

KL P38.4.5:

Kaspersky Industrial CyberSecurity Fundamentals

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 Networks 4.5
- Kaspersky Industrial CyberSecurity for Windows Nodes 4.0
- Kaspersky Endpoint Agent 4.0
- Kaspersky Industrial CyberSecurity for Linux Nodes 2.0
- Kaspersky Security Center 16

Аудитория курса

Данный курс предназначен для специалистов по информационной безопасности, которые, возможно, 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.

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

Курс:

- дает определение понятию АСУ ТП
- рассказывает об основных угрозах АСУ ТП и производственному процессу в контексте информационной безопасности

- разъясняет, в чем заключается специфика защиты промышленных сетей и почему подходы к защите корпоративных сетей не применимы для защиты промышленных сетей
- представляет и описывает основной функционал продуктов, входящих в состав решения Kaspersky Industrial CyberSecurity, и демонстрирует на реальных примерах, в каких сценариях этот функционал может быть полезен

Длительность

1 день

Содержание

1. Введение в безопасность АСУ ТП

- 1.1. Общие сведения об АСУ ТП
- 1.2. Угрозы информационной безопасности АСУ ТП
- 1.3. Особенности промышленной кибербезопасности
- 1.4. Решения для промышленной кибербезопасности от Kaspersky

2. Kaspersky Security Center

3. Kaspersky Industrial CyberSecurity for Networks

- 3.1. Общие сведения
 - Область применения KICS for Networks
 - Технологии KICS for Networks
 - Поддерживаемые устройства и протоколы
- 3.2. Развертывание программы
 - Архитектура KICS for Networks
 - Варианты установки KICS for Networks
- 3.3. Инвентаризация
 - Инвентаризация устройств
 - Инвентаризация сети
 - Разрешающие правила
 - Обнаружение рисков информационной безопасности
- 3.4. Обнаружение атак
 - Появление постороннего устройства в сети
 - Сканирование сети
 - Сетевая атака
 - Подбор пароля и эксплуатация известной уязвимости
 - Горизонтальное перемещение и эксфильтрация данных
 - Атака на карте сети
 - Вмешательство в работу промышленного устройства
- 3.5. Интеграция с другими продуктами и внешними системами
 - Интеграция с Kaspersky Security Center
 - Интеграция с KICS for Nodes
 - Интеграция с SD-WAN
 - Взаимодействие с внешними системами

4. Kaspersky Industrial CyberSecurity for Nodes

- 4.1. Общие сведения
 - Область применения KICS for Nodes
 - Варианты программы KICS for Nodes
 - Управление KICS for Nodes
 - Компоненты KICS for Nodes

4.2. Обзор функций продукта

- Появление постороннего устройства
 - Контроль подключаемых устройств
 - Проверка незащищенных устройств
- Предотвращение заражения
 - Постоянная защита файлов
 - Контроль запуска программ
- Подбор пароля
 - Анализ журналов
- Атака на узел промышленной сети
 - Защита от сетевой атаки
 - Защита от эксплойтов
- Компрометация узла
 - Мониторинг файловых операций
 - Мониторинг доступа к реестру
- Шифрование данных на узле
 - Защита от шифрования
- Попытка воздействия на технологический процесс
 - Проверка целостности проектов ПЛК

5. EDR возможности

- Как реагировать на инцидент?
- Расширенный контекст угрозы
 - Детали обнаружения
- Сдерживание угрозы
- Обнаружение аномалий с помощью Sigma-правил

6. Лицензирование и поддержка

- Лицензии KICS for Networks
- Лицензии KICS for Nodes
- Техническая поддержка KICS Enterprise