# KL 034.2:

# Kaspersky Unified Monitoring and Analysis Platform

## Featured products

The principal product

- Kaspersky Unified Monitoring and Analysis Platform 2.0.1

Integrated products that act as sources of events, enrichment sources and response tools in labs:

- Kaspersky Security Center 14
- Kaspersky Endpoint Security 11.10
- Kaspersky Security for Windows Server 11.1
- Kaspersky Anti Targeted Attack Platform 4.1

Integrated products described as enrichment sources in theoretical materials:

- Kaspersky CyberTrace 4.1
- Kaspersky Threat Lookup

## Course description

Kaspersky Unified Monitoring and Analysis Platform (KUMA) is a SIEM solution designed for collecting, storing, processing, correlating and visualizing very different data from various sources.

This course explains the solution’s architecture, introduces its capabilities and demonstrates through examples how to install and configure it.

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

Upon successful completion of this course, students will be able to:

- Deploy Kaspersky Unified Monitoring and Analysis Platform to demonstrate the solution
- Configure receiving events from different sources and in different formats
- Fine-tune normalization, aggregation and enrichment of events to meet the customer’s requirements
- Configure correlation rules to detect incidents
- Configure integration with external systems to enrich events and respond to incidents
- Handle incidents and analyze events
- Configure notifications and create reports

# Duration

2 days

# Requirements for the students

The course is aimed at technical support and presale engineers. Attendees are required to possess:

- Basic understanding of networking technologies, such as TCP/IP, DNS, email, web
- Basic Windows and Linux administering skills
- Basic knowledge of information security principles
- General idea of regular expressions

# Contents

## 7. Integrations

7.1. Integration with Kaspersky Security Center and working with assets
7.2. Integration with LDAP and working with accounts
7.3. Integration with Kaspersky Threat Lookup
7.4. Integration with Kaspersky CyberTrace
7.5. Integration with Kaspersky Endpoint Detection and Response

**Lab 5. Configure receiving of KSWS events**
**Lab 6. Configure DNS data enrichment**
**Lab 7. Configure GeoIP data enrichment**
**Lab 8. Import information about computers from KSC**
**Lab 9. Configure LDAP data enrichment**
**Lab 10. Configure enrichment with CyberTrace data**

## 8. Working with events

## 9. Correlation

9.1. Correlation rule types
9.2. Simple correlation rules
9.3. Standard correlation rules: selectors, correlation buckets
9.4. Local and global variables

**Lab 11. Create a simple correlation rule**
**Lab 12. Create a standard correlation rule**
**Lab 13. Configure an alert for events logged in a specific order**
**Lab 14. Create a correlation rule using a local variable**

9.5. Active lists and operational correlation rules
9.6. Retrospective scanning

**Lab 15. Create a technical correlation rule to fill an active list**
**Lab 16. Create a correlation rule using the active list**
**Lab 17. Run retrospective scanning**

## 10. Working with alerts

## 11. Response

11.1. Response by running a Kaspersky Security Center task
11.2. Response by running a script
11.3. Response by running a Kaspersky Endpoint Detection and Response task

**Lab 18. Configure response by running a Kaspersky Security Center task**
**Lab 19. Configure response by running a Kaspersky Endpoint Detection and Response task**

## 12. Reporting

12.1. Dashboard
12.2. Reports
12.3. Metrics

**Lab 20. Study reports**
**Lab 21. Send a request to Kaspersky Unified Monitoring and Analysis Platform via REST API (optional)**