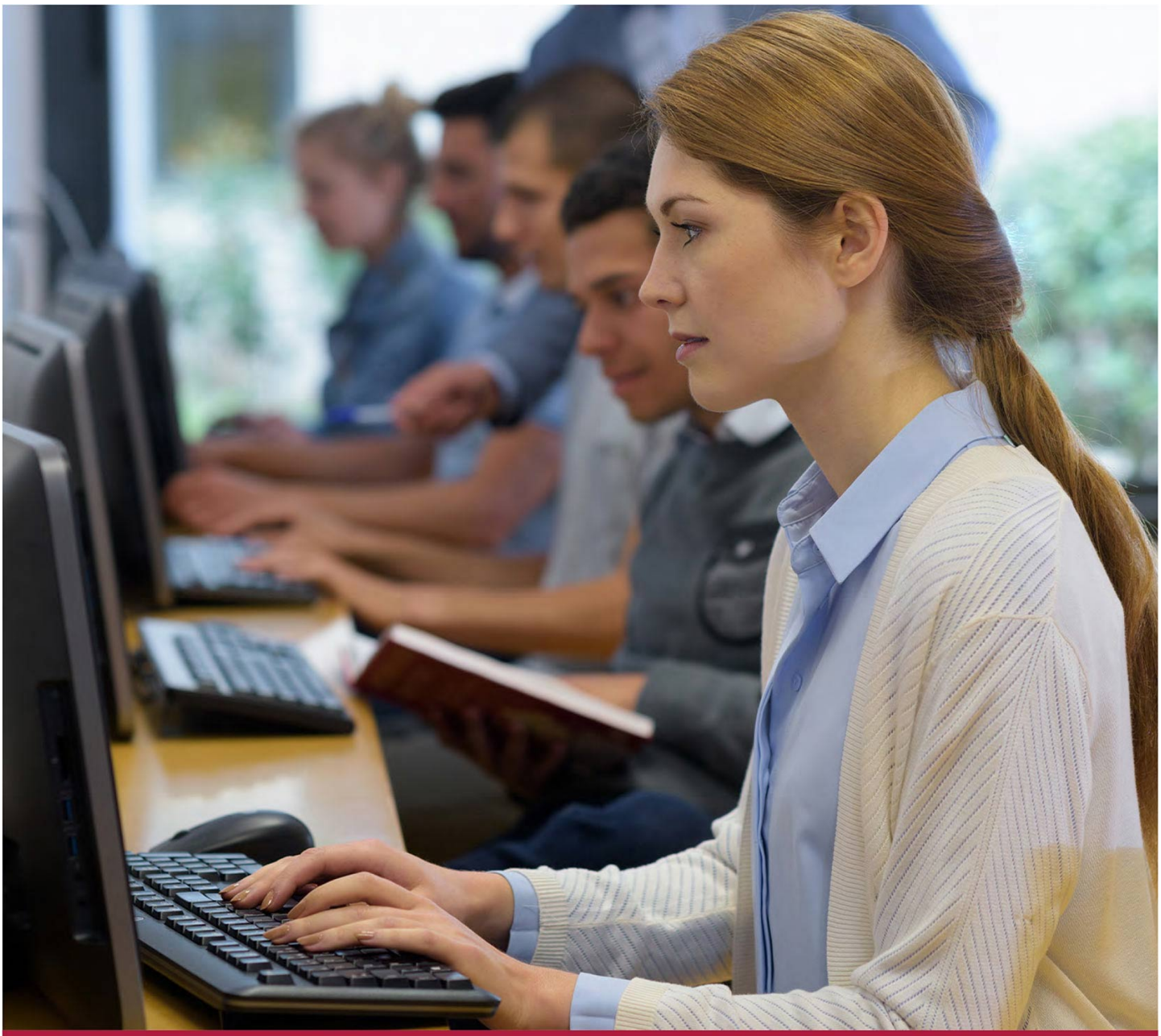
softline учебный центр



Kaspersky Industrial CyberSecurity Investigation

Код курса: KL 060.4.5

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

Kaspersky Industrial CyberSecurity Investigation

Код курса: KL 060.4.5

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

О курсе

Используя теоретические материалы и лабораторные работы, курс дает знания и навыки использования продуктов Kaspersky Industrial CyberSecurity в основных сценариях: настройка компонентов для обнаружения угроз и защиты от атак; анализ событий обнаружения угроз; расследование киберинцидентов.

