McAfee Database Event Monitor for SIEM

パフォーマンスを低下させずにデータベース トランザクションの可視性を向上

コンプライアンスを維持するには、データベース トランザクションに対して信頼性の高い監査を実施できるソリューションが必要です。しかし、従来のデータベース監査ソリューションでは、データベースのパフォーマンスやデータベース管理者の作業効率が低下することが少なくありません。コンプライアンスに対する監査要件やレポート要件は厳しさを増しています。非侵入型のMcAfee® Database Event Monitor for SIEMはこのような要件に対応し、セキュリティを強化します。

McAfee Database Event Monitor for SIEMは、重要な顧客データや会社のデータに対するアクセスを監視し、データベースとアプリケーションのセキュリティ ロギングを行う非侵入型のソリューションです。配備は簡単で、データベース トランザクション、イベント、特定のデータベース クエリーや応答を視覚的に確認できます。データにアクセスしている人物とその理由も確認できます。

McAfee Database Event Monitor for SIEMは、データベース アクティビティを中央の監査リポジトリに統合し、アクティビティの正規化、相関分析、レポート作成を実行できる唯一の製品です。

事前定義のルールとレポート、プライバシー保護機能により、コンプライアンス対応の労力を軽減し、セキュリティを強化できます。

データベース アクセスのコンテキスト情報

McAfee Database Event Monitor for SIEMは、ロギングだけでなくデータの正規化を行い、データベース トランザクションと他の情報を関連付け、リアルタイムで分析を行います。

McAfee Database Event Monitor for SIEMでは、ユーザー情報、アプリケーション コンテンツ、オペレーティング システムのアクティビティ、脆弱性、ネットワークの場所などの情報を利用し、次の操作を行うことができます。

- アプリケーション間でのユーザーの追跡
- ログオンからログオフまでの完全なセッション アクティビティの調査
- 機密データの検出とポリシー違反の識別
- 承認チャネルからのデータ漏えいの検出
- データベース アクティビティとセキュリティ イベントの相関分析
- データベース アクティビティからの監査証跡の生成
- PCI DSS、HIPAA、NERC-CIP、FISMA、GLBA、GPG13、JSOX、SOXなどに関する詳細なレポートの作成

主な特長

- データベースのパフォーマンスに影響を及ぼさないネットワーク ベースのパッシブ監視
- すべてのデータベース インスタンスを検出（非承認のインスタンスや不正なインスタンスも含む）
- 規制対象の情報が格納されたデータベースへのアクセスを監視し、ログに記録
- ログインしてからログアウトするまで、すべてのデータベース トランザクションの詳細を保存
- ワンクリックでセッションを再構築。分析が簡単に実行できます。
- McAfee Enterprise Security Managerと完全に統合。データベース トランザクションにイベント相関分析やSIEMの高度な機能を実行できます。
- 物理アプライアンスと仮想アプライアンスに対応した柔軟でハイブリッドな配備オプション

intel Security

トランザクションごとに完全な可視性を実現

McAfee Database Event Monitor for SIEMは、すべてのデータベース トランザクションを監視し、クエリー、結果、認証、権限昇格などのデータベース アクティビティから完全な監査証跡を生成します。McAfee Database Event Monitor for SIEMはすべてのトランザクションに対して完全なセッション情報を保持するので、特定のトランザクションの前後（ログインからログアウト）に発生したイベントをすぐに確認できます。

コンプライアンス プロセスの自動化

事前定義のポリシーを使用した検出ルールとコンプライアンス レポートにより、PCI DSS、HIPAA、NERC-CIP、FISMA、GLBA、GPG13、JSOX、SOXなどで必要になるデータ アクセス情報を生成できます。McAfee Database Event Monitor for SIEMはMcAfee Enterprise Security ManagerやMcAfee Enterprise Log Managerと完全に統合され、高度なイベント分析と相関分析を行い、データ アクティビティ ログを暗号化して保管します。

また、例外リストを使用すると、監視されていないデータベース サーバーだけでなく、データベースへのアクセスで不正に利用されているポートも確認できます。

ユーザーとアカウントの追跡

マカフィーのセキュリティ管理製品の高度な機能を使用すると、複数のアプリケーションやアカウントに対するユーザーや管理者の操作を簡単に追跡できます。データベースへのアクセス方法に関わらず、すべてのユーザー アクティビティの詳細レポートを作成できます。

