McAfee Database Event Monitor for SIEM

Une visibilité sur les transactions de base de données sans incidence sur les performances

Un audit fiable des transactions de base de données est obligatoire pour assurer la conformité, mais les solutions d'audit natives traditionnelles peuvent affecter les performances des bases de données et la productivité de l'administrateur. La conception non intrusive de McAfee® Database Event Monitor for SIEM permet de prendre en charge les exigences croissantes en matière de rapports et d'audits de conformité et optimise les opérations de sécurité.

McAfee Database Event Monitor for SIEM propose une journalisation de sécurité détaillée et non intrusive des bases de données et des applications, surveillant tout accès aux données d'entreprise et clients sensibles. Avec un minimum d'efforts de déploiement, vous pouvez bénéficier d'une réelle visibilité sur les transactions de base de données, sur les événements et sur les requêtes et réponses de bases de données spécifiques, notamment les utilisateurs qui accèdent à vos données et le motif de cet accès.

McAfee Database Event Monitor for SIEM est le seul produit capable de consolider les activités liées aux bases de données dans un référentiel d'audit central et pouvant assurer la normalisation, la corrélation, l'analyse ainsi que la génération de rapports sur ces activités.

Des règles et des rapports prédéfinis, ainsi que des fonctionnalités de journalisation non préjudiciables à la confidentialité facilitent le respect des réglementations de conformité, tout en renforçant votre état de sécurisation global.

Accès à la base de données en contexte

Loin de se contenter de la journalisation, McAfee Database Event Monitor for SIEM normalise les données et met en corrélation les transactions de base de données avec d'autres informations pour vous aider à effectuer une analyse en temps réel.

En étendant la visibilité de manière à inclure les informations utilisateurs, le contenu des applications, l'activité du système d'exploitation, les vulnérabilités et même l'emplacement réseau, McAfee Database Event Monitor for SIEM offre les possibilités suivantes :

- Suivi des utilisateurs d'une application à l'autre
- Examen de l'activité d'une session dans son ensemble, de la connexion à la déconnexion
- Détection des données sensibles et identification des violations de stratégie
- Détection des pertes de données par le biais de canaux autorisés
- Corrélation de l'activité des bases de données avec les événements de sécurité
- Production d'une piste d'audit concernant toute l'activité des bases de données
- Génération de rapports détaillés pour satisfaire aux normes et réglementations PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX et SOX, entres autres

Principaux avantages

- Surveillance réseau passive pour préserver les performances des bases de données
- Découverte de toutes les instances de base de données, notamment les bases non autorisées ou non fiables
- Surveillance et journalisation de l'accès aux bases de données à l'aide d'informations réglementées
- Conservation d'informations détaillées sur l'ensemble des transactions de base de données, de la connexion à la déconnexion, pour faciliter les procédures d'audit
- Simplification de l'analyse à l'aide d'une reconstruction « en un clic » des sessions
- Intégration complète avec McAfee Enterprise Security Manager pour permettre l'utilisation des transactions de base de données dans le cadre de la corrélation des événements et d'autres activités SIEM avancées
- Options de déploiement hybrides et flexibles comprenant des appliances physiques et virtuelles

intel Security

Visibilité complète sur chaque transaction

McAfee Database Event Monitor for SIEM surveille toutes les transactions de base de données et fournit une piste d'audit complète de toutes les activités, notamment les requêtes, les résultats, les sessions d'authentification et les élévations de privilèges. Étant donné que McAfee Database Event Monitor for SIEM conserve toutes les informations de session de chaque transaction, vous pouvez facilement déterminer ce qui s'est produit avant et après une transaction donnée, de la connexion à la déconnexion.

Processus de conformité automatisés

Les règles de détection et les rapports de conformité prédéfinis, basés sur des stratégies, vous permettent de générer les informations d'accès aux données requises par les normes et réglementations PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX et SOX, entre autres. En outre, McAfee Database Event Monitor for SIEM s'intègre entièrement avec McAfee Enterprise Security Manager et McAfee Enterprise Log Manager pour bénéficier d'une analyse et d'une corrélation des événements hors pair, combinées à un stockage conforme et au masquage des données sensibles dans les journaux d'activité.

Une liste d'exceptions répertorie les serveurs de base de données non surveillés, ainsi que les ports illégaux ouverts pour permettre un accès aux données des bases.

Suivi des utilisateurs et des comptes

Grâce aux fonctionnalités avancées de la gamme de produits de gestion de la sécurité McAfee, il est facile de suivre les activités des utilisateurs et des administrateurs sur plusieurs applications et comptes, ce qui permet de déterminer avec précision les responsabilités de chacun, quel que soit le mode d'accès à la base de données.

Création de profils d'activité utilisateur

McAfee Database Event Monitor segmente chaque requête SQL en commandes — liées aux objets (tableaux, affichages, procédures stockées) accessibles sur les serveurs de base de données cibles — tout en générant un profil de chaque comportement utilisateur, divulguant ainsi toutes les activités nouvelles et anormales.

