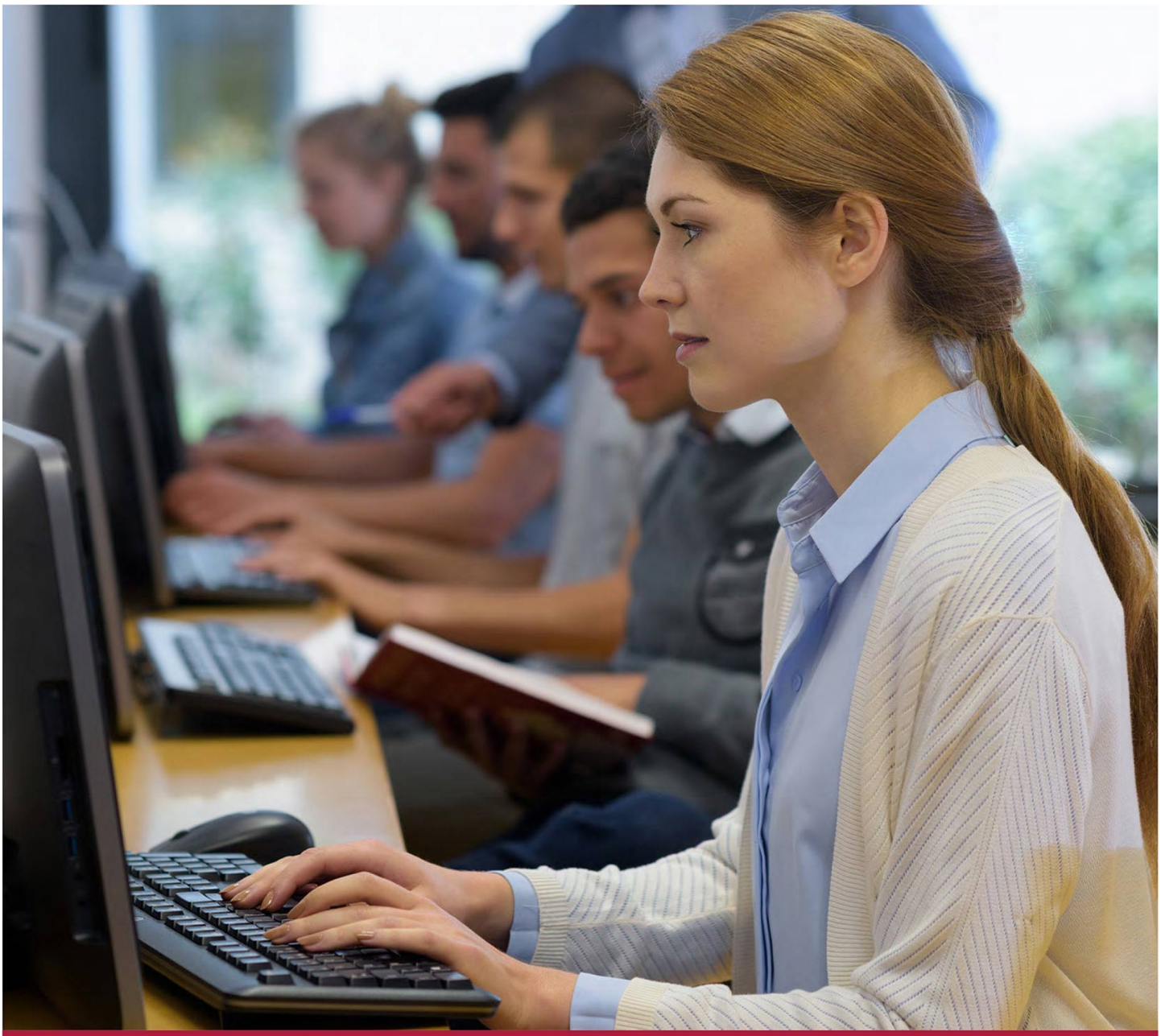
softline учебный центр



Kaspersky Industrial CyberSecurity

Код курса: KL 038.4.1

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

Kaspersky Industrial CyberSecurity

Код курса: KL 038.4.1

Длительность	32 ак. часа
Формат	Очно; Дистанционно
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: развертывание первоначальная настройка и активация настройка для обнаружения угроз и защиты от атак диагностика работы продуктов сопровождение и эксплуатация.

