KL 048.1.1:

Kaspersky NEXT XDR Expert

Course description

Kaspersky NEXT XDR Expert is a reliable cybersecurity solution that helps protect corporate IT infrastructures against advanced threats. Kaspersky NEXT XDR Expert enables you to:

- Collect data from multiple sources and store it in a convenient form for analysis. Collector services can receive data from numerous sources and convert it into a unified format. The data is stored in a high-performance ClickHouse analytical database. The product comes with a set of ready-to-use normalizers.
- Manually and automatically analyze collected data and detect threats. Correlators have flexible capabilities to implement even the most complex detection logic. The product includes a variety of correlation rules.
- Comprehensively assess the level of corporate security using data from reports and the dashboard.
- Analyze cyberthreat development stages using the investigation graph.
- Analyze threat actions using collected telemetry and KEDR Expert detection mechanisms.
- Manage and reliably protect endpoint devices using Kaspersky Endpoint Security.
- Automatically and manually respond to threats, which, combined with the product's integration capabilities, allows you to implement complex cross-product protection scenarios.
- Effectively manage collected data. The web interface provides the user with convenient methods of interaction, including contextual search and response actions, data visualization, and an investigation graph.

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

Duration

3 days (24 hours)

Requirements for participants

To successfully master all the material in this course, you need knowledge and skills in working with Kaspersky Unified Monitoring and Analysis Platform (KUMA) and Kaspersky Security Center (KSC), which can be gained by completing the following training courses:

- Kaspersky Unified Monitoring and Analysis Platform (technical training KL 034)
- Kaspersky Security Center (technical training KL 002)

Contents

16. Incidents

17. Playbooks

Lab 15. Write JQ filters

Lab 16. Run a playbook to scan for malicious objects

Lab 17. Create a playbook to block user accounts

Lab 18. Get KEDR Expert telemetry

Lab 19. Create a playbook with three actions

Lab 20. Create a playbook to perform a response action and a playbook for Telegram notifications

Lab 21. Automatic incident creation

18. Kaspersky NEXT XDR Expert administration

19. Kaspersky NEXT XDR Expert troubleshooting

20. Kaspersky NEXT XDR Expert maintenance

21. Central Node maintenance

Lab 22. Examine details of file execution in Sandbox

Lab 23. Display data about running pods and persistent volumes

Lab 24. Connect to Kaspersky NEXT XDR Expert via API

Lab 25. Work with KEDR Expert API