Możliwość dofinansowania

Szkolenie SC-300T00 Microsoft Identity And Access Administrator

Numer usługi 2025/04/03/142469/2668205

4 489,50 PLN brutto
3 650,00 PLN netto
140,30 PLN brutto/h
114,06 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,3 / 5

162 oceny

zdalna w czasie rzeczywistym
Usługa szkoleniowa
32 h
16.02.2026 do 19.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	Szkolenie jest skierowane do administratorów tożsamości i dostępu, którzy planują przystąpić do powiązanego egzaminu certyfikacyjnego lub którzy wykonują zadania administracyjne związane z tożsamością i dostępem w swojej codziennej pracy. Ten kurs jest również przydatny dla administratorów lub inżynierów IT, którzy chcieliby specjalizować się w dostarczaniu rozwiązań do obsługi tożsamości i systemów zarządzania dostępem do rozwiązań opartych na platformie Azure. Usługa adresowana również dla Uczestników projektu ***Kierunek – Rozwój,*** *projektu* ***Małopolski Pociąg do Kariery - sezon 1,*** *oraz projektu* ***Zachodniopomorskie Bony Szkoleniowe.***
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	16-01-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	32

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

Usługa przygotowuje uczestnika do samodzielnego wdrażania rozwiązań służących do zarządzania tożsamością opartych o Microsoft Azure AD i połączonych technologiach tożsamości jak również do samodzielnej rejestracji aplikacji dla przedsiębiorstw, zarządzania dostępem warunkowym oraz sprawowania nadzoru nad tożsamością i innymi narzędziami do zarządzania tożsamością w Microsoft Azure.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje podstawowe koncepcje tożsamości w Microsoft Entra ID.	Opisuje rolę Microsoft Entra ID w zarządzaniu tożsamością. Wyjaśnia różnicę między tożsamościami wewnętrznymi, zewnętrznymi i hybrydowymi.	Test teoretyczny z wynikiem generowanym automatycznie
Konfiguruje podstawowe ustawienia Microsoft Entra ID.	Przeprowadza wstępną konfigurację Microsoft Entra ID. Integruje Microsoft Entra ID z innymi systemami.	Test teoretyczny z wynikiem generowanym automatycznie
Tworzy, konfiguruje i zarządza tożsamościami w Microsoft Entra ID.	Tworzy nowe tożsamości użytkowników. Konfiguruje ustawienia tożsamości. Zarządza cyklem życia tożsamości.	Test teoretyczny z wynikiem generowanym automatycznie
Implementuje i zarządza tożsamościami zewnętrznymi.	Wdraża tożsamości zewnętrzne w Microsoft Entra ID. Zarządza dostępem użytkowników zewnętrznych.	Test teoretyczny z wynikiem generowanym automatycznie
Integruje i zarządza tożsamościami hybrydowymi.	Konfiguruje tożsamości hybrydowe. Monitoruje synchronizację tożsamości hybrydowych.	Test teoretyczny z wynikiem generowanym automatycznie
Wdraża uwierzytelnianie wieloskładnikowe dla użytkowników.	Konfiguruje uwierzytelnianie wieloskładnikowe (MFA). Zarządza politykami MFA.	Test teoretyczny z wynikiem generowanym automatycznie
Planuje, wdraża i zarządza dostępem warunkowym.	Tworzy zasady dostępu warunkowego. Monitoruje i modyfikuje zasady dostępu.	Test teoretyczny z wynikiem generowanym automatycznie
Implementuje zarządzanie dostępem do zasobów Azure.	Konfiguruje role i uprawnienia w Azure. Monitoruje dostęp do zasobów platformy Azure.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Planuje i wdraża zarządzanie uprawnieniami oraz przeglądy dostępu.	Tworzy i zarządza politykami uprawnień. Przeprowadza przeglądy dostępu.	Test teoretyczny z wynikiem generowanym automatycznie
Monitoruje i utrzymuje Microsoft Entra ID.	Konfiguruje narzędzia monitorujące. Analizuje logi i raporty w Microsoft Entra ID. Wdraża poprawki i aktualizacje systemu.	Test teoretyczny z wynikiem generowanym automatycznie
Współpracuje z innymi członkami zespołu w organizacji, korzystając z narzędzi do pracy grupowej w celu realizacji wyznaczonego celu lub projektu.	Identyfikuje wyzwania związane z wyznaczonym celem, planuje etapy ich realizacji, monitoruje ich wykonanie oraz ocenia ich efektywność. Współdzieli informacje z innym współpracownikami i wykorzystuje narzędzia do pracy nad danymi w ramach zespołów.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

