

Программа курса ArcSight ESM Analyst Basic

День 1

1. Введение в курс
2. Обзор консоли ArcSight. Активные каналы (Active Channels), фильтры и наборы полей (Field Sets). (Теория, практика)

День 2

3. Корреляция в ESM, правила (Rules). Использование функций и переменных. Активные листы (Active Lists), сессионные листы (Session Lists). (Теория, практика)

День 3

4. Инструментальные панели (Dashboards) и мониторы данных (Data Monitors). (Теория, практика)
5. Управление инцидентами в ESM. Работа с кейсами (Cases). (Теория, практика)
6. Оповещения в ESM. (Теория, практика)

День 4

7. Запросы (Queries), отчёты (Reports), панели запросов (Query Viewers), тренды (Trends). (Теория, практика)
8. Активы (Assets) и сетевая модель. (Теория, практика)
9. Пакеты в ArcSight (Packages). Установка стандартных пакетов из Marketplace и создание собственных пакетов. (Теория, практика)

День 5

10. ArcSight Command Center (ACC). Поиск событий в ACC (Event Search). (Теория, практика)
11. Управление доступом в ArcSight ESM. Пользователи (Users), ACL. (Теория, практика)
12. Пример типового кейса с последующими анализом, разработкой ресурсов, оповещением, расследованием инцидента и заведением кейса в формате SOC. (Практика)