kod szkolenia: SC-5001 / ENG DL 1d

Configure SIEM security operations using Microsoft Sentinel

A basic training course to prepare you for working with Microsoft Sentinel. The course covers configuring the Microsoft Sentinel workspace, learning about connectors, connecting event sources, creating analytical rules, and implementing automated threat response.

Training recipients

- Security analysts responsible for managing, monitoring, and responding to threats,
- IT professionals who need to implement an SMIE/SOAR system in their organization,
- For those preparing for the Microsoft Certified: Security Operations Analyst Associate (SC-200) certification, this can serve as one of the preparatory steps for that certification.

Benefits

1. Creating and configuring a Microsoft Sentinel workspace – You'll learn about the types of workspaces, management, and costs.
2. Implementing the Microsoft Sentinel Content Hub solution – You'll learn about the configuration options for event source connectors.
3. Connecting Windows hosts to Microsoft Sentinel – You will connect your first event sources.
4. Configuring analysis rules in Microsoft Sentinel – You will learn how to build analysis rules to detect threats.
5. Configuring automation in Microsoft Sentinel – You will create automation rules in Microsoft Sentinel.
6. This can serve as part of the preparation process for the SC-200 exam, providing an overview of the practical topics and competencies required for the role of a security operations analyst.

Training program

1.Create and manage Microsoft Sentinel workspaces.
- Plan a Microsoft Sentinel workspace.
- Create a Microsoft Sentinel workspace.
- Manage workspaces across tenants using Azure Lighthouse.
- Overview of Microsoft Sentinel permissions and roles.

2.Connecting Microsoft services to Microsoft Sentinel.
- Planning Microsoft service connectors.
- Connecting the Microsoft 365 connector.
- Connecting the Microsoft Entra connector.
- Connecting the Azure Activity connector.

3.Connecting Windows hosts to Microsoft Sentinel.
- Planning the Windows Host Security Events connector.
- Connecting using Windows Security Events via the AMA connector.

4.Detecting threats using Microsoft Sentinel analytics.
- What is Microsoft Sentinel analytics?
- Types of analytics rules.
- Create an analysis rule based on templates.
- Create an analysis rule using the wizard.
- Manage analysis rules.

5.Automation in Microsoft Sentinel.
- Overview of automation options.
- Create automation rules.

Expected preparation of the participant

- Basic knowledge of the Microsoft Azure platform—at the level of the “Microsoft Azure Fundamentals, AZ-900” course.
- Familiarity with incident management topics – alerts, incidents, closure, and hunting.
- Experience using Kusto Query Language (KQL).
- Completion of the “Introduction to Microsoft Security, Compliance, and Identity, SC-900” training track (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

Czas trwania

1 dni / 7 godzin

Language

- **Training**: English
- **Materials**: English