

## Развертывание и администрирование MaxPatrol SIEM (PT13)

ID PT-PT13 Цена 90 000,- руб. Длительность 3 дня

### Кому следует посетить

- Администраторы безопасности
- Администраторы корпоративных сетей
- IT-специалисты, занимающиеся защитой информации
- Консультанты и инженеры, ответственные за реагирование на инциденты ИБ
- Тем, кто готовится сдать сертификацию MaxPatrol SIEM CS

### Предварительные требования

- Знать основы сетевых технологий
- Иметь общее представление об информационной безопасности и построении защищенных корпоративных систем
- Понимать, что такое SIEM
- Знать Windows и Linux на уровне администратора
- Уметь работать с основными консольными утилитами администрирования (ls, ps, dir, df, cat, vim, nano, free, top)
- Иметь навыки работы с контейнерами (Docker и Docker Compose)

### Цели курса

После прохождения данного курса вы будете знать:

- Архитектуру и принципы работы MaxPatrol SIEM
- Методы применения MaxPatrol SIEM для мониторинга событий информационной безопасности и управления инцидентами
- Проектирование системы мониторинга и аудита информационной безопасности на базе MaxPatrol SIEM с учетом сетевой топологии и организационной структуры системы управления ИБ
- Управление задачами подключения источников событий и задачами сбора событий
- Администрирование и эксплуатацию MaxPatrol SIEM

### Содержание курса

Курс для технических специалистов или инженеров, которые хотят получить знания и навыки по проведению инсталляции и настройке основных параметров MaxPatrol SIEM для

обеспечения его работы.

### Программа курса

- Назначение MaxPatrol SIEM. Упрощенное внедрение системы Asset management, vulnerability management, SIEM
- Компоненты системы, направления развития, потоки данных Asset & vulnerability management
- Метрики CVSS 3.0
- Контекстные метрики. Банк данных угроз ФСТЭК РФ
- Пользователи и роли
- Сбор и работа с событиями. PDQL и таксономия событий
- Загрузка событий из файла и отладка
- Доставка уведомлений
- Установка системы обновлений UCS. Работа с PT KB
- Журналы и устранение неполадок
- Итоговый тест