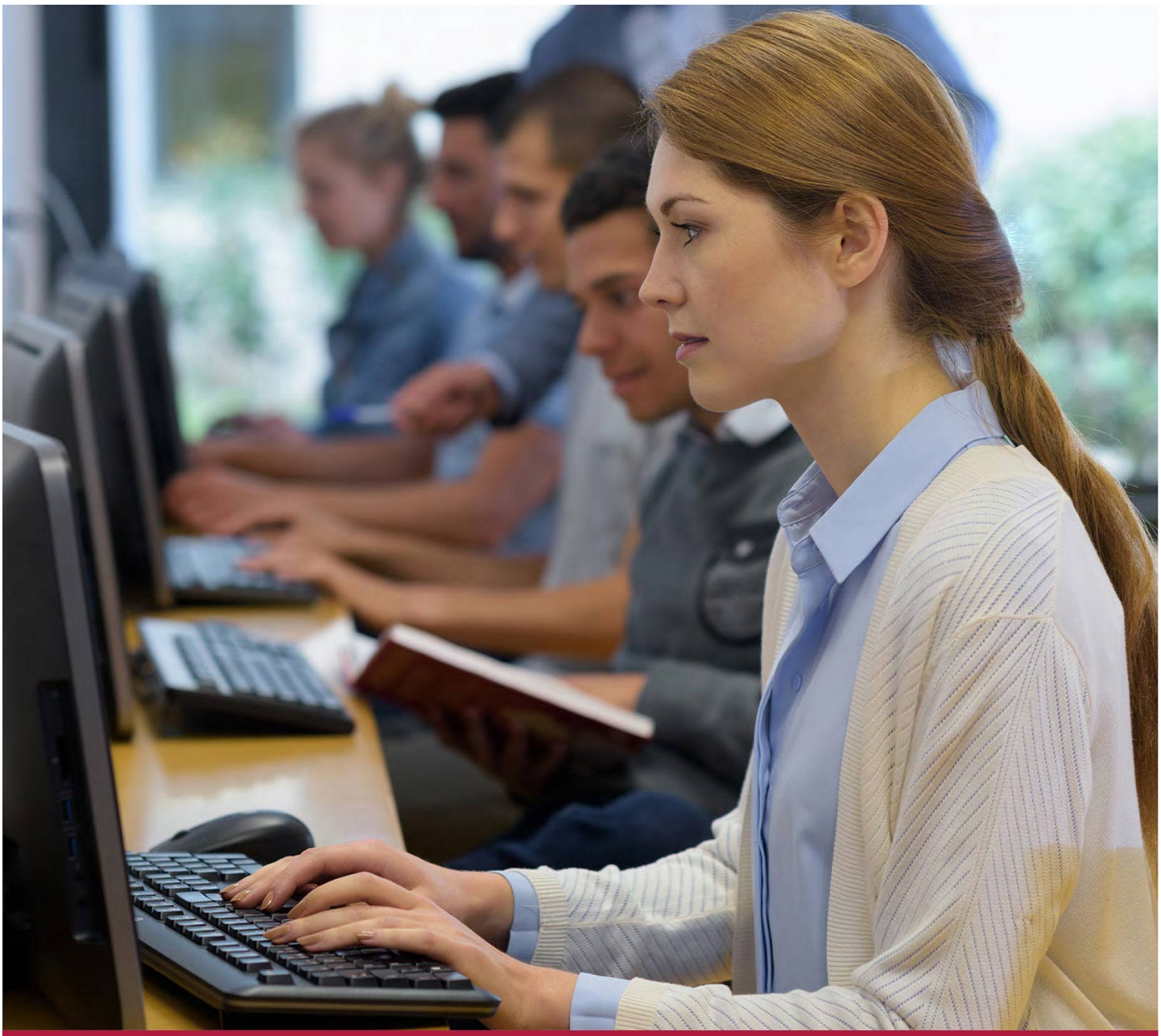
softline учебный центр



Kaspersky Industrial CyberSecurity. Investigation. Расширенный курс (комплексный)

Код курса: KL 060.4.5K

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

Kaspersky Industrial CyberSecurity. Investigation. Расширенный курс (комплексный)

Код курса: KL 060.4.5K

Длительность	24 ак. часа
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. В рамках прохождения курса предусмотрен вводный модуль, подготавливающий к более профильным и практическим задачам реализаций возможностей Kaspersky Industrial CyberSecurity. Изучаемые продукты: Kaspersky Industrial CyberSecurity for Nodes Kaspersky Industrial CyberSecurity for Linux Nodes Kaspersky Industrial CyberSecurity for Networks Kaspersky Industrial CyberSecurity Endpoint Detection and Response Изучаемые приложения: Kaspersky Industrial CyberSecurity for Windows Nodes 4.0 Kaspersky Industrial CyberSecurity for Linux Nodes 2.0 Kaspersky Industrial CyberSecurity for Networks 4.5 Kaspersky Security Center Linux 16.0 Kaspersky Endpoint Agent 4.0 Этот комплексный курс состоит из 2-х курсов: KL P38.4.5 Kaspersky Industrial CyberSecurity Fundamentals KL 060.4.5 Kaspersky Industrial CyberSecurity. Administration

Подробная информация

Профиль аудитории:

- инженеры, отвечающие за внедрение и эксплуатацию систем защиты промышленных объектов от киберугроз
- специалисты информационной безопасности, которые осуществляют мониторинг состояния защиты промышленного объекта и реагируют на инциденты
- специалисты 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

По окончании курса слушатели изучат:

- определение понятию АСУ ТП
- основной функционал продуктов, входящих в состав решения Kaspersky Industrial CyberSecurity
- настройку компонентов для обнаружения угроз и защиты от атак
- анализ событий обнаружения угроз
- расследование киберинцидентов

Программа курса

Модуль 1. Kaspersky Industrial CyberSecurity Fundamentals

- Введение в безопасность АСУ ТП
- Kaspersky Security Center
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Industrial CyberSecurity for Nodes
- EDR возможности
- Лицензирование и поддержка

Модуль 2. Мониторинг сети

- Контроль рисков
- 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

- Технологии обнаружения сетевых атак и аномалий. Управление правилами IDS.
- Обнаружение аномалий в сетевых сессиях

Модуль 3. Обнаружение атак и аномалий

- Технологии обнаружения
- Сценарий возможной атаки
- Обнаружение неразрешенных устройств и сетевых взаимодействий
- 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

Модуль 4. Аудит устройств

- Контроль конфигурации устройств Windows и Linux

Лабораторная работа 9. Настроить контроль конфигурации устройств

- Обнаружение аномалий с помощью Sigma-правил

Лабораторная работа 10. Настроить обнаружение аномалий с помощью Sigma-правил

- Аудит безопасности устройств по правилам

Лабораторная работа 11. Провести аудит безопасности компьютера SCADA

Модуль 5. Бессигнатурная защита

- Защита от эксплойтов
- Анализ журналов

Модуль 6. Сигнатурная защита

- Защита файлов
- Защита от шифрования
- Защита от сетевых угроз
- 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

Модуль 7. Портативный сканер

Модуль 8. Мониторинг состояния защиты в Kaspersky Security Center

- Формирование отчетов в KSC

Модуль 9. Функции и возможности Endpoint Agent

- Функции и возможности Endpoint Agent
- Взаимодействия Endpoint Agent

Модуль 10. Реагирование на событие обнаружения

- Как реагировать на событие обнаружения?
- 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

- Сдерживание угрозы
- 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.