training code: SC-5001 / ENG DL 1d / EN

Configure SIEM security operations using Microsoft Sentinel

Purpose of the training

Training dedicated to specialists acting as Microsoft security operations analysts who cooperate with other specialists to secure information technology systems in the organization. The Security Operations Analyst's job is to mitigate organizational risk by quickly responding to active attacks in the environment, advising on improvements to threat protection practices, and reporting violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring and response using a variety of security solutions throughout the environment. This role primarily involves investigating, responding to, and detecting threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft Defender XDR, and third-party security products. Because the security operations analyst uses the operational results of these tools, he or she is also a key stakeholder in the configuration and implementation of these technologies.

Benefits of completing the training

Acquiring knowledge and skills in using Microsoft Sentinel:

- Create and configure a Microsoft Sentinel workspace.
- Deploy a Microsoft Sentinel content hub solution.
- Connect Windows hosts to Microsoft Sentinel.
- Configure analytics rules in Microsoft Sentinel.
- Configure automation in Microsoft Sentinel

Expected Listener Preparation

Fundamental understanding of Microsoft security, compliance, and identity products. Intermediate

understanding of Microsoft Windows. Familiarity with Azure services, specifically Azure Virtual Machines. Familiarity with Azure virtual machines and virtual networking. Basic understanding of scripting concepts.

Training Language

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

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

Training agenda

1. Create and manage Microsoft Sentinel workspaces.
   - Plan for the Microsoft Sentinel workspace.
   - Create a Microsoft Sentinel workspace.
   - Manage workspaces across tenants using Azure Lighthouse.
   - Understand Microsoft Sentinel permissions and roles.
   - Manage Microsoft Sentinel settings.
   - Configure logs.
2. Connect Microsoft services to Microsoft Sentinel.
   - Plan for Microsoft services connectors.
   - Connect the Microsoft Office 365 connector.

- Connect the Microsoft Entra connector.
- Connect the Microsoft Entra ID Protection connector.
- Connect the Azure Activity connector.

3. Connect Windows hosts to Microsoft Sentinel.
   - Plan for Windows hosts security events connector.
   - Connect using the Windows Security Events via AMA Connector.
   - Connect using the Security Events via Legacy Agent Connector.
   - Collect Sysmon event logs.
4. Threat detection with Microsoft Sentinel analytics.
   - What is Microsoft Sentinel Analytics?
   - Types of analytics rules.
   - Create an analytics rule from templates.
   - Create an analytics rule from wizard.
   - Manage analytics rules.
5. Automation in Microsoft Sentinel.
   - Understand automation options.
   - Create automation rules