

MaxPatrol 8: установка, настройка и управление уязвимостями (PT04)

ID PT-PT04 Цена 90 000,- руб. Длительность 3 дня

Кому следует посетить

- Администраторы систем безопасности, администраторы корпоративных сетей, IT-специалисты, занимающиеся защитой информации
- Аудиторы в области информационной безопасности
Консультанты и инженеры, ответственные за проектирование процессов мониторинга и аудита ИБ

Предварительные требования

Для успешного усвоения материала по базовому курсу по MaxPatrol 8 вам следует иметь:

- Общее представление об архитектуре стека протоколов TCP/IP.
- Практический опыт работы с операционными системами Windows и Linux.
- Базовые знания по сетевым технологиям.
- Общее представление об информационной безопасности и основах построения защищенных корпоративных систем.

Цели курса

Вы приобретете знания:

- принципов и способов оценки защищенности, контроля соответствия требованиям стандартов сетевых устройств;
- о проектировании системы анализа защищенности и соответствия стандартам MaxPatrol 8;
- архитектуры и принципов работы системы MaxPatrol 8;
- методологии применения программы MaxPatrol 8 для мониторинга и аудита информационной безопасности на базе MaxPatrol 8.

Вы сможете:

- устанавливать и настраивать компоненты системы;
- осуществлять администрирование и эксплуатацию системы MaxPatrol 8, в том числе резервное копирование и восстановление системы,

- разграничение доступа к управлению системой и доступа к результатам сканирований.
- управлять профилями сканирования и задачами;
- проводить оценку защищенности различных операционных систем;
- работать с историей сканирования, отчётами, формируемыми программой;
- использовать систему MaxPatrol 8 для анализа защищённости Web-приложений, СУБД и приложений;
- использовать систему MaxPatrol 8 в процессе тестирования сетей на устойчивость к взлому;
- использовать систему MaxPatrol 8 в процессе аудитов и контроля соответствия требованиям международных и отраслевых стандартов;
- использовать систему MaxPatrol 8 для инвентаризации информационных ресурсов.

Программа курса

День 1

- Модуль 1. Введение. Построение процесса управления информационной безопасностью на предприятии. Система анализа защищенности и соответствия стандартам MaxPatrol 8. Режимы работы системы. Архитектура MaxPatrol 8. Схема лицензирования. Сценарии развёртывания.
- Практическая работа 1. Установка MaxPatrol 8 Server с внешней базой и дополнительным сканером.
- Модуль 2. Выявление уязвимостей методом PenTest. Способы выявления уязвимостей методом Pentest. Баннерные проверки. Подбор учётных данных. Сканирование web-приложений. Правила безопасного сканирования ИС при проведении сканирования в режиме PenTest.
- Практическая работа 2. Сканирование в режиме PenTest.
- Модуль 3. Выявление уязвимостей методом Audit. Определение сетевого транспорта. Привилегии учетной записи для сканирования. Аудит ОС Windows, Unix, Cisco и СУБД.
- Практическая работа 3. Сканирование в режиме Audit.

MaxPatrol 8: установка, настройка и управление уязвимостями (PT04)

День 2

- Модуль 4. Оценка соответствия требованиям стандартов. Адаптация MaxPatrol 8 под корпоративные требования. Управление стандартами и проверками.
- Практическая работа 4. Оценка соответствия требованиям стандартов.
- Модуль 5. Создание отчетов. Типы и параметры отчетов. Доставка отчетов. Применение отчетов. Оценка степени опасности уязвимостей.
- Практическая работа 5. Генерация отчетов.
- Модуль 6. Сканирование по расписанию. Сценарии запуска.
- Практическая работа 6. Создание расписания.

День 3

- Модуль 7. Дополнительные компоненты MaxPatrol 8. Реализация системы обновлений. Сервер обновлений. Консолидация данных.
- Практическая работа 7. Установка сервера обновлений. Работа с сервером консолидации. Загрузка и обработка результатов сканирования.
- Модуль 8. Разграничение доступа и защита данных в системе MaxPatrol 8. Пользователи и роли пользователей. Назначение прав на объекты системы.
- Практическая работа 8. Разграничение доступа в MaxPatrol 8.
- Модуль 9. Сценарий «Импорт данных».
- Практическая работа 9. Резервное копирование системы.
- Модуль 10. Резервное копирование и восстановление системы после сбоев.
- Практическая работа 10. Резервное копирование системы.
- Модуль 11. Перенос MaxPatrol 8 на другой сервер.
- Практическая работа 11. Перенос MaxPatrol 8 на другой сервер.