



Szkolenie AZ-500T00 Microsoft Azure Security Technologies

Numer usługi 2024/08/26/142469/2278457

4 489,50 PLN brutto

3 650,00 PLN netto

160,34 PLN brutto/h

130,36 PLN netto/h

SOFTRONIC

SPÓŁKA Z

OGRANICZONĄ

ODPOWIEDZIALNOŚĆ

CIA



📍 zdalna w czasie rzeczywistym

👤 Usługa szkoleniowa

🕒 28 h

📅 03.02.2025 do 06.02.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Grupa docelowa szkolenia AZ-500T00 Microsoft Azure Security Technologies to specjaliści ds. bezpieczeństwa informatycznego, administratorzy systemów, inżynierowie bezpieczeństwa i wszyscy profesjonaliści IT odpowiedzialni za zapewnienie bezpieczeństwa i zabezpieczenie środowisk chmurowych w Microsoft Azure. Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	10-01-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	28
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Szkolenie AZ-500T00 "Microsoft Azure Security Technologies" ma na celu dostarczenie uczestnikom zaawansowanej wiedzy i umiejętności z zakresu bezpieczeństwa w chmurze Azure. Uczestnicy zdobywają wiedzę niezbędną do samodzielnej identyfikacji zagrożeń, implementacji mechanizmów ochrony oraz skutecznego monitorowania i reagowania na incydenty w środowisku Azure. Ostatecznym celem szkolenia jest umożliwienie uczestnikom skutecznego zabezpieczania zasobów i danych w chmurze Microsoft Azure.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Zabezpiecza platformę Azure przy użyciu Azure Active Directory (AAD).	Konfiguruje i zarządza Azure Active Directory. Implementuje tożsamości hybrydowe. Wdraża ochronę tożsamości usługi Azure AD.	Test teoretyczny
Zarządza tożsamościami uprzywilejowanymi w Azure AD.	Konfiguruje uprzywilejowane zarządzanie tożsamościami w usłudze Azure AD. Monitoruje i kontroluje dostęp do uprzywilejowanych zasobów.	Test teoretyczny
Projektuje i wdraża polityki zabezpieczeń w Azure.	Tworzy i zarządza politykami zabezpieczeń. Implementuje zabezpieczenia obwodowe.	Test teoretyczny
Konfiguruje i zarządza zabezpieczeniami sieci w Azure.	Konfiguruje zabezpieczenia sieciowe. Monitoruje i zarządza politykami sieciowymi.	Test teoretyczny
Zabezpiecza hosty i kontenery w Azure.	Konfiguruje i zarządza zabezpieczeniami hosta. Włącza i zarządza zabezpieczeniami kontenerów.	Test teoretyczny
Wdraża i zabezpiecza Azure Key Vault.	Konfiguruje Azure Key Vault. Implementuje zabezpieczenia i zarządza kluczami oraz tajemnicami.	Test teoretyczny
Konfiguruje zabezpieczenia aplikacji i pamięci masowej w Azure.	Konfiguruje funkcje zabezpieczeń aplikacji. Wdraża i zarządza zabezpieczeniami pamięci masowej.	Test teoretyczny
Zabezpiecza i zarządza bazami danych SQL w Azure.	Konfiguruje zabezpieczenia bazy danych SQL. Zarządza uprawnieniami i monitoruje bezpieczeństwo bazy danych.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Monitoruje zabezpieczenia i zagrożenia w środowisku Azure.	Konfiguruje i zarządza Azure Monitor. Włącza i zarządza Microsoft Defender dla chmury.	Test teoretyczny
Implementuje i monitoruje zabezpieczenia z Microsoft Sentinel.	Konfiguruje i monitoruje Microsoft Sentinel. Analizuje i reaguje na incydenty bezpieczeństwa za pomocą Microsoft Sentinel.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Tak, Uczestnik szkolenia, poza certyfikatem, otrzymuje zaświadczenie o ukończeniu szkolenia z zawartym opisem efektów uczenia się.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak

Program

Szkolenie **AZ-500T00 Microsoft Azure Security Technologies** jest przeznaczone dla administratorów IT oraz specjalistów IT, którzy zajmują się bezpieczeństwem platformy Azure.

W celu przystąpienia do szkolenia Uczestnik powinien posiadać wiedzę z zakresu administracji platformą AZURE.

Szkolenie składa się z wykładu wzbogaconego o prezentację. W trakcie szkolenia każdy Uczestnik wykonuje indywidualne ćwiczenia - laboratoria, dzięki czemu zyskuje praktyczne umiejętności. W trakcie szkolenia omawiane jest również studium przypadków, w którym Uczestnicy wspólnie wymieniają się doświadczeniami. Nad case-study czuwa autoryzowany Trener, który przekazuje informację na temat przydatnych narzędzi oraz najlepszych praktyk do rozwiązania omawianego zagadnienia.

Aby Uczestnik osiągnął zamierzony cel szkolenia niezbędne jest wykonanie przez niego zadanych laboratoriów. Pomocne będzie również ugruntowanie wiedzy i wykonywanie ćwiczeń po zakończonej usłudze. Każdy Uczestnik dysponuje dostępem do laboratoriów przez okres 180 dni.

Przed rozpoczęciem szkolenia Uczestnik rozwiązuje pre-test badający poziom wiedzy na wstępie.

Walidacja: Na koniec usługi Uczestnik wykonuje post-test w celu dokonania oceny wzrostu poziomu wiedzy.

Szkolenie trwa 28 godzin zegarowych i jest realizowane w ciągu 4 dni.

W trakcie każdego dnia szkolenia przewidziane są dwie krótkie przerwy "kawowe" oraz przerwa lunchowa.