ユーザー アクティビティのプロファイリング

McAfee Database Event Monitorは、ユーザーの動作プロファイルを生成するだけでなく、SQLクエリーをデータベース サーバーでアクセスされるオブジェクト（テーブル、ビュー、ストアド プロシージャ）に分割し、新しいアクティビティと異常なアクティビティを識別します。

SQLインジェクション

すべてのSQLクエリー応答を監視し、クエリーの成否を確認します。SQLインジェクション攻撃の兆候でもある構文エラーなどの重大度の低い障害を追跡します。このエラーが連続して発生している場合には相関分析を行い、SQLインジェクション攻撃を未然に防ぎます。

リスクと脅威の検出

McAfee Database Event Monitor for SIEMは、カスタマイズ可能なポリシー ルールを使用して監視対象のすべてのアクティビティを分析し、不審なアクティビティを警告します。また、アノマリ検出により、異常なユーザー アクティビティ、クエリー、応答などの挙動を検出します。

余分な負荷をかけずに強力な機能を実行

高性能なデータ キャプチャ エンジンを搭載したMcAfee Database Event Monitor for SIEMアプライアンスがネットワーク経由でデータベースを監視します。データベース自体に余分な負荷をかけず、必要な監査データを保存します。

McAfee Enterprise Security Managerがセキュリティ/コンプライアンス エコシステムの残りの部分とデータベース モニタリングを統合し、管理機能を提供します。オプションのホスト エージェントを使用すると、ローカル ターミナルのアクティビティを可視化できます。他のホスト エージェントやネイティブの監査機能に比べると、パフォーマンスに対する影響は少なくなります。

データベース監視機能

- すべてのデータベース アクティブティを監視し、ログに記録
- コンプライアンス サポート
- 盗聴防止
- アカウンタビリティの向上
- オブジェクト、アクション、ポリシー違反に対する警告
- 重要な指標を収集し、データベースのサービス レベルとパフォーマンスを管理
- すべてのデータ パスを監視
  例:
  - アプリケーション
  - ユーザー
  - マルウェア
  - ユーティリティ
  - バックドア
  - クエリー
  - LAMPスクリプティング
  - ODBC（Open Database Connectivity）

ユースケース

コンプライアンス

McAfee Database Event Monitor for SIEMでは使用中の重要データを検出できるので、コンプライアンス対応の負担を軽減できます。データベースを監視しながら、保護対象のデータ アクセス、ユーザー アカウント アクティビティ、変更の監査証跡を生成できます。セキュリティとデータベース管理を分離し、重要データをロギングの対象外にすることもできます。レポートでは上位の顧客や保護されたレコードが強調表示されます。また、様々な法規制に対応するレポートが事前に定義されています。

データベースの検出と分類

McAfee Database Event Monitor for SIEMは、ネットワーク上でデータベース コマンドを監視し、すべてのデータベース インスタンスを検出します。また、McAfee Database Event Monitor for SIEMは、クエリーの結果を含むすべてのトランザクションを監視し、ポリシー ルールやディクショナリを使用して分析を行います。これにより、クレジットカードや社会保障番号など、重要な情報が格納されているデータベースを検出します。

セキュリティ監視

McAfee Database Event Monitor for SIEMはデータベースを直接監視し、総当り攻撃によるログイン、SQLインジェクション、異常なアクセス パターン、データベース サービスに悪影響を及ぼす兆候などをリアルタイムで検出して警告します。また、バックエンド アプリケーションのアクティビティを監視し、不正なデータ取得や不正なユーザー アカウントなど、不審なアクティビティを検出します。

ネットワーク内部から攻撃が発生した場合には、ユーザー アクティビティを追跡し、ネットワーク フローデータと比較して攻撃者の識別と特定を行います。外部からの攻撃の場合、他の送信ネットワークやアプリケーションのアクティビティを関連付け、データの流出や隠蔽された通信チャンネルを検出します。

McAfee. Part of Intel Security.
東京本社　〒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）FAX 03-5428-1480
西日本支店　〒530- 0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所　〒810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com