kod szkolenia: SC-5009 / PL DL 1d

Secure AI solutions in the cloud using Microsoft Defender for Cloud and Microsoft Entra

Szkolenie Secure AI solutions in the cloud using Microsoft Defender for Cloud and Microsoft Entra koncentruje się na zabezpieczaniu rozwiązań AI działających w chmurze. Program pokazuje, jak chronić obciążenia AI, konfigurować środowisko Microsoft Foundry, stosować natywne mechanizmy bezpieczeństwa Azure oraz wzmacniać kontrolę dostępu z wykorzystaniem Microsoft Entra.

Uczestnicy poznają, jak obciążenia AI uwierzytelniają się, jak wyznaczane są granice zaufania oraz jak zarządzanie postawą bezpieczeństwa, ochrona obciążeń i kontrola tożsamości pomagają ograniczać ryzyko. Szkolenie obejmuje pracę z Microsoft Defender for Cloud, Microsoft Foundry, Microsoft Entra ID, dostępem warunkowym, tożsamościami zarządzanymi, Azure Key Vault oraz mechanizmami ochrony tożsamości.

Odbiorcy szkolenia

Szkolenie jest przeznaczone dla osób odpowiedzialnych za zabezpieczanie rozwiązań AI, zarządzanie dostępem oraz ochronę obciążeń chmurowych w środowisku Microsoft Azure.
W szczególności kurs sprawdzi się dla:

- inżynierów bezpieczeństwa,
- administratorów środowisk chmurowych,

- administratorów tożsamości i dostępu,
- osób odpowiedzialnych za konfigurację zabezpieczeń Microsoft Foundry,
- zespołów pracujących z Microsoft Defender for Cloud i Microsoft Entra,
- specjalistów, którzy chcą lepiej zrozumieć ryzyka bezpieczeństwa AI, granice zaufania, uwierzytelnianie obciążeń oraz kontrolę dostępu do zasobów Azure.

Korzyści

• Bezpieczeństwo obciążeń AI w Azure – poznasz, jak Microsoft Defender for Cloud wspiera ochronę i zarządzanie ryzykiem dla usług AI w środowisku chmurowym.
• Zarządzanie postawą bezpieczeństwa AI – nauczysz się oceniać i poprawiać poziom bezpieczeństwa obciążeń AI z wykorzystaniem Cloud Security Posture Management.
• Ochrona obciążeń AI w czasie działania – dowiesz się, jak wykrywać zagrożenia za pomocą Cloud Workload Protection oraz analizować alerty bezpieczeństwa AI w Microsoft Defender XDR.
• Konfiguracja zabezpieczeń w Microsoft Foundry – poznasz, jak stosować bariery ochronne, listy bloków oraz mechanizmy bezpieczeństwa treści dla obciążeń AI.
• Zabezpieczanie środowisk Microsoft Foundry – nauczysz się kontrolować dostęp, zarządzać projektami, chronić sekrety z użyciem Azure Key Vault oraz izolować sieci z wykorzystaniem zarządzanej sieci wirtualnej i Private Link.
• Kontrola tożsamości i dostępu dla AI – dowiesz się, jak projektować dostęp do obciążeń AI z użyciem Microsoft Entra ID, ról Azure, tożsamości zarządzanych oraz zasad RBAC.
• Ochrona tożsamości i dostęp warunkowy – poznasz, jak planować i wdrażać polityki Conditional Access, zarządzanie sesjami, ciągłą ocenę dostępu oraz mechanizmy Microsoft Entra Identity Protection.

Program szkolenia

1. Jak Microsoft Defender for Cloud wspiera bezpieczeństwo i zarządzanie AI w Azure:
• Omówienie usług AI dostępnych w Azure.
• Identyfikacja ryzyk bezpieczeństwa związanych z AI w Azure.
• Przegląd barier i zabezpieczeń AI w Azure.
• Omówienie sposobu, w jaki narzędzia bezpieczeństwa i zarządzania Azure wspierają obciążenia AI.
2. Ochrona obciążeń AI za pomocą Microsoft Defender for Cloud:
• Włączanie planu ochrony obciążeń AI.
• Przegląd wniosków w panelu bezpieczeństwa danych i AI.
• Ocena i poprawa postawy bezpieczeństwa AI dzięki Cloud Security Posture Management.
• Wykrywanie zagrożeń AI w czasie działania dzięki Cloud Workload Protection.

