McAfee Database Event Monitor for SIEM

Obtenha visibilidade das transações do banco de dados sem afetar o desempenho

A auditoria confiável das transações de banco de dados é obrigatória para a conformidade, mas as soluções convencionais nativas de auditoria de bancos de dados podem prejudicar o desempenho do banco de dados e a produtividade do administrador deste. O projeto não intrusivo do McAfee® Database Event Monitor for SIEM atende à expansão de seus requisitos de auditoria de conformidade e geração de relatórios e aprimora as operações de segurança.

O McAfee Database Event Monitor for SIEM oferece um registro de segurança detalhado e não intrusivo dos bancos de dados e aplicativos, monitorando todo o acesso aos dados confidenciais corporativos e do cliente. Com o mínimo de trabalho na distribuição, você obtém visibilidade das transações, eventos e do banco de dados, além de consultas e respostas específicas destes, inclusive quem está acessando seus dados e por quê.

O McAfee Database Event Monitor for SIEM é o único produto de sua categoria que consolida a atividade do banco de dados em um repositório central de auditoria e oferece a normalização, correlação, análise e geração de relatórios dessa atividade.

As regras e relatórios predefinidos e os recursos de registro que favorecem a privacidade facilitam o cumprimento das regulamentações de conformidade ao mesmo tempo que fortalecem sua postura de segurança geral.

Acesso contextualizado ao banco de dados

Indo muito além do registro por si só, o McAfee Database Event Monitor for SIEM normaliza os dados e correlaciona as transações do banco de dados com outras informações, para ajudá-lo a realizar uma análise em tempo real.

Com o aumento da visibilidade para incluir informações do usuário, conteúdo do aplicativo, atividade do sistema operacional, vulnerabilidades e até mesmo a localização da rede, o McAfee Database Event Monitor for SIEM possibilita:

- Rastrear os usuários nos aplicativos
- Examinar a atividade da sessão toda, desde o login até o logoff
- Detectar dados confidenciais e identificar violações de políticas
- Detectar perda de dados por meio de canais autorizados
- Correlacionar a atividade do banco de dados aos eventos de segurança
- Produzir uma trilha de auditoria de toda a atividade do banco de dados
- Gerar relatórios detalhados para PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, SOX, e muito mais

Principais vantagens

- Utiliza monitoramento passivo com base em rede para não afetar o desempenho do banco de dados
- Descobre todas as instâncias do banco de dados, inclusive bancos de dados falsos ou não autorizados
- Possibilita o monitoramento e registro do acesso aos bancos de dados com informações controladas
- Mantém os detalhes de todas as transações do banco de dados, desde o login até o logoff, para ser compatível com a auditoria
- Simplifica a análise com a reconstrução de sessões em um só clique
- Totalmente integrado ao McAfee Enterprise Security Manager para possibilitar que as transações do banco de dados sejam utilizadas na correlação de eventos e em outras atividades avançadas de SIEM
- Opções de entrega híbridas e flexíveis incluem appliances físicos e virtuais

intel Security

Visibilidade total de cada transação

O McAfee Database Event Monitor for SIEM monitora todas as transações do banco de dados e oferece uma trilha de auditoria completa de todas as atividades deste, inclusive consultas, resultados, atividades de autenticação e escaladas de privilégios. Como o McAfee Database Event Monitor for SIEM mantém detalhes completos de sessão para todas as transações, é possível ver com facilidade o que aconteceu antes e depois de uma determinada transação, desde o login até o logout.

Processos de conformidade automatizados

Regras de detecção predefinidas e com base em políticas e relatórios de conformidade garantem que você possa gerar as informações de acesso a dados exigidas pelos padrões PCI DSS, HIPAA, NERC CIP, FISMA, GLBA, GPG13, JSOX, SOX e outros. Além disso, o McAfee Database Event Monitor for SIEM é totalmente integrado ao McAfee Enterprise Security Manager e ao McAfee Enterprise Log Manager, proporcionando correlação e análise de eventos nunca antes vistas, além de armazenamento com conformidade e mascaramento de dados confidenciais em registros de atividade.

Uma lista de exceções mostra servidores de banco de dados não monitorados, bem como portas ilegais abertas para acessar dados de bancos de dados.

Rastreamento de contas e usuários

Utilizando os avançados recursos da linha de produtos de gerenciamento de segurança da McAfee, os usuários e administradores podem ser rastreados com facilidade em diversos aplicativos e contas, identificando, de fim a fim, a responsabilidade por cada atividade dos usuários, não importando como eles acessaram o banco de dados.

