training code: SC-5004 / ENG DL 1d / EN

Defend against cyberthreats with Microsoft Defender XDR

This training prepares participants for the practical use of Microsoft Defender XDR in the role of a security operations analyst. Participants will learn how to handle incidents in the Microsoft Defender portal, deploy and configure Microsoft Defender for Endpoint, configure alerts and detections, automate responses, and conduct investigations on devices. The course also includes hands-on lab exercises on threat detection and response using Advanced Hunting (KQL).

Training recipients

- SOC analysts / Security Operations Analysts responsible for detecting, analyzing, and handling incidents.
- Security engineers and administrators who deploy and maintain Microsoft Defender for Endpoint and Microsoft Defender XDR.
- Individuals preparing for incident response and threat hunting (KQL) tasks within the Microsoft ecosystem.

Benefits

1. Incident handling in the Microsoft Defender portal – learning how to analyze and manage incidents and alerts in the Microsoft Defender portal.
2. Deployment of Microsoft Defender for Endpoint – the process of onboarding devices and configuring basic security settings.
3. Alert and Detection Configuration – configuring notifications, indicators, and settings related to threat detection.

4. Response Automation – configuring automated responses, remediation actions, and other automation mechanisms in MDE.
5. Device investigations – using telemetry data and forensic information to analyze incidents on endpoints.
6. Advanced Hunting (KQL) – basic threat hunting scenarios and event correlation in Defender XDR.

Training program

1.Incident response using Microsoft Defender.
- A unified view of incidents and alerts in the Microsoft Defender portal.
- Basics of working with incidents, related evidence, and corrective actions.

2.Deployment of the Microsoft Defender for Endpoint environment.
- Device onboarding and configuration of basic security settings.
- Roles and access (RBAC) and device groups.

3.Configuring alerts and detection in Microsoft Defender for Endpoint.
- Notifications, alert management, and alert suppression.
- Indicators as part of the detection process.

4.Automation and response in Microsoft Defender for Endpoint.
- Automation settings, automated investigations, and remediation actions.
- Overview of automation capabilities and best practices.

5.Device investigations in Microsoft Defender for Endpoint.
- Device inventory, event analysis, and telemetry data.
- Forensics and behavior blocking mechanisms.

6.Lab exercises: defending against cyber threats using Microsoft Defender XDR.
- Configuring the Defender XDR environment and deploying Microsoft Defender for Endpoint.
- Attack simulation: analysis, mitigation, and incident response, as well as the basics of Advanced Hunting (KQL).

Expected preparation of the participant

- Experience using the Microsoft Defender portal.
- Basic knowledge of Microsoft Defender for Endpoint and fundamental SOC concepts (alert, incident, triage, remediation).
- Basic knowledge of Microsoft Sentinel (recommended) and experience using Kusto Query Language (KQL).
- Completion of the “Introduction to Microsoft Security, Compliance, and Identity (SC-900)” track is recommended.

Training Includes

- manual in electronic form available on the platform: https://learn.microsoft.com/pl-pl/training/
- access to Altkom Akademia's student portal

Duration

1 days / 7 hours

Language

- Training: English
- Materials: English