**«Администрирование программного комплекса Efros Defense Operations. Модуль Integrity Check Compliance (ICC)»**

**Цель обучения:** получение теоретических знаний и практических навыков администрирования программного комплекса Efros Defense Operations (ПК EDO), включая установку, настройку сервисов, добавление объектов защиты и работу с модулем «Контроль целостности и проверки соответствия (ICC)».

**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)

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

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

**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** |  | **Мини-тесты** |
| 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** | **Мини-тесты** |
| 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 Integrity Check Compliance (ICC). Контроль целостности и проверки соответствия.** | **6** | **2** | **4** | **Мини-тесты** |
| 3.1. | Начало работы. Типы устройств и виды контроля; формирование списка устройств; настройка контроля; настройка фильтров и исключений; планировщик задач; настройка оповещений; добавление расписания. | 1 | 1 |  |  |
| 3.2. | Контроль изменений. Изменение конфигурации устройства; фиксирование изменения; демонстрация оповещений; архив | 1 | 1 |  |  |
| 3.3. | Windows-агент, установка и настройка, механизм работы; создание пользовательских отчётов для КЦ; портативные агенты и их отличия | 1 |  | 1 |  |
| 3.4. | Вложенные устройства. Автоматически формируемые вложенные устройства; синхронизация устройств; изменение типа вложенного устройства; ручное добавление вложенного устройства | 1 |  | 1 |  |
| 3.5. | Проверки безопасности. Принцип работы проверок и их результатов; формат записи проверок; создание пользовательских стандартов с использованием встроенных проверок и создания своих на основе регулярных выражений. | 1 |  | 1 |  |
| 3.6. | Профили отчётов. Создание профилей для работы с отчетами и проверками; создание пользовательского профиля, создание пользовательских отчетов (команда, файлы, права доступа) | 1 |  | 1 |  |
|  | **Всего:** | **14** | **6** | **8** |  |
|  | **Итоговый контроль знаний** | **2** |  | **2** | **Итоговое тестирование** |
|  | **Итого:** | **16** | **6** | **10** |  |