データシート

FireEye

FireEye脅威インテリジェンス・ポートフォリオ

詳細なコンテキスト情報を提供する、包括的な脅威インテリジェンス・サービス

ハイライト

- コンテキストに基づくインテリジェンスが、調査・対応計画の「答え」を提供
- 攻撃前後の脅威インテリジェンスにより、攻撃のライフサイクルを把握
- お客様のセキュリティ課題に沿った、具体的な脅威インテリジェンスを提供

セキュリティ脅威トレンドに立ち向かうために

組織は、圧倒的に不利な立場で攻撃者と戦わなければなりません。攻撃者たちは、技術、資金、組織において恵まれた立場にあり、高度な標的型攻撃技術を持つようになってきています。一方で、組織のセキュリティ担当チームは、どの脅威がもっとも危険なのかの判断方法や、発見した脅威の優先順位付けに、今日も四苦八苦させられています。

多くの組織は、まだまだ昔ながらのシグネチャベースのセキュリティが提供する「インテリジェンス」に依存しています。しかし、これらの情報では、攻撃を防御したり、対応のためのコンテクスト情報を得ることができません。そればかりか、誤検知によるアラート数の増加を招き、正確な攻撃を見分けることが困難になり、セキュリティに対する間違った意識を持つ要因になりかねません。正しい脅威インテリジェンスは、検知、レスポンス、そしてビジネス効率性において組織に貢献するものです。

豊富なコンテキスト情報で脅威を緩和

FireEye iSIGHT®脅威インテリジェンスは、世界各地の150名以上に及ぶFireEyeのセキュリティ研究者と専門家が、数十年に及ぶ経験を活かし、攻撃者の素性やその動機、意図、手口に関する情報を提供する、業界の中でも一線を画す特長を持ちます。iSight の活用例：

- 組織のリスクをプロアクティブに評価、管理
- 攻撃の検知と防御
- 発生している攻撃のコンテキストを解析
- 攻撃が発生する前に、攻撃者の開発環境情報を収集
- 日々発生するサイバー攻撃の多くを、いち早く検知、対応
- MVXテクノロジーは、未知の攻撃も検知します。今何をすべきか、を含むインテリジェンス情報により、よりよいリスク管理と攻撃に対する対処を実現します

要件に合わせた、各種脅威インテリジェンス

独立型のiSIGHT脅威インテリジェンスと、FireEye の製品技術と統合されたDynamic Threat Intelligence (DTI) 、Advanced Threat Intelligence (ATI) のインテリジェンスにより、FireEyeはお客様を支援しています。

独立型の脅威インテリジェンス

FireEye iSIGHT脅威インテリジェンスは、FireEyeセキュリティ・ソリューションはもちろん、すでにお持ちのセキュリティ・インフラストラクチャやツールとも合わせて利用可能な、戦術、運用、戦略の各レベルの脅威情報を包括的に提供するサービスです。基本的なデータ情報だけでなく、プロアクティブな防御やアラートの優先順位付け、リソース割当およびインシデント対応の改善のために必要な、将来を見据えた高いレベルのコンテキスト情報を提供します。

このサービスでは、直接マシンに取り込み可能な各種インテリジェンスの入手のほか、アナリストや専任のクライアント・サポート担当者に直接問い合わせることもできます。インテリジェンスは、次のフォーマットで提供されます。

- iSIGHT API経由の、マシンに直接フィードされるフォーマット
- MySIGHTポータル経由の、人が読むことができるフォーマット
- iSIGHT 脅威メディア・ハイライト (毎日配信する世界の主要なセキュリティ関連ニュースの解説記事)

役割や立場に応じてインテリジェンスを調整できるため、どのようなセキュリティ・チームの強化にも役立てることができます。FireEye iSIGHT脅威インテリジェンスのサブスクリプション・サービスには、戦術 (Tactical) 、運用 (Operational) 、融合 (Fusion) 、役員 (Executive) 、脆弱性 (Vulnerability) のメニューがあります。

