Обучение по программе **Управление событиями безопасности на базе решений компании Positive Technologies**

Вы научитесь:

Писать собственные правила корреляции

Настраивать централизованное обновление **MaxPatrol** в распределенных сетях

Восстанавливать работоспособность системы **MaxPatrol SIEM** в случае сбоев

Подключать сбор событий с любого источника

По итогам обучения Вы получите:

- Сертификат об обучении государственного образца
- Сертификат **Positive Technologies**
- Сертификат МЦО НЦОТ **"ROZUM"**

Продолжительность: 16 академических часов
Стоимость: 1260 бел. рублей (с НДС 20%)
Форма обучения: очная (дневная)

Содержание программы:

1. Нормализация событий. Описание таксономии.
1.1. Написание правила нормализации событий нестандартного источника. Построение графа нормализации.
2. Корреляция, модельная корреляция. Язык создания правил корреляции.
2. 1. Модификация системных правил корреляции.
2.2. Создание собственных правил корреляции.
3. Работа с табличными списками.
3.1. Создание правил корреляции с использованием табличных списков.
4. Маршрутизация данных внутри системы. Диагностика работоспособности системы.
4.1. Поиск неисправностей в системе.
5. Резервное копирование и восстановление компонент MP SIEM.

Подать заявку на обучение:

pk@ncot.by

rozum.ntec.by

+ 375(17)327-14-29
+ 375(17)328-60-16

Бизнес-центр "Имперский",
ул. К. Цеткин, 24, 11 этаж