McAfee Database Event Monitor for SIEM

Максимальный визуальный контроль за транзакциями в базах данных без ущерба для быстродействия

Надежный контроль за транзакциями в базах данных является обязательным условием обеспечения нормативно-правового соответствия, однако проведение аудитов с помощью встроенных в базы данных традиционных решений может ограничить производительность баз данных и снизить эффективность работы их администраторов. Не оказывающее влияния на работу системы решение McAfee® Database Event Monitor for SIEM обеспечивает поддержку ваших растущих требований к проведению аудиторских проверок нормативно-правового соответствия и формированию отчетов, а также повышает уровень эффективности операций по обеспечению безопасности.

McAfee Database Event Monitor for SIEM обеспечивает неинтрузивную детальную регистрацию в журнале безопасности всех действий с базами данных и приложениями, осуществляя мониторинг доступа к конфиденциальной корпоративной информации и данным клиентов. Затратив минимальные усилия на развертывание, вы сможете отслеживать транзакции и события в базах данных, а также конкретные запросы и полученные ответы, включая информацию о том, кто и почему получил доступ к вашим данным.

McAfee Database Event Monitor for SIEM — единственный в своем роде продукт, обеспечивающий как сбор информации о всех действиях с базами данных в централизованном репозитории аудита, так и нормализацию, сопоставление, анализ и формирование отчетов о таких действиях.

Готовые правила и типовые отчеты, а также функции регистрации событий с соблюдением требований конфиденциальности облегчают обеспечение нормативно-правового соответствия и повышают общий уровень безопасности вашей компании.

Доступ к базам данных в контексте

Помимо регистрации транзакций в журнале событий McAfee Database Event Monitor for SIEM также осуществляет нормализацию данных и сопоставление транзакций с прочей информацией, что помогает вам проводить анализ данных в режиме реального времени.

Расширяя объем собираемой информации за счет включения информации о пользователях, содержимом приложений, активности операционных систем, уязвимостях и даже о сетевом расположении, McAfee Database Event Monitor for SIEM позволяет вам:

- отслеживать пользователей по всем приложениям;
- изучать все действия во время сеанса приложения с момента входа в систему и до момента выхода из нее;
- обнаруживать конфиденциальные данные и выявлять нарушения политик;
- обнаруживать утечки данных по санкционированным каналам;
- сопоставлять действия с базами данных с событиями безопасности;

Ключевые преимущества

- Использование пассивного сетевого мониторинга, гарантирующее полное отсутствие негативного влияния на производительность баз данных
- Обнаружение всех экземпляров баз данных, включая несанкционированные и мошеннические
- Контроль и регистрация в журнале событий случаев доступа к базам данных, информация в которых подлежит нормативно-правовому регулированию
- Поддержка аудитов благодаря сохранению подробной информации обо всех транзакциях в базах данных с момента входа в систему и до момента выхода из нее
- Упрощенный анализ благодаря функции воспроизведения сеансов «одним щелчком мыши»

intel Security

- создавать журнал аудита всех действий с базами данных;
- генерировать подробные отчеты о соответствии требованиям стандартов PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, SOX и многих других.

Сбор всей информации о каждой транзакции

McAfee Database Event Monitor for SIEM выполняет мониторинг всех транзакций в базах данных и ведет подробный журнал аудита всех действий с базами данных, включая запросы, результаты, действия по аутентификации и случаи повышения привилегий. Поскольку McAfee Database Event Monitor for SIEM сохраняет всю информацию о сеансе для всех транзакций, вы можете легко посмотреть, что случилось до и после любой интересующей вас транзакции с момента входа в систему и до момента выхода из нее.

Автоматизированное обеспечение нормативно-правового соответствия

Благодаря наличию готовых правил обнаружения транзакций на основе политик и наличию типовых отчетов о нормативно-правовом соответствии McAfee Database Event Monitor for SIEM дает вам возможность генерировать информацию о доступе к данным в соответствии с требованиями стандартов PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX, SOX и др. Кроме того, McAfee Database Event Monitor for SIEM полностью интегрируется с решениями McAfee Enterprise Security Manager и McAfee Enterprise Log Manager, что позволяет обеспечить непревзойденный уровень анализа и сопоставления событий в дополнение к хранению и маскированию конфиденциальных данных в журналах активности в соответствии с нормативно-правовыми требованиями.

Список исключений отображает серверы баз данных, не находящиеся под наблюдением, а также несанкционированные порты, открытые для доступа к данным из баз данных.

Отслеживание пользователей и учетных записей

Расширенные возможности линейки продуктов McAfee для управления безопасностью позволяют легко отслеживать пользователей и администраторов в большом количестве разных приложений и учетных записей, обеспечивая тем самым полную индивидуальную ответственность каждого пользователя за все свои действия независимо от того, каким образом он получил доступ к базе данных.