FireEyeの製品技術に統合されたインテリジェンス

FireEye 製品向け脅威インテリジェンスサブスクリプションは、検知・調査・対応能力を強化するもので、FireEyeの検知・調査ソリューションを購入する際、追加のサブスクリプションとして提供され、DTIとATIの2種類があります。

Dynamic Threat Intelligence (DTI)

FireEye Multi-Vector Virtual Execution (MVX) エンジンによる機械学習や解析により、攻撃者の意図や、戦術/技術/手順 (TTP) を体系化し、攻撃を検知します。世界中で導入されているFireEye環境で確認された最新の攻撃が、お客様のネットワークでも検知されるように、情報は1時間ごとに更新されます。

Advanced Threat Intelligence (ATI)

攻撃が検知されると、ATIは、リソースの優先順位付けや適切な対応に役立つコンテキスト情報を提供します。具体的には、関与している攻撃者の素性や推測される目的、業種別・地域別のマルウェアの情報、お客様環境が攻撃の標的になっているかどうかの調査に役立つ指標などです。

FireEye脅威インテリジェンスの特長

FireEye iSIGHT脅威インテリジェンスは、攻撃者の素性やその動機、意図、手法に関する幅広い知見を提供します。

- 長期化する攻撃のライフサイクルや動機、ツール、手順に対する広い視野を提供。数百人のアナリストによる攻撃者の開発エコシステムの詳細解析、10年にわたって主要なサイバー攻撃の最前線で調査・実態解明に取り組んできた実績、攻撃者の意図の体系的な把握に基づき1,600万台以上の仮想脅威検知センサーで構成されるグローバル・ネットワークを通じて、最新の高度な脅威をいち早く可視化し、情報を提供
- 進化し続ける攻撃を追跡する、柔軟かつ拡張性に優れた解析エンジン。サイバー攻撃の実行者が使用するツールや戦術、手口、その支援者の関係性を動的にモデル化する、1億2,500万個以上のノードからなるグラフ・データベース
- 世界中の1万6,000種以上のセキュリティ脅威に関する金銭的・政治的な特質を徹底的に追跡、解析する、各分野の専門家
- これらの脅威インテリジェンスを利用することで、攻撃される可能性のある範囲狭めつつ、多くのリソースが求められるアラート対応型セキュリティ体制から、実効的かつ効率的な、予防重視型セキュリティ体制へ変化させることができるのです。

表1：キル・チェーンの可視化

	DTI	ATI	iSIGHTインテリジェンス
攻撃の段階	攻撃中	攻撃中	攻撃前・中・後
インテリジェンスの種類	戦術	コンテキスト	広範かつ包括的なインテリジェンスと解析ツール
FireEyeアプライアンスによる検知	X		
FireEyeアプライアンス用検知プロファイル		X	
FireEyeアラートと地域・業種の相関分析		X	
FireEyeアラートと既知の攻撃者の関連付け		X	
攻撃グループのプロファイル情報			X
業種のプロファイル情報			X
マルウェア・ファミリーのプロファイル情報			X
メディア・ハイライト			X
脅威指標（API経由）			X
APIおよびSDKによるFireEye以外のツールとの統合			X
iSIGHTブラウザ・プラグインによるiSIGHTインテリジェンスのスキャン、照会、アクセス			X
iSIGHTの脅威指標と既知の攻撃者の関連付け			X
より広範な攻撃への対応			X
役員向けインテリジェンス			X
ビジネス・システムの脆弱性の追跡			X
重要インフラの脆弱性の追跡			X
エクスプロイトの追跡			X
既存のITインフラ全体のアラートのコンテキスト			X

FireEye製品の詳細については、次のWebページをご覧ください。
www.FireEye.jp

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4割以上を含む、世界67か国以上の6,800を超える組織で利用されています。

FireEye