KL 034.2.1:

Kaspersky Unified Monitoring and Analysis Platform

Featured products

The principal product:

- Kaspersky Unified Monitoring and Analysis Platform 2.1

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 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 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 event normalization, aggregation and enrichment to meet customer 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 generate reports

Duration

2 days

Requirements for participants

The course is aimed at technical support and presale engineers. Attendees must 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 understanding of regular expressions

Contents

1. **Introduction to SIEM**
2. **KUMA architecture and operation principles**
3. **Installation**

   Lab 1. **Install Kaspersky Unified Monitoring and Analysis Platform**
4. **Collecting events**

   4.1. Collector operation principles
   4.2. Connection and connector settings
   4.3. Receiving Windows events

   Lab 2. **Configure receiving of Windows events**
   Lab 3. **Configure receiving of Kaspersky Security Center events**
   Lab 4. **Configure receiving of KATA events**
   Lab 5. **Configure connection to a Kafka database to receive EDR telemetry from KATA**
5. **Normalization**

   5.1. KUMA data model
   5.2. Normalizer settings
   5.3. Data mutation
   5.4. Extra normalizers
6. **Collector: event processing**

   6.1. Filtering
   6.2. Aggregation
   6.3. Enrichment
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 6. **Configure receiving of KSWS events**
   Lab 7. **Configure DNS data enrichment**
   Lab 8. **Configure GeoIP data enrichment**
   Lab 9. **Import information about computers from KSC**
   Lab 10. **Configure LDAP data enrichment**
   Lab 11. **Configure enrichment with CyberTrace data**

8. Working with events

Lab 12. **Configure cold storage for events in Kaspersky Unified Monitoring and Analysis Platform**

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 13. **Create a simple correlation rule**
Lab 14. **Create a standard correlation rule**
Lab 15. **Configure an alert for events logged in a specific order**

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

Lab 16. **Create a technical correlation rule to fill an active list**
Lab 17. **Create a correlation rule using the active list**
Lab 18. **Create a correlation rule using a local variable**
Lab 19. **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 20. **Configure response by running a Kaspersky Security Center task**
Lab 21. **Configure response by running a Kaspersky Endpoint Detection and Response task**

12. Reporting

12.1. Dashboard
12.2. Reports
12.3. Metrics

Lab 22. **Study reports**
Lab 23. **Send a request to Kaspersky Unified Monitoring and Analysis Platform via REST API (optional)**