• Analiza alertów bezpieczeństwa AI z wykorzystaniem szybkich dowodów w Microsoft Defender XDR.

3. Konfiguracja i zarządzanie barierami zabezpieczającymi w Microsoft Foundry:

• Omówienie barier zabezpieczających i bezpieczeństwa treści Microsoft.
• Przegląd kontroli bezpieczeństwa w Microsoft Foundry.
• Testowanie wbudowanych barier ochronnych.
• Tworzenie i zarządzanie listami bloków w Microsoft Foundry.
• Konfiguracja i stosowanie barier ochronnych w Microsoft Foundry.
• Dobór i dopracowanie odpowiednich barier zabezpieczających dla obciążeń AI.

4. Zabezpieczanie środowisk Microsoft Foundry:

• Kontrola dostępu do Microsoft Foundry za pomocą Microsoft Entra ID.
• Zarządzanie dostępem w projektach Microsoft Foundry.
• Zabezpieczanie sekretów Microsoft Foundry za pomocą Azure Key Vault.
• Izolacja sieci z wykorzystaniem zarządzanej sieci wirtualnej i Private Link.
• Włączanie logowania diagnostycznego w Microsoft Foundry.

5. Zrozumienie architektury tożsamości dla obciążeń AI:

• Omówienie tożsamości jako warstwy sterującej dla rozwiązań AI.
• Rozróżnienie płaszczyzny zarządzania i dostępu do płaszczyzny danych w obciążeniach AI.
• Przegląd przepływów uwierzytelniania dla punktów końcowych AI w Microsoft Foundry.
• Omówienie tożsamości użytkowników i obciążeń w rozwiązaniach AI.
• Analiza przypisań ról i zakresów w środowiskach AI.
• Identyfikacja typowych błędów w konfiguracji tożsamości we wdrożeniach AI.

6. Implementacja zarządzania dostępem dla zasobów Azure:

• Przypisywanie ról Azure.
• Konfiguracja własnych ról Azure.
• Tworzenie i konfigurowanie tożsamości zarządzanych.
• Uzyskiwanie dostępu do zasobów Azure z wykorzystaniem tożsamości zarządzanych.
• Analiza uprawnień ról Azure.
• Konfiguracja zasad RBAC dla Azure Key Vault.
• Odczyt obiektów z Azure Key Vault.

7. Planowanie, wdrażanie i zarządzanie dostępem warunkowym:

• Omówienie domyślnych zabezpieczeń planu.
• Planowanie polityk dostępu warunkowego.
• Implementacja kontroli i przypisań polityk dostępu warunkowego.
• Testowanie i rozwiązywanie problemów z politykami dostępu warunkowego.
• Implementacja kontroli aplikacji.
• Wdrożenie zarządzania sesjami i ciągłej oceny dostępu.
• Omówienie agenta Microsoft Entra Conditional Access Optimization.

8. Zarządzanie ochroną tożsamości Microsoft Entra:

• Przegląd podstaw ochrony tożsamości.
• Wdrażanie i zarządzanie polityką ryzyka użytkownika.
• Monitorowanie, badanie i ograniczanie podwyższonego ryzyka użytkowników.

- Implementacja bezpieczeństwa tożsamości obciążeń.
- Omówienie Microsoft Defender for Identity.
- Omówienie agenta zarządzania ryzykiem tożsamości.

Oczekiwane przygotowanie uczestnika

Ten kurs jest przeznaczony dla profesjonalistów odpowiedzialnych za zabezpieczanie i obsługę obciążeń AI w chmurze. Wśród odbiorców są inżynierowie bezpieczeństwa chmury, inżynierowie platform oraz zespoły aplikacyjne pracujące z usługami AI, które muszą zrozumieć, jak ochrona obciążenia, postawa bezpieczeństwa i kontrola tożsamości mają zastosowanie do środowisk AI. Zalecana jest znajomość Azure, koncepcji bezpieczeństwa natywnego dla chmury oraz podstawowych zasad tożsamości i dostępu

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 (80%)
- Ćwiczenia (20%)

Czas trwania

1 dni / 7 godzin

Język

- Szkolenie: polski
- Materiały: angielski