СЛОЖНОСТИ ЭКСПЛУАТАЦИИ SIEM-СИСТЕМ ПРИ ОБРАБОТКЕ БОЛЬШОГО ОБЪЕМА СОБЫТИЙ БЕЗОПАСНОСТИ

С.Н. Петров, Г.С. Смотрук

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В современной информационной среде, на фоне возрастающей сложности киберугроз, системы управления событиями и информационной безопасности (SIEM) выступают в роли ключевого инструмента обеспечения целостности и защиты информационных активов организаций. Несмотря на их важность, SIEM системы

сталкиваются с комплексом системных вызовов, которые требуют непрерывного внимания и усовершенствования.

Одной из основных проблем, является необходимость эффективной обработки и анализа огромного объема событий. В современных организациях, где сотни и тысячи устройств и приложений генерируют большое количество данных о событиях безопасности, SIEM системы должны оперативно обрабатывать эти данные для обнаружения и реагирования на угрозы в реальном времени. Однако, высокая скорость поступления информации, в сочетании с ограниченными ресурсами вычислительной мощности и хранилища данных, создает серьезные препятствия для SIEM. Это может привести к ситуации, когда система не успевает обработать все поступающие события в реальном времени, что в свою очередь может привести к упущению важных угроз или задержке их обнаружения.

Еще одной серьезной проблемой является неэффективная интеграция и корреляция данных из различных источников безопасности. Поскольку информация о безопасности формируется из множества источников, включая журналы событий операционных систем, логи сетевых устройств, журналы приложений, системы обнаружения и предотвращения вторжений и многих других, SIEM системы должны успешно интегрировать данные из всех этих источников и анализировать их в единой системе для выявления угроз и реагирования на них. Недостаточная интеграция и корреляция данных приводит к ложным срабатываниям, что в свою очередь, к избыточной нагрузке на персонал по их обработке и, в конечном итоге, к игнорированию реальных угроз.

Решение данных проблем требует комплексного подхода, включающего в себя применение передовых технологий анализа данных, таких как машинное обучение и искусственный интеллект, оптимизацию инфраструктуры и ресурсов. Для эффективного функционирования SIEM необходимо постоянное совершенствование алгоритмов анализа данных, улучшение интеграции с различными источниками информации и повышение гибкости системы. Только таким образом можно обеспечить эффективное функционирование SIEM систем и надежную защиту информационных активов организаций в условиях постоянно меняющихся угроз.