Анализ событий информационной безопасности с использованием правил обнаружения и корреляции в системах SIEM — основной метод выявления вредоносной активности в ИТ инфраструктуре. Однако этот подход не всегда эффективен из-за разнообразия методов атак, для которых сложно создать всеобъемлющие правила.

Компания Angara Security разработала инновационное решение на основе нейронной сети, которое интегрируется с SIEM. Эта сеть включает комбинированные слои, типичные как для свёрточных, так и для рекуррентных нейронных сетей. Решение было признано лучшим в категории «Разработка года» по информационной безопасности на Digital Leaders Award 2024.

Angara Security предлагает ML-модель, которая дополняет традиционные методы анализа событий и точно выявляет вредоносную активность по уникальным паттернам. Этот подход расширяет возможности обнаружения и устраняет необходимость в создании новых правил для каждой новой угрозы.

ML-модель применяется для трёх ключевых сценариев: обнаружение PowerShell-скриптов, выявление DGA-доменов и анализ журналов веб-серверов. Она позволяет автоматизировать процессы и сфокусировать ресурсы аналитиков на более сложных задачах, таких как обработка миллионов скриптов и DNS-запросов.