KL 046.12.5:

Kaspersky Next EDR Foundations

Featured applications

- **Kaspersky Security Center 14.2**
- **Kaspersky Endpoint Security for Windows 12.5**

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 12.5 and centrally manage them via Kaspersky Security Center 14.2. 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 Next EDR Foundations tier.
- Design and deploy an optimal protection solution based on Kaspersky Endpoint Security 12.5 in a Windows network and manage it via Kaspersky Security Center 14.2.
- 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

- **Deployment**
  1. General
  2. Kaspersky Next
  3. Kaspersky Security Center installation
  Lab 1. Installing Kaspersky Security Center
  4. Deploying Kaspersky Endpoint Security

Lab 2. Deploying Kaspersky Endpoint Security
5. Working with groups of managed devices
Lab 3. Creating a structure of managed devices
6. Kaspersky Next EDR Cloud Consoles
7. Kaspersky Endpoint Security Cloud Console
8. Kaspersky Security Center Cloud Console

- **Protection management**
  1. How Kaspersky Endpoint Security protects computers
  2. How to configure file protection
  3. How to configure protection against network threats
  Lab4. Configuring file protection
  Lab5. Configuring Mail Threat Protection
  Lab6. Testing Web Threat Protection
  4. How to configure protection against sophisticated threats
  Lab7. Protecting network folders against ransomware
  Lab8. Testing protection against fileless threats
  Lab9. Testing protection against exploits
  Lab10. Configuring Host Intrusion Prevention to protect against ransomware
  5. How to control network connections
  Lab11. Testing Network Threat Protection

- **Security controls**
  1. General
  2. Application control
  Lab 12. Configuring Application Control
  Lab 13. Blocking start of unknown applications in the network
  3. Device Control
  4. Web Control
  Lab 14. Configuring web access control
  Lab 15. Simulating an attack on the enterprise network

- **Root-Cause Analisys**
  1. General
  2. Root cause analysis
  3. Deployment
  4. Incident response
  Lab 16. Deploying Kaspersky Endpoint Detection and Response Optimum
  Lab 17. Preparing Kaspersky EDR for use
  Lab 18. Incident response

- **Administration**
  1. Administration Server hardening
  2. Backup, restore and maintenance
  3. Configuring policies and tasks
  Lab 19. Configuring password protection
  4. Event storage and integration with SIEM
  5. Vulnerability management
  6. Monitoring and reports
  Lab 20. Customizing the dashboard
  Lab 21. Configuring reports
  7. Checklists
  8. Contacting technical support
  Lab 22. Collecting diagnostic information