Бауманский учебный центр «Специалист»

Программа курса Мониторинг и реагирование на инциденты ИБ с использованием SIEM

Код курса: **СИЕМ**

Тема	Ак. часов
Модуль 1. Введение и основные инструменты • Назначение и задачи мониторинга информационной безопасности. • Основные процессы SOC. • Понятие события и инцидента ИБ. • Роль SIEM в выявлении подозрительной активности.	**3**
Модуль 2. Развёртывание SIEM • Основные компоненты SIEM. • Подготовка виртуальной среды. • Развёртывание системы. • Первоначальная настройка и проверка работоспособности.	**3**
Модуль 3. Сбор и анализ событий • Источники событий информационной безопасности. • Организация централизованного сбора журналов. • Просмотр и анализ событий. • Выявление признаков подозрительной активности.	**3**
Модуль 4. Разработка правил корреляции • Назначение правил корреляции. • Определение условий обнаружения подозрительной активности. • Создание и проверка правил корреляции.	**3**
Модуль 5. Работа с инцидентами • Выявление потенциальных инцидентов. • Анализ связанных событий. • Первичная оценка инцидентов. • Определение дальнейших действий.	**4**
Модуль 6. Составление карт реагирования на инциденты • Назначение и структура карт реагирования. • Описание последовательности действий при обнаружении инцидента. • Разработка карты реагирования.	**4**
Модуль 7. Построение SOC Основные элементы и функции SOC. • Основные элементы и функции SOC. • Организация процессов мониторинга и реагирования. • Роли специалистов и взаимодействие при обработке инцидентов.	**4**
Аудиторная нагрузка в классе с преподавателем	**24 ак.ч. + 24 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	Для организаций	E-mail
+7 (495) 232-32-16	**+7 (495) 780-48-44**	**info@specialist.ru**