McAfee Enterprise Security Manager

優先度に従って調査を行い、問題に対応

最も効果的なセキュリティ対策は、システム、ネットワーク、データベース、アプリケーションで発生しているすべてのアクティビティを可視化することから始まります。この効果的なセキュリティの基盤となるフレームワークがSIEM（セキュリティ情報/イベント管理）です。McAfee® Enterprise Security Managerは、McAfee SIEMソリューションの中核として機能し、セキュリティ組織が必要とするパフォーマンス、実用的な情報、ソリューション統合を提供します。これにより、優先度に基づいて調査を行い、隠れた脅威に対応し、コンプライアンス要件を満たすことができます。

McAfee Enterprise Security Managerでは、組織内のシステム、データ、リスク、アクティビティだけでなく、外部の状況（脅威、レピュテーションなど）もリアルタイムに把握できます。リスクに基づいた迅速な意思決定に必要なコンテンツとコンテキストが提供され、総合的かつ相関的な分析が可能です。変化の激しい脅威環境でもリソースを有効に活用することができます。この点は、進行の遅い攻撃や感染兆候（IoC）の調査、監査で見つかった問題の修復を行う場合に重要な要素となります。セキュリティ オペレーションの中心となるのが脅威管理とコンプライアンス対応です。McAfee Enterprise Security Managerの統合ツールを利用すると、設定と変更管理、ケース管理、ポリシーの一元管理を行うことができます。このソリューションには、ワークフローとセキュリティ オペレーションの改善に必要なツールがすべて揃っています。McAfee Enterprise Security Managerのコンテンツ パックには、高度なセキュリティの実装に必要な設定が定義されています。これにより、セキュリティ オペレーションを省力化できます。

エンタープライズクラスの設計

現在の企業環境は分散型で、状況に応じて進化しています。解析に使用するデータ量も増加しています。これらのデータを迅速に収集し、利用できるように、セキュリティ オペレーションの効率を上げていく必要があります。この課題を解決するため、McAfee Enterprise Security Managerは、大量のデータ処理に特化したデータ管理システムを使用しています。業界アナリストやユーザーは、この点をMcAfee SIEMソリューションの強みと評価しています。拡張性に優れたデータアーキテクチャがデータの収集、検索、保存を迅速に実行できるようにサポートしています。必要なときにデータが利用できなかったり、クエリーの応答で分析に時間がかかったり、処理速度の制約で部分的な検索しかできないようでは、効果的な調査を行うことはできません。

主な特長

- **インテリジェント:** 高度な分析と詳細なコンテキスト情報で脅威の優先度を特定します。
- **実用的:** 必要なデータが動的なビューに表示されます。この情報に基づいて調査、隔離、修復を実行できます。重要なアラートやパターンに対応できます。
- **統合:** 様々なセキュリティ インフラから収集したデータをモニタリングし、分析できます。オープンなインターフェースを採用しているため、双方向の統合が可能です。インシデント対応の最初のアクションを自動化できます。

数時間ではなく、数分で

インシデントの調査、高度攻撃の証拠収集、コンプライアンス問題の修復を効率的に行うには、長期間保存されているイベント データに迅速にアクセスする必要があります。履歴データを可視化し、各イベントの詳細にアクセスできるようにしなければなりません。

詳細に調整されたアプライアンスを使用して、STIXベースの脅威情報など、他のデータストリームからログ イベントを迅速に収集し、相関分析を行います。McAfee Enterprise Security Managerでは大量のイベントとフローを保存できます。これらの情報はアドホックなクエリー、フォレンジック、ルール検証、コンプライアンスですぐに利用できます。

コンテキストとコンテンツを識別

脅威データ、レピュテーション情報、IDとアクセス管理システム、プライバシー ソリューションなどのコンテキスト情報が利用できれば、より正確な分析が可能になります。ネットワーク イベント、セキュリティ イベントと資産の属性、実際のビジネス プロセス、ポリシーを関連付け、正確なトリアージを行うことができます。

スケーラビリティとパフォーマンスに優れたMcAfee Enterprise Security Managerでは、文書などのアプリケーション コンテンツ、トランザクション、通信など、より多くの情報源から大量の情報を収集し、フォレンジック調査に利用することができます。これらの情報にインデックスを作成し、正規化してから相関分析を行うので、より広範囲のリスクと脅威を検出することができます。

高度脅威の検出

ネットワーク トラフィック、ユーザー アクティビティ、アプリケーションの使用など、正常なアクティビティから逸脱がある場合、データやインフラが危険にさらされている可能性があります。McAfee Enterprise Security Managerは、収集した情報のベースライン アクティビティを計算し、潜在的な脅威を検出するために優先度付きのアラートを提供します。また、データを分析して、大規模な脅威に発展する可能性があるパターンを識別します。McAfee Enterprise Security Managerは、豊富なコンテキスト情報を使用してイベントを分析するため、セキュリティ イベントが実際のビジネス プロセスに及ぼす影響を的確に把握することができます。

McAfee Enterprise Security ManagerのCyber Threat Managerダッシュボードを使用すると、リアルタイムでモニタリングを行い、新たに発生する脅威を確認することができます。脅威情報は、STIX/TAXII、McAfee Advanced Threat Defense、サードーパーティのWeb URL経由で報告されます。これらのデータをリアルタイムで集計し、相関分析を行います。また、履歴データも使用できます（バックトレース機能を使用）。これにより、セキュリティ チームは環境内で蔓延している脅威をより詳しく分析できます。適切な権限のある人物がほぼリアルタイムにデータを処理し、的確な意思決定を行うことができます。

