Enhance security operations by using Microsoft Security Copilot (SC-5006)

Duration: 1 day
Audience: Professionnel TI

Who is this training for?

This course is intended for:

- Security Operations Analysts (SOC)
- Security Engineers and Administrators
- SOC Managers or Team Members
- IT Professionals involved in Cybersecurity
- Business Users or Business Owners wishing to understand the contribution of AI to security

Training objectives

At the end of this training, the learner will be able to:

- Explain the basic principles of generative AI and their application in cybersecurity.
- Apply the concepts of responsible generative AI in a security context.
- Describe Microsoft Security Copilot, how it works, and its terminology.
- Formulate effective prompts to analyze security incidents and signals.
- Use the core features of Microsoft Security Copilot in standalone mode.
- Leverage Copilot in Microsoft solutions (Defender XDR, Sentinel, Purview, Entra).
- Analyze security scenarios to accelerate investigation and response to threats.

Summary

Learn about Microsoft Copilot Security, an AI-powered security analytics tool that enables analysts to process security signals and respond to threats at machine speed, and the AI concepts behind it. The training is delivered by certified Microsoft experts with extensive experience in integrating Copilot into the Microsoft 365 environment. Through real-world case studies and interactive exercises, you will learn how to use Copilot strategically.

Course outline

Fundamental Concepts of AI

- Introduction to AI
- Understanding Machine Learning
- What is Computer Vision?
- Understanding Natural Language Processing
- Understanding Document Intelligence and Knowledge Mining
- Understanding
- Generative AI
- Challenges and Risks of Artificial Intelligence
- Understanding Responsible AI

Fundamentals of Generative AI

- What is Generative AI?
- What are language models?
- Use language models
- What are co-pilots?

Microsoft Copilot

- Copilot prompt considerations
- Extending and developing copilots
- Exercise: Explore Microsoft Copilot

Responsible generative AI fundamentals

- Plan a responsible generative AI solution
- Identify potential harm
- Measure potential harm
- Mitigate potential harm

- Operate a responsible generative AI solution
- Exercise: Explore content filters in Azure OpenAI Describe Microsoft Copilot for the security
- Learn about Microsoft Copilot for Security
- Describe Microsoft Copilot for Security terminology

Describe how Microsoft Copilot for Security handles prompt requests

- Describe the elements of an effective prompt
- Describe how to enable Microsoft Copilot for Security

Describe the key features of Microsoft Copilot for Security

- Describe the features available in the Microsoft Copilot for Security standalone experience
- Describe the Features available in a standalone experience session
- Describe the Microsoft plug-ins available in Microsoft Copilot for Security
- Describe the non-Microsoft plug-ins supported by Microsoft Copilot for Security
- Describe custom prompt guides
- Describe the knowledge base connections

Describe the built-in experiences of Microsoft Copilot for Security

- Describe Microsoft Copilot in Microsoft Defender XDR
- Microsoft Copilot in Microsoft Purview
- Microsoft Copilot in Microsoft Entra

Explore Microsoft Copilot use cases for security

- Explore the first-run experience
- Explore the standalone experience
- Configure the Microsoft Sentinel plug-in
- Enable a custom plug-in
- Explore file uploads via a knowledge base
- Create a custom prompt sequence

- Explore Copilot features in Microsoft Defender XDR
- Explore features by Copilot in Microsoft Purview

Approach and methodology

Practical and structured approach combining focused theory and guided workshops. Participants progressively improve security operations using Microsoft Security Copilot through real-world exercises inspired by professional scenarios, promoting immediate application of learnings. They learn how to analyze threats, automate investigations, and optimize incident response using generative AI. Led by a Microsoft certified trainer, the training focuses on interactivity and the development of directly transferable technical skills to strengthen the effectiveness of security teams in the workplace.

Prerequisites

Have a Copilot license for M365

Recommendations

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