McAfee Database Event Monitor for SIEM

Maggiore visibilità sulle transazioni database senza pregiudicare le prestazioni.

Per rispettare la conformità è essenziale disporre di una verifica affidabile delle transazioni dei database, ma le tradizionali soluzioni native di verifica possono compromettere le prestazioni dei database e la produttività del suo amministratore. Le caratteristiche non intrusive di McAfee® Database Event Monitor for SIEM consentono di rispondere più efficacemente ai requisiti di conformità nell'esecuzione di verifiche e nella creazione di reportistica e permettono operazioni di sicurezza più ampie.

McAfee Database Event Monitor for SIEM registra in un log, in modo non intrusivo e dettagliato, gli eventi legati alla sicurezza per database e applicazioni, monitorando tutti gli accessi ai dati sensibili dell'azienda e della clientela. Con un'installazione di minima difficoltà puoi avere visibilità sulle transazioni, gli eventi del database e specifiche query e risposte, fino a sapere chi sta accedendo ai dati e perché.

McAfee Database Event Monitor for SIEM è l'unico prodotto nel suo genere che raccoglie le attività del database in un deposito centralizzato per la verifica e contemporaneamente fornisce normalizzazione, correlazione, analisi e reportistica di tale attività.

Le regole e i rapporti predefiniti e le funzioni di log rispettose della privacy facilitano l'adesione ai regolamenti in materia di conformità, rafforzando al contempo le condizioni complessive di sicurezza dell'azienda.

Accesso contestualizzato al database

McAfee Database Event Monitor for SIEM va ben oltre i log tradizionali, normalizzando i dati e correlando le transazioni del database con altre informazioni per aiutarti a compiere analisi in tempo reale.

Espandendo la visibilità a informazioni sugli utenti, contenuti delle applicazioni, attività del sistema operativo, vulnerabilità e posizione della rete, McAfee Database Event Monitor for SIEM consente di:

- Tenere traccia degli utenti nelle varie applicazioni
- Esaminare l'attività di tutta la sessione, dall'accesso all'uscita
- Rilevare i dati sensibili e identificare le violazioni alle policy
- Individuare i dati perduti attraverso canali autorizzati
- Correlare l'attività del database agli eventi legati alla sicurezza
- Produrre una verifica di tutte le attività del database
- Generare rapporti dettagliati per gli standard PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, SOX e molti altri

Vantaggi principali

- Utilizza il monitoraggio passivo basato sulla rete per avere impatto zero sulle prestazioni del database
- Individua tutte le istanze del database, comprese quelle non autorizzate o non verificate
- Consente il monitoraggio e la registrazione degli accessi al database con informazioni regolamentate
- Conserva i dettagli di tutte le transazioni database, dall'accesso all'uscita, a supporto delle verifiche
- Semplifica l'analisi con la ricostruzione delle sessioni con un semplice clic
- Pienamente integrato con McAfee Enterprise Security Manager per abilitare le transazioni del database da usare nella correlazione degli eventi e nelle altre attività SIEM avanzate
- Opzioni di distribuzione ibride flessibili includono appliance fisiche e virtuali

intel Security

Visibilità completa su ogni transazione

McAfee Database Event Monitor for SIEM monitora tutte le transazioni del database e fornisce un percorso di verifica di tutte le attività, comprese query, risultati, attività di autenticazione e aumento dei privilegi. Dato che McAfee Database Event Monitor for SIEM mantiene i dati completi delle sessioni di tutte le transazioni, puoi facilmente vedere cosa è successo prima e dopo una determinata transazione, dall'accesso all'uscita.

Processi di conformità automatizzati

Le regole di rilevamento incorporate, basate sulle policy, e i rapporti sulla conformità garantiscono la possibilità di generare le informazioni pwe l'accesso ai dati richieste dagli standard PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, SOX e altri. In aggiunta, McAfee Database Event Monitor for SIEM si integra pienamente con McAfee Enterprise Security Manager e McAfee Enterprise Log Manager per offrire analisi e correlazione degli eventi senza paragoni, oltre alla memorizzazione conforme e al mascheramento dei dati sensibili nei log delle attività.

L'elenco delle eccezioni mostra i server dei database non monitorati, oltre alle porte non autorizzate che vengono aperte per accedere ai dati dei database.

