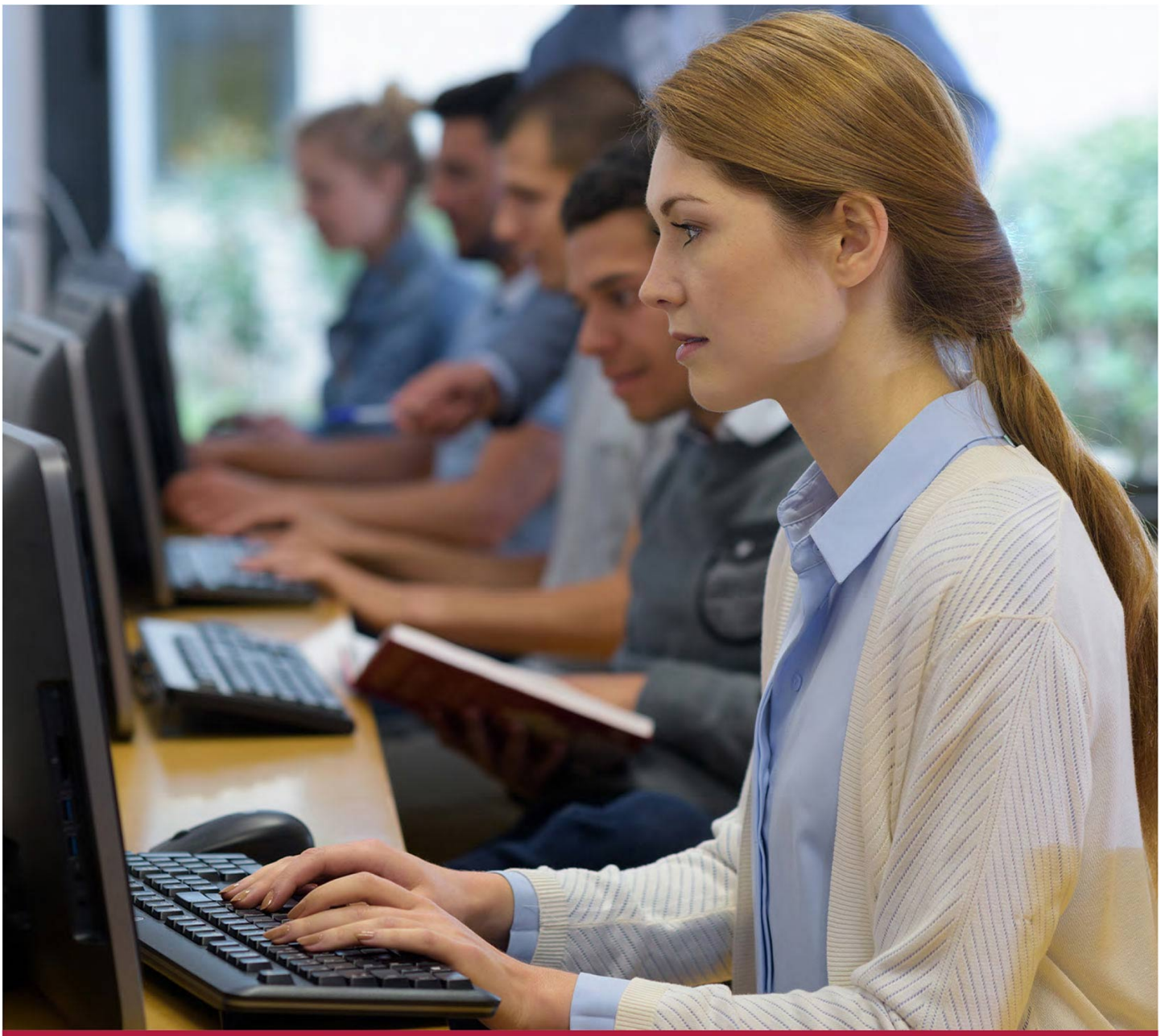
softline учебный центр



Kaspersky Industrial CyberSecurity. Administration. Расширенный курс (комплексный)

Код курса: KL 038.4.5K

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

Kaspersky Industrial CyberSecurity. Administration. Расширенный курс (комплексный)

Код курса: KL 038.4.5K

Длительность	32 ак. часа
Формат	
Разработчик курса	Лаборатория Касперского
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Данный курс предназначен для специалистов по информационной безопасности, которые еще не знакомы со спецификой обеспечения информационной безопасности на промышленных объектах, и которым необходимо сформировать общее представление о возможностях Kaspersky Industrial CyberSecurity для защиты данных объектов. 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 Nodes 4.0 Kaspersky Industrial CyberSecurity for Linux Nodes 2.0 Kaspersky Industrial CyberSecurity for Networks 4.5 Kaspersky Security Center 16 Сервер администрирования Kaspersky Security Center Агент администрирования Kaspersky Security Center Веб-консоль Kaspersky Security Center Kaspersky Endpoint Agent 4.0 Этот комплексный курс состоит из 2-х курсов: KL P38.4.5 Kaspersky Industrial CyberSecurity Fundamentals KL 038.4.5 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
- развертывание продукта
- первоначальная настройка и активация Kaspersky Industrial CyberSecurity
- настройка решения для обнаружения угроз и защиты от атак
- диагностика работы продуктов Kaspersky Industrial CyberSecurity
- сопровождение и эксплуатация

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. Kaspersky Security Center

- Базовая информация о Kaspersky Security Center
- Состав и архитектура Kaspersky Security Center
- Функции Kaspersky Security Center
- MMC-консоль Kaspersky Security Center
- Web-консоль Kaspersky Security Center
- Плагин управления
- Политики
- Задачи
- Установка
- Активация и обновление баз