Подробная информация

Профиль аудитории:

- Курс ориентирован на инженеров, отвечающих за внедрение и эксплуатацию систем защиты промышленных объектов от киберугроз.
- Сотрудникам службы информационной безопасности, которые 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.

По окончании курса слушатели смогут:

- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Industrial CyberSecurity Endpoint Detection and Response
- Изучаемые приложения:
- Kaspersky Industrial CyberSecurity for Windows Nodes 3.1
- Kaspersky Industrial CyberSecurity for Networks 4
- Kaspersky Security Center 14

- Сервер администрирования Kaspersky Security Center 14
- Агент администрирования Kaspersky Security Center 14
- Веб-консоль Kaspersky Security Center 14
- Kaspersky Endpoint Agent 3.13.

Программа курса

Модуль 1. Введение

- Введение в безопасность АСУ ТП
- Как устроен курс?
- Что такое АСУ ТП?
- Угрозы информационной безопасности АСУ ТП
- Кибербезопасность предприятия
- KICS как целостный подход к защите предприятия

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

- Развертывание Kaspersky Industrial CyberSecurity for Networks
- Принцип работы Kaspersky Industrial CyberSecurity for Networks
- Подготовка к установке
- Установка
- Лабораторная работа 1. Установите сервер Kaspersky Industrial CyberSecurity for Networks
- Первоначальная настройка
- Лабораторная работа 2. Активируйте и обновите Kaspersky Industrial CyberSecurity for Networks
- Лабораторная работа 3. Включите перехват трафика
- Инвентаризация сети
- Технологии инвентаризации
- Обнаружение устройств
- Лабораторная работа 4. Включите обнаружение активности устройств
- Лабораторная работа 5. Включите обнаружение информации об устройствах
- Лабораторная работа 6. Выполните активный опрос устройств
- Глубокий анализ промышленных протоколов
- Лабораторная работа 7. Включите обнаружение устройств для контроля процесса
- Лабораторная работа 8. Включите контроль проектов ПЛК и распознавание параметров (тегов)

проектов ПЛК
- Лабораторная работа 9. Включите контроль команд
- Лабораторная работа 10. Включите контроль параметров промышленного процесса
- Обнаружение сетевых взаимодействий
- Карта сети
- Управление рисками
- Лабораторная работа 11. Включите обнаружение рисков
- Лабораторная работа 12. Включите контроль целостности сети
- Лабораторная работа 13. Настройте карту сети
- Обнаружение атак и аномалий
- Технологии обнаружения
- Обнаружение неразрешенных устройств
- Лабораторная работа 14. Переведите Kaspersky Industrial CyberSecurity for Networks в режим наблюдения
- Лабораторная работа 15. Обнаружьте постороннее устройство в промышленной сети
- Система обнаружения вторжений (IDS)
- Лабораторная работа 16. Обнаружьте сканирование сети
- Контроль системных команд
- Контроль процесса по правилам
- Лабораторная работа 17. Обнаружьте неразрешенное взаимодействие с полевым контроллером
- Лабораторная работа 18. Обнаружьте вмешательство в работу контроллера
- Обработка событий и инцидентов
- Лабораторная работа 19. Завершите обработку инцидентов
- Обслуживание Kaspersky Industrial CyberSecurity for Networks
- Мониторинг состояния продукта
- Отчеты
- Журналы продукта
- Хранение и ротация служебных данных
- Сбор информации для обращения за поддержкой
- Интеграции Kaspersky Industrial CyberSecurity for Networks
- Возможности интеграции
- Интеграция с Kaspersky Security Center
- Лабораторная работа Подключите Kaspersky Industrial CyberSecurity for Networks к Kaspersky Security Center
- Лабораторная работа 21. Настройте технологию единого входа
- Интеграция со сторонними системами
- Интеграция Kaspersky Industrial CyberSecurity for Networks с Kaspersky Industrial CyberSecurity for Nodes
- Интеграция по REST API

