SC-5006: Enhance Security Operations by using Microsoft Security Copilot

Course Description

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.

Course Duration

1 day

Prerequisites

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

Course Outline

1 - Introduction to generative AI concepts

- 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

2 - Describe Microsoft Security Copilot

- 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
- Module assessment

3 - Describe the core features of Microsoft Security Copilot

- 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
- Describe knowledge base connections
- Module assessment

4 - Describe the embedded experiences of Microsoft Security Copilot

- 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)
- Module assessment

5 - Describe Microsoft Security Copilot agents

- 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

6 - Explore use cases of Microsoft Security Copilot

- 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
- Module assessment

Who Should Attend

This course is targeted to security professionals interested in getting started with Microsoft Security Copilot, including security analysts, security admins, and SOC managers. The person taking this course is looking to familiarize themselves with the functionality of Microsoft Security Copilot in both the standalone and embedded experiences. They should have working knowledge of security operations and incident response, experience with Microsoft security products and services, and is interested in learning how Microsoft Security Copilot, an AI-powered security analysis tool, can help them process security signals and respond to threats more quickly.