KL 038.3.1:

Kaspersky Industrial CyberSecurity

Featured products

- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks

Featured applications

- Kaspersky Industrial CyberSecurity for Windows Nodes 3.0
- Kaspersky Industrial CyberSecurity for Networks 3.1
- Kaspersky Security Center 13.2
    - Kaspersky Security Center 13.2 Administration Server
    - Kaspersky Security Center 13.2 Network Agent
    - Kaspersky Security Center 13.2 Web Console
- Kaspersky Endpoint Agent 3.11

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 the students

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

Course description

Theoretical materials and hands-on labs provide students with 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

1. Introduction to Kaspersky Industrial CyberSecurity

1.1. Constituents of the Kaspersky Industrial CyberSecurity solution
1.2. Kaspersky Industrial CyberSecurity for Networks
1.3. Kaspersky Industrial CyberSecurity for Nodes
1.4. Kaspersky Endpoint Agent
1.5. Kaspersky Security Center
1.6. Management
1.7. What we will tell you in this course and what not

2. Kaspersky Security Center basics

2.1. Kaspersky Security Center components and architecture
2.2. Kaspersky Security Center functions
2.3. Kaspersky Security Center MMC console
2.4. Kaspersky Security Center web console
2.5. Management plug-ins
2.6. Tasks
2.7. Policies
2.8. Installation
2.9. Activation

3. Deploying Kaspersky Industrial CyberSecurity for Nodes

3.1. Components and architecture of Kaspersky Industrial CyberSecurity for Nodes
3.2. Field of use
3.3. Hardware requirements
3.4. Distribution package
3.5. Installation methods
3.6. Initial product setup

Lab 1. **Configure tasks and policies of Kaspersky Industrial CyberSecurity for Nodes**
Lab 2. **Deploy Kaspersky Security Center Network Agent and Kaspersky Industrial CyberSecurity for Nodes**

3.7. MMC management console of Kaspersky Industrial CyberSecurity for Nodes

Lab 3. **Install the console of Kaspersky Industrial CyberSecurity for Nodes**

4. Protecting an industrial network with Kaspersky Industrial CyberSecurity for Nodes

4.1. Threats to industrial nodes
4.2. How Kaspersky Industrial CyberSecurity for Nodes protects network nodes
4.3. Non-signature protection
4.4. Applications launch control

Lab 4. **Configure Applications launch control of Kaspersky Industrial CyberSecurity for Nodes to run in the non-blocking mode**
Lab 5. **Block unauthorized applications on ICS nodes**

4.5. Endpoint control
4.6. Signature protection
4.7. Configuring exclusions and object processing
4.8. Protection against file encrypting ransomware

Lab 6. **Configure Kaspersky Industrial CyberSecurity for Nodes to protect ICS against ransomware**
Lab 7. **Test protection against ransomware in Kaspersky Industrial CyberSecurity for Nodes**

4.9. Network threat protection

Lab 8. Configure and test the Network threat protection component of Kaspersky Industrial CyberSecurity for Nodes

4.10. Industrial process control

Lab 9. Configure and test the File Operations Monitor component of Kaspersky Industrial CyberSecurity for Nodes to control SCADA files

4.11. PLC Integrity Check
4.12. Checking for anomalies

Lab 10. Configure and test the Windows log inspection component of Kaspersky Industrial CyberSecurity for Nodes to detect anomalies in the system

4.13. Sending data to SCADA using Kaspersky Security Gateway
4.14. Maintenance tools
4.15. Collecting diagnostic information

5. Deploying Kaspersky Industrial CyberSecurity for Networks

5.1. Components and architecture of Kaspersky Industrial CyberSecurity for Networks
5.2. Hardware requirements
5.3. Distribution package
5.4. Installing the server component

Lab 11. Install the server of Kaspersky Industrial CyberSecurity for Networks

5.5. Installing the sensor component
5.6. Connecting a sensor to the server
5.7. Creating a monitoring point

Lab 12. Configuring a monitoring point

5.8. Activating the product

Lab 13. Activate Kaspersky Industrial CyberSecurity for Networks

5.9. Users and roles

6. Network inventory and industrial configurations

6.1. Overview of technologies, training mode
6.2. Device discovery

Lab 14. Enable network inventory technologies in training mode

6.3. Network map

Lab 15. Group the discovered devices on the network map

6.4. Network interaction discovery

Lab 16. Configure subnets to discover interactions
Lab 17. Draw up allow rules

6.5. Discovering industrial devices
6.6. Vulnerability scanning

Lab 18. Find and fix vulnerabilities in industrial devices

6.7. Detecting system commands
6.8. Automatic discovery of process parameters (tags)
6.9. Importing projects

Lab 19. Get a list of tags to monitor a process by rules

7. Attack detection

7.1. Technology overview, surveillance mode
7.2. Detecting unauthorized devices

Lab 20. **Detect an adversary computer**

7.3. Detecting anomalies in protocols and ARP spoofing
7.4. Detecting network attacks with the help of rules

Lab 21. **Detect a WannaCry attack**

7.5. Detecting unauthorized system commands
7.6. Tag control rules

Lab 22. **Detect an abnormal tag value**

8. Kaspersky Industrial CyberSecurity for Networks maintenance

8.1. Updating Kaspersky Industrial CyberSecurity for Networks
8.2. Audit, events and logs of Kaspersky Industrial CyberSecurity for Networks

Lab 23. **Find information in the product logs**

8.3. Storing and rotating data (traffic, events, logs)

Lab 24. **Find stored event traffic**

8.4. Gathering diagnostic information for technical support

9. Kaspersky Industrial CyberSecurity for Networks integrations

9.1. Integration overview: Kaspersky Security Center, Kaspersky Industrial CyberSecurity for Nodes, Kaspersky Unified Monitoring and Analysis
9.2. Integrating Kaspersky Industrial CyberSecurity for Networks with Kaspersky Security Center

Lab 25. **Prepare the Kaspersky Security Center for integration with Kaspersky Industrial CyberSecurity for Networks**
Lab 26. **Connect Kaspersky Industrial CyberSecurity for Networks to Kaspersky Security Center**

9.3. Integrating Kaspersky Industrial CyberSecurity for Networks with Kaspersky Industrial CyberSecurity for Nodes

Lab 27. **Prepare Kaspersky Industrial CyberSecurity for Networks for integration with Kaspersky Industrial CyberSecurity for Nodes**
Lab 28. **Connect Kaspersky Industrial CyberSecurity for Nodes to Kaspersky Industrial CyberSecurity for Networks**