世界中、またはクラウドに導入されているFireEyeのセキュリティ・ソリューションからのテレメトリーを組み込んでいます。これには、数百万のEメール、エンドポイント、ネットワーク・セキュリティ・システムから得たインテリジェンスと、1時間に数千万件発生する不正アラートから得たインテリジェンスが含まれます。Advanced Intelligence Accessの契約者は、FireEye Mandiantの計り知れないほど多くの時間に及ぶインシデント対応、Managed Defenseの取り組み、FireEyeのダークWebインテリジェンスのリサーチ・チームから得たデータと知見を活用することができます。この知識によって、攻撃者の意図や攻撃キャンペーンを特定する能力を高め、予防的に脅威をブロックすることができるようになります。

業界トップレベルのインテリジェンス・ツール

FireEyeのセキュリティ・ツールは、セキュリティ分野での数十年にわたる経験とテクノロジーに関する専門知識の成果であり、そのメリットはAdvanced Intelligence Accessを通じて享受できます。FireEyeのインテリジェンス・アナリストとエンジニアは、これらのマルウェア解析ツールとインフラを積極的に利用し、FireEyeのインテリジェンス・データと製品テレメトリーを活用しています。FireEye Digital Threat Monitoringのテクノロジーや独自のインテリジェンス解析ツールには、インテリジェンス・インテグレーターを介してアクセスすることもできます。

専任のFireEyeインテリジェンス・インテグレーター

インテリジェンス・インテグレーターは、組織の意思決定者や最前線で対応するセキュリティ担当者向けに、カスタマイズされたインテリジェンスと解析を提供します。このサービスにおけるインテリジェンス・インテグレーターは、FireEye独自の手法、アプローチ、ツールを利用して、各組織に関連のある調査や攻撃者のTTPに関する最新情報を把握できるように支援します。また、インテグレーターは、業界、会社、従業員、システム、データを標的とする攻撃活動についての知見を提供します。意思決定者は、特定のトピックに関する知見を得るために、インテリジェンスの収集と生成に関する優先順位を設定することができます。成果物には、高度なサイバー攻撃グループに関する一連の調査情報、傾向、ニュース、解析情報が含まれます。専門知識を有するインテグレーターが具体的な対策を盛り込むことで、組織がサイバー攻撃を阻止する可能性を高めます。

効果的な早期対策の可能性

Advanced Intelligence Accessは、サイバー攻撃のコンテキスト情報を取得し、ソース・データの相関分析を行い、組織に合わせてカスタマイズした戦術インテリジェンス、運用インテリジェンス、戦略インテリジェンスを提供します。主なメリットは以下のとおりです。

- **スピード:** FireEyeのテレメトリーと脅威データに直接アクセスできるので、セキュリティ・チームはより的確な判断を迅速に行うことができます。
- **機敏性:** オンサイトのインテリジェンス・インテグレーターが、組織のニーズや要件の変更に合わせて解析や成果物を柔軟に調整します。これにより、組織は短期的にも長期的にも、脅威の進化の動向を常に把握しておくことができます。
- **予防的:** 生データ、ドラフト解析、痕跡、ブログが含まれているので、未知の脅威に対しても迅速に対応できます。
- **集中的:** 要件、収集、解析、生成というインテリジェンスのサイクルの全段階をカスタマイズすることで、焦点を絞った対策を講じ、関連性の高い結果を得ることができます。

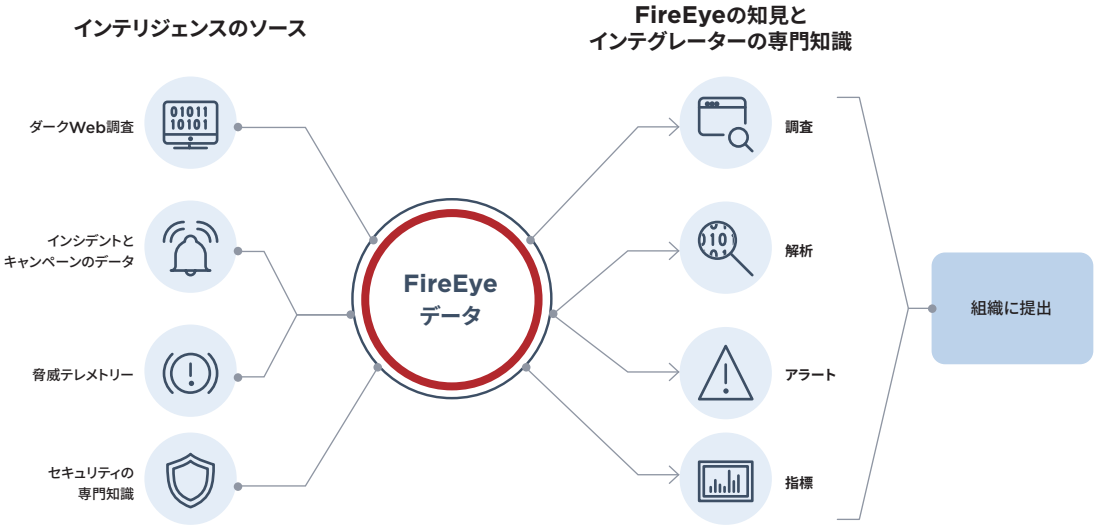

図1: Advanced Intelligence Accessで、FireEyeのデータ、知識、専門知識を最大限に活用

FireEye Advanced Intelligence Accessを活用して、脅威データを焦点を絞った実行可能なインテリジェンスに変えることができます。詳細は、**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、インシデントレスポンスといった、組織がサイバー攻撃対策をする上での課題となっていた複雑性や負担を解消します。

I-EXT-DS-JA-JP-000215-01