KL 025.7:

Kaspersky Anti Targeted Attack. Kaspersky EDR. Administration

Course description

Kaspersky Anti Targeted Attack Platform is a solution designed to protect an organization's IT infrastructure and detect sophisticated threats such as zero-day attacks, targeted attacks and advanced persistent threats (APTs). The solution is designed for enterprises and consists of three functional blocks:

- Kaspersky Anti Targeted Attack (KATA), which protects the perimeter of the corporate IT infrastructure.
- Network Detection and Response (NDR), which protects the organization's internal network.
- Kaspersky Endpoint Detection and Response (KEDR), which protects computers on the corporate local network.

The theoretical part of the course and hands-on labs provide participants with the knowledge explaining how the solution works and skills needed to deploy and administer it.

Duration

2 days (16 hours)

Requirements for participants

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

1. Pre-deployment

Components, capabilities

Deployment schemas, scaling

2. KATA platform deployment

Installation of Central Node as a cluster and Sensor installation

Installing and configuring Sandbox

Activation, updates, users

Interconnecting the servers

Connecting to traffic sources

Labs 1-4

3. Installing the Agents

Agent types

Centrally managed installation

Installation without centralized management

Installation result and data collection

Lab 5

4. KATA platform maintenance

Password policy

External API

Email notifications

Integration with SIEM

Active polling

Server monitoring using SNMP

Collecting system information

Upgrade from previous versions

Saving and restoring settings

Labs 6-9