training code: SC-5006 / ENG DL 1d / EN

Enhance security operations by using Microsoft Security Copilot

Learn about Microsoft Security Copilot, an AI-powered security analysis tool that enables analysts to process security signals and respond to threats at a machine speed, and the AI concepts upon which it's built.

Training recipients

The training is intended for:

- Admins
- Security Operations Analyst
- Security Engineers

Benefits

1. Basics of Security Copilot – You will learn how to prompt Security Copilot.
2. Hands-on learning – Through the labs, you will gain experience that you can easily translate into real tasks at work.
3. Integration between Intune and Security Copilot – You will gain knowledge on how to use both products together.
4. Understanding Security Copilot – You will learn how to analyze Pureview and Defender XDR data with the help of Security Copilot.
5. Understanding the new features – You will learn in practice how to use new plugins in Security Copilot.

Training program

1.Introduction to generative AI and agents
- Introduction
- Large language models (LLMs)
- Prompts
- AI agents
- Exercise – Explore generative AI agent scenarios

2.Describe Microsoft Security Copilot
- Introduction
- Get acquainted with Microsoft Security Copilot
- Describe Microsoft Security Copilot terminology
- Describe how Microsoft Security Copilot processes prompt requests
- Describe the elements of an effective prompt
- Describe how to enable Microsoft Security

3.Describe the core features of Microsoft Security Copilot
- Introduction
- Describe the features available in the standalone experience of Microsoft Security Copilot
- Describe the features available in a session of the standalone experience
- Describe workspaces
- Describe the Microsoft plugins available in Microsoft Security Copilot
- Describe the non-Microsoft plugins supported by Microsoft Security Copilot
- Describe custom promptbooks

4.Describe the embedded experiences of Microsoft Security Copilot
- Introduction
- Describe Copilot in Microsoft Defender XDR
- Copilot in Microsoft Purview
- Copilot in Microsoft Entra
- Copilot in Microsoft Intune
- Copilot in Microsoft Defender for Cloud (Preview)

5.Describe Microsoft Security Copilot agents
- Introduction
- Describe Microsoft Security Copilot agents
- Understand agent identities and permissions
- Describe the Threat Intelligence Briefing Agent
- Explore the Threat Intelligence Briefing Agent
- Describe the Security Copilot agents in Microsoft Entra
- Explore the Conditional Access Optimization Agent
- Describe the Security Copilot agents in Microsoft Defender
- Describe the Security Copilot agents in Microsoft Purview

- Describe the Security Copilot agents in Microsoft Intune

6.Explore use cases of Microsoft Security Copilot in the standalone and embedded experiences, through lab-like exercises.

- Introduction
- Explore the first run experience
- Explore the standalone experience
- Explore Security Copilot workspaces
- Configure the Microsoft Sentinel plugin
- Enable a custom plugin
- Explore file uploads as a knowledge base
- Create a custom promptbook
- Explore the capabilities of Copilot in Microsoft Defender XDR
- Explore the capabilities of Copilot in Microsoft Purview
- Explore the capabilities of Copilot in Microsoft Entra

Expected preparation of the participant

- Working knowledge of security operations and incident response
- Working knowledge of Microsoft security products and services

To increase the comfort of work and training’s effectiveness we suggest using an additional monitor. The lack of additional monitor does not exclude participation in the training, however, it significantly influences the comfort of work during classes.

You can find information and requirements of participation in Distance Learning trainings at: https://www.altkomakademia.pl/en/how-it-works/about-courses/

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