

## KL 059.2:

# Kaspersky XDR Expert. Investigation

## Описание курса

Kaspersky XDR Expert — надежное решение для кибербезопасности для защиты корпоративной ИТ-инфраструктуры от сложных киберугроз.

Kaspersky XDR Expert позволяет:

- Собирать телеметрию и хранить её в виде удобном для анализа.
- Вручную и автоматически анализировать собранные данные и выявлять угрозы.
- Опираясь на отчеты и панель мониторинга комплексно оценивать уровень корпоративной безопасности.
- Анализировать этапы развития киберугроз используя граф расследования.
- Автоматически и вручную реагировать на угрозы, что в комбинации с интеграционными возможностями продукта позволяет реализовывать сложные сценарии защиты.
- Эффективно работать с собранными данными. Интерфейс предоставляет пользователю удобные методы взаимодействия, включая контекстные действия по поиску и реагированию, отображению данных, построение графа расследования.

Теоретический материал и лабораторные работы дают необходимые знания и навыки, благодаря которым слушатель сможет выявлять угрозы, расследовать их, выполнять задачи по реагированию вручную и создавать плейбуки для автоматического реагирования.

По окончании курса слушатели смогут:

- Выявлять угрозы, анализируя полученную телеметрию
- Создавать правила корреляции и анализа данных для выявления угроз
- Использовать данный TI для обогащения расследования
- Использовать AI в ходе расследования
- Собирать и использовать индикаторы компрометации, правила YARA
- Создавать различные правила реагирования на угрозы
- Создать плейбуки для автоматического реагирования на угрозы

Вопросы по установке, подключению телеметрии, администрированию, интеграциям, миграции рассматриваются в курсе KL 048.2.

# Длительность

2 дня (16 часов)

## Требования к участникам

Чтобы успешно усвоить весь материал данного курса вам будут полезны знания и навыки работы с Kaspersky XDR Expert, которые вы можете получить пройдя учебный курс:

- KL 048.2 Kaspersky XDR Expert. Administration.

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

## Темы

- 1. Общие сведения
- 2. Поиск угроз
- 3. Правила детектирования
- 4. Sandbox
- 5. AI
- 6. Активы
- 7. Алерты и Инциденты
- 8. Реагирование
- 9. Плейбуки
- 10. Дашборды и API

## Лабораторные работы

|                        |                                                         |
|------------------------|---------------------------------------------------------|
| Лабораторная работа 1. | Активация продукта                                      |
| Лабораторная работа 2. | Компрометация веб-сервера с эскалацией привилегий       |
| Лабораторная работа 3. | Компрометация рабочей станции и домена Windows          |
| Лабораторная работа 4. | Фишинговая атака через HTA-файл с кражей учётных данных |
| Лабораторная работа 5. | Process Injection: внедрение кода в легитимный процесс  |
| Лабораторная работа 6. | API Kaspersky XDR Expert                                |