McAfee Threat Intelligence Exchange

セキュリティ ソリューション全体で脅威情報を共有

McAfee® Threat Intelligence Exchange はレピュテーション ブローカーとして機能し、適応型の脅威検出と応答を可能にします。組織全体のセキュリティ ソリューションから得るローカルの情報と外部のグローバル脅威データを組み合わせ、この収集情報をセキュリティ エコシステム全体で瞬時に共有し、ソリューションが情報交換をして共通の情報に基づいて動作するようにします。

脅威情報エコシステムを構築

レピュテーション ブローカーとして McAfee Threat Intelligence Exchange は、McAfee Global Threat Intelligence（McAfee GTI）やサードパーティの脅威情報（VirusTotal など）などのグローバル ソースからインポートした脅威情報とエンドポイント、ゲートウェイ、および高度な分析ソリューションなどのローカルの情報源から得た情報を統合します。Data Exchange Layer（DXL）を使用して、この収集情報を即座にセキュリティ エコシステム全体に共有し、セキュリティ ソリューションが 1 つのソリューションとして機能して組織全体の保護を高められるようにします。

DXL で簡単に統合できるので、多数のアプリケーション プログラミング インタフェース（API）統合の実装と運用にかかる費用を大幅に削減し、セキュリティを効率的かつ効果的に管理できます。DXL はオープン フレームワークとして設計されています。他社製を含むすべてのセキュリティ ソリューションを McAfee Threat Intelligence Exchange エコシステムに動的に接続できます。

脅威への適応と無効化

標的型攻撃に迅速に対応するには、脅威情報を共有し、ネットワークのどの部分でも脅威を検出できるようにする必要があります。これらの脅威は特定の組織を標的とするため、ローカルに監視システムを配備して脅威の傾向を把握し、攻撃を検知する必要があります。このようなローカルのコンテキスト データとグローバル脅威情報を組み合わせることで、これまで検出できなかった脅威を識別し、短時間での阻止が可能になります。

主な特長

- 高度な標的型脅威の検出から封じ込めまでにかかる時間を大幅に短縮し（数日～数か月から数ミリ秒）、脅威対策を最適化します。
- グローバルなデータソースから脅威情報を収集し、ローカルの脅威情報と組み合わせて総合的な脅威情報を提供します。
- エンドポイント、ゲートウェイ、ネットワーク、データセンターを保護するセキュリティ ソリューションで、関連するセキュリティ情報がリアルタイムで共有されます。
- エンドポイントのコンテキスト（ファイル、プロセス、環境属性）と総合的な脅威情報で未知のファイルに対して適切な判断を行うことができます。
- DXL によって統合を簡素化します。McAfee および他社製のセキュリティ ソリューションが統合され、脅威情報がリアルタイムで共有されるので、実装と運用のコストを削減できます。

ネットワーク内に不明なファイルが見つかった場合、McAfee Threat Intelligence Exchange に通知され、ファイルにレピュテーションが存在するかどうかが判断されます。組織の感染状況や経過時間など、説明的なメタデータも維持され、収集情報に反映されます。統合セキュリティ ソリューションはレピュテーションを要求するのに加えて、ローカルの判断に基づいて McAfee Threat Intelligence Exchange のレピュテーション情報の更新も行います。更新されたレピュテーション情報はリアルタイムですべてのシステムに反映されます。ローカルの脅威情報は今後の検出のために保存されます。同じ脅威が別のデバイスやサーバーで見つかった場合、すぐに識別されます。不明と判定されることはありません。

McAfee Threat Intelligence Exchange を利用すると、脅威情報を簡単に分析できます。セキュリティ管理者は、この統合された脅威情報を整理、オーバーライド、増強、および調整して環境や組織に合わせて保護対策をカスタマイズできます。ローカルで脅威情報を調整し、優先順位を設定できるので、今後発生する脅威にも迅速に対応できます。

施行ポイントが保護を強化

エンドポイントからネットワーク エッジまでネットワーク全体で統合されたソリューションは、利用可能なレピュテーション、メタデータ、またはデータとポイントの組み合わせに基づいてポリシーを適用します。緊密に統合された 1 つのソリューションである McAfee Endpoint Security は、ローカル情報（組織の感染状況や経過年数などのファイルのメタデータ、および他のセキュリティ コンポーネントから配信されたローカル レピュテーションなど）と現在入手可能なグローバル脅威情報を統合し、正確な判断を下します。たとえば、グローバル レピュテーションはないが組織に広く感染しているカスタム アプリケーションは、不正な複合レピュテーションを生成することはなく、実行を許可される可能性が高いでしょう。その一方で、組織でこれまで検出されたことがなく、グローバルまたはローカルのレピュテーションもなく、疑わしく圧縮されたファイルは信頼レベルが低く、ブロックされたり、追加の McAfee Endpoint Security エンジンによる詳細な調査、または McAfee Advanced Threat Defense か McAfee Cloud Threat Detection によるサンドボックス化が求められたりします。

さらに、McAfee Endpoint Security の機械学習機能である Real Protect、およびアプリケーションの動的隔離により、エンドポイントの検出と保護を強化します。Real Protect は事前および事後に実行する分析によって最新の脅威情報をクラウド参照し、アプリケーションの動的隔離はエンドポイント上の不正な活動を防いで、新しい脅威にさらされる最初のマシンを保護しながら追加分析を実行します。

高度な標的型攻撃は現実の問題

高度な標的型攻撃は、検出を回避して組織内に長期間潜伏し、重要なデータを盗み出します。最近発表された『Verizon 2015 Data Breach and Investigations Report』（2015 年データ侵害調査報告書）によると、マルウェア サンプルの 70% から 90% は特定の組織を狙ったもので、このような脅威の検出は大きな課題となっています [1]。

詳細については、**www.mcafee.com/jp/products/threat-intelligence-exchange.aspx** をご覧ください。

連携のメリット

高度な脅威分析

ファイルに関する詳細な情報が必要になると、ファイルが McAfee Threat Intelligence Exchange から McAfee Advanced Threat Defense や McAfee Cloud Threat Detection など、McAfee の高度な分析ソリューションに自動的に転送され、疑わしい新しい脅威の詳細な分析がすぐに実行されて、問題のファイルのレピュテーションが決定されます。この処理はすべて自動的に実行され、結果が記録されます。この情報は DXL 経由で共有され、セキュリティエコシステム全体の保護に利用されます。

セキュリティ イベントの管理

McAfee Enterprise Security Manager を使用すると、McAfee Threat Intelligence Exchange から取得した侵害の兆候（IoC）を詳しく分析できます。セキュリティの履歴情報を使用し、ウォッチリストを自動的に作成できるので、組織のセキュリティを効率的に管理できます。

1. http://www.verizonenterprise.com/DBIR/2015/

〒 150-0043
東京都渋谷区道玄坂 1-12-1
渋谷マークシティウエスト 20F
Tel. 03-5428-1100（代表）
www.mcafee.com/jp

McAfee および McAfee のロゴは米国法人 McAfee, LLC または米国またはその他の国の関係会社における登録商標または商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2017 McAfee, LLC. 3059_0517
2017 年 5 月