

Обучение по программе **KL 034.2.1:** **Kaspersky Unified Monitoring and Analysis Platform**

Изучаемые продукты:

Основной продукт:

- Kaspersky Unified Monitoring and Analysis Platform 2.0.1
- Kaspersky Unified Monitoring and Analysis Platform 2.1

Смежные продукты, выступающие источниками событий, источниками данных для обогащения и средствами реагирования в лабораторных работах:

- Kaspersky Security Center 14
- Kaspersky Endpoint Security 11.10
- Kaspersky Security for Windows Server 11.1
- Kaspersky Anti Targeted Attack Platform 4.1

Смежные продукты, выступающие источниками данных для обогащения в теоретических материалах:

- Kaspersky CyberTrace 4.1
- Kaspersky Threat Lookup

По итогам обучения Вы получите:

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

Продолжительность: 24 академических часа

Стоимость: 2880 бел. рублей (с НДС 20%)

Форма обучения: очная (дневная)

Содержание программы:

1. Введение в SIEM

2. Архитектура и принципы работы KUMA

3. Установка

Лабораторная работа 1. Установить Kaspersky Unified Monitoring and Analysis Platform

4. Сбор событий

4.1. Принцип работы коллектора

4.2. Настройки подключения и коннектора

4.3. Получение событий Windows

Лабораторная работа 2. Настроить получение событий Windows

Лабораторная работа 3. Настроить получение событий Kaspersky Security Center

Лабораторная работа 4. Настроить получение событий KATA

5. Нормализация

5.1. Модель данных KUMA

5.2. Настройки нормализатора

5.3. Преобразование данных

5.4. Дополнительные нормализаторы

6. Обработка событий коллектором

6.1. Фильтрация

6.2. Агрегация

6.3. Обогащение

7. Интеграции

7.1. Интеграция с Kaspersky Security Center и работа с активами

7.2. Интеграция с LDAP и работа с учетными записями

7.3. Интеграция с Kaspersky Threat Lookup

7.4. Интеграция с Kaspersky CyberTrace

7.5. Интеграция с Kaspersky Kaspersky Endpoint Detection and Response

- Лабораторная работа 5. Настроить получение событий KSWs
-
- Лабораторная работа 6. Настроить обогащение данными из DNS
-
- Лабораторная работа 7. Настроить обогащение событий данными GeoIP
- Лабораторная работа 8. Импортировать информацию о компьютерах из KSC
- Лабораторная работа 9. Настроить обогащение данными из LDAP
- Лабораторная работа 10. Настроить обогащение данными из CyberTrace

8. Работа с событиями

9. Корреляция

9.1. Виды правил корреляции

9.2. Простые правила корреляции

9.3. Стандартные корреляционные правила: селекторы, группы корреляции

9.4. Локальные и глобальные переменные

- Лабораторная работа 11. Создать простое корреляционное правило
- Лабораторная работа 12. Создать стандартное корреляционное правило
- Лабораторная работа 13. Настроить алерт на события в определенном порядке

9.5. Активные списки и операционные правила корреляции

9.6. Ретроспективный поиск

Лабораторная работа 14. Создать техническое корреляционное правило для наполнения активного списка

Лабораторная работа 15. Создать корреляционное правило с использованием активного списка

Лабораторная работа 16. Создать корреляционное правило с использованием локальной переменной

Лабораторная работа 17. Применить ретроспективный поиск

10. Работа с алертами

11. Реагирование

11.1. Реагирование задачами Kaspersky Security Center

11.2. Реагирование запуском скрипта

11.3. Реагирование задачей Kaspersky Endpoint Detection and Response

Лабораторная работа 18. Настроить реагирование запуском задачи Kaspersky Security Center

Лабораторная работа 19. Настроить реагирование запуском задачи Kaspersky Endpoint Detection and Response

12. Отчетность

12.1. Панели мониторинга

12.2. Отчеты

12.3. Метрики

Лабораторная работа 20. Изучить отчетность

Лабораторная работа 21. Отправить запрос в Kaspersky Unified Monitoring and Analysis Platform через REST API (опционально)

13. Что нового в KUMA 2.1

Лабораторная работа 22. Обновить Kaspersky Unified Monitoring and Analysis до версии 2.1

Лабораторная работа 23. Добавить актуальный контент из репозитория доступных обновлений Лаборатории Касперского

Лабораторная работа 24. Настроить «холодное» хранение событий в Kaspersky Unified Monitoring and Analysis Platform

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