Обучение по программе **Развертывание и администрирование MaxPatrol SIEM**

Вы научитесь:

Работать с историей событий информационной системы

Управлять задачами на подключение источников событий и задачами по сбору событий

Проектировать системы мониторинга и аудита информационной безопасности на базе MaxPatrol

Осуществлять администрирование и эксплуатацию системы MaxPatrol SIEM

По итогам обучения Вы получите:

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

Продолжительность: 24 академических часа

Стоимость: 1900 бел. рублей (с НДС 20%)

Форма обучения: очная (дневная)

Содержание программы:

1. **Назначение SIEM-системы. Упрощенное внедрение системы. Компоненты системы, потоки данных.**

1.1. Установка системы, первичная настройка компонентов.

2. **Asset and vulnerability management. Метрики CVSSv2, CVSSv3. Контекстные метрики. БДУ ФСТЭК РФ.**

2.1. Задачи, профили, активы.

3. **Пользователи и роли.**

3.1. Пользователи и роли, инфраструктуры.

4. **Сбор и работа с событиями. PDQL и таксономия события.**

4.1. Сбор событий: WinEventLog, WMInotification, File via SSH, Checkpoint Gaia 80.10, Kaspersky Security Center (необязательная работа), группировка событий.

5. **Корреляции. Обзор системных правил корреляции.**

5.1. Корреляции и генераторы.

5.2. Сбор событий по протоколу syslog.

6. **Инциденты и доставка уведомлений.**

6.1. Работа с инцидентами и почтовыми уведомлениями: работа с автоматически созданным инцидентом, самостоятельное создание инцидента.

7. **Статистика и отчеты.**

7. 1. Статистика.

7.2. Построение отчетов.

8. **Обзор документации. Журналы и решение проблем.**

8. 1. Файлы журналов.

8.2. Клиент к базе данных Elasticsearch.

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