

## CHECK POINT CYBER SECURITY ENGINEERING (CCSE) R80.10

### ДЛЯ КОГО ПРЕДНАЗНАЧЕН КУРС?

Для опытных пользователей и посредников, которым нужно выполнять сложные развертывания программных блейдов Check Point.

### НАЗНАЧЕНИЕ КУРСА:

Подтвердить понимание и навыки, необходимые для настройки и управления межсетевыми экранами Check Point следующего поколения.

### НЕОБХОДИМЫЕ ЗНАНИЯ:

- Обучение/аттестация CCSA
- Опыт работы с Windows, UNIX, сетевыми технологиями и интернетом

### ТЕМЫ КУРСА

- Системное администрирование
- Автоматизация и комбинирование (Orchestration)
- Избыточность
- Ускорение
- SmartEvent
- Мобильный и удаленный доступ
- Предотвращение угроз

### ЛАБОРАТОРНЫЕ ЗАНЯТИЯ

- Обновление Security Management Server до версии R80.10
- Применение исправлений (Hotfixes) Check Point
- Настройка нового кластера шлюзов безопасности
- Основные элементы текстового интерфейса администрирования межсетевого экрана
- Настройка неавтоматических правил преобразования сетевых адресов
- Управление объектами с помощью Check Point API
- Включение Check Point VRRP
- Развертывание дополнительного сервера Security Management Server
- Просмотр модулей цепочек (Chain Modules)
- Работа с ClusterXL
- Работа с CoreXL
- Оценка угроз с помощью SmartEvent
- Управление мобильным доступом
- Системы предотвращения вторжений (IPS)
- Развертывание защиты с географической привязкой в системе предотвращения вторжений (IPS Geo Protection)
- Анализ настроек и видов предотвращения угроз
- Развертывание эмуляции угроз и извлечения угроз

### СОДЕРЖАНИЕ КУРСА

- Расширенные команды интерфейса командной строки.
- Процедуры управления системой, включая обновление системы и применение патчей и исправлений.
- Инфраструктура межсетевого экрана Check Point.
- Дополнительные методы сбора важных данных шлюза с помощью CPView и CPInfo.
- Гибкая архитектура API Check Point, поддерживающая автоматизацию и комбинирование.
- Дополнительные функции ClusterXL.
- Преимущества избыточности сети VRRP.
- Использование технологии ускорения SecureXL для повышения производительности.
- Использование технологии ускорения CoreXL для повышения производительности.
- Компоненты SmartEvent для хранения журналов сетевой активности, поиск отдельных событий.
- Процесс SmartEvent, который определяет, какие действия в сети могут привести к проблемам с безопасностью.
- Использование SmartEvent для выявления, исправления и предотвращения угроз безопасности.
- Обсуждение программного блейда Mobile Access и его использования для защиты связи и данных.
- Варианты развертывания Mobile Access.
- Решения Check Point Remote Access.
- Компоненты Check Point Capsule и их функции защиты мобильных устройств и бизнес-документации.
- Решения Check Point для защиты от таких атак, как уязвимости нулевого дня и целевые кибератаки.
- Возможности «Песочницы», «Эмуляции угроз» и «Извлечения угроз» для предотвращения инцидентов, связанных с нарушением безопасности.
- Платформа Check Point Mobile Threat Prevention для защиты информации при доступе со смартфонов и планшетов компании.

### ИНФОРМАЦИЯ ОБ АТТЕСТАЦИИ

# CCSE

Подготовьтесь к экзамену №156-315.80 на веб-сайте [VUE.com/checkpoint](http://VUE.com/checkpoint)