

# Развертывание и администрирование PT Application Firewall

ID PT-PT23 Цена 60 000,- руб. Длительность 2 дня

## Кому следует посетить

- Администраторам корпоративных сетей.
- Администраторам безопасности.
- Разработчикам веб-приложений.

## Предварительные требования

Для успешного прохождения курса слушателям требуются следующие знания и навыки:

- общее представление об архитектуре стека протоколов TCP/IP;
- практический опыт работы с операционными системами семейства Windows;
- базовые знания о сетевых технологиях;
- общее представление об информационной безопасности и основах построения защищенных корпоративных систем;
- базовые знания в области веб-технологий.

## Цели курса

Вы приобретете знания и систематизируете сведения:

- о рисках, связанных с использованием веб-технологий;
- о механизмах и способах атак на веб-приложения;
- о методологии разработки безопасных приложений.

Вы сможете:

- грамотно защищать веб-приложения при помощи решения PT AF;
- использовать сведения об уязвимостях, полученных при помощи PT AI, при настройке PT AF;
- использовать PT AF для мониторинга и анализа атак в сети, в том числе постфактум при наличии дампа сетевого трафика; использовать возможности PT AF для расширенного анализа безопасности веб-приложений.

## Содержание курса

PT AF — web application firewall (WAF), инновационная система защиты, которая точно обнаруживает и блокирует атаки, включая атаки из списка OWASP Top 10 и классификации WASC, L7 DDoS и атаки нулевого дня. PT AF обеспечивает непрерывную защиту приложений, пользователей и инфраструктуры и помогает соответствовать стандартам безопасности.

## Программа курса

### Модуль 1.

- Введение.
- Распределенные приложения.
- Модель «клиент-сервер», веб-приложения.
- Проблемы и основные понятия безопасности веб-технологий.
- Угрозы безопасности веб-приложений.
- Список OWASP TOP 10.
- Классификация угроз Web Application Security Consortium.
- Практическая работа 1. Внедрение SQL-кода

### Модуль 2.

- Обзор технологий минимизации рисков.
- Фильтрация пользовательского ввода.
- Стандарт Content Security Policy.
- Специализированные межсетевые экраны и системы обнаружения атак.
- Устройство и принципы работы системы защиты приложений Positive Technologies Application Firewall (PT AF).
- Модели развертывания.
- Использование защитных механизмов уровня операционной системы при выборе программной модели развертывания.
- Схема лицензирования.
- Варианты подключения.
- Анализ зашифрованного трафика.
- Практическая работа 2. Развертывание PT AF

### Модуль 3.

- Анализ событий.
- Концепция интерфейса.

## Развертывание и администрирование PT Application Firewall (PT23)

---

- Работа с консолью PT AF (dashboard).
- Использование запросов и фильтров. Геолокация.
- Практическая работа 3. Работа с фильтрами в Консоли PTAF

### Модуль 4.

- Выявление ложных срабатываний, подтверждение наличия уязвимости.
- Практическая работа 4. Фильтрация ложных срабатываний

### Модуль 5.

- Настройка модулей защиты трафика.
- Профили защиты.
- Защитные модули PT Application Firewall.
- Корреляция событий.
- Практическая работа 5. Настройка профиля защиты

### Модуль 6.

- Механизмы реагирования.
- Оповещения.
- Модификация трафика.
- Блокировка.
- Интеграция с системами управления событиями безопасности.
- Практическая работа 6. Настройка механизмов реагирования