kod szkolenia: SC-5009 / PL DL 1d

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

Zabezpiecz rozwiązania AI w chmurze poprzez konfigurację obciążeń AI, stosowanie natywnych zabezpieczeń chmurowych oraz wzmacnianie wyników bezpieczeństwa za pomocą kontroli tożsamości. Dowiedz się, jak obciążenia AI uwierzytelniają się, jak ustalane są granice zaufania oraz jak postawa bezpieczeństwa i ochrona obciążeń zmniejszają ryzyko, korzystając z Microsoft Defender for Cloud i Microsoft Foundry. Rozszerzaj te ochrony, wykorzystując Microsoft Entra do projektowania i stosowania kontroli tożsamości oraz dostępu, które wyjaśniają i wzmacniają wcześniejsze decyzje dotyczące bezpieczeństwa.

Odbiorcy szkolenia

Szkolenie przeznaczone jest dla:

- Inżynierowie Bezpieczeństwa
- Administratorzy
- Administratorzy tożsamości i dostępu

Korzyści

Zdobyte umiejętności obejmują:

- Zastosowanie zarządzania posturą bezpieczeństwa i ochrony obciążeń dla usług AI za pomocą Microsoft Defender for Cloud

- Konfigurację i zabezpieczanie środowiska Microsoft Foundry za pomocą natywnych mechanizmów bezpieczeństwa w chmurze
- Zastosowanie kontroli tożsamości i dostępu dla obciążeń AI za pomocą Microsoft Entra

Program szkolenia

1.Zrozum, jak Microsoft Defender for Cloud wspiera bezpieczeństwo i zarządzanie AI w Azure
- Zrozum usługi AI w Azure
- Zrozum ryzyka bezpieczeństwa AI w Azure
- Bariery i zabezpieczenia AI w Azure
- Jak narzędzia bezpieczeństwa i zarządzania Azure wspierają obciążenia AI

2.Chroń obciążenia AI za pomocą Microsoft Defender for Cloud
- Włącz plan obciążeń AI
- Przejrzyj wnioski w panelu bezpieczeństwa danych i AI
- Oceń i popraw postawę bezpieczeństwa AI dzięki Cloud Security Posture Management (CSPM)
- Wykrywanie zagrożeń AI w czasie działania dzięki Cloud Workload Protection (CWP)
- Zbadaj alerty bezpieczeństwa AI za pomocą szybkich dowodów w Microsoft Defender XDR

3.Konfiguruj i zarządzaj barierami zabezpieczającymi w Microsoft Foundry
- Zrozum bariery zabezpieczające i bezpieczeństwo treści Microsoft
- Zrozumienie kontroli bezpieczeństwa w Microsoft Foundry
- Wypróbuj wbudowane bariery ochronne
- Tworzenie i zarządzanie listami bloków w Microsoft Foundry
- Konfiguruj i stosuj bariery ochronne w Microsoft Foundry
- Wybierz i dopracuj odpowiednie bariery zabezpieczające dla swoich obciążeń AI

4.Bezpieczne środowiska Microsoft Foundry
- Kontroluj dostęp do Microsoft Foundry za pomocą Microsoft Entra ID
- Zarządzaj dostępem w projektach Microsoft Foundry
- Secure Microsoft Foundry secrets with Azure Key Vault (preview)
- Izoluj sieci za pomocą zarządzanej sieci wirtualnej i Private Link
- Włącz logowanie diagnostyczne w Microsoft Foundry

5.Zrozum architekturę tożsamości dla obciążeń AI
- Tożsamość jako warstwa sterująca dla rozwiązań AI
- Płaszczyzna zarządzania i dostęp do płaszczyzny danych w obciążeniach AI
- Przepływy uwierzytelniania dla punktów końcowych AI w Microsoft Foundry
- Tożsamość człowieka i obciążenia w obciążeniach AI
- Przydziały ról i zakres w środowiskach AI
- Typowe błędy 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
- Dostęp do zasobów Azure z zarządzanymi tożsamościami
- Analiza uprawnień ról Azure
- Konfiguracja Azure Key Vault RBAC policies
- Odczyt obiektów z Azure Key Vault

7.Planowanie, wdrażanie i zarządzanie dostępem warunkowym

- Domyślne zabezpieczenia planu
- Planuj polityki dostępu warunkowego
- Implementacja kontroli i przypisania polityk dostępu warunkowego
- Testuj i rozwiązuj problemy z politykami dostępu warunkowego
- Implementacja kontroli aplikacji
- Wdrożenie zarządzania sesjami i ciągłej oceny dostępu
- Microsoft Entra Conditional Access Optimization agent

8.Zarządzaj ochroną tożsamości Microsoft Entra

- Przegląd podstaw ochrony tożsamości
- Wdrażanie i zarządzanie polityką ryzyka użytkownika
- Monitoruj, badaj i zwalczaj podwyższone ryzyko użytkowników
- Implementacja bezpieczeństwa tożsamości obciążeń
- Poznaj Microsoft Defender dla tożsamości
- Poznaj 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