Подробная информация

Профиль аудитории:

В первую очередь курс разработан для инженеров, отвечающих за внедрение и эксплуатацию систем защиты промышленных объектов от киберугроз.

Материалы курса могут также быть интересны:

- сотрудникам службы информационной безопасности, который осуществляют мониторинг состояния защиты промышленного объекта и реагируют на инциденты;
- специалистам предпродажной подготовки, которые консультируют заказчика по вопросам возможностей и оптимальных сценариев внедрения и использования продукта.

Предварительные требования:

Понимание основ компьютерных и сетевых технологий. Хорошее понимание стека протоколов TCP/IP. Базовые навыки администрирования ОС Windows и Linux. Базовые знания об информационной безопасности. Представление о назначении, принципе построения и работы систем промышленной автоматизации.

Программа курса

Часть I. Kaspersky Industrial CyberSecurity for Networks

- Мониторинг сети

- 1.Контроль рисков
- 2. Информация о сетевых сессиях
- Лабораторная работа 1. Настроить интеграцию KICS for Nodes с KICS for Networks
- Лабораторная работа 2. Включить обнаружение рисков
- Лабораторная работа 3. Включить регистрацию сетевых сессий
- 3.Технологии обнаружения сетевых атак и аномалий
- Управление правилами IDS
- Обнаружение аномалий в сетевых сессиях
- Обнаружение атак и аномалий
- 1.Технологии обнаружения
- 2. Сценарий возможной атаки
- 3.Обнаружение неразрешенных устройств и сетевых взаимодействий
- 4.Обнаружение сетевых вторжений (IDS)
- Лабораторная работа 4. Обнаружить постороннее устройство в сети
- Лабораторная работа 5. Обнаружить сканирование сети
- Лабораторная работа 6. Обнаружить подбор пароля к сетевому сервису
- Лабораторная работа 7. Обнаружить неразрешенное взаимодействие с ПЛК
- Лабораторная работа 8. Обнаружить вмешательство в работу ПЛК
- Аудит устройств
- 1.Контроль конфигурации устройств Windows и Linux
- Лабораторная работа 9. Настроить контроль конфигурации устройств
- 2.Обнаружение аномалий с помощью Sigma-правил
- Лабораторная работа 10. Настроить обнаружение аномалий с помощью Sigma-правил
- 3.Аудит безопасности устройств по правилам
- Лабораторная работа 11. Провести аудит безопасности компьютера SCADA

Часть II. Kaspersky Industrial CyberSecurity for Nodes

- Бессигнатурная защита
- 1.Защита от эксплойтов
- 2.Анализ журналов
- Сигнатурная защита
- 1.Защита файлов
- 2.Защита от шифрования
- 3.Защита от сетевых угроз
- 4.AMSI-защита
- Лабораторная работа 12. Настроить защиту узла от программ-вымогателей
- Лабораторная работа 13. Настроить защиту узла от сетевых атак
- Лабораторная работа 14. Настроить анализ журналов Windows для выявления аномалий в системе
- Портативный сканер
- Мониторинг состояния защиты в Kaspersky Security Center
- 1.Формирование отчетов в KSC

Часть III. Функции EDR

- Функции и возможности Endpoint Agent
- 1.Функции и возможности Endpoint Agent
- 2.Взаимодействия Endpoint Agent

- Реагирование на событие обнаружения
- 1.Как реагировать на событие обнаружения?
- 2.Детали обнаружения
- Лабораторная работа 15. Имитировать атаку на сервер SCADA
- Лабораторная работа 16. Имитировать атаку на рабочую станцию Admin-OT
- Лабораторная работа 17. Изучить следы атаки в Kaspersky Security Center
- 3. Сдерживание угрозы
- 4. Проверка компьютеров на наличие индикаторов компрометации
- Лабораторная работа 18. Найти индикаторы компрометации
- Лабораторная работа 19. Настроить запрет запуска вредоносных скриптов

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.