

KL 025.8:

Kaspersky Anti Targeted Attack Platform Administration

Изучаемые продукты

- Kaspersky Anti Targeted Attack Platform 8.0
- Kaspersky Security Center 16 Administration Server
- Kaspersky Endpoint Security for Windows 12.12
- Kaspersky Endpoint Security for Linux 12.4

Описание курса

Kaspersky Anti Targeted Attack Platform – решение, предназначенное для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats ("АПТ"). Решение разработано для корпоративных пользователей и включает в себя два функциональных блока:

- Kaspersky Anti Targeted Attack ("KATA"), обеспечивающий защиту периметра IT-инфраструктуры предприятия.
- Network Detection and Response ("NDR"), обеспечивающий защиту внутренней сети предприятия.

Теоретический материал и лабораторные работы дают необходимые знания и навыки, благодаря которым слушатель понимает принципы использования решения и сможет выполнять задачи по развертыванию и администрированию Kaspersky Anti Targeted Attack Platform

Длительность

2 дня

Требования к участникам

Базовые навыки управления приложениями для защиты конечных узлов с помощью Сервера администрирования 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. Подготовка к внедрению

- 1.1. Состав и возможности
- 1.2. Схемы развертывания, масштабирование, совместимость

2. Развертывание KATA platform

- 2.1. Установка Central Node и Sensor
- 2.2. Установка и настройка Sandbox
- 2.3. Подготовка Central Node к эксплуатации
- 2.4. Подключение серверов друг к другу
- 2.5. Подключение к источникам трафика
- 2.6. Ретроспективный анализ трафика

Лабораторная работа 1: Установка и первоначальная настройка Central Node

Лабораторная работа 2: Создание распределенного решения

Лабораторная работа 3: Настройка KATA Sandbox

Лабораторная работа 4: Подключение KATA Platform к сетевой инфраструктуре

3. Установка и настройка Endpoint Agent

- 3.1. Централизованная установка
- 3.2. Локальная установка
- 3.3. Настройка NDR Агентов
- 3.4. Отправка файлов в Sandbox
- 3.5. Проверка результатов установки

Лабораторная работа 5: Установка KES с помощью Сервера администрирования

4. Обслуживание KATA Platform

- 4.1. Парольные политики
- 4.2. Коннекторы
- 4.3. KATA API
- 4.4. NDR API
- 4.5. Почтовые уведомления (KATA, NDR)
- 4.6. Интеграция с SIEM (KATA, NDR, KUMA)
- 4.7. Активный опрос
- 4.8. Интеграция с NGFW
- 4.9. Мониторинг сервера по SNMP
- 4.10. Журналы KATA Platform
- 4.11. Сбор данных для обращения в техническую поддержку
- 4.12. Резервное копирование и восстановление данных
- 4.13. Обновление KATA Platform

Лабораторная работа 6: Отправка уведомлений и событий NDR по электронной почте и в SIEM-систему

Лабораторная работа 7: Работа с API

Лабораторная работа 8: Интеграция KATA Platform с Active Directory и добавление доменных пользователей

Лабораторная работа 9: Просмотр логов и создание резервной копии