

# Управление событиями безопасности на базе решений компании Positive Technologies (PT15)

ID PT-PT15 Цена 60 000,- руб. Длительность 2 дня

## Кому следует посетить

- Аналитики ИБ
- Инженеры технической поддержки
- Консультанты-аналитики
- Инженеры внедрения
- Операторы систем
- Тем, кто готовится сдать сертификацию MaxPatrol SIEM CP

## Предварительные требования

- Что такое MaxPatrol SIEM
- MaxPatrol SIEM 7.0: что нового
- MaxPatrol SIEM + MaxPatrol VM. Что дает синергия двух продуктов
- Как экспертиза в мониторинге событий ИБ помогает создавать качественные продукты

## Цели курса

После прохождения курса вы будете знать:

- Таксономию событий
- Синтаксис правил обогащения
- Синтаксис правил корреляции
- Возможности, которые дает применение табличных списков
- Принципы подключения новых источников и написания правил нормализации
- Как писать собственные правила нормализации, корреляции и обогащения
- Как работать с SDK из консоли и с помощью графических утилит
- Отладку правил на потоке данных
- Как работать с мастером добавления правил корреляции

## Содержание курса

Курс для технических специалистов, которые хотят получить экспертные знания и навыки управления MaxPatrol SIEM, чтобы проводить расследования и адаптировать экспертизу

продукта к обнаружению инцидентов в инфраструктуре заказчика.

## Программа курса

- Установка системы MaxPatrol SIEM в конфигурации для высоконагруженных систем
- Нормализация, обогащение и корреляция событий
- Создание виджетов
- Агрегация инцидентов
- Сертификационная лабораторная работа