Бауманский учебный центр «Специалист»

Программа курса KL 051.4: Kaspersky Unified Monitoring and Analysis Platform. Investigation (Поиск угроз и реагирование на инциденты ИБ для специалистов ИБ)

Код курса: **КЛ051**

Тема	Ак. часов
Модуль 1. Введение	**1**
Модуль 2. Сбор событий	**3**
Модуль 3. Работа с активами	**3**
Модуль 4. Поиск событий	**3**
Модуль 5. Корреляция	**3**
Модуль 6. AI	**2**
Модуль 7. Реагирование	**3**
Модуль 8. Панели мониторинга и отчеты	**2**
Модуль 9. Лабораторные работы • **Лабораторная работа 1.** Активация KUMA. • **Лабораторная работа 2.** Нормализация событий нового источника. • **Лабораторная работа 3.** Нормализация событий еще одного нового источника. • **Лабораторная работа 4.** Настройка обогащения событий. • **Лабораторная работа 5.** Сбор данных и эксфильтрация, установка C&C туннеля. • **Лабораторная работа 6.** Сбор данных о системе, использование стеганографии, эксфильтрация данных. • **Лабораторная работа 7.** Kerberoasting, эксфильтрация данных через HTTP GET. • **Лабораторная работа 8.** Атака Pass-the-hash, эксфильтрация данных через ssh. • **Лабораторная работа 9.** Атака HTA. • **Лабораторная работа 10.** Shadow session и Dll hijacking. • **Лабораторная работа 11.** Закрепление в системе. • **Лабораторная работа 12.** Самостоятельное задание. • **Лабораторная работа 13.** Отображение текущего состояния.	
Аудиторная нагрузка в классе с преподавателем	**20 ак.ч. + 20 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru