

**KL 013.11.4:**

# Kaspersky Endpoint Security for Linux

## Featured products

- Kaspersky Endpoint Security for Linux 11.4
- Kaspersky Security Center Linux 14.2

## Course description

Kaspersky Endpoint Security for Linux and Kaspersky Security Center Linux together form an EPP (Endpoint Protection Platform) solution that helps protect Linux devices against a wide range of threats.

The theoretical part of the course and the hands-on labs provide participants with the knowledge and skills needed to deploy, understand, configure and maintain the solution.

## Duration

1 day

## Requirements for participants

Basic understanding of networking technologies, basic Linux administrator skills. Understanding of contemporary threats and information technologies.

## Contents

### 1. How and why to protect Linux

- 1.1. Why protect Linux?
- 1.2. What can protect Linux?

### 2. How to deploy protection

- 2.1. Installation scenario
- 2.2. MariaDB installation and configuration
- 2.3. PostgreSQL installation and configuration
- 2.4. Installing the Administration Server
- 2.5. Web console installation

**Lab 1.**      How to install Kaspersky Security Center Linux

- 2.6. What to do after deploying KSC
- 2.7. Initial server setup
- 2.8. How to discover devices on the network

**Lab 2.**      How to configure Kaspersky Security Center Linux

- 2.9. Network Agent installation
- 2.10. KESL installation

**Lab 3.**      Install Kaspersky Endpoint Security on the managed devices

**3.    How to configure protection**

- 3.1. How to organize devices
- 3.2. How to assign tags
- 3.3. How to apply policies

**Lab 4.**      How to manage devices

**4.    How to protect devices**

- 4.1. How to protect devices against malware
- 4.2. How to prevent malicious files from infiltrating a device
- 4.3. How to protect a device against network threats
- 4.4. How to protect against file-encrypting ransomware
- 4.5. How to protect against new threats

**Lab 5.**      Configuring server protection

**5.    How to harden a system**

- 5.1. Why control a system?
- 5.2. Application control
- 5.3. Inventory
- 5.4. Firewall management
- 5.5. Device control

**Lab 6.**      How to collect information about executable files

**Lab 7.**      Test protection against vulnerability exploitation

**6.    Managing KESL via the command line**

- 6.1. Why use the command line?
- 6.2. How to manage tasks

**Lab 8.**      How to manage protection using kesi-control