kod szkolenia: AZ-500 / PL AA 4d

# Secure cloud resources with Microsoft security technologies

Szkolenie zostanie wycofane przez Microsoft z dniem 31.08.2026 i zastąpione nowym szkoleniem SC-500, które wkrótce pojawi się w naszej ofercie.

**Autoryzowane szkolenie** Secure cloud resources with Microsoft security technologies **AZ-500** szkolenie w formule **stacjonarnej**

**Administrator**, **administrator IT, specjalista IT** - docelowa grupa odbiorców.

Zobacz film: https://youtu.be/HW5A8qvSCyM

**Wywiad: 15 minut z ekspertem z tematyki Microsoft Azure:**

**Zobacz film: https://youtu.be/sXfpx7KEqQ8**

**Wywiad: 15 minut z ekspertem z tematyki bezpieczeństwa usług chmurowych Microsoft 365:**

Zobacz film: https://youtu.be/8p5ioOu4WX8

## Odbiorcy szkolenia

Grupę docelową szkolenia stanowią:

- Inżynierowie bezpieczeństwa platformy Azure, planujący przystąpienie do egzaminu certyfikacyjnego

związanych z bezpieczeństwem Azure.
- Osoby odpowiedzialne za wdrażanie i utrzymywanie kontroli bezpieczeństwa oraz zarządzanie pozycją bezpieczeństwa w organizacji.
- Specjaliści zajmujący się identyfikacją i usuwaniem luk w zabezpieczeniach przy użyciu narzędzi bezpieczeństwa.
- Administratorzy, architekci i deweloperzy chcący poszerzyć kompetencje w zakresie bezpieczeństwa platform cyfrowych opartych na Azure.
- Profesjonaliści pragnący aktywnie uczestniczyć w ochronie danych i bezpieczeństwie systemów organizacji.

## Korzyści

Uzyskanie wiedzy i praktycznych umiejętności w zakresie zarządzania bezpieczeństwem na platformie Azure. W tym zapoznanie się z:
- Wdrażaniem strategii zarządzania przedsiębiorstwem, w tym kontrola dostępu oparta na rolach, zasady platformy Azure i blokady zasobów.
- Implementacją infrastruktury usługi Azure AD, w tym użytkowników, grupy i uwierzytelnianie wieloskładnikowe.
- Implementacją usługi Azure AD Identity Protection, w tym zasady ryzyka, dostęp warunkowy i przeglądy dostępu.
- Implementacją Privileged Identity Management usługi Azure AD, w tym role usługi Azure AD i zasoby platformy Azure.
- Implementacją Azure AD Connect, w tym metody uwierzytelniania i lokalna synchronizacja katalogów.
- Implementacją strategii zabezpieczeń sieci obwodowej, w tym zapora platformy Azure.
- Wdrażaniem strategii bezpieczeństwa sieci, w tym grupy bezpieczeństwa sieci i grupy bezpieczeństwa aplikacji.
- Wdrażaniem strategii bezpieczeństwa hosta, w tym ochrona punktów końcowych, zarządzanie dostępem zdalnym, zarządzanie aktualizacjami i szyfrowanie dysków.
- Implementacją strategii zabezpieczeń kontenerów, w tym Azure Container Instances, Azure Container Registry i Azure Kubernetes.
- Implementacją Azure Key Vault, w tym certyfikaty, klucze i wpisy tajne.
- Implementacją strategii bezpieczeństwa aplikacji, w tym rejestrację aplikacji, tożsamości zarządzane i punkty końcowe usług.
- Implementacją strategii zabezpieczeń magazynu, w tym sygnatury dostępu współdzielonego, zasady przechowywania obiektów blob i uwierzytelnianie Azure Files.
- Wdrażaniem strategii bezpieczeństwa baz danych, w tym uwierzytelnianie, klasyfikacja danych, dynamiczne maskowanie danych i zawsze szyfrowane.
- Implementacją Azure Monitor, w tym połączone źródła, analiza dzienników i alerty.
- Implementacją Azure Security Center, w tym zasady, zalecenia i dostęp do maszyn wirtualnych na

czas.
- Implementacją usługi Azure Sentinel, w tym skoroszyty, incydenty i poradniki.

Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf

## Program szkolenia

1. Ścieżka szkoleniowa: Tożsamość i dostęp
   - Azure Active Directory
   - Tożsamości hybrydowe
   - Azure AD Identity Protection
   - Azure AD Privileged Identity Management
   - Zarządzanie przedsiębiorstwem
   - Bezpieczeństwo aplikacji
2. Ścieżka szkoleniowa: Wdrożenie ochrony platformy
   - Bezpieczeństwo obwodowe
   - Bezpieczeństwo sieci
   - Bezpieczeństwo hosta
   - Bezpieczeństwo kontenerów
3. Ścieżka szkolenia: Bezpieczeństwo danych i aplikacji
   - Azure Key Vault
   - Bezpieczeństwo przechowywania
   - Bezpieczeństwo baz danych
4. Ścieżka szkolenia: Operacje bezpieczeństwa
   - Azure Monitor
   - Microsoft Defender dla Chmury
   - Microsoft Sentinel

## Oczekiwane przygotowanie uczestnika

Przed przystąpieniem do tego kursu studenci muszą posiadać wiedzę w zakresie:

- Najlepszych praktyk w zakresie bezpieczeństwa i branżowych wymagań bezpieczeństwa, takich jak dogłębna ochrona, zasada najmniejszych uprawnień, kontrola dostępu oparta na rolach, uwierzytelnianie wieloskładnikowe, wspólna odpowiedzialność i model zerowego zaufania.
- Znajomości protokołów bezpieczeństwa, takich jak wirtualne sieci prywatne (VPN), protokół zabezpieczeń internetowych (IPSec), Secure Socket Layer (SSL), metody szyfrowania dysków i danych.
- Oraz posiadać już pewne doświadczenie we wdrażaniu obciążeń platformy Azure. Ten kurs nie

obejmuje podstaw administrowania platformą Azure, zamiast tego zawartość kursu opiera się na tej wiedzy, dodając informacje dotyczące zabezpieczeń.
- Doświadczenia w pracy z systemami operacyjnymi Windows i Linux oraz językami skryptowymi. Laboratoria szkoleniowe mogą korzystać z programu PowerShell i interfejsu wiersza polecenia.
- Umiejętność korzystania z anglojęzycznych materiałów.

Szkolenia poprzedzające:AA_10961 oraz AZ-104
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/distance-learning/#FAQ

## Szkolenie obejmuje

* podręcznik w formie elektronicznej dostępny na platformie: https://learn.microsoft.com/pl-pl/training/
* dostęp do portalu słuchacza Altkom Akademii
Metoda szkolenia:
- Wykład
- Demonstracja
- Laboratoria

Ilość teorii do praktyki
- 50% teoria
- 50% praktyka

## Język

- Szkolenie: polski
- Materiały: angielski

## Metoda egzaminacyjna

Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf
Egzamin w formie on-line. Zapis na stronie https://home.pearsonvue.com/Clients/Microsoft.aspx

### Czas trwania

4 dni / 28 godzin

## Opis egzaminu

Microsoft Certified: Azure Security Engineer Associate
Exam URL: https://docs.microsoft.com/en-us/learn/certifications/exams/AZ-500
Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf