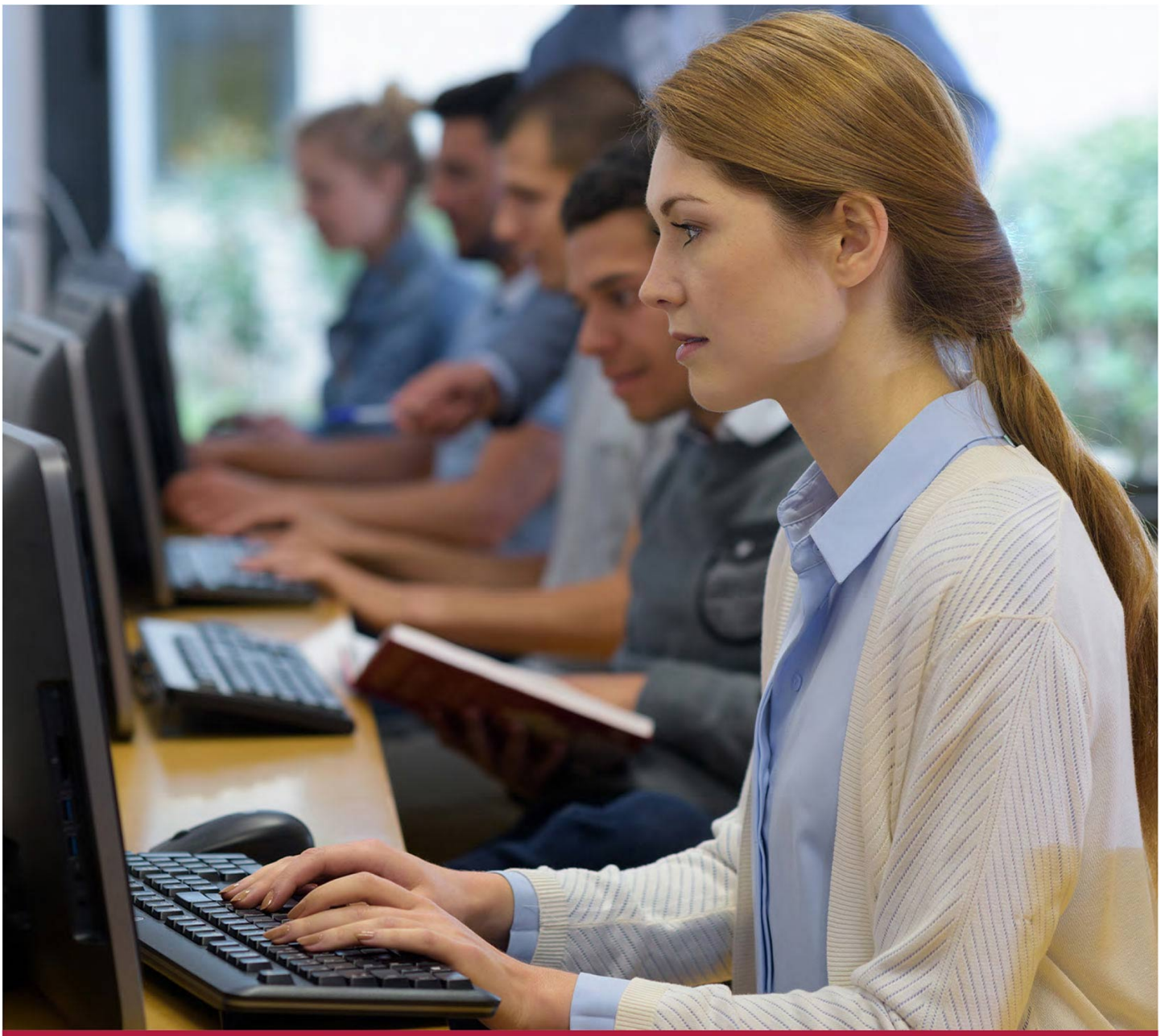
softline учебный центр



Администрирование "Континент 4"

Код курса: АК-4

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

Администрирование "Континент 4"

Код курса: АК-4

Длительность	40 ак. часов
Формат	
Разработчик курса	Код безопасности
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Учебный курс "Администрирование "Континент" 4" разработан для изучения работы сертифицированного изделия "Комплекс безопасности "Континент". Версия 4". В результате обучения слушатели получат теоретические знания и практические навыки, необходимые для внедрения, настройки и обслуживания сетевых компонентов комплекса. В процессе обучения слушатели на практике будут изучать возможности Континент по настройке межсетевого экранирования и маршрутизации трафика, по применению технологии NAT, по организации виртуальных частных сетей на основе общих сетей передачи данных, по мониторингу и аудиту компонентов системы.

Подробная информация

Профиль аудитории:

- специалисты в сфере информационной безопасности;
- системные администраторы;
- руководители ИТ-служб;
- архитекторы систем информационной безопасности.

Предварительные требования:

- Опыт администрирования Windows и Linux.
- Базовые принципы работы сетей передачи данных.
- Знание стека протоколов TCP/IP.
- Опыт настройки оборудования локальной сети.

По окончании курса слушатели изучат:

- управлять узлами Континент;
- настраивать межсетевое экранирование;
- формировать и устанавливать политики СОВ;
- применять технологии NAT;
- выполнять резервирование и восстановление конфигурации;

- выполнять мониторинг и аудит.

