SC-5006-A: Enhance security operations by using Microsoft Security Copilot

Overview

Course Duration: 1 Days

About This Course

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 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

Course Outline

Module 1: **Introduction to Generative AI and agents**

Generative AI powers applications that can create content, answer questions, and assist with tasks. In this module, you'll explore the fundamentals of generative AI, including large language models (LLMs), prompts, and AI agents.

Lesson

- Describe core concepts of generative AI.
- Explain how large language models (LLMs) work.
- Consider how to create effective prompts for LLMs.
- Describe core concepts of agents and agentic AI solutions.

Module 2: Describe Microsoft Security Copilot

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

Lesson

- 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.

Lesson

- 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 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.

Lesson

- 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 5: Explore use cases of Microsoft Security Copilot

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

Lesson

- Set up Microsoft Security Copilot.
- Work with sources in Copilot.
- Create a custom promptbook.
- Use the capabilities of Copilot embedded within our security solutions, including Microsoft Purview, Microsoft Entra, and Microsoft Defender for Cloud

Prerequisites

Before attending this course, students should have understood:

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