Technofocus

Implementing Gen AI-powered security with Microsoft Security Copilot

Course Overview

Duration - 12 Hours | Level - Intermediate

Microsoft Security Copilot is a generative AI-powered security solution that helps increase the efficiency and capabilities of your security solutions to improve security outcomes at machine speed and scale. Learn how Security Copilot can help you as a security professional in supporting end-to-end scenarios such as incident response, threat hunting, intelligence gathering, and posture management.

Course Modules

Day 1

Get started with Microsoft Security Copilot

Microsoft Secure Future Initiative overview

Introduction to Microsoft Security Copilot

Empowering Security Operations

Working mechanism

Security Copilot standalone and embedded experience

Security Copilot – Requirements and Onboarding

Exploring the Standalone and Embedded Experience

Responsible AI

Microsoft Security Copilot Pricing

Interactive Simulated Lab Experience

Lab 1 - Setting up the environment for Microsoft Security Copilot

Lab 2 - Connecting Microsoft Sentinel in the Microsoft Defender Portal for Threat Hunting, Triage, Investigation, and Response

Day 2

Securing and expanding capabilities of Security? Copilot

Authentication

Prompting

Promptbooks

Extending Copilot for Securing using Plugins

Microsoft Security Copilot Connectors

Security Copilot sample use cases

Interactive Simulated Lab Experience

Lab 3 - Creating a multi-stage incident in Microsoft Defender

Lab 4 - Creating a DLP policy and generating an alert in Microsoft Purview

Lab 5 - Activating Security Copilot using Azure subscription and analyzing the alerts generated in Microsoft Purview

Day 3

Security Copilot – Integrations

Security Copilot in Microsoft Defender XDR

Security Copilot in Microsoft Defender for Cloud

Security Copilot in Entra

Security Copilot in Intune

Security Copilot in Microsoft Surface Management Portal

Security Copilot in Defender EASM

Security Copilot in Defender Threat Intelligence

Security Copilot in Purview

Supercharge DSPM with Security Copilot

Azure AI Search plugin (Preview)

Azure Firewall plugin (Preview)

Azure Web Application Firewall (Preview)

Microsoft Sentinel plugin (Preview)

Interactive Simulated Lab Experience

Lab 6 - Security Copilot – Microsoft Defender embedded Copilot to standalone Copilot investigation

Lab 7 - Identity Risk Investigation and Mitigation with Microsoft Security Copilot in Microsoft Entra

Lab 8 - Using Security Copilot standalone portal to get threat intelligence

Lab 9 - Adding custom plugins to extend the capabilities of Security Copilot

Lab 10 - Analyze Microsoft Defender for Cloud Recommendations with Security Copilot

Lab 11 - Investigate Microsoft Sentinel Incidents using Defender for Cloud and Security Copilot