

Программа курса ArcSight ESM Admin Extended

День 1

1. Введение в курс.
2. ArcSight Flex Connector, назначение, виды флексов. Общая структура конфигурации флекса (Теория)
3. Работа с простейшим флексом — Log File Fixed Format. (Практика)
4. Основы Regex. Создание конфигурации для Regex File Connector. (Теория, практика)

День 2

5. Разработка конфигурации для Syslog Flex Connector, использование QuickFlex. (Практика)
6. Разработка конфигурации для нестандартного журнала событий Windows. (Практика)

День 3

7. Введение в SQL. Инструменты для построения и проверки SQL, DBFlex. (Теория)
8. Разработка конфигурации для ID-Based Database Connector. (Практика)
9. Разработка конфигурации для Time-Based Database Connector. (Практика)

День 4

10. Установка SOAR, Forwarding Connector, интеграция ESM и SOAR. (Практика)

День 5

11. ArcSight CounterACT Connector, конфигурация, разработка скриптов, применение. Введение в Python. (Теория, практика)

Дополнительно при наличии времени может быть разработана 1-2 конфигурации флекса коннектора из окружения Заказчика