Модуль 4. Kaspersky Industrial CyberSecurity for Nodes

- Развертывание Kaspersky Industrial CyberSecurity for Nodes
- Область применения Kaspersky Industrial CyberSecurity for Nodes
- Состав и архитектура Kaspersky Industrial CyberSecurity for Nodes
- Требования к оборудованию
- Комплект поставки
- Способы установки

- Результаты установки
- Лабораторная работа 22. Подготовьте инфраструктуру к развертыванию Kaspersky Industrial CyberSecurity for Nodes
- Лабораторная работа 23. Разверните агент администрирования Kaspersky Security Center и Kaspersky Industrial CyberSecurity for Nodes
- Консоль управления Kaspersky Industrial CyberSecurity for Nodes
- Лабораторная работа 24. Установите консоль администрирования Kaspersky Industrial CyberSecurity for Nodes
- Лабораторная работа Подключите Kaspersky Industrial CyberSecurity for Nodes к Kaspersky Industrial CyberSecurity for Networks
- Защита узлов промышленной сети с помощью Kaspersky Industrial CyberSecurity for Nodes
- Меры, реализуемые Kaspersky Industrial CyberSecurity for Nodes для защиты узлов сети
- Как вредоносные программы попадают на устройства
- Что вредоносные программы делают на узлах АСУ ТП?
- Типы защит Kaspersky Industrial CyberSecurity for Nodes
- Бессигнатурная защита
- Контроль запуска программ
- Лабораторная работа 26. Настройте Контроль запуска программ в Kaspersky Industrial CyberSecurity for Nodes для работы в неблокирующем режиме
- Лабораторная работа 27. Заблокируйте запуск неавторизованных приложений на узлах АСУ ТП
- Защита от эксплойтов
- Контроль устройств
- Контроль Wi-Fi соединений
- Управление сетевым экраном
- Сигнатурная защита
- Постоянная защита файлов
- Настройка исключений и параметров обработки объектов
- Защита от шифрования
- Защита от сетевых атак
- Лабораторная работа 28. Настройте Kaspersky Industrial CyberSecurity for Nodes для защиты узла АСУ ТП от программ-вымогателей
- Лабораторная работа 29. Настройте Kaspersky Industrial CyberSecurity for Nodes для защиты от сетевых атак
- AMSI-защита
- Контроль технологического процесса
- Мониторинг файловых операций
- Лабораторная работа 30. Настройте Мониторинг файловых операций Kaspersky Industrial CyberSecurity for Nodes для контроля файлов SCADA
- Анализ журналов
- Лабораторная работа 31. Настройте Анализ журналов Windows в Kaspersky Industrial CyberSecurity for Nodes для выявления аномалий в системе
- Мониторинг доступа к реестру
- Контроль целостности ПЛК
- Лабораторная работа 32. Настроить проверку целостности проектов ПЛК
- Портативный сканер
- Интеграции Kaspersky Industrial CyberSecurity for Nodes
- Передача данных в SCADA при помощи Kaspersky Security Gateway
- Интеграция с SIEM
- Обслуживание Kaspersky Industrial CyberSecurity for Nodes

Модуль 5. Kaspersky Endpoint Agent

- Принцип работы Kaspersky Endpoint Agent
- Что такое Kaspersky Endpoint Agent
- Подготовка к установке
- Лабораторная работа 33. Подготовьте инфраструктуру к демонстрации хакерской атаки
- Лабораторная работа 34. Имитируйте хакерскую атаку в промышленной сети
- Лабораторная работа 35. Изучить следы атаки на предприятие в Kaspersky Industrial CyberSecurity for Networks
- Как реагировать на событие обнаружения?
- Детали обнаружения
- Сдерживание угрозы
- Настройка отображения событий обнаружения в Kaspersky Security Center
- Детали обнаружения
- Лабораторная работа 36. Изучить следы атаки на предприятие в Kaspersky Security Center
- Сдерживание угрозы
- Лабораторная работа 37. Найти индикаторы компрометации
- Лабораторная работа 38. Настроить запрет запуска вредоносных скриптов
- Аудит безопасности
- Что такое аудит безопасности?
- Проведите аудит безопасности
- Лабораторная работа 39. Провести аудит безопасности компьютера SCADA

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.