



## **Kaspersky Anti Targeted Attack. Administration**

Код курса: KL 025.8

## Kaspersky Anti Targeted Attack. Administration

Код курса: KL 025.8

<b>Длительность</b>	16 ак. часов
<b>Формат</b>	
<b>Разработчик курса</b>	Лаборатория Касперского
<b>Тип</b>	Учебный курс
<b>Способ обучения</b>	Под руководством тренера

### О курсе

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

### Подробная информация

Профиль аудитории:

- 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
- Пресейл-специалисты

Предварительные требования:

- 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.

По окончании курса слушатели изучат:

- Спланировать и выполнить развертывание и настройку решения
- Понимать принципы использования решения

- Выполнять задачи по его обслуживанию

## Программа курса

### Модуль 1. «Подготовка к внедрению»

- Состав, возможности
- Схемы развертывания, масштабирование

### Модуль 2. «Развертывание KATA Platform»

- Установка Central Node и Sensor
- Установка и настройка Sandbox
- Подготовка Central Node к эксплуатации
- Подключение серверов друг к другу
- Подключение к источникам трафика
- 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

### Модуль 3. «Установка и настройка Endpoint Agent»

- Централизованная установка
- Локальная установка
- Настройка NDR Агентов
- Отправка файлов в Sandbox
- Проверка результатов установки
- Лабораторная работа 5: Установка KES с помощью Сервера администрирования

### Модуль 4. «Обслуживание платформы KATA»

- Парольные политики
- Коннекторы
- KATA API
- NDR API
- Почтовые уведомления (KATA, NDR)
- Интеграция с SIEM (KATA, NDR, KUMA)
- Активный опрос
- Интеграция с NGFW
- Мониторинг сервера по SNMP
- Журналы KATA Platform
- Сбор данных для обращения в техническую поддержку
- Резервное копирование и восстановление данных
- 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

[Посмотреть расписание курса и записаться на обучение](#)

**Обращайтесь по любым вопросам**  
к менеджерам Учебного центра Softline

**8 (800) 505-05-07** | [edusales@softline.com](mailto:edusales@softline.com)

**Ждём вас на занятиях в Учебном центре Softline!**



## Почему Учебный центр Softline?

**Лидер** на рынке корпоративного обучения.

**Более 300 тысяч** подготовленных IT-специалистов.

**Гибкий индивидуальный подход** в обучении, скидки и акции.

**Широкая сеть представительств** в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

**Высокотехнологичное** оборудование

Более **18 лет** опыта работы

**Международные сертификаты** для IT-специалистов и пользователей в Центрах тестирования

**Сертифицированные тренеры** с богатым практическим опытом работы

**Авторизации от мировых производителей ПО** (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

**Разработка курсов и тестов под заказ**, внедрение корпоративных систем обучения.

**Подробнее об Учебном центре Softline**

Вы можете узнать из [профайла](#).