KL 002.12.1:

Kaspersky Endpoint Security and Management

Featured products

- Kaspersky Security Center
- Kaspersky Endpoint Security for Windows

Course objective

The main objective of the course is to provide participants with all the knowledge required to deploy, configure, and manage the solution.

The course teaches how to design, deploy, and maintain protection systems based on Kaspersky Endpoint Security and centrally manage them via Kaspersky Security Center. It describes products designed to protect a network of up to 1000 endpoints in a single location. Endpoints in this course are servers and workstations running Windows.

The theoretical part of the course and hands-on labs provide participants with the knowledge and skills necessary to:

- Describe the capabilities of Kaspersky Endpoint Security for Windows and Kaspersky Security Center.
- Design and deploy an optimal protection solution based on Kaspersky Endpoint Security in a Windows network and manage it via Kaspersky Security Center.
- Maintain the deployed system.

Duration

3 days.

Requirements for participants

Basic understanding of networking technologies, such as TCP/IP, DNS, email, web. Basic Windows administrator skills. Basic knowledge of information security principles.

Contents

1. Deployment

1.1. General
1.2. Kaspersky Security Center installation

Lab 1. Installing Kaspersky Security Center

1.3. Deploying Kaspersky Endpoint Security

Lab 2. Deploying Kaspersky Endpoint Security

1.4. Working with groups of managed devices

Lab 3. Creating a structure of managed devices

1.5. Kaspersky Security Center Cloud Console

2. Protection management

2.1. How Kaspersky Endpoint Security protects computers
2.2. How to configure file protection
2.3. How to configure protection against network threats

Lab 4. Configuring file protection
Lab 5. Configuring Mail Threat Protection
Lab 6. Testing Web Threat Protection

2.4. How to configure protection against sophisticated threats

Lab 7. Protecting network folders against ransomware
Lab 8. Testing protection against fileless threats
Lab 9. Testing protection against exploits
Lab 10. Configuring Host Intrusion Prevention to protect against ransomware

2.5. How to control network connections

Lab 11. Testing Network Threat Protection

3. Control

3.1. General
3.2. Application control

Lab 12. Configuring Application Control
Lab 13. Blocking start of unknown applications in the network

3.3. Device Control
3.4. Web Control

Lab 14. Configuring web access control

3.5. Adaptive Anomaly Control

Lab 15. Configuring Adaptive Anomaly Control

4. Kaspersky Endpoint Detection and Response Optimum

4.1. General
4.2. Deploying Kaspersky Endpoint Detection and Response Optimum
4.3. Incident response

Lab 16. Simulating an attack on the enterprise network
Lab 17. Deploying Kaspersky Endpoint Detection and Response Optimum
Lab 18. Preparing Endpoint Detection and Response Optimum
Lab 19. Responding to an incident

5. Administration

5.1. Administration Server hardening
5.2. Backup, restore and maintenance
5.3. Configuring policies and tasks

Lab 20. Configuring password protection

5.4. Event storage and integration with SIEM
5.5. Vulnerability management
5.6. Monitoring and reports

Lab 21. Customizing the dashboard
Lab 22. Configuring reports

5.7. Checklists
5.8. Contacting technical support

Lab 23. Collecting diagnostic information

What's new

Course materials and labs have been updated for version 14.1 of Kaspersky Security Center and version 12.1 of Kaspersky Endpoint Security.

The following information has been added to the presentation and student guide:

- New Kaspersky Endpoint Detection and Response Optimum module
- Tips for hardening Administration Server to prevent compromise
- Specifics of protection deployment in Kaspersky Security Center Cloud Console
- Vulnerability management
- Integration with SIEM