McAfee Database Event Monitor for SIEM

Übersicht über Datenbanktransaktionen ohne Leistungseinbußen

Zur Gewährleistung von Compliance ist die zuverlässige Prüfung von Datenbanktransaktionen zwingend erforderlich. Gleichzeitig beeinträchtigen herkömmliche Datenbank-Audit-Lösungen die Leistung der Datenbank sowie die Produktivität der Datenbank-Administratoren. Dank des Aufbaus von McAfee® Database Event Monitor for SIEM, bei dem kein Benutzereingriff erforderlich ist, unterstützt diese Lösung Sie bei den ständig zunehmenden Anforderungen an Compliance-Audits sowie Berichte und verbessert die Sicherheitsabläufe.

McAfee Database Event Monitor for SIEM erstellt detaillierte Sicherheitsprotokolle zu Datenbanken sowie Anwendungen, ohne deren Leistung und Produktivität zu beeinträchtigen. Zudem überwacht die Lösung den gesamten Zugriff auf vertrauliche Unternehmens- und Kundendaten. Mit geringem Implementierungsaufwand erhalten Sie einen Überblick über Datenbanktransaktionen, Ereignisse sowie spezifische Datenbankabfragen und -antworten, einschließlich Informationen dazu, wer warum auf Ihre Daten zugreift.

McAfee Database Event Monitor for SIEM ist das einzige Produkt, das die Datenbankaktivitäten in einem zentralen Audit-Repository zusammenfasst und diese Aktivitäten normalisiert, korreliert, analysiert und dokumentiert.

Dank vordefinierter Regeln und Berichte sowie datenschutzkonformer Protokollierungsfunktionen können Sie Compliance-Vorgaben einhalten und gleichzeitig die Gesamtsicherheit Ihres Unternehmens erhöhen.

Datenbankzugriff im Kontext

McAfee Database Event Monitor for SIEM geht weit über bloße Protokollerstellung hinaus: Die Lösung normalisiert Daten und setzt Datenbanktransaktionen zu anderen Informationen in Beziehung, um Echtzeitanalysen zu vereinfachen.

Dank des Einblicks in Informationen wie Benutzerdetails, Anwendungsinhalte, Betriebssystemaktivitäten, Schwachstellen sowie den Netzwerkstandort bietet McAfee Database Event Monitor for SIEM folgende Vorteile:

- Überwachung von Benutzern in unterschiedlichen Anwendungen
- Überprüfung aller Sitzungsaktivitäten von der An- bis zur Abmeldung
- Erkennung von vertraulichen Daten und Richtlinienverletzungen
- Erkennung von Datenverlusten über zulässige Kanäle
- Korrelation von Datenbankaktivitäten mit Sicherheitsereignissen
- Erstellung eines Audit-Protokolls zu allen Datenbankaktivitäten
- Generierung detaillierter Berichte zu Standards und Normen wie PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX und SOX

Hauptvorteile

- Passive netzwerkbasierte Überwachung zur Vermeidung von Nachteilen für die Datenbankleistung
- Ermittlung aller Datenbankinstanzen, einschließlich nicht autorisierter Datenbanken
- Überwachung und Protokollierung des Zugriffs auf Datenbanken, die regulierte Informationen enthalten
- Speicherung von Details zu allen Datenbanktransaktionen von der An- bis zur Abmeldung zur Vereinfachung von Audits
- Vereinfachte Analysen durch die Rekonstruktion von Sitzungen mit einem einzigen Mausklick
- Vollständige Integration in McAfee Enterprise Security Manager, damit Datenbanktransaktionen zur Ereigniskorrelation sowie für andere wichtige SIEM-Aktivitäten hinzugezogen werden können
- Flexible Hybrid-Bereitstellungsoptionen mit physischen und virtuellen Appliances

intel Security

Vollständiger Überblick über alle Transaktionen

McAfee Database Event Monitor for SIEM überwacht alle Datenbanktransaktionen und erstellt ein komplettes Audit-Protokoll aller Datenbankaktivitäten, einschließlich Abfragen, Ergebnissen, Authentifizierungsaktivitäten und erhöhten Berechtigungen. Da McAfee Database Event Monitor for SIEM die vollständigen Sitzungsdetails zu allen Transaktionen speichert, können Sie schnell erkennen, was vor und nach einer bestimmten Transaktion geschehen ist – von der An- bis zur Abmeldung.

Automatisierte Compliance-Abläufe

Die vorkonfigurierten richtlinienbasierten Erkennungsregeln und Compliance-Berichte gewährleisten, dass Sie die von PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX und SOX sowie anderen Normen und Standards geforderten Datenzugriffsinformationen generieren können. Zudem ist McAfee Database Event Monitor for SIEM vollständig mit McAfee Enterprise Security Manager sowie McAfee Enterprise Log Manager verzahnt und ermöglicht dadurch bisher unerreichte Ereignisanalysen und -korrelationen sowie Funktionen zur vorschriftenkonformen Speicherung und Maskierung vertraulicher Daten in Aktivitätsprotokollen.

In einer Ausnahmenliste werden nicht überwachte Datenbank-Server sowie illegale Ports angezeigt, die für den Zugriff auf Daten aus Datenbanken geöffnet sind.

Benutzer- und Kontoüberwachung

Mithilfe der erweiterten Möglichkeiten der McAfee-Produkte zur Sicherheitsverwaltung können die Benutzer- und Administratoren-Aktivitäten über mehrere Anwendungen und Konten hinweg überwacht werden. Auf diese Weise lassen sich alle Benutzeraktivitäten konkreten Benutzern zuordnen – unabhängig davon, wie auf die Datenbank zugegriffen wurde.

