

Программа курса ArcSight ESM Analyst Extended

День 1

1. Введение в курс
2. Файлы (Files), база знаний в ESM. (Теория, практика)
3. Категоризация в ESM. Мар-файлы в коннекторах. (Теория, практика)

День 2

4. Продвинутое использование функций и переменных, Velocity Templates (VTL). (Теория, практика)
5. Автоматизация в правилах, управление коннекторами, выполнение через CounterACT коннектор. (Теория, практика)

День 3

6. Интеграционные команды (Integration Commands). (Теория, практика)
7. Написание своих собственных инструментов для консоли (Tools). (Практика)

День 4

8. SOAR, плейбуки, работа с инцидентами и интеграция процессов. (Теория, практика)
9. ArcSight Logger, поиск событий, создание отчётов. (Теория, практика)

День 5

10. Разработка ресурсов под Use Cases, аналитика, расследование, автоматизация, проведение по процессу. (Практика)
11. Ответы на дополнительные вопросы, создание нескольких кейсов для системы Заказчика. (Практика)