Обучение по программе **KL 025.4: Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response**

Платформа **Kaspersky Anti Targeted Attack** совместно с **Kaspersky EDR** представляет собой решение класса **XDR (Extended Detection and Response)** нативного типа и помогает организациям построить надежную систему защиты корпоративной инфраструктуры от сложных кибератак.

Изучаемые продукты:

- Kaspersky Anti Targeted Attack Platform 4.0
- Kaspersky Endpoint Detection and Response 2.0
- Kaspersky Endpoint Agent 3.12
- Kaspersky Security Center 13.2
- Kaspersky Endpoint Detection and Response (Cloud) — отдельный модуль

По итогам обучения Вы получите:

- Сертификат об обучении государственного образца
- Сертификат Лаборатории Касперского
- Сертификат МЦО НЦОТ "ROZUM"

Продолжительность: 24 академических часа

Стоимость: 2580 бел. рублей (с НДС 20%)

Форма обучения: очная (дневная)

Содержание программы:

5.2. Активация и первоначальная настройка Kaspersky Endpoint Agent

5.3. Технологии обнаружения KEDR

5.4. Расследование инцидента

Лабораторная работа 19. Проверить, что подсистема TAA работает
Лабораторная работа 20. Симулировать вредоносную нагрузку
Лабораторная работа 21. Продемонстрировать результаты работы KATA
Лабораторная работа 22. Демонстрация анализа и реагирования на обнаружение TAA
Лабораторная работа 23. Изучить подробности выполнения файла в песочнице
Лабораторная работа 24. Добавить сторонние правила IDS
Лабораторная работа 25. Написать свое правило IDS
Лабораторная работа 26. Создать исключение для IDS-правила
Лабораторная работа 27. Написать свое правило Yara
Лабораторная работа 28. Настроить интеграцию с Active Directory

5.5. Реагирование на инцидент

6. Технология Sandbox

6.1. Результаты анализа Sandbox

7. Обслуживание платформы KATA

7.1. External API

7.2. Отчеты

7.3. Уведомления и SIEM

7.4. Обновление

7.5. Сбор информации о системе

7.6. Сохранение и восстановление настроек

7.7. Обновление версии

7.8. Изменение системных настроек

7.9. Kaspersky Private Security Network (KPSN)

8. Отдельный модуль Kaspersky Endpoint Detection and Response (Cloud)

Подать заявку на обучение:

pk@ncot.by

rozum.ntec.by

+ 375(17)327-60-69
+ 375(17)328-60-16

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

rozum