データシート

McAfee Global Threat Intelligence for Enterprise Security Manager

McAfee® Labs の力で状況認識

McAfee® Global Threat Intelligence for Enterprise Security Manager により、McAfee Labs の調査結果を利用して企業のセキュリティ監視を強化できます。1 億以上のグローバル脅威センサーから McAfee Labs が集めた IP レピュテーションは、初めてセキュリティ情報とイベント管理（SIEM）ソリューションに利用できるようになりました。この情報は常時更新されて McAfee Enterprise Security Manager に提供され、不審な IP や不正な IP との通信に関連するイベントを迅速に検出することで状況認識を強化します。これにより、セキュリティ管理者はどのホストが攻撃者と通信したか、または現在通信しているかを判断して、既知の攻撃者が脅威活動の元となっている条件をすぐに識別できます。

主な特長

- McAfee Labs の力で SIEM を強化します。
- イベントのリスクを正確に把握できます。
- パフォーマンスに影響を及ぼさずに McAfee GTI からの大量の脅威情報を利用できます。
- McAfee Enterprise Security Manager で新しいソース レピュテーションを自動的に受信し、処理します。
- 脅威検出の精度を高め、対応までの時間を短縮できます。
- 攻撃経路や既知の攻撃者との通信を迅速に識別します。たとえば、ボットネット、分散型サービス拒否（DDoS）、ネットワーク プローブを含む電子メール / スパムを配信するマルウェア、マルウェアの存在、DNS ホスティング、侵入攻撃が生成するアクティビティなどを識別します。

外部コンテキストの必要性

セキュリティ イベントは、ある瞬間に基づくセキュリティ関連アクティビティに関する情報を提供します。SIEM にはこれらのイベントを相互に関係づける機能がありますが、それでも多くの問題がオペレーター頼りになっています。この活動は許容できるか？ 最も緊急な問題をどう見分けるか？ ノイズをあまり作らない高度な攻撃をどうやって検出するか？ これらの問題の数に企業の日々のイベント数をかけると、2 億 5 千万以上に上ります。このことから、レガシーの SIEM が焦点を置く既知のパターンの検出は氷山の一角をセキュリティ監視しているに過ぎないことは明らかです。未知の問題の背後にある最も重要なコンテキスト要素の一つは、外部システムのレピュテーションを理解することです。今までは、セキュリティ イベントの外部システムのレピュテーションを理解することは不可能でした。

McAfee Labs の力を SIEM に

McAfee Global Threat Intelligence for Enterprise Security Manager は、高速でインテリジェントな McAfee SIEM を使用して、McAfee Labs の力をセキュリティ監視フローで利用しています。これにより、ビッグデータを活用したセキュリティを構築しています。このオプションの契約サービスは、1 億 4,000 万を超える IP アドレスのレピュテーション情報を継続して提供および調整しています。外部システムのレピュテーションをセキュリティ イベント ストリームに直接取り入れることで、既知の攻撃者との接続を迅速に特定できます。

McAfee Global Threat Intelligence（GTI）の IP レピュテーションは、1 億以上のグローバル センサーと 500 人以上の研究者を活用してすべての主要な脅威ベクトルから得た脅威情報の相関分析から生成されます。

McAfee Global Threat Intelligence for Enterprise Security Manager の利点

- **ネットワーク全体で保護を強化：**ネットワーク内のノードが不審な相手や既知の攻撃者と接続すると、McAfee Global Threat Intelligence for Enterprise Security Manager はすぐにその接続を検出し、脅威の経路を特定できます。
- **リスクを基準に優先度を設定：**McAfee Enterprise Security Manager は、ルールではなく IP レピュテーションを使用してリスクを評価し、自動的に対応の優先度を決めています。
- **24 時間年中無休の脅威監視：**McAfee Labs は常に脅威情報を収集して、新しく感染したシステムや不正なシステムを検出します。そしてこれらのシステムが駆除されると、正確な最新のグローバル脅威状況に関する情報を組織に提供します。

不正なアクティビティをリアルタイムで特定

McAfee Global Threat Intelligence for Enterprise Security Manager があれば、異種ファイアウォール、侵入防止システム、ルーター、およびエンドポイントを含む、すべてのイベントの IP レピュテーションを理解する力を持てます。McAfee Enterprise Security Manager のダイナミックなウォッチ リスト機能を活用して、イベントを自動的にソースレピュテーションのスコアに関連付け、リスクを調整します。グローバルな脅威が日々変わる中、McAfee GTI は McAfee Enterprise Security Manager に最新情報を提供し、サーバーとシステムが常に正確なレピュテーション スコアを持っているようにします。これは組織がリスクを理解するのに役立つだけでなく、緊急の問題をリアルタイムで特定し、インシデント対応までの時間を縮小し、正確なリスク分析を行うことを可能にします。

知らなかったことを発見

McAfee Enterprise Security Manager の強みは、何年分もの相関分析データの履歴を格納、取得、および実行する能力です。今、McAfee GTI を使えばセキュリティ アナリストは何年分ものデータを遡って分析し、攻撃者との過去の接続を理解できます。これは、ボットネット、クロスサイト スクリプティング、SQL 挿入の試みによって繰り返される「低く遅い」攻撃の検出に必要不可欠です。

対応時間を短縮

McAfee GTI は McAfee Enterprise Security Manager のアラーム / アラート機能とシームレスに統合されています。そのため、既知の不正なシステムと接続すると、すぐに通知されます。

McAfee のデータベースにより、ビッグ セキュリティ データを構築

データが増大してきていることから、McAfee Labs の有用なセキュリティ関連知識を SIEM に適用することが検討されました。McAfee Enterprise Security Manager は、パフォーマンスに影響を及ぼすことなく、McAfee GTI の膨大な IP レピュテーションデータを格納、相関分析、更新できる点でユニークです。McAfee Enterprise Security Manager には独自のデータベースがあり、このデータベースは SIEM が時間のかかるデータ管理をする必要を省くだけでなく、大量のイベントおよび関連データを非常に高速に受信および処理するために設計されています。McAfee Global Threat Intelligence for Enterprise Security Manager があれば、McAfee GTI の知識は確実にリアルタイムで共有されます。

仕様

サポートされるバージョン
McAfee Enterprise Security Manager 9.4 と McAfee Event Reporter Appliance 9.4

- McAfee Labs 脅威情報ネットワーク : 120 ヶ国以上で 1 億ノード以上
- 平均 IP レピュテーション : 脅威の状況によって異なります

〒 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