KL 034.4:

Kaspersky Unified Monitoring and Analysis Platform. Administration

Course description

Kaspersky Unified Monitoring and Analysis Platform (KUMA) is a SIEM solution designed to collect, store, process, correlate and visualize a wide variety of data from different sources.

This course explains the architecture of the solution, introduces its capabilities and demonstrates how to install and configure it using examples.

Our course consists of theoretical materials that describe the principles of operation and configuration and hands-on labs that help provide practical experience.

Upon successful completion of the course, participants will be able to:

- Deploy Kaspersky Unified Monitoring and Analysis Platform to demonstrate the solution
- Configure receiving of events from different sources and in various formats
- Configure integration with external systems to enrich events and respond to incidents
- Monitor the status of sources and system components

Duration

2.5 days (20 hours)

Requirements for participants

The course is aimed at technical support and presale engineers. Attendees must possess:

- Understanding of the basics of networking technologies such as TCP/IP, DNS, email, web
- Basic Windows and Linux administration skills
- Basic knowledge of information security principles

Contents

1. **General**
2. **Architecture**

3. **Deployment**
4. **Event collecting and processing**
5. **Integrations**
6. **Event storage**
7. **Correlation**
8. **Alerts**
9. **Response**
10. **Monitoring source statuses and metrics**

Labs

Lab 1. Install Kaspersky Unified Monitoring and Analysis Platform

Lab 2. Configure receiving of events using Windows Agent (WMI)

Lab 3. Configure receiving of DNS events

Lab 4. Configure receiving of events from Kaspersky Endpoint Security for Windows

Lab 5. Configure receiving of Linux events

Lab 6. Configure receiving of Kaspersky Security Center events

Lab 7. Configure receiving of Kaspersky Anti Targeted Attack Platform events

Lab 8. Configure receiving of EDR telemetry from KATA

Lab 9. Import information about computers from Kaspersky Security Center

Lab 10. Configure event enrichment using Active Directory

Lab 11. Configure integration with Kaspersky Endpoint Detection and Response

Lab 12. Configure integration with CyberTrace

Lab 13. Configure cold storage for events in KUMA

Lab 14. Configure source status monitoring

Lab 15. Back up Core (optional)

Lab 16. Configure receiving of events using Windows Agent (WEC) (optional)

Lab 17. Configure event routing (optional)

Lab 18. Configure authentication via Active Directory

Lab 19. Configure receiving of events using rsyslog

Lab 20. Make Core fault tolerant

Lab 21. Make Collector fault tolerant