Создание профилей активности пользователей

McAfee Database Event Monitor помечает соответствующие каждому SQL-запросу команды и объекты (таблицы, представления, сохраненные процедуры), доступ к которым был получен на целевом сервере баз данных, и составляет профиль поведения каждого пользователя, что позволяет обнаруживать как новые, так и аномальные действия пользователей.

Внедрение SQL-кода

Все пакеты ответов на SQL-запросы проверяются на предмет того, был запрос успешным или нет. Ошибки низкой степени тяжести, такие как синтаксические ошибки, характерные для атак с внедрением SQL-кода, отслеживаются и сопоставляются друг с другом в том случае, если они происходят последовательно одна за другой. Это надежный способ упреждающего обнаружения попыток атак с внедрением SQL-кода.

Обнаружение рисков и угроз

McAfee Database Event Monitor for SIEM анализирует все наблюдаемые действия на предмет соответствия заданному пользователем набору правил, обнаруживает все подозрительные действия и оповещает о них. Кроме того, функция обнаружения аномального поведения позволяет выявлять аномальную деятельность пользователей, аномальные запросы, аномальные ответы и прочие ненадлежащие действия.

Ключевые преимущества (продолжение)

- Полная интеграция с решением McAfee Enterprise Security Manager, позволяющая использовать транзакции в базах данных для сопоставления событий и реализации других сложных функций SIEM
- Наличие смешанных вариантов поставки с использованием физических и виртуальных устройств

Функции мониторинга баз данных

- Мониторинг и регистрация всех действий в базах данных
- Поддержка процессов обеспечения нормативно-правового соответствия
- Предотвращение перехвата данных
- Повышение уровня подотчетности
- Уведомления об объектах, действиях и нарушениях политик
- Сбор показателей, необходимых для управления уровнем обслуживания и производительностью баз данных
- Мониторинг всех каналов доступа к данным, включая:
  - приложения;
  - пользователей;
  - вредоносные программы;
  - служебные программы;
  - бэкдоры;
  - запросы;
  - скрипты LAMP;
  - интерфейс Open Database Connectivity (ODBC).

Производительность без дополнительной нагрузки

Аппаратные устройства McAfee Database Event Monitor for SIEM, включающие в себя высокопроизводительный модуль для сбора данных, осуществляют мониторинг вашей базы данных через сеть, не влияя на производительность самой базы данных и гарантируя сохранение всей требуемой для аудита информации.

McAfee Enterprise Security Manager обеспечивает управление и интегрирует мониторинг баз данных в вашу целостную систему обеспечения безопасности и нормативно-правового соответствия. Для сбора информации о действиях локальных терминалов предлагаем дополнительно использовать агент узла, который меньше влияет на производительность системы, чем агенты узлов других поставщиков и встроенные службы аудита.

Примеры использования

Соответствие требованиям

McAfee Database Event Monitor for SIEM способен обнаруживать используемые конфиденциальные данные, что помогает в обеспечении нормативно-правового соответствия. Вы можете осуществлять мониторинг баз данных с конфиденциальными данными и вести журнал аудита для отслеживания доступа к защищенным данным, активности учетных записей пользователей и вносимых изменений. В целях усиления контроля обязанности по обеспечению безопасности могут быть отделены от администрирования баз данных, а записи о конфиденциальных данных в журнале могут быть замаскированы. В отчеты можно включить информацию о наиболее активных «потребителях» защищенной информации. При необходимости имеется возможность генерировать типовые отчеты, соответствующие разным нормативам.

Обнаружение и классификация баз данных

Осуществляя мониторинг сети и отслеживая команды баз данных, McAfee Database Event Monitor for SIEM способен обнаруживать все экземпляры баз данных, включая несанкционированные и мошеннические базы данных. Кроме того, McAfee Database Event Monitor for SIEM выполняет мониторинг всех транзакций, включая результаты запросов, и анализирует их на предмет соответствия правилам политик и словарям с целью обнаружения баз данных, содержащих информацию о кредитных картах, паспортные данные и прочую конфиденциальную информацию.

Защитный мониторинг

McAfee Database Event Monitor for SIEM осуществляет непосредственный мониторинг ваших баз данных и способен в режиме реального времени обнаруживать попытки взлома методом полного перебора пароля, атаки с внедрением SQL-кода, аномальные случаи доступа и другие признаки возможного взлома вашего сервера баз данных и сразу оповещать вас об этом. Вы можете осуществлять мониторинг приложений для управления базами данных и обнаруживать подозрительные действия, включая хищение данных и использование нелегальных учетных записей.

Если источник атаки находится внутри сети, то вы можете проследить поведение пользователей и сопоставить его с данными о сетевых потоках, что позволит идентифицировать злоумышленника и определить его местоположение. В случае атаки извне нарушение может быть сопоставлено с прочими действиями в исходящем трафике сети и приложений, что даст возможность обнаружить источник утечки данных, скрытые каналы связи и другие причины утери информации.

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com