データシート

FireEye Detection On Demand

ワークフローのあらゆる段階でコンテンツをスキャンして脅威を検知

ハイライト

- あらゆる場所で、既知および未知のマルウェアを検知して防御
- ブラウザとクラウド・ストレージにFireEyeがサポートするプラグインを導入
- 検知されたマルウェアのコンテキスト解析をJSONフォーマットで入手

はじめに

脅威はあらゆる場所からやって来るため、各企業はそのニーズ、業種、環境に応じて異なるセキュリティ・アプローチをとっています。しかし、どの企業にも共通しているのは、十分なコンテキストに基づく解析機能を備え、インテリジェンスベースで、検証済みの脅威検知機能を必要としているという点です。

FireEyeのお客様がAPIを介してFireEye Detection On Demandを活用すると、ファイルを安全に送信でき、Microsoft WindowsやApple OS X、またはアプリケーションの脆弱性を悪用する昨今の脅威から確実に保護されます。

FireEye Detection On Demandは、既存のFireEye Multi-Vector Virtual Execution™（MVX）検知エンジンやIntelligence Driven Analysis（IDA）を利用して、送信されたファイルの判定をすばやく行います。MVXは、従来型のシグネチャやポリシーに基づくセキュリティ対策をすり抜ける攻撃を検知する、シグネチャレスのダイナミックな解析エンジンです。IDAは、マシン、攻撃者、被害者に関する最新のインテリジェンスに基づき、攻撃をリアルタイムかつ遡及的に検知およびブロックする、コンテキストに基づくダイナミックなルール・エンジンです。

あらゆるセキュリティ・アーキテクチャで最高レベルの脅威検知能力

FireEye Detection On Demandは、クラウド上の脅威検知サービスです。送信されたコンテンツを迅速にスキャンし、そこに潜むマルウェアを見つけ出します。ファイル整合性アルゴリズム、社内の脅威ポリシーの管理、静的チェックのメカニズムに基づくファイル・セキュリティ・ソリューションとは異なり、送信されたコンテンツは、定評のある数多くのFireEyeの製品やサービスと同じテクノロジーを用いて処理されます。

FireEye Detection On Demandへのアクセスは、APIで簡単に設定できます。自社のセキュリティ・オペレーション・センター（SOC）のワークフロー、SIEM解析、データ・リポジトリ、カスタマーWebアプリケーションなどに組み込むことで、ファイルやコンテンツに対するフレキシブルな解析機能が得られ、企業が必要とする場所で不正な振る舞いを特定することができます。

Detection On Demandを通じて送信されたファイルやコンテンツのそれぞれについて判定を受け取るほか、ファイル、レジストリ、プロセス、ネットワークの変更といった付随するコンテキスト情報も提供されます。また、常時更新されているFireEye Dynamic Threat Intelligenceからも関連する調査結果が提供されます。

Detection On Demandのしくみ

FireEye Detection On Demandは、静的解析、AI、機械学習を活用して、送信物を最新の既知の戦術や攻撃者のシグネチャに照らし合わせて比較します。また、FireEyeは攻撃ライフサイクルのあらゆる段階で、副次的な影響や組み合わせによる影響が生じる可能性を判断し、未知のエクスプロイトやマルウェアを見つけ出します。

図1：Detection On Demandのしくみ

FireEye Developer Hub

FireEye Developer Hub（https://fireeye.dev）では、プラグインやサンプルコードを入手できるほか、FireEye Detection On Demandの開発コミュニティと協働することも可能です。

購入方法

Detection On Demandの購入は、FireEye販売代理店または営業担当へご連絡ください。AWS Marketplaceで直接購入することもできます（送信数が少ない場合）。

サービスを購入する際には、1年当たりのスキャンする送信物の見込み数に基づいて、必要量を指定します。AWS Marketplaceでの購入では、1か月当たりの送信クォータを提供します。請求は1年単位となります。ファイル送信の上限は毎分100件、ハッシュ送信の上限は毎分200件です。

Detection On Demandに送信されたファイルとその他の送信物は、送信1回よりも大きい送信値に割り当てられることがあります。標準送信値については、FireEyeからお知らせします。

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

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。