

KL 038.4.5:

Kaspersky Industrial CyberSecurity

Administration

Featured products

- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Industrial CyberSecurity Endpoint Detection and Response

Featured applications

- Kaspersky Industrial CyberSecurity for Nodes 4.0
- Kaspersky Industrial CyberSecurity for Linux Nodes 2.0
- Kaspersky Industrial CyberSecurity for Networks 4.5
- Kaspersky Security Center 16
 - Kaspersky Security Center Administration Server
 - Kaspersky Security Center Network Agent
 - Kaspersky Security Center Web Console
- Kaspersky Endpoint Agent 4.0

Audience

The course is primarily designed for engineers responsible for deploying and maintaining industrial cybersecurity systems.

Course materials may also interest:

- Information security personnel who monitor protection of an industrial site and respond to incidents;
- Presales specialists who advise customers on the products' capabilities and best practices.

Requirements for participants

Basic understanding of computer and networking technologies. Knowledge of TCP/IP. Basic Windows and Linux administration skills. Basic knowledge of information security principles. Understanding of the purpose, structure and operation of industrial automation systems.

Course description

Theoretical materials and hands-on labs provide participants with the knowledge and skills needed to use Kaspersky Industrial CyberSecurity products in the following scenarios:

- Deployment
- Initial setup and activation
- Configuring threat detection and protection against attacks
- Diagnostics
- Maintenance

Duration

3 days

Contents

Unit I. Kaspersky Security Center basics

1. Kaspersky Security Center components and architecture
2. Kaspersky Security Center functions
3. Kaspersky Security Center MMC
4. Kaspersky Security Center web console
5. Management plug-ins
6. Policies:
7. Tasks
8. Installation
9. Activation and database updates

Unit II. Kaspersky Industrial CyberSecurity for Networks

1. KICS for Networks deployment

- 1.1. Architecture and operation principles
- 1.2. Pre-installation
- 1.3. Installation

[Lab 1.](#) Install the KICS for Networks server

- 1.4. Initial setup

[Lab 2.](#) Activate and update KICS for Networks

[Lab 3.](#) Enable traffic capture

- 1.5. Integration with Kaspersky Security Center

2. Network inventory

- 2.1. Inventory technologies
- 2.2. Device inventory

[Lab 4.](#) Enable Device Activity Detection

[Lab 5.](#) Enable Device Information Detection

[Lab 6.](#) Perform active device polling

- 2.3. Analyzing industrial protocols

[Lab 7.](#) Enable Device Discovery for Process Control

[Lab 8.](#) Enable PLC Project Control and Unknown Tag Detection

- [Lab 9.](#) Enable Command Control
- [Lab 10.](#) Control a PLC configuration
- [Lab 11.](#) Enable control for industrial process parameters

- 2.4. Discovering network interactions
- 2.5. Network sessions

- [Lab 12.](#) Enable Network Integrity Control
- [Lab 13.](#) Configure network map

3. KICS for Networks: maintenance

- 3.1. Product status monitoring
- 3.2. Reports
- 3.3. Product logs
- 3.4. Storing and rotating service data
- 3.5. Gathering information for technical support

- [Lab 14.](#) Complete configuring KICS for Networks

4. KICS for Networks: integrations

- 4.1. Integration capabilities
- 4.2. Integration with Kaspersky Security Center

- [Lab 15.](#) How to configure the display of data from KICS for Networks in Kaspersky Security Center

- 4.3. Integration with other systems
- 4.4. Integration via REST API
- 4.5. Integration with KICS for Nodes

- [Lab 16.](#) How to collect diagnostic information

Unit III. Kaspersky Industrial CyberSecurity for Nodes

1. Deployment

- 1.1. Why KICS for Nodes
- 1.2. Components and architecture of KICS for Nodes
- 1.3. Hardware requirements
- 1.4. Distribution package
- 1.5. Installation methods
- 1.6. KICS for Nodes deployment procedure
- 1.7. Installation results

- [Lab 17.](#) Prepare the infrastructure for deploying KICS for Nodes

- [Lab 18.](#) Deploy Kaspersky Security Center Network Agent and KICS for Nodes

- 1.8. KICS for Nodes console

- [Lab 19.](#) Install the KICS for Nodes console

- [Lab 20.](#) Connect KICS for Nodes to KICS for Networks

2. Protecting an industrial network with KICS for Nodes

- 2.1. How KICS for Nodes protects network nodes
- 2.2. How malware infiltrates devices
- 2.3. What can malware do on ICS nodes?
- 2.4. Types of protection provided by KICS for Nodes
- 2.5. Non-signature protection
- 2.6. Applications Launch Control

- [Lab 21.](#) Configure Applications Launch Control to run in non-blocking mode

- [Lab 22.](#) Block unauthorized applications on ICS nodes

- 2.7. Device Control
- 2.8. Wi-Fi Control
- 2.9. Firewall Management

- 2.10. Industrial process control
- 2.11. File Integrity Monitor

[Lab 23](#). Configure the File Integrity Monitor component of KICS for Nodes to control ICS files

- 2.12. Log Inspection
- 2.13. Registry Access Monitor
- 2.14. PLC Project Integrity Check

[Lab 24](#). Configure integrity check for PLC projects

3. Integrations

- 3.1. Sending data to SCADA using Kaspersky Security Gateway
- 3.2. Integration with SIEM

4. Maintenance

- 4.1. Configuring application access permissions
- 4.2. Monitoring the protection status (health check)
- 4.3. Collecting diagnostic data

[Lab 25](#). Complete configuring KICS for Nodes

Unit IV. Kaspersky Industrial CyberSecurity for Linux Nodes

1. Why Linux needs protection

- 1.1. KICS for Linux Nodes components

[Lab 26](#). Configure Kaspersky Security Center Linux

[Lab 27](#). Install KICS for Linux Nodes on managed devices

2. How to protect devices

- 2.1. How to protect against network attacks
- 2.2. How to protect against malware

[Lab 28](#). Set up essential protection for a Linux computer

[Lab 29](#). Set up advanced protection for a Linux server

- 2.3. How to reinforce protection

[Lab 30](#). Security controls on a Linux computer

3. Managing KICS for Linux Nodes using the kesi-control utility

- 3.1. Why use the command line?
- 3.2. How to check KICS for Linux Nodes state
- 3.3. How to manage tasks
- 3.4. Working with events

[Lab 31](#). Manage protection using kics-control

[Lab 32](#). Manage Linux accounts and devices