ソリューション概要

SIEM: より大きなビジネス問題を解決する5つの要件

セキュリティ情報/イベント管理（SIEM）が登場して10年以上が経過しました。このソリューションも成熟したものと考えられています。イベント収集、相関アラート、コンプライアンス状況の通知、などの機能は基礎的なもので大半のSIEMソリューションで採用されています。しかし、状況は常に変化しています。標的型攻撃や持続型攻撃などの新たな脅威が出現し、モバイル、クラウド、仮想化などの新しいトレンドが生まれています。顧客の獲得、運用の効率性、コスト削減など、ビジネスの優先順位も変化しています。より大きなビジネス問題を解決するため、SIEMにもより高度な機能が求められています。

SIEMのユーザーはSIEMの基本的な問題として次の5つ点を挙げています。

- ビッグデータ セキュリティ
- 状況認識
- リアルタイム コンテキスト
- 簡単な管理
- 統合セキュリティ

SIEMで効果的なセキュリティ管理とリスク管理を行うには、この5つの問題を解決しなければなりません。脅威の回避、トレンド対応、ビジネスの優先度に関連する場合には特に重要な課題となります。以下では、それぞれの問題と事例、用途について紹介します。

1 ビッグデータ セキュリティ

ビッグデータ　セキュリティが使用できれば非常に効果的です。従来のSIEMソリューションは大量のエンドポイント、ネットワーク、データソースを統合するように設計されていません。また、イベントの処理率が高いプロセスに対応したものではなく、長期間ポリシーを維持する設計にもなっていません。リレーショナル データベースや類似した従来のSIEMは基本的にネットワーク　イベントの処理を目的としているため、現在の動的なITインフラのセキュリティ要件には対応していません。効率よく利用するには、速度と拡張性の点で問題が残ります。

事例: 政府機関

ある政府機関が数ペタバイトのSIEMリレーショナル　データベースを使用して高度な分析を実施しました。単純なレポートでも生成に数時間かかりました。レポートの生成に1日以上かかり、SIEMをフォレンジックに利用できないこともありました。

SIEMソリューションをMcAfee® Enterprise Security Managerに切り替えた結果、統合可能なデバイスの数と種類が増えました。これにより、データとユーザーを中心としたコンテキストで分析が可能になり、イベントの処理率と格納されるデータが増加しました。現在では、レポートが数分で生成されるため、フォレンジック分析が全体的に向上しています。

2 状況認識

ファイアウォールと侵入防止システムのイベントを相関分析し、脆弱性評価データを適用するツールとしてSIEMが利用されていた時期がありました。現在でも、ネットワーク　フロー　データを中心とするSIEMが存在します。これらのソースはすべて重要ですが、アプリケーション、データ コンテキスト、識別情報を追加し、ソース情報を補完する必要があります。これらの情報がない状態で有効な情報をタイムリーに提供するには、より多くの時間とリソースを使用してイベントの認識と優先順位の設定を行う必要があります。

事例: 医療機関

ある地域の医療機関が、スタッフの生産性を向上させるため、BYOD（Bring Your Own Device）の導入を検討していました。病院側では過去の事件から内部不正を懸念していました。この医療機関が使用しているSIEMソリューションでは、デバイス（ラップトップ、デスクトップ、タブレット、仮想デスクトップ）に関わらず、どのユーザーが機密データを使用しているのか把握することができませんでした。

用途: ビッグデータ セキュリティ

- フィードを提供するソースを増加してデータ収集機能を強化
- 非常に大きなデータセットを使用して分析とフォレンジックを実行
- ビッグデータ セキュリティの処理速度とデータ量を最適化
- 従業員とプロセスの生産性を向上

用途: 状況認識

- IDソリューションを追加して状況認識を強化
- ユーザー、時期、方法、場所、対象を識別
- 期間、ユーザー、対象を把握
- ラップトップやスマートフォンなどのBYOD資産を追加

このため、McAfee Enterprise Security Managerを導入して、IDとモバイルの管理、Active Directory、LDAP製品の統合を実現し、ユーザーとデバイスの位置情報を取得できるようになりました。ネイティブ データベース サポートにより構造データと非構造データのストアが統合され、DLP（Data Loss Prevention）とDAM（Database Activity Monitoring）が利用できるので、より完全な状況を把握し、内部からの脅威を回避することができます。

3 リアルタイム コンテキスト

初期のSIEMの用途はログの管理で、いくつかのオプション機能を使用して収集、保存、クエリを実行していました。現在もログはSIEMの重要なコンポーネントですが、現在のSIEMはリアルタイム コンテキストを必要としてます。

たとえば、McAfee Global Threat Intelligence（McAfee GTI）やMcAfee Vulnerability Managerのコンテンツが必要になります。McAfee GTIはクラウド上で実行され、リアルタイムでレピュテーション情報を提供します。McAfee Vulnerability Managerは資産の脆弱性情報を収集します。

事例: 小売業

SIEMとMcAfeeのソリューションを利用していないFortune 100の小売業が概念実証を行いました。最初の1週間で確認されたトラフックの30%以上は不正なソースから送信されているか、不正なペイロードを含むものでした。