Программа курса

День 1

Глава 1. «Общие сведения по Континент 4»

- Назначение и состав комплекса
- Принципы функционирования комплекса
- Управление комплексом
- ПАК "Соболь"
- Типовые аппаратные платформы и их производительность
- Политика лицензирования
- Порядок ввода комплекса в эксплуатацию
- Лабораторный модуль №1 "Развертывание ЦУС Континент, рабочего места главного администратора и подчиненных узлов безопасности"
- Лабораторная работа №1 "Развертывание центра управления сетью Континент и регистрация главного администратора"
- Лабораторная работа №2 "Подготовка рабочего места главного администратора"
- Лабораторная работа №3 "Настройка подключения к подсистеме мониторинга"
- Лабораторная работа №4 "Развертывание подчиненных узлов безопасности"
- Контрольные вопросы

День 2

Глава 2. Управление узлами Континент

- Роли администраторов. Назначение администраторов
- Дистанционный доступ по протоколу SSH
- Лабораторный модуль №2 "Управление узлами Континент"
- Лабораторная работа №1 "Управление ролями и учетными записями администраторов"
- Лабораторная работа №2 "Настройка дистанционного доступа по протоколу SSH"
- Контрольные вопросы

Глава 3. Настройка межсетевого экранирования

- Обработка трафика узлом безопасности
- Межсетевое экранирование
- Сетевые функции
- Виды объектов ЦУС
- Правила фильтрации
- Правила трансляции
- Установка политики
- Лабораторный модуль №3 "Настройка многофункционального межсетевого экрана на узлах безопасности в режиме UTM"
- Некоторые особенности обработки сетевого трафика компонентами многофункционального межсетевого экрана в режиме UTM
- Лабораторная работа №1 "Настройка правил фильтрации"

- Лабораторная работа №2 "Настройка правил трансляции"
- Контрольные вопросы

Глава 4. Система обнаружения и предотвращения вторжений

- Концепция управления СОВ
- Управление детектором атак в режимах Monitor и Inline
- Установка БРП. Создание собственных сигнатур
- Формирование и установка политик СОВ
- Лабораторный модуль №4 "Инициализация, настройка и проверка функциональности детектора атак"
- Лабораторная работа №1 "Инициализация детектора атак"
- Лабораторная работа №2 "Настройка детектора атак: установка БРП, создание профиля и применение политик"

День 3

Глава 4. Система обнаружения и предотвращения вторжений

- Лабораторный модуль №4 "Инициализация, настройка и проверка функциональности детектора атак"
- Лабораторная работа №3 "Проверка функциональности детектора атак"
- Лабораторная работа №4 "Настройка СОВ в составе UTM-узла безопасности"
- Контрольные вопросы

Глава 5. Построение VPN

- VPN-туннель
- Шифрование
- Топология
- L3VPN IPSec
- VPN удаленного доступа
- Лабораторный модуль №5 "Построение VPN"
- Лабораторная работа №1 "Организация проприетарного L3VPN между защищаемыми сетями"
- Лабораторная работа №2 "Построение L3VPN IPSec между пересекающимися сетями"
- Лабораторная работа №3 "Организация L3VPN между удаленным пользователем и защищаемой сетью"

День 4

Глава 5. Построение VPN

- L2VPN-туннель
- Лабораторный модуль №5 "Построение VPN"
- Лабораторная работа №4 "Организация L3VPN между удаленным пользователем и защищаемой сетью за другим УБ Континент"
- Лабораторная работа №5 "Организация L2VPN"
- Контрольные вопросы

Глава 6. Обеспечение отказоустойчивости комплекса

- Резервирование и восстановление конфигурации
- Аппаратное резервирование и восстановление узла безопасности
- Резервирование БД ЦУС
- Лабораторный модуль №6 "Резервирование и восстановление"
- Лабораторная работа №1 "Резервирование узла безопасности"
- Лабораторная работа №2 "Резервирование БД ЦУС"
- Лабораторная работа №3 "Резервное копирование и восстановление данных узла безопасности или ЦУС"
- Контрольные вопросы

Глава 7. Мониторинг и аудит

- Общие сведения по системе мониторинга: инициализация, объекты мониторинга и типы информации, применение правил и шаблонов
- Просмотр сведений журналов
- Аудит
- Лабораторный модуль №7 "Мониторинг и аудит"
- Лабораторная работа №1 "Настройка параметров аудита. Работа с подсистемой мониторинга"
- Лабораторная работа №2 "Локальная работа с журналами аудита"
- Контрольные вопросы

День 5

Глава 8. Настройка Multi-WAN

- Лабораторный модуль №8 "Настройка Multi-WAN"
- Лабораторная работа №1 "Обеспечение отказоустойчивости канала связи"
- Лабораторная работа №2 "Настройка балансировки трафика между двумя внешними интерфейсами узла безопасности"
- Контрольные вопросы

Глава 9. Виртуальная маршрутизация

- Краткое описание механизма виртуальной маршрутизации
- Настройка VRF-зон
- Просмотр сведений о VRF-зонах в локальном меню узла безопасности
- Управление сетевыми интерфейсами в составе VRF-зоны
- Лабораторный модуль №9 "Настройка и применение виртуальной маршрутизации"
- Лабораторная работа №1 "Настройка и применение виртуальной маршрутизации"
- Контрольные вопросы

Глава 10. Поддержка динамической маршрутизации

- Протоколы динамической маршрутизации
- Лабораторный модуль №10 "Поддержка динамической маршрутизации"
- Лабораторная работа №1 "Настройка динамической маршрутизации по протоколу BGP"

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!

Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **18 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline
Вы можете узнать из профайла.