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 **SC-300T00 Microsoft Identity And Access Administrator** jest przeznaczone dla administratorów tożsamości i dostępu, którzy planują przystąpić do powiązanego egzaminu certyfikacyjnego lub którzy wykonują zadania administracyjne związane z tożsamością i dostępem w swojej codziennej pracy. Ten kurs jest również przydatny dla administratorów lub inżynierów IT, którzy chcieliby specjalizować się w dostarczaniu rozwiązań do obsługi tożsamości i systemów zarządzania dostępem do rozwiązań opartych na platformie Azure.

W celu przystąpienia do szkolenia Uczestnik powinien znać najlepsze praktyki w zakresie bezpieczeństwa i branżowe wymagania dotyczące bezpieczeństwa, takie jak dogłębna obrona, najmniej uprzywilejowany dostęp, współodpowiedzialność i model zerowego zaufania, znać pojęcia dotyczących tożsamości: uwierzytelnianie, autoryzacja i usługa Active Directory, doświadczenie we wdrażaniu obciążeń platformy Azure. Pomocne będzie również posiadanie przez Uczestnika doświadczenia w pracy z systemami operacyjnymi Windows i Linux oraz znajomość języków skryptowych.

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.

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.

STRUKTURA KURSU:

Kurs obejmuje 32 h dydaktyczne (45 min) = w przeliczeniu 24 h zegarowych (60 min) prowadzonych na żywo (on-line), na platformie Microsoft Teams, na żywo z trenerem.

Szkolenie jest realizowane w ciągu 4 dni.

Czas trwania przerw nie wlicza się do ogólnej liczby godzin trwania usługi szkoleniowej.

Trener ma możliwość przesunięcia przerw, tak aby dostosować harmonogram do potrzeb uczestników.

Program szkolenia:

Wprowadzenie do ochrony przed zagrożeniami na platformie Microsoft 365

Ograniczanie incydentów przy użyciu usługi Microsoft 365 Defender

Ochrona tożsamości przy użyciu usługi Azure AD Identity Protection

Usuwanie zagrożeń za pomocą usługi Microsoft Defender dla usługi Office 365

Ochrona infrastruktury dzięki usłudze Microsoft Defender for Identity

Zabezpieczanie aplikacji i usług w chmurze dzięki usłudze Microsoft Defender dla Cloud Apps

Reagowanie na alerty dotyczące zapobiegania utracie danych przy użyciu platformy Microsoft 365

Zarządzanie ryzykiem wewnętrznym w Microsoft Purview

Badanie zagrożeń przy użyciu funkcji inspekcji w usługach Microsoft 365 Defender i Microsoft Purview Standard

Badanie zagrożeń przy użyciu audytu w usługach Microsoft 365 Defender i Microsoft Purview (Premium)

Badanie zagrożeń za pomocą wyszukiwania zawartości w usłudze Microsoft Purview

Ochrona przed zagrożeniami dzięki usłudze Microsoft Defender dla punktów końcowych

Wdrażanie środowiska usługi Microsoft Defender dla programu Endpoint

Wdrażanie ulepszeń zabezpieczeń systemu Windows w usłudze Microsoft Defender dla programu Endpoint

Przeprowadzanie badań urządzeń w usłudze Microsoft Defender dla programu Endpoint

Wykonywanie akcji na urządzeniu przy użyciu usługi Microsoft Defender dla programu Edpoint

