

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:

1. Обзор решения

1.1. Изучаемые продукты и приложения

1.2. Ландшафт угроз

2. Подготовка к внедрению

2.1. Архитектура решения

2.2. Системные требования

2.3. Масштабирование

2.4. Типичные топологии

3. Развертывание платформы KATA

3.1. Организация процесса

3.2. Установка серверов

Лабораторная работа 1. Установить и настроить центральный узел

3.3. Активация и первоначальная настройка

Лабораторная работа 2. Настроить **Kaspersky Sandbox**

Лабораторная работа 3. Подключить центральный узел к **Sandbox**

Лабораторная работа 4. Активировать Центральный узел

Лабораторная работа 5. Создать учетную запись сотрудника службы информационной безопасности

3.4. Распределенная установка

4. Эксплуатация KATA

4.1. Подключение к источникам трафика

Лабораторная работа 6. Подключить центральный узел к сетевой инфраструктуре (**SPAN**)

Лабораторная работа 7. Проверить, что анализ трафика работает

Лабораторная работа 8. Подключить центральный узел к почтовой системе по протоколу **SMTP**

Лабораторная работа 9. Настроить почтовый сервер посылать копии сообщений на центральный узел

Лабораторная работа 10. Проверить, что анализ почты работает

Лабораторная работа 11. Устранить многократную проверку почтовых сообщений

Лабораторная работа 12. Подключить сенсор к прокси-серверу (**ICAP**)

Лабораторная работа 13. Проверить, что анализ **ICAP**-трафика работает

Лабораторная работа 14. Устранить многократную проверку **http**-трафика

4.2. Обработка обнаружений

4.3. Проверка работы технологий обнаружения

4.4. Идентификация угроз в трафике

5. Эксплуатация KEDR

5.1. Развертывание **Kaspersky Endpoint Agent**

Лабораторная работа 15. Включить **Kaspersky Endpoint Agent** задачей изменений компонентов **Kaspersky Endpoint Security**

Лабораторная работа 16. Установить **Kaspersky Endpoint Agent** с помощью **KSC**

Лабораторная работа 17. Подключить **Kaspersky Endpoint Agent** к центральному узлу

Лабораторная работа 18. Активировать **Kaspersky Endpoint Agent**

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

roz
um