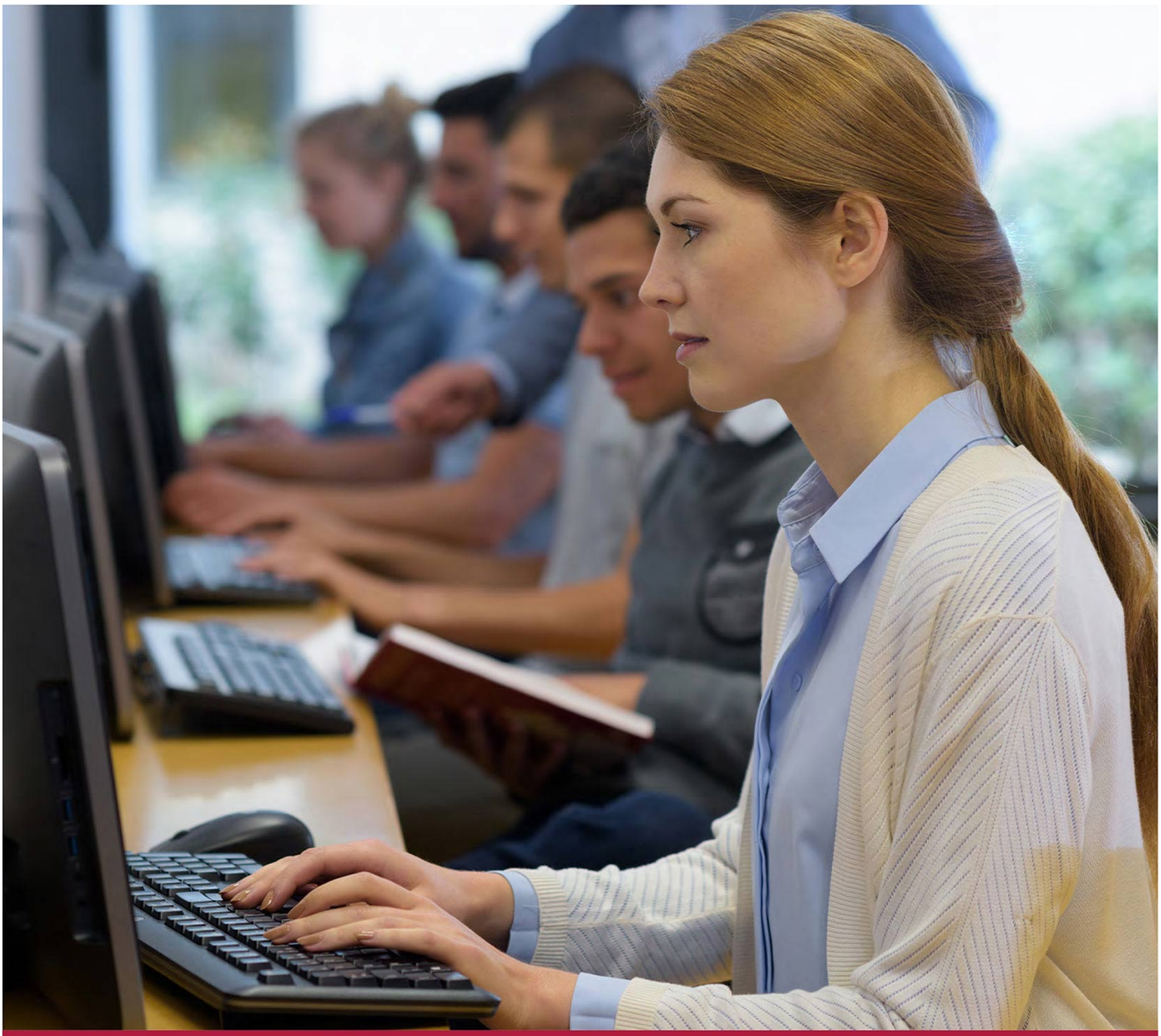
softline учебный центр



Инженер безопасности Check Point R81.20

Код курса: CCSE R81.20

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

Инженер безопасности Check Point R81.20

Код курса: CCSE R81.20

Длительность	24 ак. часа
Формат	Очно; Дистанционно
Разработчик курса	Check Point
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Курс, основанный на курсе Check Point Security Administrator R81.20 и являющийся его продолжением и развитием, обеспечивает знание концепций и навыки, необходимых для развертывания, настройки и отладки работы шлюзов безопасности и серверов управления, построенных на основе программных блейдов. В процессе обучения слушатели изучат тонкости работы шлюзов безопасности, механизмы обновления, автоматизацию и оркестрацию, способы обеспечения отказоустойчивости, варианты ускорения обработки трафика, кластеризацию, построение VPN туннелей между сайтами, возможности безопасного подключения удаленных пользователей.

Подробная информация

Профиль аудитории:

- Этот трехдневный курс рекомендован тем, кто занимается поддержкой, установкой или администрированием систем безопасности на основе оборудования Check Point Blades: системным администраторам, системным инженерам, менеджерам по безопасности, сетевым инженерам.

Предварительные требования:

- Данный курс предполагает предварительное прохождение курса Check Point Security Administrator R81.20или наличие у слушателей эквивалентных знаний и навыков; а также базового знания сетевых технологий, умения работать с Windows Server 2008 и UNIX, понимания TCP/IP и умения работать в Интернете.

По окончании курса слушатели смогут:

- Запускать скрипты;
- Использовать API;
- Строить распределенную систему хранения лог-записей;
- Развертывать и настраивать сервер SmartEvent;
- Строить и работать с кластером в режиме HA;

- Расшифровывать и инспектировать HTTPS трафика;
