

Kaspersky Industrial CyberSecurity. Administration (038.4.5)

ID KL-038.4.5 Цена 87 500,- руб. Длительность 3 дня

Кому следует посетить

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.

Цели курса

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.

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

Программа курса

Часть I. Kaspersky Security Center

1. Базовая информация о Kaspersky Security Center

- 1.1. Состав и архитектура Kaspersky Security Center
- 1.2. Функции Kaspersky Security Center
- 1.3. MMC-консоль Kaspersky Security Center
- 1.4. Web-консоль Kaspersky Security Center
- 1.5. Плагин управления
- 1.6. Политики
- 1.7. Задачи
- 1.8. Установка
- 1.9. Активация и обновление баз

Часть II. Kaspersky Industrial CyberSecurity for Networks

1. Развертывание Kaspersky Industrial CyberSecurity for Networks

- 1.1. Архитектура и принцип работы
- 1.2. Подготовка к установке
- 1.3. Установка
Лабораторная работа 1. Установить сервер KICS for Networks
- 1.4. Первоначальная настройка
Лабораторная работа 2. Активировать и обновить KICS for Networks
- 1.5. Интеграция с Kaspersky Security Center
Лабораторная работа 3. Включить перехват трафика

2. Инвентаризация сети

- 2.1. Технологии инвентаризации
- 2.2. Инвентаризация устройств
Лабораторная работа 4. Включить обнаружение активности устройств
Лабораторная работа 5. Включить обнаружение информации об устройствах
Лабораторная работа 6. Выполнить активный опрос устройств
- 2.3. Анализ промышленных протоколов

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

- 2.4. Обнаружение сетевых взаимодействий
- 2.5. Карта сети

Лабораторная работа 12. Включить контроль целостности сети

Лабораторная работа 13. Настроить карту сети

3. Обслуживание Kaspersky Industrial CyberSecurity for Networks

- 3.1. Мониторинг состояния продукта
- 3.2. Отчеты
- 3.3. Журналы продукта
- 3.4. Хранение и ротация служебных данных
- 3.5. Сбор информации для обращения в поддержку

Лабораторная работа 14. Завершить настройку KICS for Networks

4. Интеграции Kaspersky Industrial CyberSecurity for Networks

- 4.1. Возможности интеграции
- 4.2. Интеграция с Kaspersky Security Center

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

- 4.3. Интеграция с другими системами
- 4.4. Интеграция по REST API
- 4.5. Интеграция с KICS for Nodes

Лабораторная работа 16. Собрать информацию о работе программы

Часть III. Kaspersky Industrial CyberSecurity for Nodes

1. Развертывание Kaspersky Industrial CyberSecurity for Nodes

- 1.1. Область применения KICS for Nodes
- 1.2. Состав и архитектура KICS for Nodes
- 1.3. Требования к оборудованию
- 1.4. Комплект поставки
- 1.5. Способы установки
- 1.6. Порядок развертывания KICS for Nodes
- 1.7. Результаты установки

Лабораторная работа 17. Подготовить инфраструктуру к развертыванию KICS for Nodes

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

- 1.8. Консоль управления KICS for Nodes

Лабораторная работа 19. Установить Консоль управления KICS for Nodes

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

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

- 2.1. Меры, реализуемые KICS for Nodes для защиты узлов сети
- 2.2. Как вредоносные программы попадают на устройства
- 2.3. Что вредоносные программы делают на узлах АСУ ТП
- 2.4. Типы защит KICS for Nodes
- 2.5. Бессигнатурная защита
- 2.6. Контроль запуска программ

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

- 2.7. Контроль устройств
- 2.8. Контроль Wi-Fi соединений

- 2.9. Управление сетевым экраном
- 2.10. Контроль технологического процесса
- 2.11. Мониторинг файловых операций

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

- 2.12. Анализ журналов
- 2.13. Мониторинг доступа к реестру
- 2.14. Контроль целостности ПЛК

Лабораторная работа 24. Настроить проверку целостности проектов ПЛК

3. Интеграции Kaspersky Industrial CyberSecurity for Nodes

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

4. Обслуживание Kaspersky Industrial CyberSecurity for Nodes

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

Лабораторная работа 25. Завершить настройку KICS for Nodes

Часть IV. Kaspersky Industrial CyberSecurity for Linux Nodes

1. Почему Linux требует защиты

- 1.1. Компоненты KICS for Linux Nodes

Лабораторная работа 26. Настроить Kaspersky Security Center Linux

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

2. Как защитить устройства

- 2.1. Как защититься от сетевых атак
- 2.2. Как защититься от вредоносного ПО

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

Лабораторная работа 29. Настроить расширенную защиту

сервера с операционной системой Linux

- 2.3. Как укрепить компьютер

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

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

- 3.1. Зачем использовать командную строку
- 3.2. Как узнать статус приложения KICS for Linux Nodes
- 3.3. Как управлять задачами
- 3.4. Работа с событиями

Лабораторная работа 31. Управление защитой с помощью kics-control

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