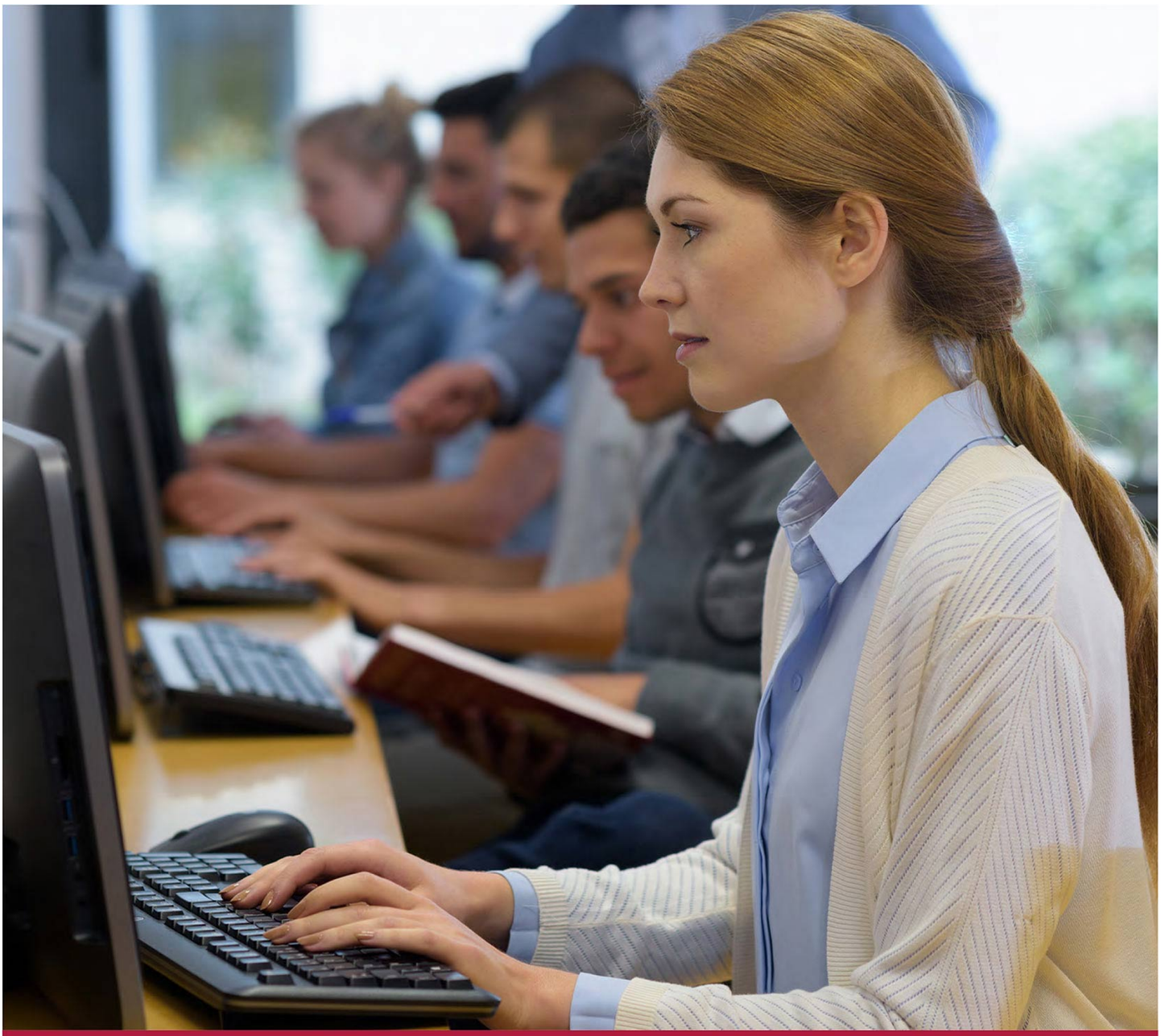
softline учебный центр



Kaspersky XDR Expert. Investigation

Код курса: KL 059.2

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

Kaspersky XDR Expert. Investigation

Код курса: KL 059.2

Длительность	16 ак. часов
Формат	
Разработчик курса	Лаборатория Касперского
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

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

Подробная информация

Профиль аудитории:

- сотрудникам службы информационной безопасности
- пресейл-специалисты

Предварительные требования:

- 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
- представление о современных угрозах и тенденциях развития информационных технологий

По окончании курса слушатели изучат:

- 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 индикаторв компрометации, правила YARA
- создавать различные правила реагирования на угрозы
- создать плейбуки для автоматического реагирования на угрозы

Программа курса

Модуль 1. Общие сведения

Модуль 2. Поиск угроз

Модуль 3. Правила детектирования

Модуль 4. Sandbox

Модуль 5. AI

Модуль 6. Активы

Модуль 7. Алерты и инциденты

Модуль 8. Реагирование

Модуль 9. Плейбуки

Модуль 10. Дашборды и API

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 учетных данных

Лабораторная работа 5. Process Injection: внедрение кода в легитимный процесс

Лабораторная работа 6. API Kaspersky XDR Expert

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!

Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **18 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline
Вы можете узнать из профайла.