

Применение системы MaxPatrol VM в процессе управления уязвимостями (РТ33)

ID РТ-РТ33 Цена 60 000,- руб. Длительность 2 дня

Кому следует посетить

Курс предназначен для широкого круга технических специалистов, начинающих изучение продукта РТ MaxPatrol VM.

Предварительные требования

Для успешного усвоения материала по курсу необходимы:

- 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;
- Общее представление о базе данных общеизвестных уязвимостей информационной безопасности CVE (Common Vulnerabilities and Exposures).

Желательно иметь:

- Знания принципов работы сканеров уязвимостей;
- Опыт работы с MP SIEM, MP8 и другими продуктами Позитив Текнолоджиз;
- Опыт работы с SQL запросами в любой БД;
- Понимание стандарта Common Vulnerability Scoring System (CVSS).

Цели курса

Вы приобретете знания:

- о предназначении продукта РТ MaxPatrol VM;
- использовать продукт, используя веб-интерфейс;
- по работе с веб-интерфейсом продукта;
- по способам сканирования ИТ инфраструктуры;
- о методологии применения РТ MaxPatrol VM для анализа защищенности инфраструктуры.

Вы сможете:

- самостоятельно устанавливать продукт;
- использовать продукт, используя веб-интерфейс;
- управлять профилями сканирования и задачами;
- сканировать узлы на базе любой операционной системы;
- работать с историей сканирования, отчётами, формируемыми РТ MaxPatrol VM;
- использовать систему MaxPatrol VM для инвентаризации информационных ресурсов

Содержание курса

Базовый курс по MaxPatrol VM, охватывающий основные возможности системы, методологию её использования для автоматизации задач, возникающих при реализации процесса управления уязвимостями. В курсе рассматриваются режимы сканирования информационных систем, классификация и оценка активов, приоритизация уязвимостей, генерация отчётов.

Программа курса

Модуль 1. Процесс управления уязвимостями. Задачи процесса VM. Основные этапы процесса VM.

Модуль 2. О MaxPatrol VM. Архитектура MaxPatrol VM.

Модуль 3. Выявление уязвимостей. Поиск узлов. Выявление уязвимостей методом Pentest. Выявление уязвимостей методом Audit.

Модуль 4. Работа с активами. Синтаксис PDQL запросов. HCC-Lite PDQL-запросы.

Модуль 5. Построение процесса управления уязвимостями в MaxPatrol VM. Инвентаризация активов. Классификация активов. Анализ защищенности. Контроль защищенности. Устранение уязвимостей. Контроль устранения уязвимостей.

Модуль 6. Практическая работа. Работа с активами и уязвимостями. Определение значимости активов.

Определение сроков актуальности для сканирования активов методами пентест и аудит. Создание статических и динамических групп. Работа с уязвимостями. Паспорта уязвимостей. Экземпляры уязвимостей на активах. Политики по устранению уязвимостей. Статусы уязвимостей. Просроченные уязвимости на активах. Трендовые уязвимости.

Модуль 7. Создание отчетов. Создание отчета на основе стандартного. Создание отчета в конструкторе.

Модуль 8. Обновление продукта и базы знаний.