**«Администратор Программного Комплекса Efros Defense Operations. Модуль Vulnerability Control»**

**Цель обучения:** приобретение теоретических знаний в области защиты информации в части применения программного комплекса программного комплекса Efros Defense Operations (ПК EDO) на уровне администратора комплекса, изучение функциональных возможностей компонентов комплекса ПК EDO, а также практических навыков: установка, настройка сервисов добавление объектов защиты и устройств, создание отчетов, получение навыков работы с модулем «Анализа уязвимостей и построения векторов атак (VC)».

**Для кого этот курс?**

- начальники отделов и специалисты служб безопасности (информационной безопасности);

- руководители и сотрудники отделов автоматизации, вычислительных центров, информационно-технических отделов;

- руководители и сотрудники специализированных подразделений по защите конфиденциальной информации;

- администраторы безопасности компьютерных сетей.

**Профессиональный стандарт**: 06.032 Специалист по безопасности компьютерных систем и сетей 14.09.2022

**Срок обучения:**16 академических часов (2 учебных дня)

**Формат**: очный/дистанционный, с отрывом от работы.

**Режим занятий**: 8 академических часов в день

**Структура курса**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №№п.п. | Наименование разделов и тем | Всего часов | В том числе | Форма контроля |
|  |  |  | Лекции | Практ. занятия |  |
| **1** | **Назначение и структура программного комплекса Efros Defense Operations (ПК EDO).** | **2** | **2** |  | **Контр.вопросы** |
| 1.1. | Назначение ПК EDO, основные возможности и преимущества. Структура ПК EDO, функциональные модули, микросервисы. Политика лицензирования | 1 | 1 |  |  |
| 1.2. | Подготовка к установке, предварительные требования. Виды дистрибутивов. | 1 | 1 |  |  |
| **2.** | **Установка и удаление ПК EDO. Настройка и администрирование.** | **6** | **2** | **4** | **Контр.вопросы** |
| 2.1. | Установка и первоначальная настройка серверной части ПК EDO на ОС Astra Linux. Использование скриптов, работа с контейнерами Docker.Ознакомление с необходимыми командами для удаления ПК EDO | 2 | 1 | 1 |  |
| 2.2. | Начало работы. Знакомство с веб-интерфейсом, активация лицензии | 1 | 1 |  |  |
| 2.3. | Раздел «Администрирование» (управление учетными записями (УЗ) пользователей, назначение ролей, привилегий; создание групп пользователей; использование настроек безопасности УЗ и парольной политики; предустановленные задачи; настройка оповещений; использование сертификатов)Раздел «Настройки» (управление сроками и объёмом хранения данных, событий и потокам данных способах; интеграции с почтовым сервером (SMTP, Microsoft Exchange); настройка параметров отправки почтовых сообщений; сервер DNS как источник данных для базы знаний; загрузка модулей, обновления, включения/отключения) | 1 |  | 1 |  |
| 2.4. | Раздел «Объекты сети» (отображение, создание, редактирование, удаление объектов защиты (ОЗ), добавление возможностей; подразделы База знаний, Сканирование; использование автоматизированной возможности формирования списка подключенных устройств.Раздел «Мониторинг» (использование виджетов для отображения информации о метриках комплекса – работа с вкладками, создание, настройка виджетов).Раздел «События» (типы событий; работа с событиями, связанными с действиями пользователя при работе с комплексом – фильтрация, экспорт, классы и типы событий; работа со списком событий безопасности, полученных от ОЗ – фильтрация, экспорт, типы событий, важность; экспорт событий) | 2 |  | 2 |  |
| **3.** | **Модуль Vulnerability Control (VC). Анализ уязвимостей и построение векторов атак.** | **6** | **2** | **4** | **Контр.вопросы** |
| 3.1. | Начало работы. Типы устройств и виды контроля; принцип разделения и настройки модулей; формирование списка устройств; активация различных типов контроля. | 1 | 1 |  |  |
| 3.2. | Уязвимости устройств. Настройка подключения к базе данных уязвимостей; формат записи уязвимостей, ссылки на источники; демонстрация БДУ и возможностей работы из раздела БДУ; добавление расписания для загрузки отчетов (уязвимости), демонстрация вариантов настройки расписания. | 2 | 1 | 1 |  |
| 3.3. | Сканеры уязвимостей. Типы сканеров; способы получения данным от сканеров; отличие от уязвимостей, полученных из БДУ; База знаний. | 1 |  | 1 |  |
| 3.4. | Карта сети. Формирование карты сети; поддерживаемые устройства для отображения (АСО, МЭ, СВТ и др.); настройка зон видимости, использование фильтров; построение маршрутов, анализ результатов | 1 |  | 1 |  |
| 3.5. | Векторы атак и модель нарушителя. Механизм построения векторов атак; механизм работы модели нарушителя, отличие от обычного построения вектора; логика расчёта вероятности компрометации узла; планировщик задач, настройка оповещений | 1 |  | 1 |  |
|  | **Всего:** | **14** | **6** | **8** |  |
|  | **Итоговый контроль знаний** | **2** |  | **2** | **Итоговая аттестация: тестирование** |
|  | **Итого:** | **16** | **6** | **10** |  |