Модуль 3. Kaspersky Industrial CyberSecurity for Networks

1. **Развертывание Kaspersky Industrial CyberSecurity for Networks**

- Архитектура и принцип работы
- Подготовка к установке
- Установка
- Первоначальная настройка
- Интеграция с Kaspersky Security Center

2. **Инвентаризация сети**

- Технологии инвентаризации
- Инвентаризация устройств
- Анализ промышленных протоколов
- Обнаружение сетевых взаимодействий
- Карта сети

3. **Обслуживание Kaspersky Industrial CyberSecurity for Networks**

- Мониторинг состояния продукта
- Отчеты
- Журналы продукта
- Хранение и ротация служебных данных
- Сбор информации для обращения в поддержку

4. **Интеграции Kaspersky Industrial CyberSecurity for Networks**

- Возможности интеграции
- Интеграция с Kaspersky Security Center
- Интеграция с другими системами
- Интеграция по REST API
- Интеграция с KICS for Nodes

Лабораторная работа 1. Установить сервер KICS for Networks

Лабораторная работа 2. Активировать и обновить KICS for Networks

Лабораторная работа 3. Включить перехват трафика

Лабораторная работа 4. Включить обнаружение активности устройств

Лабораторная работа 5. Включить обнаружение информации об устройствах

Лабораторная работа 6. Выполнить активный опрос устройств

Лабораторная работа 7. Включить обнаружение устройств для контроля процесса

Лабораторная работа 8. Включить контроль проектов ПЛК и распознавание параметров (тегов) проектов ПЛК

Лабораторная работа 9. Включить контроль команд

Лабораторная работа 10. Выполнить контроль конфигурации ПЛК

Лабораторная работа 11. Включить контроль параметров промышленного процесса

Лабораторная работа 12. Включить контроль целостности сети

Лабораторная работа 13. Настроить карту сети

Лабораторная работа 14. Завершить настройку KICS for Networks

Лабораторная работа 15. Настроить отображение данных из KICS for Networks в Kaspersky Security

Center

Лабораторная работа 16. Собрать информацию о работе программы

Модуль 4. Kaspersky Industrial CyberSecurity for Nodes

1. **Развертывание Kaspersky Industrial CyberSecurity for Nodes**

- Область применения KICS for Nodes
- Состав и архитектура KICS for Nodes
- Требования к оборудованию
- Комплект поставки
- Способы установки
- Порядок развертывания KICS for Nodes
- Результаты установки
- Консоль управления KICS for Nodes

2. **Защита узлов промышленной сети с помощью Kaspersky Industrial CyberSecurity for Nodes**

- Меры, реализуемые KICS for Nodes для защиты узлов сети
- Как вредоносные программы попадают на устройства
- Что вредоносные программы делают на узлах АСУ ТП
- Типы защит KICS for Nodes
- Бессигнатурная защита
- Контроль запуска программ
- Контроль устройств
- Контроль Wi-Fi соединений
- Управление сетевым экраном
- Контроль технологического процесса
- Мониторинг файловых операций
- Анализ журналов
- Мониторинг доступа к реестру
- Контроль целостности ПЛК

3. **Интеграции Kaspersky Industrial CyberSecurity for Nodes**

- Передача данных в SCADA при помощи Kaspersky Security Gateway
- Интеграция с SIEM

4. **Обслуживание Kaspersky Industrial CyberSecurity for Nodes**

- Настройка прав доступа к программе
- Наблюдаем за состоянием защиты (Health Check)
- Сбор диагностической информации

Лабораторная работа 17. Подготовить инфраструктуру к развертыванию KICS for Nodes

Лабораторная работа 18. Развернуть Агент администрирования Kaspersky Security Center и KICS for Nodes

Лабораторная работа 19. Установить Консоль управления KICS for Nodes

Лабораторная работа 20. Подключить KICS for Nodes к KICS for Networks

Лабораторная работа 21. Настроить Контроль запуска программ в KICS for Nodes для работы в неблокирующем режиме

Лабораторная работа 22. Заблокировать запуск неавторизованных приложений на узлах АСУ ТП

Лабораторная работа 23. Настроить Мониторинг файловых операций KICS for Nodes для контроля файлов АСУ ТП

Лабораторная работа 24. Настроить проверку целостности проектов ПЛК

Лабораторная работа 25. Завершить настройку KICS for Nodes

Модуль 5. Kaspersky Industrial CyberSecurity for Linux Nodes

1. **Почему Linux требует защиты**

- Компоненты KICS for Linux Nodes

2. **Как защитить устройства**

- Как защититься от сетевых атак
- Как защититься от вредоносного ПО
- Как укрепить компьютер

3. **Управление KICS for Linux Nodes при помощи утилиты kics-control**

- Зачем использовать командную строку
- Как узнать статус приложения KICS for Linux Nodes
- Как управлять задачами
- Работа с событиями

Лабораторная работа 26. Настроить Kaspersky Security Center Linux

Лабораторная работа 27. Установить KICS for Linux Nodes на управляемые устройства

Лабораторная работа 28. Настроить базовую защиту компьютера с операционной системой Linux

Лабораторная работа 29. Настроить расширенную защиту сервера с операционной системой Linux

Лабораторная работа 30. Работа с контролем безопасности на компьютере с ОС Linux

Лабораторная работа 31. Управление защитой с помощью kics-control

Лабораторная работа 32. Управление учетными записями в Linux и администрирование устройств

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.