

KL 025.5:

Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response

Featured products

- Kaspersky Anti Targeted Attack Platform 5.0
- Kaspersky Endpoint Detection and Response 5.0
- Kaspersky Endpoint Agent 3.14
- Kaspersky Security Center 14.0
- Kaspersky Endpoint Detection and Response (Cloud)

Course description

Kaspersky Anti Targeted Attack platform and Kaspersky EDR together form a native eXtended Detection and Response (XDR) solution that helps organizations build a reliable protection system against advanced cyberattacks.

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

Duration

3 days

Requirements for participants

Basic understanding of Kaspersky Security Center.

Basic understanding of networking technologies, such as DNS, routing, email, web. Basic Windows and Linux management skills. Understanding of contemporary threats and information technologies.

Contents

1. Introduction

- 1.1. Featured products and applications
- 1.2. Threat landscape
- 1.3. Challenges in building an information security system
- 1.4. Approaches to building a cybersecurity system
- 1.5. The tasks KATA Platform helps the customer to solve

2. Pre-deployment

- 2.1. Main capabilities
- 2.2. Applications and components
- 2.3. System requirements
- 2.4. Scaling
- 2.5. Typical topologies

3. KATA platform deployment

- 3.1. Planning
- 3.2. Server installation
- 3.3. Activation and initial setup
- 3.4. Distributed installation
- 3.5. Kaspersky Endpoint Agent installation

Lab 1. Install and configure the central node

Lab 2. Configure Kaspersky Sandbox

Lab 3. Connect the central node to the sandbox

Lab 4. Activate the central node

Lab 5. Create an account for an information security specialist

4. KATA operation

- 4.1. Connecting to traffic sources
- 4.2. KATA detection technologies
- 4.3. Processing alerts
- 4.4. Identification of threats in traffic

Lab 6. Connect the central node to the network infrastructure (SPAN)

Lab 7. Make sure traffic is being analyzed

Lab 8. Connect the central node to the mail system using SMTP

Lab 9. Configure the mail server to send copies of messages to the central node

Lab 10. Make sure mail is being analyzed

Lab 11. Prevent superfluous mail processing

Lab 12. Connect a sensor to the proxy server (ICAP)

Lab 13. Make sure ICAP traffic is being analyzed

Lab 14. Prevent superfluous http traffic processing

5. KEDR operation

- 5.1. KEDR detection technologies
- 5.2. Incident investigation
- 5.3. Incident response

6. Sandbox technology

7. KATA platform maintenance

- 7.1. VIP status
- 7.2. Scanning password-protected archives
- 7.3. External API
- 7.4. Reports
- 7.5. Email notifications
- 7.6. Integration with SIEM
- 7.7. Server monitoring using SNMP
- 7.8. Collecting system information
- 7.9. Updates
- 7.10. Saving and restoring settings
- 7.11. Version update
- 7.12. Modifying system settings
- 7.13. Kaspersky Private Security Network (KPSN)

Lab 15. Install Kaspersky Endpoint Agent using KSC

Lab 16. Connect Kaspersky Endpoint Agent to the central node

Lab 17. Activate Kaspersky Endpoint Agent

Lab 18. Make sure the TAA subsystem operates properly

Lab 19. Simulate a malicious payload

Lab 20. Demonstrate KATA operation results

Lab 21. Demonstrate analysis and response to a TAA alert

Lab 22. Examine details of file execution in the sandbox

Lab 23. Add third-party IDS rules

Lab 24. Write a custom IDS rule

Lab 25. Add an exception to an IDS rule

Lab 26. Write a custom YARA rule

Lab 27. Configure integration with Active Directory

Lab 28. Working with API

8. Kaspersky Endpoint Detection and Response (Cloud) *[a separate module]*