

Kaspersky Unified Monitoring and Analysis Platform. Investigation (051.4)

ID KL-051.4 Цена 48 000,- руб. Длительность 2,5 дня

Предварительные требования

Чтобы успешно усвоить весь материал данного курса вам будут полезны знания и навыки работы с KUMA, которые вы можете получить пройдя учебный курс [Kaspersky Unified Monitoring and Analysis Platform. Administration \(034.4\)](#).

Также необходимы общие знания о типах современных атак, способах их выявления.

Цели курса

Теоретический материал и лабораторные работы дают необходимые знания и навыки, благодаря которым слушатель сможет выполнять задачи по детектированию и обнаружению угроз, используя Kaspersky Unified Monitoring and Analysis Platform.

По окончании курса слушатели смогут:

- Настраивать обработку событий (нормализация, агрегация, обогащение и т.д.).
- Создавать правила корреляции и анализа данных для выявления угроз
- Создавать различные правила реагирования на угрозы
- Использовать ресурсы и функции KUMA для анализа и выявления угроз (активные списки, словари, переменные, API и т.п.)
- Выявить угрозы, анализируя полученные события.

Содержание курса

Kaspersky Unified Monitoring and Analysis Platform (KUMA) является решением класса SIEM для сбора, хранения, обработки, корреляции и визуализации разрозненных данных.

Программа курса

- 1. Введение

- 2. Сбор событий
- 3. Работа с активами
- 4. Поиск событий
- 5. Корреляция
- 6. AI
- 7. Реагирование
- 8. Панели мониторинга и отчеты

- Лабораторная работа 1 Активация KUMA
- Лабораторная работа 2 Нормализация событий нового источника
- Лабораторная работа 3 Нормализация событий еще одного нового источника
- Лабораторная работа 4 Настройка обогащения событий
- Лабораторная работа 5 Сбор данных и эксфильтрация, установка C&C туннеля
- Лабораторная работа 6 Сбор данных о системе, использование стеганографии, эксфильтрация данных
- Лабораторная работа 7 Kerberoasting, эксфильтрация данных через HTTP GET
- Лабораторная работа 8 Атака Pass-the-hash, эксфильтрация данных через ssh
- Лабораторная работа 9 Атака HTA
- Лабораторная работа 10 Shadow session и Dll hijacking
- Лабораторная работа 11 Закрепление в системе
- Лабораторная работа 12 Самостоятельное задание
- Лабораторная работа 13 Отображение текущего состояния