

## 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

## 1. Introduction

## 2. Capabilities

## 3. Kaspersky NEXT XDR Expert Architecture

## 4. Central Node architecture

## 5. Kaspersky NEXT XDR Expert installation

## 6. Central Node, Sensor, Sandbox installation

- Lab 1. Install and configure Central Node
- Lab 2. Check KATA Platform Sandbox settings
- Lab 3. Prepare KEDR Expert for work
- Lab 4. Install Kaspersky NEXT XDR Expert. Task A

## 7. Installing agents

## 8. Kaspersky NEXT XDR Expert post-installation

## 9. Central Node post-installation

## 10. Integrations

- Lab 4. Install Kaspersky NEXT XDR Expert. Tasks B and C
- Lab 5. Configure integration with an arbitrary server
- Lab 6. Configure integration with KATA Platform
- Lab 7. Configure integration with Microsoft Active Directory
- Lab 8. Configure integration with Kaspersky Security Center
- Lab 9. Install KES using KSC
- Lab 10. Connect KES to Central Node

## 11. Alerts

## 12. Threat Hunting in Kaspersky NEXT XDR Expert

## 13. Central Node: threat hunting

## 14. Central Node: response actions

## 15. Sandbox: threat hunting

- Lab 11. Attack a corporate Linux server
- Lab 12. Attack a corporate Windows computer
- Lab 13. Create a custom TAA rule
- Lab 14. Create a custom YARA rule

**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