KL 060.4.5:

Kaspersky Industrial CyberSecurity

Investigation

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 Windows Nodes 4.0
- Kaspersky Industrial CyberSecurity for Linux Nodes 2.0
- Kaspersky Industrial CyberSecurity for Networks 4.5
- Kaspersky Security Center Linux 16.0
- Kaspersky Endpoint Agent 4.0

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:

- настройка компонентов для обнаружения угроз и защиты от атак;
- анализ событий обнаружения угроз;
- расследование киберинцидентов.

Длительность

2 дня

Содержание

Часть I. Kaspersky Industrial CyberSecurity for Networks

1. Мониторинг сети

1.1. Контроль рисков
1.2. Информация о сетевых сессиях

Лабораторная работа 1. Настроить интеграцию KICS for Nodes с KICS for Networks
Лабораторная работа 2. Включить обнаружение рисков
Лабораторная работа 3. Включить регистрацию сетевых сессий

1.3. Технологии обнаружения сетевых атак и аномалий
Управление правилами IDS
Обнаружение аномалий в сетевых сессиях

2. Обнаружение атак и аномалий

2.1. Технологии обнаружения
2.2. Сценарий возможной атаки
2.3. Обнаружение неразрешенных устройств и сетевых взаимодействий
2.4. Обнаружение сетевых вторжений (IDS)

Лабораторная работа 4. Обнаружить постороннее устройство в сети
Лабораторная работа 5. Обнаружить сканирование сети
Лабораторная работа 6. Обнаружить подбор пароля к сетевому сервису
Лабораторная работа 7. Обнаружить неразрешенное взаимодействие с ПЛК
Лабораторная работа 8. Обнаружить вмешательство в работу ПЛК

3. Аудит устройств

3.1. Контроль конфигурации устройств Windows и Linux

Лабораторная работа 9. Настроить контроль конфигурации устройств

3.2. Обнаружение аномалий с помощью Sigma-правил

Лабораторная работа 10. Настроить обнаружение аномалий с помощью Sigma-правил

3.3. Аудит безопасности устройств по правилам

Лабораторная работа 11. Провести аудит безопасности компьютера SCADA

Часть II. Kaspersky Industrial CyberSecurity for Nodes

4. Бессигнатурная защита

4.1. Защита от эксплойтов
4.2. Анализ журналов

5. Сигнатурная защита

5.1. Защита файлов
5.2. Защита от шифрования
5.3. Защита от сетевых угроз
5.4. AMSI-защита

Лабораторная работа 12. Настроить защиту узла от программ-вымогателей
Лабораторная работа 13. Настроить защиту узла от сетевых атак
Лабораторная работа 14. Настроить анализ журналов Windows для выявления аномалий в системе

6. Портативный сканер

7. Мониторинг состояния защиты в Kaspersky Security Center

7.1. Формирование отчетов в KSC

Часть III. Функции EDR

8. Функции и возможности Endpoint Agent

8.1. Функции и возможности Endpoint Agent
8.2. Взаимодействия Endpoint Agent

9. Реагирование на событие обнаружения

9.1. Как реагировать на событие обнаружения?
9.2. Детали обнаружения

Лабораторная работа 15. Имитировать атаку на сервер SCADA
Лабораторная работа 16. Имитировать атаку на рабочую станцию Admin-OT
Лабораторная работа 17. Изучить следы атаки в Kaspersky Security Center

9.3. Сдерживание угрозы
9.4. Проверка компьютеров на наличие индикаторов компрометации

Лабораторная работа 18. Найти индикаторы компрометации
Лабораторная работа 19. Настроить запрет запуска вредоносных скриптов