KL 060.4.5:

Kaspersky Industrial CyberSecurity

Investigation

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 Windows Nodes 4.0
- Kaspersky Industrial CyberSecurity for Linux Nodes 2.0
- Kaspersky Industrial CyberSecurity for Networks 4.5
- Kaspersky Security Center Linux 16.0
- 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:

- Configuring components designed to detect threats and protect against attacks
- Analysis of threat detection events
- Incident response

Duration

2 days

Contents

Part I. Kaspersky Industrial CyberSecurity for Networks

1. Network monitoring

1.1. Risk Detection
1.2. Information about network sessions

Lab 1. Configure integration of KICS for Nodes with KICS for Networks
Lab 2. Enable Risk Detection
Lab 3. Enable monitoring of network sessions

1.3. Technologies that detect network attacks and anomalies

Managing IDS rules
Detecting anomalies in network sessions

2. Detecting attacks and anomalies

2.1. Detection technologies
2.2. Potential attack scenario
2.3. Detecting unauthorized devices and network interactions
2.4. Intrusion Detection (IDS)

Lab 4. Detect an unauthorized device on the network
Lab 5. Detect network scanning
Lab 6. Detect brute-forcing of a network service
Lab 7. Detect unauthorized interaction with a PLC
Lab 8. Detect interference with PLC operation

3. Device audit

3.1. Windows and Linux device configuration control

Lab 9. Set up device configuration control

3.2. Anomaly detection using Sigma rules

Lab 10. Configure Anomaly Detection using Sigma rules

3.3. Device security audit based on rules

Lab 11. Perform security audit on the SCADA machine

Part II. Kaspersky Industrial CyberSecurity for Nodes

4. Non-signature protection

4.1. Exploit Prevention
4.2. Log Inspection

5. Signature-based protection

5.1. File Protection
5.2. Anti-Cryptor
5.3. Network Threat Protection
5.4. AMSI Scanner

Lab 12. Configure node protection against ransomware
Lab 13. Configure node protection against network attacks
Lab 14. Configure the Log Inspection component to detect anomalies in the system

6. Portable Scanner

7. Protection status monitoring in Kaspersky Security Center

Reports in KSC

Part III. EDR functions

8. Endpoint Agent functions and capabilities

8.1. Endpoint Agent functions and capabilities
8.2. Endpoint Agent interactions

9. Incident response

9.1. How to respond to an incident
9.2. Incident details

Lab 15. Simulate an attack on the SCADA server
Lab 16. Simulate an attack on the Admin-OT workstation
Lab 17. Use Kaspersky Security Center to investigate the attack

9.3. Threat containment
9.4. Scanning computers for indicators of compromise

Lab 18. Find indicators of compromise
Lab 19. Configure blocking of malicious scripts