

KL 009.12:

Kaspersky Security Center. Vulnerability and Patch Management

Featured products

- Kaspersky Security Center

Course description

Kaspersky Vulnerability and Patch Management (previously known as Kaspersky Systems Management) covers a large number of varied tools necessary for monitoring, management and troubleshooting.

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

- Manage vulnerabilities and software updates on the network computers
- Capture, reconfigure and install operating system images
- Work with the hardware and software registries, manage the licenses of third-party applications, and configure integration with SIEM systems

Duration

1 day

Requirements for the students

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

The course is aimed at Microsoft Windows system administrators, security experts and administrators, technical support and presale engineers.

What's new compared to the previous version (009.11)

- The course structure has been changed to focus on the Vulnerability and Patch Management functionality
- The presentation and labs now demonstrate the Vulnerability and Patch Management functionality using the Web Console

Contents

1. Introduction

- 1.1. Vulnerability and Patch Management in Kaspersky Security Center
- 1.2. Licensing
- 1.3. Access to the Vulnerability and Patch Management functionality in the Kaspersky Security Center interface

2. Vulnerability and patch management

- 2.1. Problem statement
- 2.2. Search for vulnerabilities and required updates
- 2.3. Windows Update synchronization

Lab 1. How to prepare Kaspersky Security Center for the WSUS server role

- 2.4. Installing required updates and fixing vulnerabilities

Lab 2. How to scan for vulnerabilities and required updates

Lab 3. How to install critical Windows Updates on workstations

Lab 4. How to fix the vulnerability exploited by the WannaCry malware

- 2.5. Installing software using the Kaspersky database of third-party applications

Lab 5. How to install only approved updates for third-party software in a group of computers

Lab 6. How to automatically update all browsers on the client computers

Lab 7. How to fix vulnerabilities in all programs except, for example, Java

Lab 8. How to install all available third-party updates in a group of computers

Lab 9. How to install a third-party application using the Kaspersky database

- 2.6. Monitoring

3. Capturing and deploying computer images

- 3.1. Problem statement
- 3.2. Preparation
- 3.3. How to create an operating system image
- 3.4. How to customize an operating system image
- 3.5. How to deploy an operating system image
- 3.6. Image deployment using a PXE server

Lab 10. How to capture an operating system image

Lab 11. How to deploy an operating system image on a managed computer

Lab 12. How to deploy an operating system image to a bare-metal computer

4. Integration with SIEM and other capabilities of Kaspersky Vulnerability & Patch Management

- 4.1. Control over the third-party licenses used

Lab 13. How to manage third-party licenses

- 4.2. Hardware information

- 4.3. Remote connection to a client computer via Windows Desktop Sharing

- 4.4. SIEM integration

Lab 14. How to configure integration with a SIEM system