Erstellung von Benutzeraktivitätsprofilen

McAfee Database Event Monitor wandelt alle SQL-Abfragen in Befehle und Objekte (Tabellen, Ansichten, gespeicherte Prozeduren) um, auf die auf den Zieldatenbank-Servern zugegriffen wird. Zudem wird ein Profil zum Verhalten jedes Benutzers erstellt, sodass neue und ungewöhnliche Aktivitäten sichtbar werden.

SQL-Injektion

Alle SQL-Abfrage-Antwort-Pakete werden auf Abfrageerfolge und -fehler überwacht. Fehler mit geringem Schweregrad wie beispielsweise Syntax-Fehler, die für SQL-Injektionsangriffe typisch sind, werden überwacht und – sobald sie nacheinander auftreten – zueinander in Beziehung gesetzt. Dadurch können SQL-Injektionsangriffsversuche präventiv erkannt werden.

Risiko- und Bedrohungserkennung

McAfee Database Event Monitor for SIEM analysiert alle überwachten Aktivitäten anhand anpassbarer Richtlinienregelsätze und erkennt sowie meldet alle verdächtigen Aktivitäten. Die Funktion zur Erkennung anormaler Ereignisse kennzeichnet ungewöhnliche Benutzeraktivitäten, Abfragen, Reaktionen sowie anderes abweichendes Verhalten.

Leistungsstark, ohne Mehraufwand zu erfordern

McAfee Database Event Monitor for SIEM-Appliances enthalten ein leistungsstarkes Datenerfassungsmodul und überwachen Ihre Datenbank über das Netzwerk – ohne die Datenbank selbst zu belasten. Gleichzeitig werden die erforderlichen Audit-Daten gespeichert.

McAfee Enterprise Security Manager bietet Verwaltungsfunktionen und verknüpft die Datenbanküberwachung mit den anderen Komponenten Ihrer Sicherheits- und Compliance-Infrastruktur. Zur Überwachung von Aktivitäten an lokalen Terminals können Sie einen optionalen Host-Agenten einsetzen, der die Leistung weniger beeinträchtigt als native Audit-Tools oder Host-Agenten von Wettbewerbern.

Datenbanküberwachungsfunktionen

- Überwachung und Protokollierung aller Datenbankaktivitäten
- Unterstützung von Compliance-Maßnahmen
- Verhinderung von Abhörversuchen
- Verbesserte Verantwortlichkeit
- Warnmeldungen zu Objekten, Aktionen und Richtlinienverletzungen
- Erfassung wertvoller Kennzahlen zur Datenbank-Service-Level- und Leistungsverwaltung
- Überwachung aller Pfade zu Daten, einschließlich:
  - Anwendungen
  - Benutzer
  - Malware
  - Dienstprogramme
  - Backdoor-Anwendungen
  - Abfragen
  - LAMP-Skripte
  - Open Database Connectivity (ODBC)

Anwendungsszenarien

Compliance

McAfee Database Event Monitor for SIEM erkennt gerade verwendete vertrauliche Daten und unterstützt Sie auf diese Weise bei der Gewährleistung von Compliance. Sie können diese Datenbanken überwachen und ein Audit-Protokoll über den Zugriff auf geschützte Daten, Benutzerkontoaktivitäten sowie Änderungen erstellen. Sicherheitsaufgaben lassen sich von der Datenbank-Administration trennen, um strengere Kontrollen zu ermöglichen. Zudem können vertrauliche Daten für die Protokollierung maskiert werden. In Berichten können die häufigsten Nutzer geschützter Datensätze gekennzeichnet werden. Außerdem haben Sie die Möglichkeit, jederzeit die vorkonfigurierten Berichte zu den verschiedenen Vorschriften zu erstellen.

Datenbankerkennung und Klassifizierung

Durch die Überwachung des Netzwerks auf Datenbankbefehle kann McAfee Database Event Monitor for SIEM alle Datenbankinstanzen erkennen – einschließlich unbekannter oder nicht autorisierter Datenbanken. Zudem überwacht McAfee Database Event Monitor for SIEM alle Transaktionen (einschließlich Abfrageergebnissen) und analysiert diese anhand von Richtlinienregeln und Wörterbüchern, um zu ermitteln, welche Datenbanken Kreditkarten- oder Steueridentifikationsnummern oder andere vertrauliche Informationen speichern.

Sicherheitsüberwachung

McAfee Database Event Monitor for SIEM überwacht Ihre Datenbanken direkt. Dabei erkennt die Lösung in Echtzeit Brute-Force-Anmeldeversuche, SQL-Injektionsangriffe, ungewöhnliches Zugriffsverhalten sowie andere Hinweise auf Kompromittierungen Ihrer Datenbank-Server und warnt Sie sofort über diese Aktivitäten. Sie können Back-End-Anwendungsaktivitäten überwachen und verdächtige Aktivitäten erkennen, einschließlich nicht autorisierter Benutzerkonten sowie betrügerischer Versuche, Daten abzurufen.

Wenn der Angriff von innerhalb des Netzwerks ausgeht, können Sie die Benutzeraktivitäten überwachen und mit den Netzwerkflussdaten in Beziehung setzen, um den Akteur zu identifizieren und zu lokalisieren. Bei einem Angriff von außen kann der Einbruchversuch mit anderen ausgehenden Netzwerk- und Anwendungsaktivitäten in Beziehung gesetzt werden, um Datenverluste, verdeckte Kommunikationskanäle sowie andere Datenverlust-Vektoren zu erkennen.

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com