- Развертывать систему Identity Awareness;
- Настраивать Threat Prevention;
- Строить VPN удаленного доступа;
- Настраивать Mobile Access VPN;
- Отлаживать механизм проверки Compliance;
- Работать со шлюзами.

Программа курса

Модуль 1. Продвинутые механизмы внедрения

- Обзор основ механизмов развертывания
- Интерфейсы автоматизации
- Обзор API, способы запуска скриптов
- Сервер автоматизации
- Запуск скриптов из командной строки
- Использование внешнего механизма запуска скриптов
- Использование Web-сервисов для запуска скриптов
- Написание скриптов

Лабораторная работа. Использование API

Модуль 2. Дублирование сервера управления

- Механизм обеспечения отказоустойчивости сервера управления
- Развертывание дублирующего сервера управления
- Мониторинг статуса серверов
- Состояние Active и Standby, смена состояния
- Резервное копирование и восстановление
- Выделенный лог-сервер, выделенный сервер SmartEvent
- Развертывание серверов логирования и SmartEvent
- Отладка работы механизма отказоустойчивости

Лабораторная работа. Развертывание дублирующего сервера управления

Лабораторная работа. Построение распределенной системы хранения лог-записей

Лабораторная работа. Развертывание сервера SmartEvent

Модуль 3. Продвинутые варианты развертывания шлюзов

- Необходимость отказоустойчивой конфигурации шлюзов

- Введение в технологию кластеризации и работа компонента ClusterXL
- Синхронизация состояния модулей
- Обработка сбоев в работе модулей, требования, рекомендации, ограничения
- Развертывание кластера
- Виртуальные IP-адреса, адреса в отличающихся сетях
- Виртуальные MAC-адреса
- Протокол управления кластером (CCP)
- Кластер из модулей разных версий
- Отказ от синхронизации конкретных сервисов
- Cluster Correction Layer
- Настройка NAT и Proxy ARP для кластера
- Обзор работы режима моста, кластер и отдельный модуль в режиме моста
- Разделение управляющих и обрабатывающих компонентов шлюзов

