



Эксперт по поиску и устранению неисправностей Check Point (R80.30+)

Код курса: CSTE R80.X

Эксперт по поиску и устранению неисправностей Check Point (R80.30+)

Код курса: CSTE R80.X

Длительность	16 ак. часов
Формат	Очно; Дистанционно
Разработчик курса	Check Point
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Курс предназначен для специалистов в области сетевой безопасности, отвечающих за администрирование и мониторинг продуктов Check Point, и желающих получить глубокие знания о процессах поиска и устранения неисправностей.

Подробная информация

Профиль аудитории:

Инженеры и специалисты в области сетевой безопасности, отвечающие за администрирование политики безопасности, реализованной с использованием продуктов Check Point, мониторинг и решение связанных проблем.

Предварительные требования:

- Опыт работы с Windows и Linux системами;
- Знания TCP/IP;
- Знания в объеме курсов CCSA и CCSE.

По окончании курса слушатели смогут:

- Использовать диагностические утилиты Check Point для определения состояния сети;
- Использовать анализаторы сетевого трафика и утилиты захвата пакетов для анализа сетевого трафика;
- Использовать утилиты Linux для мониторинга системы;
- Получить комплексные знания об архитектуре Security Management;
- Понимать структуру и представление объектов в Management Database;
- Знать основные процессы Management Server и методы их отладки;
- Работать с утилитой GuiDBEdit;
- Понимать обработку трафика ядром и выполнять поиск и устранение неисправностей, связанных с chain modules;
- Использовать два способа отладки Firewall Kernel, знать, чем они отличаются;

- Знать пользовательские процессы и выполнять их отладку;
- Включать Core Dump;
- Знать процессы, задействованные при применении политик;
- Выполнять поиск и устранение неисправностей, связанных с Application Control и URL Filtering;
- Выполнять поиск и устранение неисправностей, связанных с HTTPS Inspection;
- Выполнять поиск и устранение неисправностей, связанных с Content Awareness;
- Понимать принципы работы IPS и решать проблемы, связанные с производительностью;
- Выполнять поиск и устранение неисправностей, связанных с Anti-Bot и Antivirus;
- Выполнять поиск и устранение неисправностей, связанных с Site-to-Site VPN;
- Выполнять поиск и устранение неисправностей, связанных с Remote Access VPN;
- Использовать команды по работе с SecureXL;
- Понимать влияние оборудования и настроек операционной системы на производительность Security Gateway.

Программа курса

Модуль 1 «Комплексный поиск и устранение неисправностей»

- Диагностические утилиты Check Point
- Утилиты для захвата сетевого трафика
- Утилиты Linux
- Лабораторная работа «Мониторинг сетевого трафика»

Модуль 2 «Management Database и связанные процессы»

- Архитектура Check Point Security Management
- Management Database
- API Server
- Процессы Security Management и их отладка
- GuiDBEdit и DBedit
- SmartEvent
- Высокая доступность Management Server
- Лабораторная работа «Отладка процессов Management Server»
- Лабораторная работа «Обзор баз данных Postgres и Sorl»
- Лабораторная работа «Поиск и устранение неисправностей, связанных с синхронизацией Management Server»

Модуль 3 «Отладка процессов режима ядра»

- Check Point Kernel
- Отладка Firewall Kernel
- Лабораторная работа «Анализ сетевого трафика с использованием отладки ядра»

Модуль 4 «Отладка процессов пользовательского режима»

- Процессы пользовательского режима на Security Gateway
- Проблемы, связанные с процессами пользовательского режима
- Core Dump

- Лабораторная работа «Отладка процессов пользовательского режима»

Модуль 5 «Архитектура Access Control»

- Установка политики Access Control и отладка связанных процессов
- Application Control and URL Filtering
- HTTPS Inspection
- Content Awareness
- Лабораторная работа «Поиск и устранение неисправностей, связанных с политикой Access Control»

Модуль 6 «Работа с политиками Threat Prevention»

- Политика Threat Prevention
- Check Point IPS
- Anti-Bot и Antivirus
- Лабораторная работа «Поиск и устранение неисправностей, связанных с IPS»
- Лабораторная работа «Обзор продуктов Threat Prevention»

Модуль 7 «Поиск и устранение неисправностей, связанных с VPN»

- Процессы VPN
- Поиск и устранение неисправностей, связанных с Site-to-Site VPN
- Поиск и устранение неисправностей, связанных с Client-to Site VPN
- Remote Access VPN
- Mobile Access VPN
- Лабораторная работа «Поиск и устранение неисправностей, связанных с Site-to-Site VPN»
- Лабораторная работа «Поиск и устранение неисправностей, связанных с Remote Access VPN»
- Лабораторная работа «Тестирование Mobile Access VPN»

Модуль 8 «Акселерация и оптимизация производительности»

- Технологии акселерации
- Команды SecureXL
- Команды отладки
- Таблицы ядра SecureXL
- Настройка CoreXL
- Работа с ClusterXL
- Оптимизация аппаратных компонентов и операционной системы
- Лабораторная работа «Проверка SecureXL»
- Лабораторная работа «Настройка параметров CoreXL»
- Лабораторная работа «Оптимизация аппаратных компонентов»
- Лабораторная работа «Оптимизация программного обеспечения»

[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](#).