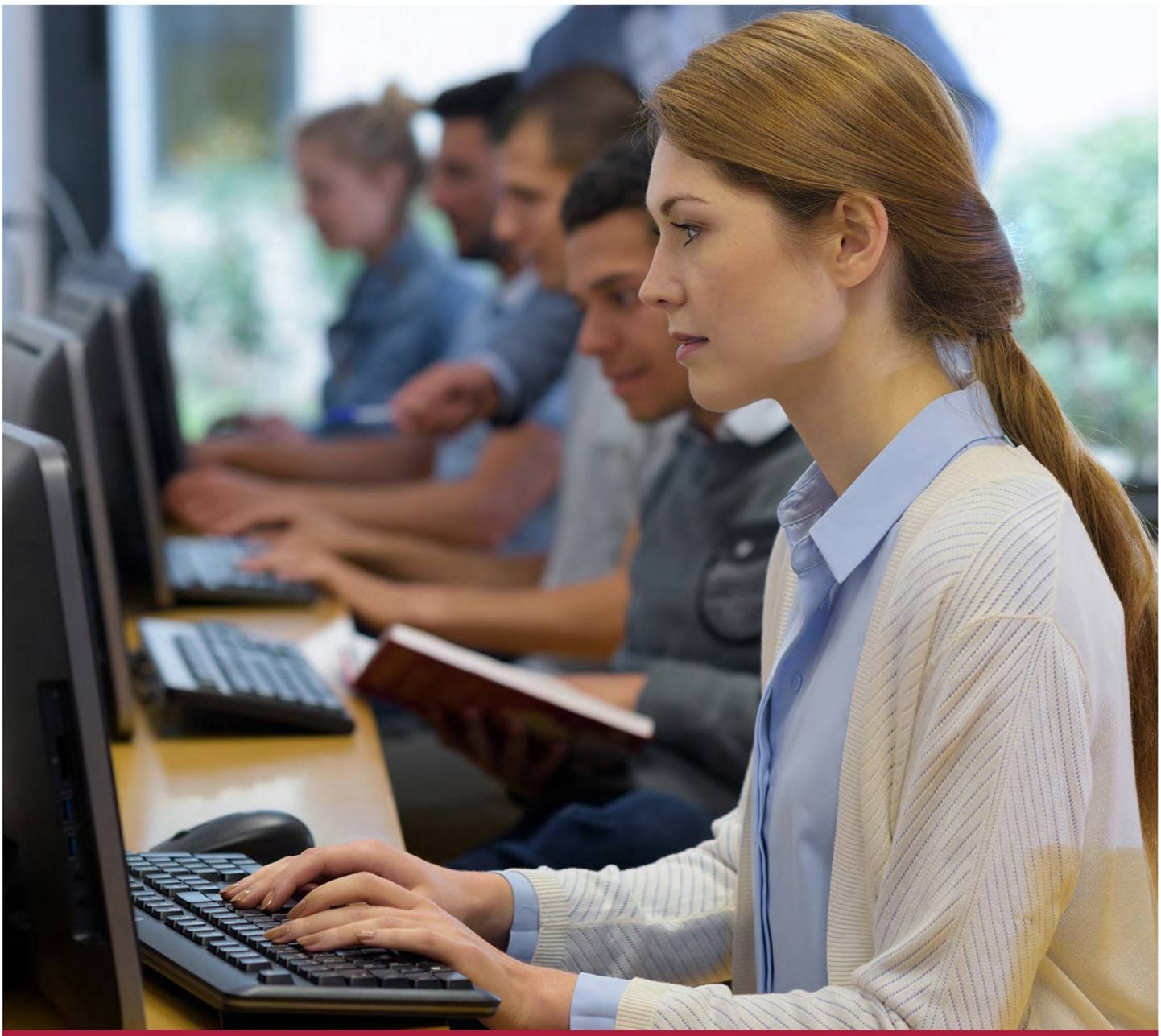
softline учебный центр



# Kaspersky EDR Optimum2.0

Код курса: KL 024.2

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

**Kaspersky EDR Optimum2.0**

Код курса: KL 024.2

| | |
|---|---|
| **Длительность** | 8 ак. часов |
| **Формат** | Очно; Дистанционно |
| **Разработчик курса** | Лаборатория Касперского |
| **Тип** | Учебный курс |
| **Способ обучения** | Под руководством тренера |

## О курсе

Кибератаки с каждым годом становятся сложнее и наносят всё больший ущерб бизнесу. Однако основная мишень киберпреступников остается прежней – рабочие места сотрудников. В то же время развиваются и средства защиты – трендом последних лет в области информационной безопасности стали технологии класса EDR. Они помогают обнаружить атаки, обходящие традиционные средства защиты, и точно на них отреагировать. Kaspersky EDR Optimum объединяет новейшие технологии защиты рабочих мест и гибкие инструменты контроля с технологиями EDR, которые эффективно противодействуют сложным атакам и повышают прозрачность инфраструктуры. Благодаря управлению всеми функциями из единой консоли и автоматизированным инструментам, решение повышает прозрачность инфраструктуры и экономит время администраторов.

## Подробная информация

**Профиль аудитории:**

- администраторы Kaspersky Security Center и Kaspersky Endpoint Security
- специалисты, отвечающие за обеспечение безопасности конечных точек (Endpoint Security) в корпоративной сети

**Предварительные требования:**

- знания основ работы с Kaspersky Security Centeри Kaspersky Endpoint Security
- представление о современных угрозах, типичных этапах развития атаки и типичных процедурах по расследованию инцидентов компьютерной безопасности

**По окончании курса слушатели смогут:**

- смогут рассказать, из каких приложений состоит и какие возможности предоставляет Kaspersky EDR Optimum
- смогут развернуть продукт, продемонстрировать его возможности и анализировать детали события обнаружения вредоносной активности

# Программа курса

**Модуль 1. Введение**

- Чего не хватает EPP решению
- Расширение возможностей Kaspersky Endpoint Security для бизнеса

**Модуль 2. Развертывание**

- Аппаратные и программные требования
- План внедрения
- Лабораторная работа: Как развернуть Kaspercky Endpoint Detection and Response
- План миграции
- Как включить Kaspersky Endpoint Detection and Response
- Лабораторная работа 2. Как подготовить Kaspersky EDR к работе

**Модуль 3. Обогащенное событие обнаружения**

- Обогащенные и необогащенные события
- Детали обнаружения
- Требования для создания карточки обнаружения

**Модуль 4. Анализ деталей события обнаружения**

- Информация об обнаруженном объекте
- Информация о созданных файлах
- Информация о внедрениях и сетевых соединениях
- Информация об изменениях в реестре
- Информация о родительском процессе
- Лабораторная работа: Как работать с карточкой обнаружения

**Модуль 5.  Сдерживание угрозы**

- Изоляция устройства
- Запрет запуска объекта
- Лабораторная работа: Как настроить запрет запуска объекта
- Помещение файлов на карантин

**Модуль 6. Проверка на наличие индикаторов компрометации**

- Создание индикатора компрометации
- Задача поиска индикаторов компрометации

**Модуль 7. Устранение последствий**

- Лабораторная работа: Как создавать и искать индикаторы компрометации

**Модуль 8. Интеграция с Kaspersky Sandbox**

**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.