

KL 025.8:

Kaspersky Anti Targeted Attack Platform Administration

Featured products

- 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

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 the following 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.

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

Requirements for participants

Basic skills in managing endpoint protection applications using Kaspersky Security Center Administration Server.

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

- 1.1. Components and capabilities
- 1.2. Deployment schemas, scaling, compatibility

2. KATA Platform deployment

- 2.1. Central Node and Sensor installation
- 2.2. Installing and configuring Sandbox
- 2.3. Preparing Central Node for operation
- 2.4. Interconnecting the servers
- 2.5. Connecting to traffic sources
- 2.6. Retrospective traffic analysis

Lab 1: Central Node installation and initial setup

Lab 2: Creating a distributed solution

Lab 3: Configuring KATA Sandbox

Lab 4: Connecting KATA Platform to the infrastructure

3. Installing and configuring Endpoint Agent

- 3.1. Centralized installation
- 3.2. Local installation
- 3.3. Configuring NDR agents
- 3.4. File submission to Sandbox
- 3.5. Checking installation health

Lab 5: KES installation using Administration Server

4. KATA Platform maintenance

- 4.1. Password policies
- 4.2. Connectors
- 4.3. KATA API
- 4.4. NDR API
- 4.5. Email notifications (KATA, NDR)
- 4.6. Integration with SIEM (KATA, NDR, KUMA)
- 4.7. Active polling
- 4.8. NGFW integration
- 4.9. Server monitoring using SNMP
- 4.10. KATA Platform logs
- 4.11. Gathering diagnostic data for technical support
- 4.12. Data backup and restore
- 4.13. KATA Platform upgrade

Lab 6: Sending notifications and NDR events by email and to the SIEM system

Lab 7: Working with the API

Lab 8: KATA Platform integration with Active Directory and adding domain users

Lab 9: Viewing logs and creating a backup copy