KL 034.3.2:

Kaspersky Unified Monitoring and Analysis Platform

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
- Fine-tune 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

3 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. Deployment

Installation options: all-in-one, distributed, high availability

4. Collecting events

Collector operation principles, configuring connection and connector, receiving of events.

5. Normalization

KUMA data model, normalizer settings, data mutation, extra normalizers

6. Collector: event processing

Filtering, aggregation, enrichment.

7. Integrations

Integration with Kaspersky Security Center and working with assets; integration with LDAP and working with accounts; integration with Kaspersky Threat Lookup, Kaspersky CyberTrace, and Kaspersky Endpoint Detection and Response.

8. Working with events

9. Correlation

Correlation rule types, variables, active lists and retroscanning.

10. Working with alerts

11. Response

Response by running a script, Kaspersky Security Center task, or Kaspersky Endpoint Detection and Response task.

12. Reporting

Dashboard, reports, MITRE ATT&CK coverage, metrics

Labs

Lab 1. Install Kaspersky Unified Monitoring and Analysis Platform

Lab 2. Configure receiving of events from Windows Event Log

Lab 3. Configure receiving of events from Windows DNS Analytic log (optional)

Lab 4. Configure receiving of Linux events (optional)

Lab 5. Configure receiving of Kaspersky Security Center events

Lab 6. Configure receiving of Kaspersky Anti Targeted Attack Platform events

Lab 7. Configure receiving of EDR telemetry from KATA

Lab 8. Configure DNS data enrichment

Lab 9. Configure GeoIP data enrichment

Lab 10. Import information about computers from Kaspersky Security Center

Lab 11. Configure event enrichment using Active Directory

Lab 12. Configure enrichment with CyberTrace data

Lab 13. Configure cold storage for events in KUMA

Lab 14. Create a simple correlation rule

Lab 15. Create a standard correlation rule

Lab 16. Configure an alert for events logged in a specific order

Lab 17. Create a correlation rule using a local variable

Lab 18. Create a technical correlation rule to fill an active list

Lab 19. Create a correlation rule using the active list

Lab 20. Run retrospective scanning

Lab 21. Configure response by running a Kaspersky Security Center task

Lab 22. Configure response by running a Kaspersky Endpoint Detection and Response task

Lab 23. Study reports

Lab 24. Send a request to KUMA via REST API (optional)

Lab 25. Configure Event router service (optional)

Lab 26. Create a rule based on entropy calculation function (optional)