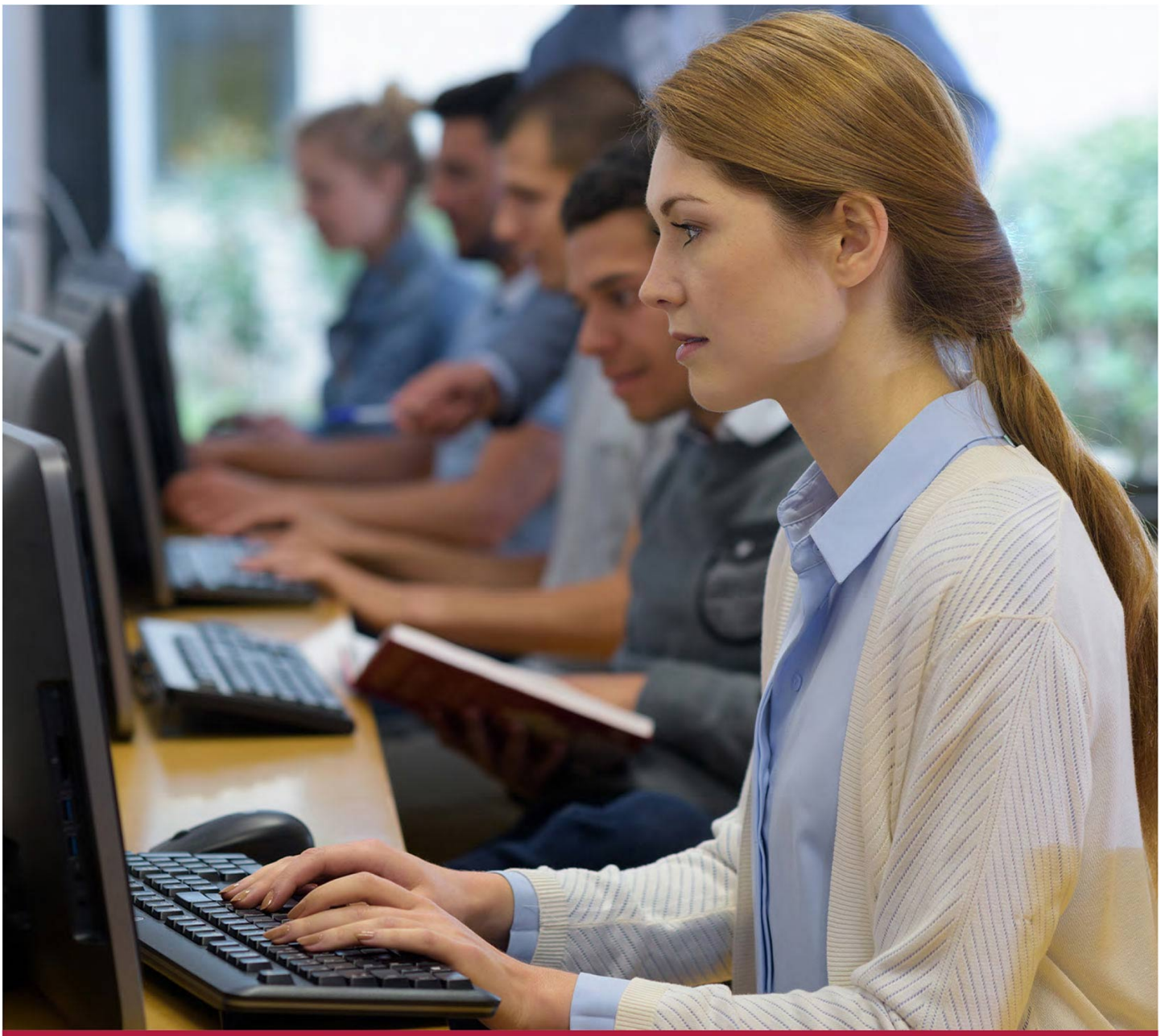
softline учебный центр



Kaspersky Symphony XDR Core

Код курса: KL 032.1.1

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

Kaspersky Symphony XDR Core

Код курса: KL 032.1.1

Длительность	12 ак. часов
Формат	
Разработчик курса	Лаборатория Касперского
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Kaspersky Symphony XDR Core — надежное решение для кибербезопасности для защиты корпоративной ИТ-инфраструктуры от сложных киберугроз. Kaspersky Symphony XDR Core позволяет: Собирать данные из множества различных источников и хранить их в виде удобном для анализа. Службы-коллекторы способны получать и приводить к единому формату данные из множества различных источников. Данные хранятся в аналитической высокопроизводительной СУБД ClickHouse. Продукт поставляется с набором готовых к использованию нормализаторов. Вручную и автоматически анализировать собранные данные и выявлять угрозы. Корреляторы имеют гибкие возможности для реализации даже самой сложной логики детектирования. В комплект поставки включен набор разнообразных правил корреляции. Опираясь на отчеты и панель мониторинга комплексно оценивать уровень корпоративной безопасности. Анализировать этапы развития киберугроз используя граф расследования. Анализировать действия угрозы, используя собранную телеметрию, при интеграции с решением KEDR. Управлять конечными устройствами и надежно защищать их с помощью Kaspersky Endpoint Security. Автоматически и вручную реагировать на угрозы, что в комбинации с интеграционными возможностями продукта позволяет реализовывать сложные кросс-продуктовые сценарии защиты. Эффективно работать с собранными данными. Веб-интерфейс предоставляет пользователю удобные методы взаимодействия, включая контекстные действия по поиску и реагированию, визуализации данных, построение графа расследования. Теоретический материал и лабораторные работы дают необходимые знания и навыки, благодаря которым слушатель сможет спланировать и выполнить развертывание и настройку решения, будет понимать принципы использования решения и сможет выполнять задачи по его обслуживанию.

Подробная информация

Профиль аудитории:

Системные администраторы, пользователи.

Предварительные требования:

Для успешного прохождения курса желательно обладать знаниями и навыками работы с Kaspersky Unified Monitoring and Analysis Platform (KUMA) и Kaspersky Security Center (KSC).