Injection de code SQL

Tous les paquets de réponses de requêtes SQL sont surveillés pour identifier les réussites et les échecs des requêtes. Les échecs sans gravité, tels que les erreurs de syntaxe, symptomatiques d'une attaque par injection de code SQL, sont suivis et corrélés s'ils se répètent, ce qui constitue un moyen fiable de détecter ce type d'attaque.

Détection des risques et des menaces

McAfee Database Event Monitor for SIEM analyse toutes les activités surveillées et les compare à un ensemble de règles de stratégie personnalisables, puis détecte et signale toute activité suspecte. Par ailleurs, une détection basée sur les anomalies signale toute activité utilisateur, requête et réponse anormales, ainsi que tout autre comportement atypique.

La puissance sans la surcharge

Doté d'un moteur de capture de données hautes performances, McAfee Database Event Monitor for SIEM surveille votre base de données sur l'ensemble du réseau, sans imposer de surcharge à la base de données elle-même et en assurant la conservation des données d'audit nécessaires.

McAfee Enterprise Security Manager assure la gestion et connecte la surveillance des bases de données au reste de votre écosystème de conformité et de sécurité. Pour assurer la visibilité sur l'activité du terminal local, vous pouvez utiliser un agent d'hôte facultatif, qui offre une incidence réduite sur les performances par rapport aux agents concurrents ou à un audit natif.

Fonctions de surveillance des bases de données

- Surveiller et journaliser toutes les activités des bases de données
- Soutenir les mesures de mise en conformité
- Prévenir l'espionnage
- Déterminer les responsabilités individuelles des utilisateurs
- Émettre des alertes concernant les objets, les actions et les violations de stratégie
- Capturer des mesures précieuses pour la gestion des performances ou des niveaux de service des bases de données
- Surveiller l'ensemble des vecteurs d'accès aux données, notamment :
  - Applications
  - Utilisateurs
  - Logiciels malveillants
  - Utilitaires
  - Portes dérobées (*backdoor*)
  - Requêtes
  - Scripts LAMP
  - ODBC (Open Database Connectivity)

Scénarios d'utilisation

Conformité

Pour vous aider à garantir la conformité, McAfee Database Event Monitor for SIEM peut identifier les données sensibles en cours d'utilisation. Vous pouvez surveiller ces bases de données et établir une piste d'audit pour l'accès aux données protégées, l'activité des comptes d'utilisateur et les modifications. Les tâches de sécurité peuvent être isolées de l'administration des bases de données pour un contrôle plus strict. Les données sensibles peuvent, par ailleurs, être masquées dans les journaux. Les rapports peuvent mettre en surbrillance les principaux utilisateurs accédant à des rapports protégés. Des rapports prédéfinis, conçus pour différentes réglementations, peuvent être générés à tout moment.

Détection et classification des bases de données

En surveillant le réseau pour identifier les commandes de base de données, McAfee Database Event Monitor for SIEM est en mesure de détecter toutes les instances de base de données, y compris les bases inconnues ou non fiables. En outre, McAfee Database Event Monitor for SIEM surveille toutes les transactions, notamment les résultats des requêtes, et les analyse en les comparant aux règles de stratégie et aux dictionnaires afin de détecter les bases de données qui contiennent des informations de carte de crédit, des numéros de sécurité sociale ou d'autres données sensibles.

Surveillance de la sécurité

McAfee Database Event Monitor for SIEM surveille vos bases de données directement et peut détecter et signaler, en temps réel, les connexions forcées, les attaques par injection de code SQL, les modèles d'accès anormaux et d'autres indices suggérant que votre serveur de base de données pourrait être compromis. Vous pouvez surveiller les applications principales et détecter les activités suspectes, notamment l'exploitation de données frauduleuses et les comptes d'utilisateur non fiables.

Si l'attaque émane du réseau, vous pouvez suivre l'activité de l'utilisateur concerné et la corréler aux données du trafic réseau pour identifier et localiser le responsable du délit. En cas d'attaque extérieure, la violation peut être corrélée aux autres activités réseau et applicatives en sortie afin de détecter les fuites de données, les canaux de communication secrets et d'autres vecteurs de compromissions.

Intel et le logo Intel sont des marques commerciales déposées d'Intel Corporation aux États-Unis et/ou dans d'autres pays. McAfee et le logo McAfee sont des marques commerciales ou des marques commerciales déposées de McAfee, Inc. ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms et marques sont la propriété de leurs détenteurs respectifs. Les plans, les spécifications et les descriptions des produits mentionnés dans le présent document sont donnés à titre indicatif uniquement. Ils peuvent être modifiés sans préavis et sont fournis sans aucune garantie, implicite ou explicite. Copyright © 2014 McAfee, Inc. 61321ds_db-event-monitor_0914

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com