kod szkolenia: SC-5006 / PL DL 1d

# Enhance security operations by using Microsoft Security Copilot

Szkolenie Enhance security operations by using Microsoft Security Copilot wprowadza w możliwości Microsoft Security Copilot — narzędzia wspieranego przez sztuczną inteligencję, które pomaga analizować sygnały bezpieczeństwa, przetwarzać dane i reagować na zagrożenia szybciej oraz skuteczniej.

Program obejmuje podstawy generatywnej AI, promptów i agentów, a następnie pokazuje, jak Microsoft Security Copilot wspiera pracę zespołów bezpieczeństwa w środowiskach Microsoft. Uczestnicy poznają funkcje dostępne w samodzielnym doświadczeniu Security Copilot, przestrzenie robocze, wtyczki, promptbooki oraz doświadczenia wbudowane w Microsoft Defender XDR, Microsoft Purview, Microsoft Entra, Microsoft Intune i Microsoft Defender for Cloud.

## Odbiorcy szkolenia

Szkolenie jest przeznaczone dla osób odpowiedzialnych za operacje bezpieczeństwa, administrację środowiskami Microsoft oraz analizę i obsługę zdarzeń bezpieczeństwa.
W szczególności kurs sprawdzi się dla:

- administratorów,
- analityków operacji bezpieczeństwa,
- inżynierów bezpieczeństwa,
- osób korzystających z Microsoft Defender XDR, Microsoft Purview, Microsoft Entra lub Microsoft Intune,
- zespołów bezpieczeństwa, które chcą poznać praktyczne zastosowanie Microsoft Security Copilot w analizie sygnałów, obsłudze promptów, pracy z wtyczkami i wykorzystaniu agentów.

## Korzyści

1. 1. Podstawy Microsoft Security Copilot – poznasz, jak działa Security Copilot, jak przetwarza prompty i jak wspiera analizę sygnałów bezpieczeństwa.
   2. Tworzenie skutecznych promptów – nauczysz się formułować zapytania, które pomagają uzyskać trafniejsze odpowiedzi i lepiej wykorzystywać możliwości Security Copilot.
   3. Praca z funkcjami Security Copilot – dowiesz się, jak korzystać z samodzielnego doświadczenia, sesji, przestrzeni roboczych, wtyczek oraz niestandardowych promptbooków.
   4. Wykorzystanie doświadczeń wbudowanych – poznasz, jak Security Copilot działa w Microsoft Defender XDR, Microsoft Purview, Microsoft Entra, Microsoft Intune i Microsoft Defender for Cloud.
   5. Praca z agentami Security Copilot – nauczysz się rozumieć role agentów, ich tożsamości, uprawnienia oraz zastosowanie w obszarach takich jak Entra, Defender, Purview i Intune.
   6. Analiza danych bezpieczeństwa – dowiesz się, jak wykorzystywać Security Copilot do pracy z danymi Microsoft Defender XDR, Microsoft Purview oraz Microsoft Entra.
   7. Praktyczne wykorzystanie narzędzia – przećwiczysz scenariusze obejmujące konfigurację wtyczki Microsoft Sentinel, włączanie niestandardowej wtyczki, przesyłanie plików jako bazy wiedzy i tworzenie promptbooków.

## Program szkolenia

1. Wprowadzenie do generatywnej sztucznej inteligencji i agentów:
• Omówienie podstaw generatywnej sztucznej inteligencji.
• Przegląd dużych modeli językowych.
• Omówienie zasad tworzenia promptów.
• Przedstawienie roli agentów AI.
• Eksploracja scenariuszy wykorzystania generatywnych agentów AI w ramach ćwiczenia.
2. Omówienie Microsoft Security Copilot:
• Wprowadzenie do Microsoft Security Copilot.
• Przegląd możliwości Microsoft Security Copilot.
• Omówienie terminologii Microsoft Security Copilot.
• Opis sposobu przetwarzania żądań promptów przez Microsoft Security Copilot.
• Omówienie elementów skutecznego promptu.
• Przedstawienie sposobu włączania Microsoft Security Copilot.
3. Omówienie podstawowych funkcji Microsoft Security Copilot:
• Przegląd funkcji dostępnych w samodzielnym środowisku Microsoft Security Copilot.
• Omówienie funkcji dostępnych w sesji samodzielnego środowiska.
• Przedstawienie przestrzeni roboczych.

