KL 046.12.7:

Kaspersky Next EDR Foundations

Featured products

- Kaspersky Security Center Linux 12.2
- Kaspersky Endpoint Security for Windows 12.7
- Kaspersky Endpoint Security for Linux 15.2

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. In this course, endpoints are Windows and Linux servers and workstations.

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 and Kaspersky Security Center.
- Design and deploy an optimal protection solution based on Kaspersky Endpoint Security in a not-too-large network and manage it via Kaspersky Security Center.
- Maintain the deployed system.

Duration

4 days

Requirements for participants

The course is aimed at technical support and presale engineers. Attendees must possess:

- Basic understanding of networking technologies, such as TCP/IP, DNS, email, web
- Basic Windows and Linux administering skills
- Basic knowledge of information security principles

Contents

1. Deployment
2. Management of Windows protection
3. Windows security controls
4. EDR Optimum (Windows)
5. Protection for Linux
6. Administration

Labs

Lab 1. Install Kaspersky Security Center Linux
Lab 2. Configure Kaspersky Security Center Linux
Lab 3. Deploy Kaspersky Endpoint Security for Windows
Lab 4. Create a structure of managed computers
Lab 5. Configure file protection
Lab 6. Configure Mail Threat Protection
Lab 7. Test Web Threat Protection
Lab 8. Protect shared folders against ransomware
Lab 9. Test protection against fileless threats
Lab 10. Test protection against exploits
Lab 11. Configure Host Intrusion Prevention to protect against ransomware
Lab 12. Test Network Threat Protection
Lab 13. Configure Application Control
Lab 14. Block launch of unknown applications in the network
Lab 15. Configure web access control
Lab 16. Simulate an attack on the enterprise network
Lab 17. Deploy Kaspersky Endpoint Detection and Response
Lab 18. Prepare Kaspersky EDR for use
Lab 19. Investigate an incident
Lab 20. Install Kaspersky Endpoint Security for Linux on managed devices
Lab 21. Add Linux computers to the Managed Devices structure

Lab 22. Set up essential protection for a Linux server

Lab 23. Set up advanced protection for a Linux server

Lab 24. Configure security controls on a Linux computer

Lab 25. Manage protection using kesl-control

Lab 26. Manage Linux accounts and devices

Lab 27. Configure password protection

Lab 28. Customize the dashboard

Lab 29. Configure reports

Lab 30. Collect diagnostic information