McAfee Advanced Correlation Engine

価値に基づく脅威検出

今日の巧妙な脅威は、脅威の検出ルールに基づいた基準に従いません。McAfee® Advanced Correlation Engineソリューション を McAfee Enterprise Security Manager と一緒に使用すると、ルールとリスクの両方のロジックに従って脅威イベントをリアルタイムで識別し、評価することができます。McAfee Advanced Correlation Engineソリューション に重要な資産 (ユーザーまたはグループ、アプリケーション、特定のサーバー、サブネットなど) を登録すると、資産への脅威が発生したときにアラートで通知します。監査証跡と履歴再生でフォレンジック、コンプライアンス対応、ルールの調整を行うことができます。

McAfee Enterprise Security ManagerのMcAfee Advanced Correlation Engineソリューションは、拡張性に優れたエンジンと高性能な機能が相互に作用し合います。

- リスク検出エンジンは、ルールレスリスクスコアと相互に作用し、リスクスコアを生成します。
- 従来のルール ベースのイベント相関による脅威を検出する脅威検出エンジン。

単独-McAfee Advanced Correlation Engine は、企業全体のイベント相関分析に必要な処理能力をご提供します。このデータ エンジンはネットワークの規模に合わせて拡張できます。

リアルタイムな履歴データによる脅威検出

McAfee Advanced Correlation Engineソリューションは、リアルタイム モードまたは履歴モードで配備できます。リアルタイム モードで配備すると、McAfee Advanced Correlation Engineソリューションは収集したイベントをすぐに分析し、脅威とリスクを検出します。

- 発生に応じて検出される脅威データをリアルタイムにルール相関
- 発症する脅威の検出をリアルタイムにルールレス相関

従来モードで、どの収集データも再帰的な脅威とリスク検出のどちらの相関エンジンでも「再生」できます。ゼロデイ攻撃が見つかると、McAfee Advanced Correlation Engineソリューションは、組織が過去に攻撃を受けたことに関わらず、サブゼロデイ脅威検出を遡って識別します。

主な特長

- 開始のお手続きは簡単です: 更新、署名、その他厄介な決まりはありません。
- 重要度の高いユーザー、資産、アプリケーション、アクティビティに対する攻撃が発生したときにアラートを取得できます。
- ルールに基づいたものとそうでないものとが同時に相互に作用する確かな精度。
- 過去の検出履歴から新しい攻撃と脆弱性を検査します。
- 特殊な作用と進行リソースをMcAfee Enterprise Security Managerに追加。
- アプライアンスと仮想配備で利用できます。

必要に応じて拡張性に優れたパフォーマンス

McAfee Advanced Correlation Engineソリューションは、セルフアプライアンスまたは、仮想サービスのため、イベント収集およびその管理に関してMcAfee Enterprise Security Managerの機能に及ぼす影響は全くありません。McAfee Enterprise Security Managerユーティリティを最大限活用して、危害を受けることなく、McAfee Advanced Correlation Engineアプリケーションのすべての機能を完全にお使いいただけます。

ルール ベースのイベント相関

ルール相関は、従来の相関を利用して、リアルタイムに収集された情報を論理的に分析します。すべてのログ、イベント、ネットワーク フローと 識別情報、役割、脆弱性など)のコンテキスト情報を関連させて、より大きな脅威の兆候を示すパターンを検出します。ネットワークの広さ、ルール相関は、すでにすべてのMcAfee Enterprise Security Managerソリューションに直接対応していますが、McAfee Advanced Correlation Engineソリューションは、既存の相関操作に全く関わることなく、はるかに多くの量のデータ相関を実行する拡張性に優れたリソースを提供します。

ルールを使用しないリスク スコア相関

ルール相関は、従来のセキュリティ情報やイベント管理に関して必要で価値の高い機能（SIEM）なので、このシステムを利用すると、一定の署名調整や効率的な更新に関わる既知の脅威パターンだけを検出します。その回答は、ルールレス相関技術を利用した従来のイベント相関を補足します。ルールレス相関システムでは、署名の検出は一度簡単な設定に置き換えられます。McAfee Advanced Correlation Engineソリューションは、ビジネスに重要な内容を簡単に通知します。特定のサービスやアプリケーション、ユーザーグループ、または特定タイプのデータかもしれません。