セキュリティ オペレーションの最適化

アナリスト向けに設計されたMcAfee Enterprise Security Managerは、柔軟性に優れたユーザー エクスペリエンスを提供します。カスタマイズを簡単に行い、調査結果に基づき迅速な対応を行うことができます。ワークフローが簡素化されているため、よりタイムリーかつ効率的にインシデントを管理できます。脅威情報を簡単に利用できるため、経験の浅いアナリストでも脅威の優先度をすばやく判断し、調査・対応を行うことができます。

McAfee Enterprise Security Managerには非常に多くのビュー、ルール、アラートが用意されています。このソリューションは導入後すぐに利用できます。カスタマイズも簡単です。ベースラインを設定することで、ネットワークの標準的な利用状況を把握し、アラートをカスタマイズできます。McAfee Enterprise Security Managerのダッシュボードを使用すると、環境全体の状況をすばやく確認し、調査を行い、最も関連性のあるセキュリティ情報を報告できます。また、豊富なデータとコンテキストを相関分析し、的確な判断を迅速に行うことができます。

McAfee Enterprise Security Managerのコンテンツ パックを使用すると、事前設定のユースケースを利用できます。これのより、セキュリティ オペレーションを省力化し、高度脅威対策やコンプライアンス管理機能に迅速にアクセスできます。コンテンツ パックには、一般的なセキュリティ ユースケース用に作成されたルール、アラーム、ビュー、レポート、変数、ウォッチリストのセットが定義されています。また、追加のセキュリティや自動修復が必要になる動作のトリガーも定義されます。

コンプライアンス対応の負荷を軽減

McAfee Enterprise Security Managerでは、コンプライアンスのモニタリングとレポーティングを一元管理し、自動化しています。労力を要する手作業を減らすことができます。Unified Compliance Framework（UCF）との統合により、1回の収集で複数の法規制に対応できます。最小の労力とコストでコンプライアンス要件を満たすことができます。UCFのサポートにより、法規制ごとの相違を正規化し、コンプライアンス対応を効率的に行うことができます。収集したイベントの1つのセットから個々の法規制に簡単に対応できます。

McAfee Enterprise Security Managerには、数百のダッシュボードと包括的な監査証跡が事前に用意されているため、コンプライアンスを簡単かつ迅速に管理できます。PCI-DSS、HIPAA、NERC-CIP、FISMA、GLBA、GPG13、JSOX、SOXなど、240以上の法規制に対する対応状況を報告できます。McAfee Enterprise Security Managerのコンプライアンス レポート、ルール、ダッシュボードはすぐに使えるだけでなく、必要に応じてカスタマイズできます。

ITインフラの統合

セキュリティ インフラを統合することで、組織のセキュリティ状況をリアルタイムで的確に把握することができます。McAfee Enterprise Security Managerは、他のセキュリティベンダーのデバイスや脅威情報の提供元から重要なデータを収集します。McAfee Global Threat Intelligence（McAfee GTI）との統合により、世界各地にある1億台のMcAfee Labsグローバル脅威センサーから収集した情報を利用し、既知の不正なIPアドレスに関する最新の情報を提供します。McAfee Enterprise Security Managerは、STIX/TAXIIまたはサードパーティのWeb URLから脅威情報を収集し、分析結果に基づいてアクションを実行します。

McAfee Enterprise Security Managerには、McAfeeやMcAfee Security Innovation Allianceパートナーが提供する様々なインシデント管理/分析ソリューションを統合できます。

たとえば、McAfee Threat Intelligence Exchangeは、グローバル、サードパーティ、ローカルの脅威情報を利用し、まだ広範囲に拡散していない攻撃のデータを集計します。McAfee Threat Intelligence Exchangeは、McAfee Advanced Threat Defenseなどの製品と連携して詳細な分析を行い、不正なファイルを特定します。

インシデント対応チームと管理者は、McAfee Active Responseを使用して、メモリー内のアクティブ プロセスだけでなく、システムに潜伏して休眠状態になっている不正なファイルも検出できます。McAfee Active Responseは、コレクターを使用してエンドポイントを継続的にモニタリングし、特定のIoCを検出します。環境内でIoCが見つかると、自動的にアラートで警告します。標準的なセキュリティ アプローチとは異なり、検出から封じ込め、修復までを網羅したワークフローを利用できます。

McAfeeは、新たに発生する攻撃を未然に防ぐ統合セキュリティ システムを提供しています。より少ないリソースで、より多くの脅威を迅速に解決できます。弊社の統合アーキテクチャと集中管理機能により、煩雑さを解消し、セキュリティ インフラ全体を効率よく運用できます。McAfeeは、最高のセキュリティ パートナーとして完全な統合セキュリティを提供します。

詳細情報

McAfee Enterprise Security Managerの詳細については、**www.mcafee.com/jp/products/siem/index.aspx**をご覧ください。

統合ソリューションの詳細については、**www.mcafee.com/jp/solutions/intelligent-security-operations.aspx**をご覧ください。

McAfee Together is power.

〒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