Localizzazione di utenti e account

Con le funzioni avanzate della linea di prodotti McAfee per la gestione della sicurezza, utenti e amministratori possono essere facilmente localizzati su applicazioni e account multipli, mantenendo la responsabilità end-to-end degli utenti per le loro attività, indipendentemente da come hanno avuto accesso al database.

Profilo delle attività degli utenti

McAfee Database Event Monitor applica la tecnologia di tokenization per scomporre ogni query SQL nei comandi corrispondenti agli oggetti (tabelle, visualizzazioni, stored procedure) per i quali viene richiesto l'accesso sui server dei database, generando al contempo un profilo del comportamento di ogni utente, per rivelare sia le attività nuove che quelle anormali.

Iniezione SQL

Tutti i pacchetti delle risposte SQL vengono monitorati per conoscere l'esito positivo o negativo di ogni query. Errori di scarsa gravità come quelli sintattici, sintomatici di un attacco a iniezione SQL, vengono tracciati e messi in relazione se si verificano in successione. In tal modo i tentativi di iniezione SQL vengono tempestivamente individuati.

Rilevamento di rischi e minacce

McAfee Database Event Monitor for SIEM analizza tutte le attività monitorate rispetto a un insieme di policy personalizzabili, rilevando eventuali attività sospette per le quali genera degli allarmi. Inoltre, il rilevamento basato sulle anomalie segnala attività degli utenti, query, risposte anormali e altri comportamenti fuori luogo.

Potenza senza appesantimenti

Le appliance McAfee Database Event Monitor for SIEM, caratterizzate da un motore di raccolta dati ad alte prestazioni, monitorano il tuo database in rete senza imporre carichi su di esso e assicurando la conservazione di tutti i dati di verifica di cui necessiti.

McAfee Enterprise Security Manager gestisce e connette il monitoraggio del database con il resto dell'ecosistema di sicurezza e conformità. Per aggiungere visibilità sull'attività del terminale locale, è possibile usare un agente host opzionale che ha un impatto minore sulle prestazioni rispetto agli agenti host della concorrenza o alla verifica nativa.

Funzioni di monitoraggio del database

- Monitoraggio e registrazione di tutte le attività del database
- Supporto alla conformità
- Scoraggia le intercettazioni
- Maggiore responsabilità
- Allarmi relativi a oggetti, azioni e violazioni delle policy
- Raccolta di parametri preziosi per la gestione del livello di servizio e delle prestazioni del database
- Monitoraggio di tutte le vie di accesso ai dati, compresi:
  - Applicazioni
  - Utenti
  - Malware
  - Aziende di servizi
  - Back-door
  - Query
  - Script LAMP
  - Open Database Connectivity (ODBC)

Casi di utilizzo

Conformità

Per aiutarti a mantenere la conformità, McAfee Database Event Monitor for SIEM individua i dati sensibili in uso. Puoi monitorare tali database e stabilire un percorso di verifica dell'accesso ai dati protetti, dell'attività degli account utente e delle modifiche. Per un maggiore controllo è possibile isolare le attività di protezione dall'amministrazione del database e mascherare i dati sensibili nella registrazione del log. I report possono evidenziare i maggiori fruitori di dati protetti. I report predefiniti per le diverse normative possono essere generati in qualsiasi momento.

Rilevamento e classificazione dei database

Monitorando i comandi dei database in rete, McAfee Database Event Monitor for SIEM è in grado di rilevare tutte le istanze, comprese quelle dei database sconosciuti o maligni. Inoltre, McAfee Database Event Monitor for SIEM monitora tutte le transazioni, compresi i risultati delle query, analizzandole rispetto alle regole delle policy e ai dizionari per individuare quei database che memorizzano dati di carte di credito, codici fiscali o altri dati sensibili.

Monitoraggio della sicurezza

McAfee Database Event Monitor for SIEM monitora i tuoi database direttamente, avvisandoti in tempo reale di accessi di tipo brute-force, attacchi a iniezione SQL, andamenti anormali degli accessi, oltre a fornire altre indicazioni di possibili violazioni del server database. Puoi monitorare l'attività delle applicazioni back-end e rilevare attività sospette, compresi il recupero fraudolento di dati e gli account di utenti non identificati.

Se l'attacco ha avuto origine nella rete, puoi identificare e individuare la posizione dell'autore tracciando l'attività degli utenti e correlandola al flusso dei dati. Nel caso di un attacco esterno, la violazione può essere messa in relazione all'attività delle applicazioni e in uscita dalla rete per scoprire perdite di dati, canali di comunicazione occulti e altri vettori.

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com