По окончании курса слушатели смогут:

- Включать шифрование на рабочих станциях.
- Управлять шифрованием на рабочих станциях и съемных накопителях.
- Восстанавливать доступ к данным на зашифрованных носителях.
- Собирать данные из множества различных источников и хранить их 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.
- Анализировать действия угрозы, используя собранную телеметрию, при интеграции с решением KEDR.
- Управлять конечными устройствами и надежно защищать их с помощью Kaspersky Endpoint Security.
- Автоматически и вручную реагировать на угрозы, что в комбинации с интеграционными возможностями продукта позволяет реализовывать сложные кросс-продуктовые сценарии защиты.
- Эффективно работать с собранными данными.

Программа курса

Модуль 1 «Введение»

Модуль 2 «Возможности»

Модуль 3 «Архитектура»

Модуль 4 «Требования»

Модуль 5 «Установка»

- Лабораторная работа №1.1 «Установка Kaspersky Symphony XDR Core»

Модуль 6 «Интеграции»

- Kaspersky Anti Targeted Attack Platform и Kaspersky Endpoint Detection and Response Expert
- Kaspersky Security Center
- Kasepersky Threat Intelligence Portal
- Интеграция с Microsoft Active Directory
- Kaspersky Automated Security Awareness Platform
- Kaspersky Industrial CyberSecurity for Networks
- Пользовательская интеграция

Модуль 7 «Алерты»

Модуль 8 «Поиск угроз»

- Лабораторная работа №1.2 «Установка Kaspersky Symphony XDR Core (продолжение)»

- Лабораторная работа №2 «Интеграция с KATA Platform»
- Лабораторная работа №3 «Интеграция с Microsoft Active Directory»
- Лабораторная работа №4 «Интеграция с Kaspersky Security Center»

Модуль 9 «Инциденты»

Модуль 10 «Плейбуки»

- Общие свойства
- Триггер
- Алгоритм
- Лабораторная работа №5 «Написание JQ-фильтров»
- Лабораторная работа №6 «Запуск плейбука проверки на наличие вредоносных объектов»
- Лабораторная работа №7 «Запуск плейбука изоляции хоста в автоматическом режиме»
- Лабораторная работа №8 «Создание плейбука для блокировки учетных записей пользователей»
- Лабораторная работа №9 «Создание плейбука выполняющего два действия»
- Лабораторная работа №10 «Автоматическое создание инцидентов»

Модуль 11 «Администрирование»

Модуль 12 «Troubleshooting»

Модуль 13 «Обслуживание»

- Лабораторная работа №11 «Вывод данных о запущенных подах»
- Лабораторная работа №12 «Подключение к Kaspersky Symphony XDR Core по API»

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.