

KL 048.2:

Kaspersky XDR Expert. Administration

Course description

Kaspersky XDR Expert is a reliable cybersecurity solution that helps protect corporate IT infrastructures against advanced threats.

Kaspersky XDR Expert allows users to:

- Collect, store and conveniently analyze telemetry.
- Manually and automatically analyze collected data and detect threats.
- Comprehensively assess the level of corporate security using data from reports and the dashboard.
- Analyze cyber kill chain using the investigation graph.
- Automatically and manually respond to threats. When combined with the product's integration capabilities, this ability lets you implement complex protection scenarios.
- Effectively manage collected data. The interface provides the user with convenient methods of interaction, including contextual search and response actions, data representation, 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.

Threat detection, investigation and response are described in technical training KL 059.2.

Duration

1.5 days (12 hours)

Requirements for participants

Basic understanding of networking technologies, such as DNS and routing. Basic Windows and Linux management skills. Basic understanding and experience with containerization systems. Understanding of contemporary threats and information technologies.

Contents

- **1. General**
- **2. Capabilities**
- **3. Architecture**
- **4. Deployment**
- **5. Event collecting and processing**
- **6. Integrations**
- **7. Administration**
- **8. Maintenance**

Labs

- Lab 1.** Install Kaspersky XDR Expert
- Lab 2.** Configure telemetry collection in Kaspersky XDR Expert
- Lab 3.** Configure Kaspersky XDR Expert integration with Sandbox
- Lab 4.** Configure authentication in Kaspersky XDR Expert via Active Directory
- Lab 5.** Configure Kaspersky XDR Expert integration with Kaspersky Threat Intelligence Portal
- Lab 6.** Configure Kaspersky XDR Expert integration with a mail server
- Lab 7.** Metrics and logs in Kaspersky XDR Expert
- Lab 8.** Kaspersky XDR Expert backup and restore
- Lab 9.** Migration from EDR 7.1 to Kaspersky XDR Expert