Лабораторная работа. Построение кластера в режиме HA

Лабораторная работа. Работа с кластером

Модуль 4. Дополнительные возможности настройки политики

- Обзор базовых возможностей политики безопасности
- Обзор процессов модулей Check Point
- Обзор установки политики
- Работа с учетными записями пользователей
- Обновляемые объекты
- Работа с внешними списками объектов
- Логирование и мониторинг
- Расшифровка и инспекция HTTPS трафика
- Дополнительные инструменты

Лабораторная работа. Настройка обновляемых объектов

Лабораторная работа. Ускоренная установка политики

Лабораторная работа. Инспекция HTTPS трафика

Модуль 5. Работа с учетными записями пользователей

- Обзор функционала Identity Awareness
- Варианты развертывания системы Identity Awareness
- Обзор настроек Identity Awareness, включение, выбор источников данных
- Дефолтные порты, используемые технологией Identity Awareness
- Объекты Access Role, их использование в политике

Лабораторная работа. Развертывание системы Identity Awareness

Модуль 6. Настройка Threat Prevention в режиме Custom

- Обзор функционала Threat Prevention
- Компоненты Threat Prevention
- Настройки антивируса, анти-бота, работы песочницы, технологии Threat Extraction, антифишинга, защиты интернета вещей
- Движок Threat Prevention
- Облако Check Point
- Индикаторы угроз
- Анализ SSH пакетов
- Настройка Threat Prevention в режиме Custom, инструментарий политики

Лабораторная работа. Настройка Threat Prevention

Модуль 7. Углубленная настройка Site-to-Site VPN

- Обзор VPN
- Построение VPN на основе доменов
- Аутентификация сторонними сертификатами

Лабораторная работа. Построение VPN между шлюзами, управляемыми разными серверами

Модуль 8. VPN удаленного доступа (IPSec)

- Введение в VPN удаленного доступа
- Аутентификация
- Клиенты удаленного доступа
- Лицензионные требования
- Особенности коммуникации клиента со шлюзом
- Проверка настройки клиентской машины на соответствие требованиям
- Безопасность оконечного устройства
- Обеспечение отказоустойчивости VPN удаленного доступа
- Использование компонента SSL Network Extender
- Настройка VPN удаленного доступа

Лабораторная работа. Построение VPN удаленного доступа

Модуль 9. Mobile Access VPN (SSL)

- Введение в технологию Mobile Access VPN, ее принцип работы
- Политика безопасности Mobile Access VPN
- Настройка Mobile Access VPN
- Приложения и возможности

Лабораторная работа. Настройка Mobile Access VPN

Модуль 10. Углубленное логирование и мониторинг

- Функционал проверки соответствия требованиям (Compliance)
- Работа системы SmartEvent

Лабораторная работа. Настройка проверки Compliance

Лабораторная работа. Развертывание системы SmartEvent

Модуль 11. Настройка производительности

- Обзор возможностей настройки производительности
- Обзор технологии SecureXL, пути прохождения трафика, настройка, команды
- Использование утилиты CPView
- Обзор технологии CoreXL, прохождение трафика, настройка, команды
- Обзор технологии Multi-Queue, настройка, команды
- Обзор технологии HyperFlow

Лабораторная работа. Настройка производительности шлюза

Модуль 12. Углубленное обслуживание шлюзов

- Обзор механизмов обновления и миграции
- Подготовка к апгрейду
- Мастер скачивания и обновления
- Встроенный механизм обновления

- Пакет инструментов для апгрейда и миграции сервера управления
- Обзор вариантов апгрейда сервера, продвинутый вариант, миграция
- Обзор механизма Blink
- Варианты апгрейда шлюза или модуля кластера.
- Централизованный апгрейд через SmartConsole (рекомендованный вариант), добавление пакетов в репозиторий, обновление кластера
- Обзор инструмента Central Deployment Tool
- Обновление кластера без потери сессий

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.