

Программа курса ArcSight SOAR Standard

День 1 (6 учебных часов)

1. Введение в курс
2. Настройка Alert Source и Integrations в SOAR. Credentials и Parameters.
3. Создание и структура инцидента (Case) в ArcSight SOAR. Обогащение и выполнение стандартных скриптов для анализа инцидента. Управление инцидентом: эскалация, изменение стадии, добавление связанных инцидентов и т.д.
4. Плейбуки (Playbooks) в ArcSight SOAR, настройка свойств, Enrichments, Actions, Automation Bits. Создание плейбуков их тестирование, проверка статуса и очереди.

День 2 (6 учебных часов)

4. Написание собственных плагинов и Automation Bits. Разбор внутреннего API SOAR, библиотека конфигураций и плагинов (Configuration).
5. Пример разработки Automation Bits и плагина для выполнения действий через REST API ArcSight ESM (не дефолтный плагин). Разработка Enrichment для Arcsight ESM. Разработка плагина и Automation Bit для Telegram.

День 3 (6 учебных часов)

6. Плейбуки по расписанию (Sheduled Playbooks), списки (Lists), триггеры и Analyst Tasks.
7. Изменение шаблонов сообщений, нотификация. Добавление новых свойств для кейсов (Statuses, Severities, Types, Labels).
8. Дополнительные функции. Сессия вопросов и ответов.