• Omówienie wtyczek Microsoft dostępnych w Microsoft Security Copilot.
• Omówienie wtyczek innych niż Microsoft obsługiwanych przez Microsoft Security Copilot.
• Przedstawienie niestandardowych promptbooków.
4. Omówienie doświadczeń wbudowanych Microsoft Security Copilot:
• Wprowadzenie do doświadczeń wbudowanych Microsoft Security Copilot.
• Omówienie Copilota w Microsoft Defender XDR.
• Omówienie Copilota w Microsoft Purview.
• Omówienie Copilota w Microsoft Entra.
• Omówienie Copilota w Microsoft Intune.
• Omówienie Copilota w Microsoft Defender for Cloud.
5. Omówienie agentów Microsoft Security Copilot:
• Wprowadzenie do agentów Microsoft Security Copilot.
• Przegląd agentów Microsoft Security Copilot.
• Omówienie tożsamości i uprawnień agentów.
• Przedstawienie agenta ds. odpraw wywiadu zagrożeń.
• Przegląd agenta informacyjnego ds. zagrożeń.
• Omówienie agentów Security Copilot w Microsoft Entra.
• Przedstawienie agenta optymalizacji dostępu warunkowego.
• Omówienie agentów Security Copilot w Microsoft Defender.
• Omówienie agentów Security Copilot w Microsoft Purview.
• Omówienie agentów Security Copilot w Microsoft Intune.
6. Poznanie zastosowań Microsoft Security Copilot w środowiskach samodzielnych i wbudowanych:
• Wprowadzenie do ćwiczeń przypominających laboratorium.
• Eksploracja doświadczenia pierwszego użycia.
• Eksploracja samodzielnego środowiska Microsoft Security Copilot.
• Eksploracja przestrzeni roboczych Security Copilot.
• Konfiguracja wtyczki Microsoft Sentinel.
• Włączanie niestandardowej wtyczki.
• Eksploracja przesyłania plików jako bazy wiedzy.
• Tworzenie niestandardowego promptbooka.
• Poznanie możliwości Copilota w Microsoft Defender XDR.
• Poznanie możliwości Copilota w Microsoft Purview.
• Poznanie możliwości Copilota w Microsoft Entra.

## Oczekiwane przygotowanie uczestnika

- Praktyczna wiedza z zakresu operacji bezpieczeństwa i reagowania na incydenty

- Praktyczna znajomość produktów i usług bezpieczeństwa Microsoftu
- Zalecamy wcześniejszy udział w szkolenaich: AI-900, AZ-900, SC-900

Dla zwiększenia komfortu pracy oraz efektywności szkolenia zalecamy skorzystanie z dodatkowego ekranu. Brak dodatkowego ekranu nie jest przeciwwskazaniem do udziału w szkoleniu, ale w znaczący sposób wpływa na komfort pracy podczas zajęć
Informacje oraz wymagania dotyczące uczestniczenia w szkoleniach w formule zdalnej dostępne na: https://www.altkomakademia.pl/jak-dzialamy/o-szkoleniach/?distance-learning

## Szkolenie obejmuje

* podręcznik w formie elektronicznej dostępny na platformie: https://learn.microsoft.com/pl-pl/training/
* dostęp do portalu słuchacza Altkom Akademii
Produkt zawiera:

- Wykład i prezentacja produktu (60%)
- Ćwiczenia (40%)

## Czas trwania

1 dni / 7 godzin

## Język

- Szkolenie: polski
- Materiały: angielski