

KL 036.3:

Kaspersky Secure Mail Gateway

Featured products

- Kaspersky Secure Mail Gateway 3.0

Course description

This training course is intended for administrators who need to protect corporate email traffic from malicious objects and spam, while preventing confidential data leaks. This course explains how to integrate the product into an existing infrastructure, protect email, and configure incoming mail verification using SPF, DKIM and DMARC. The program includes new technologies: analysis of QR codes in emails and attachments, Content Disarm and Reconstruction (CDR) to neutralize zero-day threats, and scanning of encrypted archives using passwords extracted from the email body.

Duration

1 day

Requirements for participants

Basic knowledge of email protocols and mail server operation principles.

Basic understanding of network technologies: TCP/IP, DNS. Basic knowledge of cybersecurity principles.

Contents

Introduction

- 1.1. How email works
- 1.2. Protection against mail threats
- 1.3. New challenges for mail gateways
- 1.4. SMTP standards
- 1.5. Mail sender authentication
- 1.6. Kaspersky Secure Mail Gateway operation principles

2. How to deploy Kaspersky Secure Mail Gateway

- 2.1. OS installation and configuration as a Virtual Appliance
- 2.2. KSMG installation from an rpm/deb package (Standalone)
- 2.3. Integration with the filtering system
- 2.4. Configuring an email relay for Virtual Appliance
 - [Lab 1.](#) Install Kaspersky Secure Mail Gateway
- 2.5. Initial setup and activation
 - [Lab 2.](#) Check health of Kaspersky Secure Mail Gateway
 - [Lab 3.](#) Configure connection to Active Directory
 - [Lab 4.](#) Configure access to the KSMG web console using SSO

3. Managing protection

- 3.1. Lists
- 3.2. Anti-Spam
- 3.3. Anti-Virus
- 3.4. Scanning encrypted attachments
 - [Lab 5.](#) Lists
 - [Lab 6.](#) Header analysis and Anti-Spam
 - [Lab 7.](#) Anti-Virus
 - [Lab 8.](#) Analysis of encrypted attachments
- 3.5. Anti-Phishing
- 3.6. Content filtering
- 3.7. Mail sender authentication
- 3.8. QR code analysis
 - [Lab 9.](#) Content filtering
 - [Lab 10.](#) Anti-Phishing
 - [Lab 11.](#) Configure sender authentication for incoming mail
- 3.9. Content Disarm and Reconstruction
 - [Lab 12.](#) Configuring Content Disarm and Reconstruction

4. Maintenance

- 4.1. Dashboard, logs and reports
- 4.2. Message queue
- 4.3. Notifications and warnings
- 4.4. Backup
 - [Lab 13.](#) Configuring the dashboard

5. Licensing

6. Advanced settings

- 6.1. Encryption and DKIM
- 6.2. Accounts
- 6.3. Scaling and maintenance
- 6.4. Integration with other systems