

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

Лабораторная работа 5. Включить обнаружение информации об устройствах

Лабораторная работа 6. Выполнить активный опрос устройств

2.3. Глубокий 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. Включить контроль параметров промышленного процесса

2.4. Обнаружение сетевых взаимодействий

2.5. Карта сети

2.6. Управление рисками

Лабораторная работа 11. Включить обнаружение рисков

Лабораторная работа 12. Включить контроль целостности сети

Лабораторная работа 13. Настроить карту сети

3. Обнаружение атак и аномалий

3.1. Технологии обнаружения

3.2. Обнаружение неразрешенных устройств

Лабораторная работа 14. Перевести Kaspersky Industrial CyberSecurity for Networks в режим наблюдения

Лабораторная работа 15. Обнаружить постороннее устройство в промышленной сети

3.3. Система обнаружения вторжений (IDS)

Лабораторная работа 16. Обнаружить сканирование сети

3.4. Контроль системных команд

3.5. Контроль процесса по правилам

Лабораторная работа 17. Обнаружить неразрешенное взаимодействие с полевым контроллером

Лабораторная работа 18. Обнаружить вмешательство в работу контроллера

3.6. Обработка событий и инцидентов

Лабораторная работа 19. Завершить обработку инцидентов

4. Обслуживание Kaspersky Industrial CyberSecurity for Networks

4.1. Мониторинг состояния продукта

4.2. Отчеты

4.3. Журналы продукта

4.4. Хранение и ротация служебных данных

4.5. Сбор информации для обращения за поддержкой

5. Интеграции Kaspersky Industrial CyberSecurity for Networks

5.1. Возможности интеграции

5.2. Интеграция с Kaspersky Security Center

Лабораторная работа 20. Настроить отображение данных из Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center

Лабораторная работа 21. Настроить технологию единого входа

5.3. Интеграция со сторонними системами

5.4. Интеграция Kaspersky Industrial CyberSecurity for Networks с Kaspersky Industrial CyberSecurity for Nodes

5.5. Интеграция по REST API

Часть IV. Kaspersky Industrial CyberSecurity for Nodes

1. Развертывание Kaspersky Industrial CyberSecurity for Nodes

1.1. Область применения Kaspersky Industrial CyberSecurity for Nodes

- 1.2. Состав и архитектура Kaspersky Industrial CyberSecurity for Nodes
- 1.3. Требования к оборудованию
- 1.4. Комплект поставки
- 1.5. Способы установки
- 1.6. Результаты установки

Лабораторная работа 22. Подготовить инфраструктуру к развертыванию Kaspersky Industrial CyberSecurity for Nodes

Лабораторная работа 23. Развернуть агент администрирования Kaspersky Security Center и Kaspersky Industrial CyberSecurity for Nodes

- 1.7. Консоль управления Kaspersky Industrial CyberSecurity for Nodes

Лабораторная работа 24. Установить консоль администрирования Kaspersky Industrial CyberSecurity for Nodes

Лабораторная работа 25. Подключить Kaspersky Industrial CyberSecurity for Nodes к Kaspersky Industrial CyberSecurity for Networks

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

- 2.1. Меры, реализуемые Kaspersky Industrial CyberSecurity 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 Kaspersky Industrial CyberSecurity for Nodes
- 2.5. Бессигнатурная защита
- 2.6. Контроль запуска программ

Лабораторная работа 26. Настроить Контроль запуска программ в Kaspersky Industrial CyberSecurity for Nodes для работы в неблокирующем режиме

Лабораторная работа 27. Заблокировать запуск неавторизованных приложений на узлах АСУ ТП

- 2.7. Защита от эксплойтов
- 2.8. Контроль устройств
- 2.9. Контроль Wi-Fi соединений
- 2.10. Управление сетевым экраном
- 2.11. Сигнатурная защита
- 2.12. Постоянная защита файлов
- 2.13. Настройка исключений и параметров обработки объектов
- 2.14. Защита от шифрования
- 2.15. Защита от сетевых атак

Лабораторная работа 28. Настроить Kaspersky Industrial CyberSecurity for Nodes для защиты узла АСУ ТП от программ-вымогателей

Лабораторная работа 29. Настроить Kaspersky Industrial CyberSecurity for Nodes для защиты от сетевых атак

- 2.16. AMSI-защита
- 2.17. Контроль технологического процесса
- 2.18. Мониторинг файловых операций

Лабораторная работа 30. Настроить Мониторинг файловых операций Kaspersky Industrial CyberSecurity for Nodes для контроля файлов SCADA

- 2.19. Анализ журналов

Лабораторная работа 31. Настроить Анализ журналов Windows в Kaspersky Industrial CyberSecurity for Nodes для выявления аномалий в системе

- 2.20. Мониторинг доступа к реестру
- 2.21. Контроль целостности ПЛК

Лабораторная работа 32. Настроить проверку целостности проектов ПЛК

- 2.22. Портативный сканер

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

Часть V. Kaspersky Endpoint Agent

1. Принцип работы Kaspersky Endpoint Agent

1.1. Что такое Kaspersky Endpoint Agent

1.2. Подготовка к установке

Лабораторная работа 33. Подготовить инфраструктуру к демонстрации хакерской атаки

Лабораторная работа 34. Имитировать хакерскую атаку в промышленной сети

Лабораторная работа 35. Изучить следы атаки на предприятие в Kaspersky Industrial CyberSecurity for Networks

2. Реагирование на событие обнаружения

2.1. Как реагировать на событие обнаружения?

2.2. Детали обнаружения

2.3. Сдерживание угрозы

2.4. Настройка отображения событий обнаружения в Kaspersky Security Center

2.5. Детали обнаружения

Лабораторная работа 36. Изучить следы атаки на предприятие в Kaspersky Security Center

2.6. Сдерживание угрозы

Лабораторная работа 37. Найти индикаторы компрометации

Лабораторная работа 38. Настроить запрет запуска вредоносных скриптов

3. Аудит безопасности

3.1. Что такое аудит безопасности?

3.2. Проведите аудит безопасности

Лабораторная работа 39. Провести аудит безопасности компьютера SCADA