УДК 004.042

РАЗРАБОТКА ПОДХОДА К ПРЕДКОРРЕЛЯЦИОННОЙ ОБРАБОТКЕ СОБЫТИЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В ЦЕЛЯХ ОПТИМИЗАЦИИ ПРОЦЕССА КОРРЕЛЯЦИИ В SIEM-СИСТЕМАХ

Ермилов А.К. (Университет ИТМО)**, Кучукян А.Р.** (Университет ИТМО)
Научный руководитель – д.т.н., доцент Лившиц И.И.
(Университет ИТМО»)

Проводимая перед произведением автоматической корреляции обработка исходных событий информационной безопасности, поступающих на вход SIEM-систем, является важнейшим этапом жизненного цикла информации в процессе её автоматического анализа. Отдельно в данном этапе можно выделить процессы непосредственного получения событий, их нормализации, категоризации и обогащения. Авторами разработан подход, позволяющий оптимизировать процессы пред-корреляционной обработки в SIEM с целью снижения общего количества корреляционных правил, необходимых для обработки потока событий, и увеличения их производительности.

Цель работы заключается в исследовании жизненного цикла событий внутри SIEM-системы, а также рассмотрении последовательности действий, необходимых для пред-корреляционной обработки событий в SIEM-системе, делающих возможным автоматический анализ состояния инфраструктуры в контексте совершаемых в ней компьютерных атак. Ввиду отсутствия единого общепринятого формата описания событий безопасности, применяемых различными производителями конечных устройств, особенно остро встаёт вопрос корректной пред-корреляционной обработки.

Для приведения событий информационной безопасности в вид, допускающий автоматическую обработку средствами SIEM-системы, необходимо произвести нормализацию, категоризацию и обогащение событий, реализация которых в совокупности делает возможным применение автоматического корреляционного анализа событий вне зависимости от исходного формата сообщений, используемого производителем устройства-источника данных.

На основе проведённого анализа процессов корреляционной обработки в SIEM-системах разработан подход к единообразной нормализации событий, а также предложен перечень полей категорий, необходимых для возможности корректного сопоставления событий устройств различных производителей в ходе корреляционного анализа.