Практическая работа 3. Выявление сложных многошаговых атак (APT - Advanced Persistent Threats)

Цель работы: Атаки APT могут длиться часами и днями, включать множество этапов (сканирование → фишинг → привилегии → эксфильтрация). Нужно обучить модель распознавать шаблоны APT на основе временной последовательности действий/событий.

Попробуем сделать без теории и я оставлю это на самостоятельное обучение, данные датасетов можете подобрать на основе логов из SIEM-систем, Windows Event Logs, MITRE ATT&CK события.

Мы как всегда делаем:

1. Очистку данных(какие именно вы возьмете, например логи), группировку событий по пользователю/хосту/сессии.
2. Кодирование действий: преобразуем в категориальные индексы или one-hot.
3. Строим модель с использованием LSTM или GRU.
4. Обучение и тестирование: разделение на обучающую и валидационную выборку, использование классов на “нормальное поведение” или “APT-атака”
5. Используем анализ, показываем примеры ложноположительных/ложноотрицательных сессий, визуализация ошибок.
6. Строим multi-label(для предсказаний этапов атаки) и timeline-heatmap(для действий атакующего)