リアルタイムの追跡と警告

McAfee Advanced Correlation Engineソリューションは、関連のあるすべてのアクティビティの追跡を開始し、リアルタイムなアクティビティに基づいて生じる動的なリスクを構築します。リスクスコアがしきい値を超過した場合、イベントは、McAfee Advanced Correlation Engineソリューション内で生成します。このイベントは、セキュリティアナリストへの進化する脅威条件へのアラートになり、さらに大きなインシデントとして従来のルール相関エンジンに適用されます。McAfee Advanced Correlation Engineソリューションは、リスク スコアの完全な監査証跡を記録します。脅威条件の変化を詳細に分析し、調査できます。

ユースケース

企業のリスクのモデリング

McAfee Advanced Correlation Engineソリューションは、企業のリスクを効率的にモデリングするプラットフォームを提供します。レベルの高い従業員が高度な文書にアクセスすることにより、組織防衛へのリスクが構成される可能性はありますが、重病と診断された有名人の記録は病院のリスクを構成しているかもしれません。McAfee Advanced Correlation Engineソリューションは、正常なしきい値が超過した際は、事象の属性をスコアリングしたり、ベースラインを調整したり、通知を送信することにより 組織のリスクに関して完璧なモデリングを提供します。

重要なデータに対するプロアクティブなリスク評価

McAfee Advanced Correlation Engineソリューションはデータをリアルタイムで監視します。2 つの相関エンジンを同時に使用してリスクを検出し、脅威を未然に防ぎます。リスクスコアは、従来の相関ロジック内で利用できます。例えば、従来のルールに基づいた脅威検出署名は、ブルートフォースがイベントにログインした後に発生するマルウェアイベントかもしれません。通常、この署名を誘発すると、イベントは、すでに発症しています。代わりに、McAfee Advanced Correlation Engineソリューションでは、ブルートフォースログインイベントに続いて生じるリスクスコアが20%増で組み込まれます。このイベントが通知されると、McAfee Advanced Correlation Engineソリューションは、逼迫したインシデントにプロアクティブなアラートを提供し、未然に干渉を許可します。

再帰的な脅威評価

すべての関連性について、脅威が識別されたり、違反が明らかになることは珍しいことではありません。McAfee Advanced Correlation Engineソリューションを履歴モードに設定することにより、システム内にセットされた履歴データがルールレス相関エンジンを介して再生されます。

新しく検出された脅威がまず具体化されると、その条件の根本原因が識別できます。

運用モード

リアルタイム相関モード:

- 発生に応じて検出される脅威データをリアルタイムにルール相関
- 発症する脅威の検出をリアルタイムにルールレス相関

履歴相関モード:

- 再帰的な脅威検出のための履歴イベントデータに関するルール相関
- 再帰的な脅威評価のための履歴イベントデータに関するルールレス相関

相関機能

- ルール相関とルールレス並行相関
- 任意の対応済みデータソースからの相関データ
- 分散ネットワークおよびコレクターからの相関データ
- 数百もの事前定義イベント相関ルールを提供
- ルールレス相関設定エディターを提供
- ルールをカスタマイズまたは、新しく作成するのに便利なGUIイベント相関ルールエディターを提供

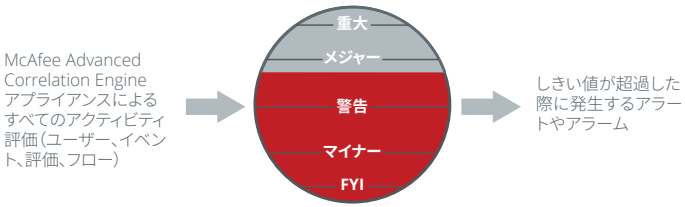

図1. リスクに基づいた相関により、重要度の高い資産に迫る脅威が検出できます。

詳細についてはこちらをご覧ください。

詳細については、www.mcafee.com/siemをご覧ください。

〒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