KL 038.4.1:

Kaspersky Industrial CyberSecurity

Featured products

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

Featured applications

- Kaspersky Industrial CyberSecurity for Windows Nodes 3.1
- Kaspersky Industrial CyberSecurity for Networks 4.1
- Kaspersky Security Center 14.2
    - Kaspersky Security Center 14.2 Administration Server
    - Kaspersky Security Center 14.2 Network Agent
    - Kaspersky Security Center 14.2 Web Console
- Kaspersky Endpoint Agent 3.15

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 protocols. 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

4 days

Contents

Part I. Introduction to industrial cybersecurity

1. Introduction to industrial control system security

1.1. How the course is organized
1.2. What an industrial control system is
1.3. Cybersecurity threats to an ICS
1.4. Industrial cybersecurity
1.5. KICS as an integral approach to protecting an industrial environment

Unit II. Kaspersky Security Center

1. Kaspersky Security Center basics

1.1. Kaspersky Security Center components and architecture
1.2. Kaspersky Security Center functions
1.3. Kaspersky Security Center MMC
1.4. Kaspersky Security Center web console
1.5. Management plug-ins
1.6. Policies
1.7. Tasks
1.8. Deployment
1.9. Activation and database updates

Unit III. Kaspersky Industrial CyberSecurity for Networks

1. Kaspersky Industrial CyberSecurity for Networks deployment

1.1. Operating principles of Kaspersky Industrial CyberSecurity for Networks
1.2. Pre-installation
1.3. Deployment

Lab 1. Install the server of Kaspersky Industrial CyberSecurity for Networks

1.4. Initial setup

Lab 2. Activate and update Kaspersky Industrial CyberSecurity for Networks
Lab 3. Enable traffic interception

2. Network inventory

2.1. Inventory technologies
2.2. Device discovery

Lab 4. Enable Device Activity Detection
Lab 5. Enable Device Information Detection
Lab 6. Perform active device polling

2.3. Deep analysis of 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. Enable control for industrial process parameters

2.4. Discovering network interactions
2.5. Network map
2.6. Risk management

Lab 11. **Enable risk detection**
Lab 12. **Enable Network Integrity Control**
Lab 13. **Configure network map**

3. Detecting attacks and anomalies

3.1. Detection technologies
3.2. Detecting unauthorized devices

Lab 14. **Switch Kaspersky Industrial CyberSecurity for Networks to Monitoring mode**
Lab 15. **Detect an unauthorized device on the industrial network**

3.3. Intrusion Detection System (IDS)

Lab 16. **Detect network scanning**

3.4. Command Control
3.5. Rule-based Process Control

Lab 17. **Detect unauthorized interaction with the field controller**
Lab 18. **Detect interference with the controller's operation**

3.6. Processing events and incidents

Lab 19. **Complete incident processing**

4. Kaspersky Industrial CyberSecurity for Networks: maintenance

4.1. Product status monitoring
4.2. Reports
4.3. Product logs
4.4. Storing and rotating service data
4.5. Gathering information for technical support

5. Kaspersky Industrial CyberSecurity for Networks integrations

5.1. Integration capabilities
5.2. Integration with Kaspersky Security Center

Lab 20. **Configure representation of data from Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center**
Lab 21. **Configure single sign-on**

5.3. Integration with third-party systems
5.4. Integrating Kaspersky Industrial CyberSecurity for Networks with Kaspersky Industrial CyberSecurity for Nodes
5.5. Integration via REST API

Unit IV. Kaspersky Industrial CyberSecurity for Nodes

1. Deploying Kaspersky Industrial CyberSecurity for Nodes

1.1. Why Kaspersky Industrial CyberSecurity for Nodes
1.2. Components and architecture of Kaspersky Industrial CyberSecurity for Nodes
1.3. Hardware requirements
1.4. Distribution package
1.5. Installation methods
1.6. Installation results

Lab 22. **Prepare the infrastructure for deploying Kaspersky Industrial CyberSecurity for Nodes**
Lab 23. **Deploy Kaspersky Security Center Network Agent and Kaspersky Industrial CyberSecurity for Nodes**

1.7. Kaspersky Industrial CyberSecurity for Nodes Console

Lab 24. Install the console of Kaspersky Industrial CyberSecurity for Nodes
Lab 25. Connect Kaspersky Industrial CyberSecurity for Nodes to Kaspersky Industrial CyberSecurity for Networks

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

2.1. How Kaspersky Industrial CyberSecurity for Nodes protects network nodes
2.2. How malware infiltrates devices
2.3. What malware does on ICS nodes
2.4. Protection types provided by Kaspersky Industrial CyberSecurity for Nodes
2.5. Non-signature protection
2.6. Applications Launch Control

Lab 26. Configure Applications launch control of Kaspersky Industrial CyberSecurity for Nodes to run in non-blocking mode
Lab 27. Block unauthorized applications on ICS nodes

2.7. Exploit Prevention
2.8. Device Control
2.9. Wi-Fi Control
2.10. Firewall management
2.11. Signature-based protection
2.12. Real-Time File Protection
2.13. Configuring exclusions and object processing
2.14. Anti-Cryptor
2.15. Network Threat Protection

Lab 28. Configure Kaspersky Industrial CyberSecurity for Nodes to protect ICS against ransomware
Lab 29. Configure protection against network attacks in Kaspersky Industrial CyberSecurity for Nodes

2.16. AMSI Protection
2.17. Industrial process control
2.18. File Integrity Monitor

Lab 30. Configure the File Integrity Monitor component of Kaspersky Industrial CyberSecurity for Nodes to control SCADA files

2.19. Log Inspection

Lab 31. Configure the Windows Log Inspection component of Kaspersky Industrial CyberSecurity for Nodes to detect anomalies in the system

2.20. Registry Access Monitor
2.21. PLC Integrity Check

Lab 32. Configure integrity check for PLC projects

2.22. Portable Scanner

3. Kaspersky Industrial CyberSecurity for Nodes integrations

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

4. Kaspersky Industrial CyberSecurity for Nodes maintenance

Unit V. Kaspersky Endpoint Agent

1. Kaspersky Endpoint Agent operation principles

1.1. What Kaspersky Endpoint Agent is
1.2. Pre-installation

Lab 33. Prepare the infrastructure for demonstrating a hacker attack

Lab 34. **Imitate a hacker attack on an industrial network**
Lab 35. **Use Kaspersky Industrial CyberSecurity for Networks to investigate an attack on an enterprise**

2. Incident response

2.1. How to respond to an alert
2.2. Alert details
2.3. Threat containment
2.4. Configuring the display of detection events in Kaspersky Security Center
2.5. Alert details

Lab 36. **Use Kaspersky Security Center to investigate an attack on an enterprise**

2.6. Threat containment

Lab 37. **Find indicators of compromise**
Lab 38. **Configure blocking of malicious scripts**

3. Security audit

3.1. What security audit is
3.2. Perform security audit

Lab 39. **Perform security audit on the SCADA machine**