EMC
GROUP OF COMPANIES
EUROPEAN MEDICAL CENTER

JSC "European Medical Center"
АО «Европейский Медицинский Центр»
35, ul. Schepkina, Moscow, Russia, 129110
129110, Россия, Москва, ул. Щепкина, 35

Tel./тел.: +7 (495) 933 66 55
www.emcmos.ru
ОГРН 1027739031418

Генеральному директору ООО «РуСИЕМ»
Воронину Роману Александровичу

Благодарственное письмо

«Европейский медицинский центр» благодарит команду RuSIEM за качественную и эффективную помощь при внедрении SIEM-системы RuSIEM в инфраструктуру нашей организации. Как ведущая частная клиника в России, мы стремимся не только оказывать качественную и эффективную помощь нашим пациентам, но и надежно защитить их персональные данные и чувствительную информацию. Внедрение RuSIEM стало важным этапом на этом пути.

Проект внедрения системы стартовал в 2023 году с пилотного тестирования, в рамках которого SIEM-система была развернута в выделенной части нашей инфраструктуры.

После тестирования и рекомендаций специалистов к системе были подключены основные источники данных, а также написаны правила корреляции, которые отражают специфику защиты информации о пациентах и их конфиденциальных данных. К ним, например, относится многократное открытие сотрудником электронной медицинской карты пациента, который не записан на прием.

SIEM-система RuSIEM была задействована в отслеживании аномальной активности и выявлении попыток злоумышленников получить доступ к данным с помощью фишинговых писем. Функционал решения позволяет установить адрес отправителей писем и их жертв. Таким образом, специалисты информационной безопасности клиники могут предупреждать сотрудников о вредоносной рассылке.

В наших планах дальнейшее расширение возможностей по защите данных. В настоящий момент мы используем модуль RuSIEM Analytics для расширенного обнаружения угроз и поведенческих аномалий, а также тестируем модуль для обогащения системы данными об индикаторах компрометации RuSIEM IoC.

Директор по экономической
и информационной безопасности
АО «Европейский медицинский центр»

Братухин Андрей Валерьевич