

MS-SC5006: ENHANCE SECURITY OPERATIONS BY USING MICROSOFT SECURITY COPILOT



DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Beginner	Security	Instructor-led	NA

INTRODUCTION

Explore the transformative power of AI in security with Microsoft Security Copilot. This course starts by introducing you to the fundamental concepts of generative AI. The course then delves into the cutting-edge AI functionality of Microsoft Security Copilot that empowers analysts to respond to threats quickly, process signals at machine speed, and assess risk exposure more quickly than may otherwise be possible. Lastly, the course guides the learner through a series of simulation-based exercises that mimic real-world situations.

AUDIENCE PROFILE

This course is targeted at security professionals interested in getting started with Microsoft Security Copilot, including security analysts, security admins, and SOC managers.

PREREQUISITES

Before attending this course, delegates must have:

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

COURSE OBJECTIVES

After completing this course, delegates will be able to:

- Understand machine learning, computer vision, natural language processing, document intelligence, and knowledge mining.
- Learn about generative AI and its challenges and risks.
- Understand responsible AI practices.
- Understand the role of copilots and how to use them effectively.
- Explore considerations for Copilot prompts and extending/developing copilots.
- Plan and develop responsible generative AI solutions.
- Identify, measure, and mitigate potential harms.
- Operate a responsible generative AI solution.
- Get acquainted with Microsoft Copilot for Security and its terminology.
- Learn how to enable Microsoft Copilot for Security.
- Explore the features available in the standalone experience.
- Learn about Microsoft and non-Microsoft plugins, custom promptbooks, and knowledge base connections.
- Understand how Microsoft Copilot integrates with Microsoft Defender XDR, Microsoft Purview, Microsoft Entra, Microsoft Intune, and Microsoft Defender for Cloud.
- Experience the first run and standalone experiences.
- Configure plugins and explore file uploads as a knowledge base.
- Create custom promptbooks and explore capabilities in various Microsoft security products.

COURSE CONTENT

Module 1: Introduction to generative AI concepts

In this module, you explore the way in which language models enable AI applications and services to generate original content based on natural language input.

Lessons

- Introduction
- What is generative AI?
- How do language models work?
- Understand how transformers advance language models

- Understand differences in language models
- Improve prompt results
- Create responsible generative AI solutions
- Module assessment
- Summary

By the end of this module, you'll be able to:

- Understand what generative AI can do and how it appears in today's applications.
- Understand how language models can understand and generate language.

- Describe ways you can engineer good prompts and quality responses.
- Describe responsible generative AI concepts.

Module 2: Describe Microsoft Security Copilot

Get acquainted with Microsoft Security Copilot. You are introduced to some basic terminology, how Microsoft Security Copilot processes prompts, the elements of an effective prompt, and how to enable the solution.

Lessons

- 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 Copilot.
- Knowledge check.
- Summary and resources.

By the end of this module, you'll be able to:

- Describe what Microsoft Security Copilot is.
- Describe the terminology of Microsoft Security Copilot.
- Describe how Microsoft Security Copilot processes prompt requests.
- Describe the elements of an effective prompt
- Describe how to enable Microsoft Security Copilot.

Module 3: Describe the core features of Microsoft Security Copilot

Microsoft Security Copilot has a rich set of features. Learn about available plugins, promptbooks, the ways you can export and share information from Copilot, and much more.

Lessons

- 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 the Microsoft plugins available in Microsoft Security Copilot
- Describe the non-Microsoft plugins supported by Microsoft Security Copilot
- Describe custom promptbooks
- Describe knowledge base connections
- Knowledge check
- Summary and resources

By the end of this module, you'll be able to:

- Describe the features available in the standalone Copilot experience.
- Describe the plugins available in Copilot.
- Describe custom promptbooks.
- Describe knowledge base connections.

Module 4: Describe the embedded experiences of Microsoft Security Copilot

Microsoft Security Copilot is accessible directly from some Microsoft security products. This is referred to as the embedded experience. Learn about the scenarios supported by the Copilot embedded experience in Microsoft's security solutions.

Lessons

- 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)
- Knowledge check
- Summary and resources

By the end of this module, you'll be able to:

- Describe Copilot in Microsoft Defender XDR.
- Describe Copilot in Microsoft Purview.
- Describe Copilot in Microsoft Entra.
- Describe Copilot in Microsoft Intune.
- Describe Copilot in Microsoft Defender for Cloud.

Module 5: Describe Microsoft Security Copilot agents

Automate threat detection and response with Microsoft Security Copilot agents—AI-powered tools that streamline cybersecurity operations, reduce manual workloads, and scale protection across your digital environment.

Lessons

- Introduction
- Describe Microsoft Security Copilot agents
- Describe the Threat Intelligence Briefing Agent
- Explore the Threat Intelligence Briefing Agent

- Describe the Conditional Access Optimization Agent
- Explore the Conditional Access Optimization Agent
- Describe the Phishing Triage Agent
- Module assessment
- Summary and resources

By the end of this module, you're able to:

- Describe the role and functionality of Microsoft Security Copilot agents in automating security workflows.
- Describe the Threat Intelligence Briefing Agent.
- Describe the Conditional Access Optimization Agent.
- Describe the Phishing Triage agent.

Module 6: Explore use cases of Microsoft Security Copilot

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

Lessons

- Introduction
- Explore the first run experience
- Explore the standalone experience
- 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
- Knowledge check
- Summary and resources

By the end of this module, you'll be able to:

- "Set up Microsoft Security Copilot."
- "Work with sources in Copilot."
- "Create a custom promptbook."
- "Use the capabilities of Copilot in Defender XDR."
- "Use the capabilities of Copilot in Microsoft Purview."

ASSOCIATED CERTIFICATIONS & EXAM

There is no Associated Certification or Exam for this course.