KL 005.11:

Protecting Windows Servers and Embedded Systems

Featured products

- Kaspersky Security for Windows Server
- Kaspersky Embedded Systems Security

Course objective

This course educates engineers how to deploy, configure and maintain Kaspersky Security 11 for Windows Server at midsize or large enterprises.

The training describes the actions to be taken by the administrator step by step to successfully deploy and configure the product in a corporate network. Special attention is paid to configuring Kaspersky Security 11 for Windows Server to solve specific tasks, for example, protection against crypto-ransomware, or deploying Default Deny policy, or storage protection.

Labs demonstrate today’s methods of protecting an information system. The administrator manages the whole infrastructure from the workstation through the Kaspersky Security Center Administration Console and Kaspersky Security Console. Almost every section of the theoretical part of the course is accompanied by a hands-on lab where you can put your knowledge into practice and get a real feel for how the product would perform.

Duration

2–3 days.

Requirements for the students

Basic knowledge of Kaspersky Security Center and Kaspersky Endpoint Security. Understanding of contemporary threats, typical phases of the cyber kill chain and cyber security incident investigation procedures.

Contents

1. General

2. Deployment

3. Configuring group tasks

4. File system protection

5. Network Threat Protection

6. Protection for Remote Desktop Services

6.1. Threat model for Remote Desktop Services sessions
6.2. Traffic Security: Driver Interceptor
6.3. Components of protection for Remote Desktop Services sessions
6.4. Traffic Security: Redirector
6.5. Traffic Security: External Proxy

Lab 11. **Configure Traffic Security in Driver Interceptor mode**
Lab 12. **Configure Traffic Security to scan mail traffic**
Lab 13. **Configure Traffic Security to the External Proxy mode**

7. Server control components

7.1. Applications Launch Control

Lab 14. **Enable Applications Launch Control in Test Mode**
Lab 15. **Switch Application Startup Control into active mode**
Lab 16. **Create allow rules for installation packages and updates**

7.2. Device Control

8. System inspection

8.1. File Integrity Monitor
8.2. Log Inspection

Lab 17. **Configure the System Inspection components**

9. Protection for storages

9.1. Storage protection capabilities
9.2. Real-Time File Protection for storages

Lab 18. **Protect a NetApp Clustered Data ONTAP storage**

9.3. Anti-Cryptor for NetApp

Lab 19. **Configure Anti-Cryptor for NetApp**

10. Additional settings

10.1. Protection for shared cluster resources
10.2. Firewall Management
10.3. SIEM integration
10.4. Managing applications
10.5. Collecting diagnostic information
10.6. Monitoring the protection status (health check)