Determinação de perfil da atividade dos usuários

O McAfee Database Event Monitor cria tokens de cada consulta SQL em comandos: objetos (tabelas, visualizações, procedimentos armazenados) acessados nos servidores de banco de dados de destino ao gerar um perfil do comportamento de cada usuário, revelando atividades novas e atípicas.

Injeção de SQL

Todos os pacotes de respostas às consultas SQL são monitorados para verificar se a consulta obteve êxito ou apresentou falhas. Falhas de baixa gravidade, como erros de sintaxe, que são característicos de um ataque de injeção de SQL, são rastreadas e correlacionadas caso ocorram em sequência: uma forma garantida de detectar tentativas de injeção de SQL de forma proativa.

Detecção de ameaças e riscos

O McAfee Database Event Monitor for SIEM analisa todas as atividades monitoradas em comparação a um conjunto de regras de políticas personalizáveis e detecta e alerta sobre qualquer atividade suspeita. Além disso, a detecção com base em anomalias indica atividades, consultas e respostas atípicas dos usuários e outros comportamentos impróprios.

Eficiência sem sobrecarga

Com um mecanismo de captura de dados de alto desempenho, os appliances do McAfee Database Event Monitor for SIEM monitoram seu banco de dados por meio da rede, sem sobrecarregar o banco de dados e garantindo que os dados de auditoria necessários sejam mantidos.

O McAfee Enterprise Security Manager oferece gerenciamento e conecta o monitoramento de banco de dados ao restante do seu ecossistema de segurança e conformidade. Para obter visibilidade sobre a atividade de terminal local, utilize um agente de host opcional, o qual tem um impacto ao desempenho menor do que auditoria nativa ou agentes de host concorrentes.

Funções de monitoramento do banco de dados

- Monitoramento e registro de toda a atividade do banco de dados
- Compatibilidade com as iniciativas de conformidade
- Repressão de espionagem
- Aumento da apuração de responsabilidades
- Alertas sobre objetos, ações e violações de políticas
- Captura de parâmetros valiosos para o nível de serviço do banco de dados/gerenciamento de desempenho
- Monitoramento de todos os caminhos de dados, inclusive:
  - Aplicativos
  - Usuários
  - Malware
  - Utilitários
  - Backdoors
  - Consultas
  - Scripts LAMP
  - ODBC (Open Database Connectivity)

Casos de uso

Conformidade

Para ajudar a garantir a conformidade, o McAfee Database Event Monitor for SIEM pode descobrir os dados confidenciais em uso. É possível monitorar esses bancos de dados e estabelecer uma trilha de auditoria para acesso a dados protegidos, atividade da conta de usuário e alterações. As funções de segurança podem ser separadas da administração do banco de dados para obter um controle mais rígido, e é possível mascarar os dados confidenciais nos registros. Os relatórios podem destacar os principais consumidores de registros protegidos. É possível gerar relatórios predefinidos para regulamentos diferentes a qualquer momento.

Detecção e classificação do banco de dados

Com o monitoramento da rede em busca de comandos do banco de dados, o McAfee Database Event Monitor for SIEM consegue detectar todas as instâncias de banco de dados, inclusive dos desconhecidos ou não autorizados. Além disso, o McAfee Database Event Monitor for SIEM monitora todas as transações, inclusive resultados de consultas, e as analisa em relação a dicionários e regras de políticas para detectar quais bancos de dados armazenam números de cartões de crédito, CPF ou outros dados confidenciais.

Monitoramento de segurança

O McAfee Database Event Monitor for SIEM monitora seus bancos de dados diretamente e pode detectar e enviar alertas em tempo real sobre logins de força bruta, ataques de injeção de SQL, padrões de acesso atípicos e outros indícios de que o seu banco de dados possa ter sido violado. É possível monitorar a atividade dos aplicativos back-end e detectar atividades suspeitas, inclusive recuperação de dados fraudulentos e contas de usuários não autorizados.

Caso o ataque venha de dentro da rede, você poderá rastrear a atividade dos usuários e correlacionar com os dados do fluxo de rede para identificar e localizar o infrator. Em caso de ataques externos, a violação pode ser correlacionada com outra atividade de saída da rede ou de aplicativos para descobrir perda de dados, canais de comunicação ocultos e outros vetores de perda.

61321ds_db-event-monitor_0914

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com