

Kaspersky Anti Targeted Attack. Kaspersky EDR. Administration

ID KL-025.7 Цена 70 000,- руб. Длительность 2 дня

Кому следует посетить

- Инженеры, отвечающие за внедрение и эксплуатацию систем защиты промышленных объектов от киберугроз.
- Сотрудникам службы информационной безопасности, которые осуществляют мониторинг состояния защиты промышленного объекта и реагируют на инциденты.
- Пресеил-специалисты.

Предварительные требования

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

Цели курса

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

Содержание 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 ("APT").

Решение разработано для корпоративных пользователей и включает в себя три функциональных блока:

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

- Kaspersky Endpoint Detection and Response ("KEDR"), обеспечивающий защиту компьютеров локальной сети организации.

Программа курса

Модуль 1. «Подготовка к внедрению»

- Состав, возможности
- Схемы развертывания, масштабирование

Модуль 2. «Развертывание платформы КАТА»

- Установка центрального узла в виде кластера и установка сенсора
- Установка и настройка Sandbox
- Активация, обновление, пользователи
- Подключение серверов друг к другу
- Подключение к источникам трафика
- Лабораторные работы 1-4

Модуль 3. «Установка Агентов»

- Типы агентов
- Установка с центральным управлением
- Установка без центрального управления
- Результат установки и сбор данных
- Лабораторная работа 5

Модуль 4. «Обслуживание платформы КАТА»

- Парольная политика
- External API
- Почтовые уведомления
- Интеграция с SIEM
- Активный опрос
- Мониторинг сервера по SNMP
- Сбор информации о системе
- Обновление с предыдущих версий
- Сохранение и восстановление настроек
- Лабораторные работы 6-9