

kod szkolenia: AZ-500 / PL DL 4d

Microsoft Azure Security Technologies

Autoryzowane szkolenie Microsoft Azure Security Technologies AZ-500 szkolenie w formule **Distance Learning**.

Administrator, administrator IT, specjalista IT - docelowa grupa odbiorców. Zobacz film: https://youtu.be/3XFvR5s_BbY



Przeznaczenie szkolenia

Szkolenie skierowane do osób zajmujących następujące stanowiska w organizacji:

- **Administrator**
- **Administrator IT**
- **Specjalista IT**

Cel kursu:

- Zapoznanie się z podstawami bezpieczeństwa platformy **Microsoft Azure**.

Szkolenie skierowane do:

- Osób odpowiedzialnych na platformie Azure za wdrożenie kontroli bezpieczeństwa, utrzymywania pozycji bezpieczeństwa organizacji oraz identyfikacji i usuwania luk w zabezpieczeniach za pomocą różnych narzędzi bezpieczeństwa. Kurs w szczególności jest przeznaczony dla inżynierów zabezpieczeń platformy Azure, którzy planują przystąpić do skojarzonego egzaminu certyfikacyjnego lub wykonują zadania związane z bezpieczeństwem w swojej codziennej pracy. Szkolenie jest również zalecane dla administratorów, architektów i deweloperów, którzy chcą specjalizować się w zapewnianiu bezpieczeństwa platform cyfrowych opartych na platformie Azure i odgrywać integralną rolę w ochronie danych organizacji



Korzyści wynikające z ukończenia szkolenia

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.



Metoda egzaminowania

Egzamin w formie **on-line**. Zapis na stronie <https://home.pearsonvue.com/Clients/Microsoft.aspx>
<https://www.altkomakademia.pl/vouchery-microsoft-promocja/>



Opis egzaminu

Po kursie **AZ-500** można przystąpić do certyfikowanego egzaminu **Microsoft**. Szczegóły na: <https://docs.microsoft.com/en-us/learn/certifications/exams/az-500>



Oczekiwane przygotowanie słuchaczy

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**), protokoły 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: **MS 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>



Język szkolenia

- **Szkolenie:** polski
- **Materiały:** angielski

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

Czas trwania

4 dni / 28 godzin

Agenda szkolenia

Ścieżka szkoleniowa 01: Tożsamość i dostęp

- Azure Active Directory
- Tożsamości hybrydowe
- Azure AD Identity Protection
- Azure AD Privileged Identity Management
- Zarządzanie przedsiębiorstwem
- Bezpieczeństwo aplikacji

Ścieżka szkoleniowa 02: Wdrożenie ochrony platformy

- Bezpieczeństwo obwodowe
- Bezpieczeństwo sieci
- Bezpieczeństwo hosta
- Bezpieczeństwo kontenerów

Ścieżka szkolenia 03: Bezpieczeństwo danych i aplikacji

- Azure Key Vault

- Bezpieczeństwo przechowywania
- Bezpieczeństwo baz danych

Ścieżka szkolenia 04: Operacje bezpieczeństwa

- Azure Monitor
- Microsoft Defender dla Chmury
- Microsoft Sentinel