KL 038.4.1:

Kaspersky Industrial CyberSecurity

Изучаемые продукты

- 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 4.1
- Kaspersky Security Center 14.2
    - Сервер администрирования Kaspersky Security Center 14.2
    - Агент администрирования Kaspersky Security Center 14.2
    - Веб-консоль Kaspersky Security Center 14.2
- Kaspersky Endpoint Agent 3.15

Аудитория курса

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.

Требования к участникам

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.

Описание 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.

Длительность

4 дня

Содержание

Часть I. Введение

1. Введение в безопасность АСУ ТП

1.1. Как устроен курс?
1.2. Что такое АСУ ТП?
1.3. Угрозы информационной безопасности АСУ ТП
1.4. Кибербезопасность предприятия
1.5. KICS как целостный подход к защите предприятия

Часть II. 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 III. Kaspersky Industrial CyberSecurity for Networks

1. Развертывание Kaspersky Industrial CyberSecurity for Networks

1.1. Принцип работы Kaspersky Industrial CyberSecurity for Networks
1.2. Подготовка к установке
1.3. Установка

Лабораторная работа 1. Установить сервер Kaspersky Industrial CyberSecurity for Networks

1.4. Первоначальная настройка

Лабораторная работа 2. Активировать и обновить Kaspersky Industrial CyberSecurity for Networks
Лабораторная работа 3. Включить перехват трафика

2. Инвентаризация сети

2.1. Технологии инвентаризации
2.2. Обнаружение устройств

Лабораторная работа 4. Включить обнаружение активности устройств