McAfee Enterprise Security Managerの導入により、McAfee GTIとイベント情報の相関分析が可能になり、各店舗とデータセンターを狙った攻撃を迅速に識別し、攻撃の種類を把握できるようになりました。McAfee SIEMソリューションは脅威の重大度を判断し、応答の優先順位を決定します。SIEMとリアルタイム コンテキストを併用することで、脅威をより迅速に検出し、優先順位の設定と修復を行うことができます。

4 単純な管理

従来のSIEMは非常に強固なアーキテクチャですが、いくつかの重要な機能が含まれていません。たとえば、非対応だったデバイスを統合して情報を使用することはできません。次世代のSIEMはカスタマイズが簡単で、特定の環境に合わせて自由に変更できます。次世代のSIEMでは、多くの組織に対応する戦略を提供しています。

事例: 公益企業

ある大手公益企業が、Stuxnetなどの攻撃によるインフラへの影響を回避して顧客喪失を防ぐため、セキュリティ管理の配備を計画していました。この会社はMcAfee Enterprise Security Managerを導入し、会社のIT、SCADA、工業制御システム（ICS）ゾーンで状況認識が可能になり、ネイティブのデバイス、アプリケーション、プロトコルがサポートされるようになりました。

用途: リアルタイム コンテキスト

- 環境の内外に存在する脅威を把握
- リアルタイム コンテキストでSIEMの機能を向上
- インシデント識別と対応に要する時間を短縮
- 脅威の識別と優先順位の設定に他のセキュリティ情報も利用

用途: 単純な管理

- 動的なホワイトリストとハードウェア支援のセキュリティでSIEMを配備し、専用端末を保護
- カスタマイズ可能なドリルダウンでフォレンジックを簡素化
- SIEMとファイアウォール、侵入防止システム（IPS）の統合で、迅速なインシデント対応を実施
- セキュリティの向上で従来資産の使用期間を延長

McAfee SIEMでは、ユーザーがツールを使用してSCADAやICSサービスとの統合を設定できます。また、この3つのすべてのゾーンで相関分析、アノマリ検出、傾向分析を実行できます。イベント収集のカスタマイズ以外にも固有のダッシュボード、レコード、相関ルール、アラートを簡単に作成できます。SIEMはセキュリティ、コンプライアンス状況の確認、資産管理に非常に重要なツールとなります。

5 統合セキュリティ

SIEMは、戦略的セキュリティの重要なコンポーネントですが、その中の一つに過ぎません。セキュリティとコンプライアンスの統合ソリューションは個々のソリューションを集めた場合よりも多くの機能を提供します。単独のソリューションを個別に使用した場合、アーキテクチャが複雑になりますが、戦略的なセキュリティの構築を阻む大きな要因がここにあります。

事例: 金融サービス

国際的に事業を展開する金融機関が複数のベンダーから異なる製品を導入しました。一部の製品は常時使用されていますが、リソースの制約で定期的に使用していない機能もあります。このため、SIEMを利用してエンドポイント、ネットワーク、データの管理機能を統合し、リスク回避とコスト削減を図ることにしました。

これにより、ベンダー数とコスト削減に成功しました。トレーニング費用を抑え、エージェント、コンソール　サーバーなどの数も減らすことができました。また、契約費用や関連費用の削減にも成功しました。既存のソリューションとMcAfee Enterprise Security Managerを完全に統合したことで、コストの削減だけでなく、セキュリティ管理と可視性が向上しました。

検討事項

- ビッグデータセキュリティが抱える収集、保存、アクセス、処理、分析の問題を簡単に解決できるかどうか
- セキュリティ関係者が意思決定に必要な情報を取得し、アクションをタイムリーに実行できるかどうか
- セキュリティ チームがリスクと攻撃の識別に必要なコンテキストをリアルタイムで確認できるかどうか
- SIEMで直観的なドリルダウンとカスタム ビューを使用したときのセキュリティとリソースに対する影響はどのくらいか
- インフラの統合でセキュリティ、可視性、プロセス、脅威対応がどのくらい向上するのか

用途: 統合セキュリティ

- セキュリティと運用のワークフローを簡素化
- 自動化と簡単なカスタマイズで複雑さを排除
- 複数のセキュリティ　ソリューションを連携させ、可視性と状況認識を向上
- インテリジェンスと統合でセキュリティを向上

従来のSIEMでは現在の要件を満たすことはできません。ビッグデータ、セキュリティ情報、状況認識、パフォーマンス、使いやすさ、統合に関する新しい要件により、SIEMの用途は広がっています。SIEMは複雑さを排除するものであり、生み出すものではありません。SIEMからより多くのことを期待できます。

現在のSIEMは、セキュリティとビジネスの要件が調整されたセキュリティ　フレームワークの一部として使用する必要があります。SIEMは、戦略的セキュリティとビジネス価値を実現する上で重要な役割を果たしています。

McAfeeのSIEMソリューションについては、
www.mcafee.com/SIEMをご覧ください。

統合セキュリティ

McAfeeは統一された統合フレームワークを提供し、多くの製品、サービス、パートナーが互いに学び合い、コンテキスト固有のデータをリアルタイムに共有し、一つのチームとして情報とネットワークを保護できるようにします。このプラットフォームの革新的なコンセプトと最適化されたプロセスにより、どの組織でもセキュリティを強化し、運用コストを最小限に抑えることができます。

〒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