KL 025.6:

Kaspersky Anti Targeted Attack, Kaspersky Endpoint Detection and Response Expert

Изучаемые продукты

- Kaspersky Anti Targeted Attack Platform 6.0
- Kaspersky Endpoint Detection and Response 6.0
- Kaspersky Endpoint Security для Windows и Linux
- Kaspersky Security Center

Описание курса

Платформа Kaspersky Anti Targeted Attack совместно с Kaspersky EDR представляет собой решение класса XDR (Extended Detection and Response) нативного типа и помогает организациям построить надежную систему защиты корпоративной инфраструктуры от сложных кибератак.

Теоретический материал и лабораторные работы дают слушателям необходимые знания и навыки, благодаря которым слушатель сможет спланировать и выполнить развертывание и настройку решения, будет понимать принципы использования решения и сможет выполнять задачи по его обслуживанию.

Что нового в версии 6.0

Курс был переработан с учетом новых функциональных возможностей продукта. Мы так же отказались от развертывания кластера в пользу одноузловой конфигурации Центрального узла. В лабораторных работах изменились инструменты для симуляции атаки на корпоративные ресурсы, что позволяет глубже изучить возможности продукта:

1. Развертывание KES для Linux, симуляция атаки и реагирование на linux-сервере.
2. Настройка ICAP-интеграции в режиме блокирования
3. Анализ сырого трафика

Длительность

3 дня

Требования к участникам

Понимание основ работы с Kaspersky Security Center.

Понимание основ сетевых технологий: DNS, маршрутизации, электронной почты, Web. Базовые навыки администрирования Windows и Linux. Представление о современных угрозах и тенденциях развития информационных технологий.

Содержание

1. Введение

- Ландшафт угроз
- Проблемы при построении системы ИБ
- Подходы к построению системы ИБ
- Какие задачи заказчика помогает решить KATA Platform

2. Подготовка к внедрению

- Состав, возможности
- Схемы развертывания, масштабирование, совместимость

3. Развертывание платформы KATA

- Установка центрального узла в виде кластера и установка сенсора
- Установка и настройка Sandbox
- Активация, обновление, пользователи
- Подключение серверов друг к другу

Лабораторная работа 1	Установить и настроить центральный узел
Лабораторная работа 2	Проверить настройки KATA Sandbox
Лабораторная работа 3	Подготовить KATA-платформу к работе

4. Эксплуатация KATA

- Подключение к источникам трафика
- Технологии обнаружения KATA

Лабораторная работа 4	Подключить центральный узел к сетевой инфраструктуре (SPAN)
Лабораторная работа 5	Подбор паролей по протоколу SSH
Лабораторная работа 6	SYN-флуд атака на корпоративный сервер
Лабораторная работа 7	Создать пользовательское IDS-правило

Лабораторная работа 8	Подключить центральный узел к почтовой системе по протоколу SMTP
Лабораторная работа 9	Подключить сенсор к прокси-серверу (ICAP)
Лабораторная работа 10	Устранить многократную проверку http-трафика
Лабораторная работа 11	Создание пользовательского правила YARA

5. Установка Агентов

Типы агентов

Установка с центральным управлением

Установка без центрального управления

Результат установки и сбор данных

Лабораторная работа 12	Установить KES с помощью KSC
Лабораторная работа 13	Подключить KES к центральному узлу

6. Эксплуатация KEDR

Технологии обнаружения KEDR

Расследование инцидента

Реагирование на инцидент

7. Результаты анализа Sandbox

Карточка обнаружения Sandbox

Результаты анализа в виртуальной среде

Отладочная информация Sandbox

Лабораторная работа 14	Атака на linux-сервер компании
Лабораторная работа 15	Атака на компьютер компании с ОС Windows
Лабораторная работа 16	Изучить подробности выполнения файла в песочнице
Лабораторная работа 17	Создайте пользовательское TAA правило

8. Обслуживание платформы KATA

VIP-статус

Проверка архивов с паролем

External API

Отчеты

Почтовые уведомления

Интеграция с SIEM

Мониторинг сервера по SNMP

Сбор информации о системе

Обновление