# KL 025.6:

# Kaspersky Anti Targeted Attack, Kaspersky Endpoint Detection and Response Expert

## Featured products

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

## Course description

Kaspersky Anti Targeted Attack platform and Kaspersky EDR together form a native eXtended Detection and Response (XDR) solution that helps organizations build a reliable protection system against advanced cyberattacks.

The theoretical part of the course and the hands-on labs provide participants with the knowledge and skills needed to plan and deploy the solution, understand how it works, configure and maintain it.

## What’s new in version 6.0

The course has been redesigned taking into account new product functions. We use a single-node configuration of the Central Node instead of cluster deployment now. Tools for simulating an attack on corporate resources have been changed in the labs, which allow us to dive deeper when exploring product capabilities. The following topics have been added:

1. Deploying KES for Linux, attack simulation and response on a Linux server
2. Configuring ICAP integration in blocking mode
3. Raw traffic analysis

## Duration

3 days

# Requirements for participants

Basic understanding of Kaspersky Security Center.

Basic understanding of networking technologies, such as DNS, routing, email, web. Basic Windows and Linux management skills. Understanding of contemporary threats and information technologies.

# Contents

## 5. Installing the Agents

Agent types

Centrally managed installation

Installation without centralized management

Installation result and data collection

Lab 12 Install KES using KSC

Lab 13 Connect KES to Central Node

## 6. KEDR operation

KEDR detection technologies

Incident investigation

Incident response

## 7. Sandbox analysis results

Sandbox alert card

Results of analysis in a virtual environment

Sandbox debug information

Lab 14 Attack on a corporate Linux server

Lab 15 Attack on a corporate Windows computer

Lab 16 Examine details of file execution in the sandbox

Lab 17 Create a custom TAA rule

## 8. KATA platform maintenance

VIP status

Scanning password-protected archives

External API

Reports

Email notifications

Integration with SIEM

Server monitoring using SNMP

Collecting system information

Updates

Upgrade from previous versions

Saving and restoring settings

Modifying system settings

Kaspersky Private Security Network (KPSN)

Lab 18 Configure integration with Active Directory

Lab 19 Working with API