McAfee Enterprise Security Manager

McAfee Enterprise Security Manager — это решение для управления информацией о безопасности и событиями безопасности (Security Information and Event Management — SIEM), обеспечивающее сбор информации об угрозах и интеграцию средств защиты с целью приоритизации, расследования и устранения угроз.

В основе SIEM-системы от McAfee лежит решение Enterprise Security Manager, которое осуществляет сбор, корреляцию, оценку и распределение приоритетов событий безопасности. Являясь частью архитектуры Security Connected, решение McAfee Enterprise Security Manager тесно интегрировано с программным обеспечением McAfee ePolicy Orchestrator (McAfee ePO), решением McAfee Risk Advisor, и технологией Global Threat Intelligence, обеспечивая контекст, необходимый для автономного и гибкого управления угрозами безопасности.

Состав и возможности решения:

- McAfee Enterprise Security Manager.
- Технология McAfee Global Threat Intelligence for Enterprise Security Manager (ESM), предназначенная для работы с «большими данными в сфере безопасности», позволяет использовать результаты работы McAfee Labs непосредственно для мониторинга безопасности.
- McAfee Enterprise Log Manager автоматизирует управление всеми типами журналов и их анализ, включая журналы событий Windows, журналы баз данных, журналы приложений и системные журналы (Syslogs).
- McAfee Advanced Correlation Engine выполняет мониторинг данных в режиме реального времени, позволяя одновременно использовать системы корреляции событий как основанные на правилах, так и не использующие правил с целью обнаружения рисков и угроз до их возникновения.
- McAfee Application Data Monitor выполняет дешифрование полного сеанса приложения до Уровня 7, обеспечивая комплексный анализ всей информации — от используемых протоколов и целостности сеанса до непосредственного содержимого приложения, такого как текст электронного письма или вложений к нему.
- McAfee Database Event Monitor for SIEM обеспечивает детальную регистрацию в журнале безопасности транзакций в базах данных.
- McAfee Event Receiver собирает данные событий и журналов сторонних поставщиков.

Наши контактные данные:

ул. Ленина, д.20, (четвертый этаж), каб. 422, 423. Остановка "Яблонька".
e-mail: info@ooo-skb.ru(ссылка для отправки email)
тел. 53-20-18