Program szkolenia:

Zapewnienie bezpiecznych rozwiązań platformy Azure przy użyciu usługi Azure Active Directory

Wdrażanie tożsamości hybrydowej

Wdrażanie ochrony tożsamości usługi Azure AD

Konfigurowanie uprzywilejowanego zarządzania tożsamościami w usłudze Azure AD

Projektowanie polityk Azure

Wdrażanie zabezpieczeń obwodowych

Konfigurowanie zabezpieczeń sieci

Konfigurowanie zabezpieczeń hosta i zarządzanie nimi

Włączanie zabezpieczeń kontenerów

Wdrażanie i zabezpieczanie usługi Azure Key Vault

Konfigurowanie funkcji zabezpieczeń aplikacji

Wdrażanie zabezpieczeń pamięci masowej

Konfigurowanie zabezpieczeń bazy danych SQL i zarządzanie nimi

Konfigurowanie usługi Azure Monitor i zarządzanie nią

Włączanie usługi Microsoft Defender dla chmury i zarządzanie nią

Konfigurowanie i monitorowanie usługi Microsoft Sentinel

SOFTRONIC Sp. z o. o. zastrzega sobie prawo do zmiany terminu szkolenia lub jego odwołania w przypadku niezbrania się minimalnej liczby Uczestników tj. 3 osób.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 489,50 PLN

Koszt przypadający na 1 uczestnika netto	3 650,00 PLN
Koszt osobogodziny brutto	160,34 PLN
Koszt osobogodziny netto	130,36 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Patryk Łączny

Patryk Łączny – Microsoft Certified Trainer. Absolwent Politechniki Poznańskiej ze specjalnością Matematyczne Metody Informatyki. Zdobył m.in. certyfikaty: Microsoft Certified Professional, Microsoft® Certified Solutions Associate, Microsoft Office Specialist, Microsoft Certified Systems Engineer, Microsoft® Certified IT Professional, Microsoft® Certified Technology Specialist Microsoft Certified Trainer oraz certyfikat ECDL. Specjalizuje się w prowadzeniu szkoleń z zakresu aplikacji Microsoft Office, Exchange, SharePoint, Windows Server, Office 365, które prowadzi w SOFTRONIC od 2006 roku. Posiada uprawnienia pedagogiczne. W zewnętrznym systemie ewaluacji szkoleń Metrics That Matter uzyskał wysoką średnią notę 8,8pkt/9.

Zrealizował szkolenia dla setek Klientów z sektora publicznego oraz prywatnego co potwierdzają liczne referencje. Trener jest również twórcą autorskich szkoleń z zakresu Windows Server oraz bezpieczeństwa IT.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu Uczestnikowi zostaną przekazane autoryzowane materiały szkoleniowe, które są dostępne na koncie Uczestnika na dedykowanym portalu. Uczestnik uzyskuje również 180-dniowy dostęp do laboratoriów Microsoft, z których korzysta w dowolny sposób i w dowolnym momencie, za pośrednictwem przeglądarki internetowej.

Poza dostępnymi przekazywanymi Uczestnikowi, w trakcie szkolenia, Trener przedstawia i omawia autoryzowaną prezentację.

Warunki uczestnictwa

Znajomość najlepszych praktyk w zakresie bezpieczeństwa i wymagań branżowych w zakresie bezpieczeństwa;

Znajomość protokołów bezpieczeństwa, takich jak wirtualne sieci prywatne (VPN), Internet

Protokół bezpieczeństwa (IPSec), Secure Socket Layer (SSL), metody szyfrowania dysku i danych;

Pewne doświadczenie we wdrażaniu obciążeń platformy Azure. (Ten kurs nie obejmuje podstaw

administracji platformy Azure, zamiast tego zawartość kursu opiera się na tej wiedzy poprzez dodawanie

informacje dotyczące bezpieczeństwa.);

Doświadczenie z systemami operacyjnymi Windows i Linux oraz językami skryptowymi.

Laboratoria kursów mogą wymagać użycia programu PowerShell i interfejsu wiersza polecenia.

Informacje dodatkowe

Istnieje możliwość zastosowania zwolnienia z podatku VAT dla szkoleń mających charakter kształcenia zawodowego lub służących przekwalifikowaniu zawodowemu pracowników, których poziom dofinansowania ze środków publicznych wynosi co najmniej 70% (na podstawie § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. zmieniającego rozporządzenie w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r. poz. 1722 ze zm.)

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój;

kompetencja związana z cyfrową transformacją;

Warunki techniczne

Szkolenie realizowane jest w formule distance learning - szkolenie **on-line w czasie rzeczywistym**, w którym możesz wziąć udział z każdego miejsca na świecie.

Szkolenie odbywa się za pośrednictwem platformy **Microsoft Teams**, która umożliwia transmisję dwukierunkową, dzięki czemu Uczestnik może zadawać pytania i aktywnie uczestniczyć w dyskusji. Uczestnik, który potwierdzi swój udział w szkoleniu, przed rozpoczęciem szkolenia, drogą mailową, otrzyma link do spotkania wraz z hasłami dostępu.

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 20Mb/s.
- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/głośniki oraz mikrofon.
- zainstalowana przeglądarka internetowa - Microsoft Edge/ Internet Explorer 10+ / **Google Chrome** 39+ (sugerowana) / Safari 7+
- aplikacja MS Teams może zostać zainstalowana na komputerze lub można z niej korzystać za pośrednictwem przeglądarki internetowej

Kontakt



Agata Wojciechowska

E-mail agata.wojciechowska@softronic.pl

Telefon (+48) 618 658 840