Wykonywanie analiz materiałów i jednostek przy użyciu usługi Microsoft Defender for Endpoint

Konfigurowanie automatyzacji i zarządzanie nią przy użyciu usługi Microsoft Defender for Endpoint

Konfigurowanie alertów i wykrywania w usłudze Microsoft Defender dla punktów końcowych

Korzystanie z funkcji zarządzania zagrożeniami w usłudze Microsoft Defender for Endpoint

Planowanie ochrony obciążeń w chmurze przy użyciu usługi Microsoft Defender for Cloud

Łączenie Azure Assets z usługą Microsoft Defender for Cloud

Łączenie zasobów spoza platformy Azure z usługą Microsoft Defender for Cloud

Zarządzanie stanem zabezpieczeń w chmurze

Wyjaśnienie ochrony przed obciążeniami w chmurze w usłudze Microsoft Defender for Cloud

Usuwanie alertów zabezpieczeń przy użyciu usługi Microsoft Defender for Cloud

Struktura poleceń KQL dla usługi Microsoft Sentinel

Analizowanie wyników zapytań przy użyciu języka KQL

Tworzenie instrukcji wielu tablic przy użyciu języka KQL

Praca z danymi w Microsoft Sentinel przy użyciu języka zapytań Kusto

Wprowadzenie do Microsoft Sentinel

Tworzenie obszarów roboczych Microsoft Sentinel i zarządzanie nimi

Rejestry zapytań w Microsoft Sentinel

Używanie list obserwowanych w aplikacji Microsoft Sentinel

Korzystanie z analizy zagrożeń w usłudze Microsoft Sentinel

Nawiązywanie połączeń między danymi a usługą Microsoft Sentinel przy użyciu łączników danych

Łaczenie usług firmy Microsoft z usługą Microsoft Sentinel

Podłączanie usługi Microsoft 365 Defender do usługi Microsoft Sentinel

Podłączanie hostów systemu Windows do usługi Microsoft Sentinel

Łączenie dzienników Common Event Format z usługą Microsoft Sentinel

Podłączanie źródeł danych syslog do usługi Microsoft Sentinel

Podłączanie wskaźników zagrożeń do Microsoft Sentinel

Wykrywanie zagrożeń za pomocą analizy Microsoft Sentinel

Automatyzacja w Microsoft Sentinel

Zarządzanie incydentami bezpieczeństwa w Microsoft Sentinel

Identyfikowanie zagrożeń za pomocą analizy behawioralnej

Przeprowadzanie normalizacji danych w usłudze Microsoft Sentinel

Zapytania, wizualizacja i monitorowanie danych w usłudze Microsoft Sentinel

Zarządzanie zawartością w usłudze Microsoft Sentinel

Wyjaśnienie koncepcji wykrywania zagrożeń w usłudze Microsoft Sentinel

Wykrywanie zagrożeń za pomocą programu Microsoft Sentinel

Używanie zadań wyszukiwania w usłudze Microsoft Sentinel

Wyszukiwanie zagrożeń przy użyciu skryptów w Microsoft Sentinel

SOFTRONIC Sp. z o. o. zastrzega sobie prawo do zmiany terminu szkolenia lub jego odwołania w przypadku niezebrania 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	140,30 PLN
Koszt osobogodziny netto	114,06 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

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 dostęp do laboratoriów Microsoft.

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

Warunki uczestnictwa

Przed przystąpieniem do kursu zalecamy: Znajomość najlepszych praktyk w zakresie zabezpieczeń oraz wymagań branżowych, takich jak: ochrona warstwowa (defense in depth), zasada najmniejszych uprawnień, współdzielona odpowiedzialność oraz model Zero Trust. Zrozumienie podstawowych pojęć związanych z tożsamością, takich jak uwierzytelnianie, autoryzacja oraz Active Directory. Praktyczne

doświadczenie we wdrażaniu obciążeń na platformie Azure. Szkolenie nie obejmuje podstaw administracji platformy Azure — zakłada ich znajomość i koncentruje się na zagadnieniach związanych z zabezpieczeniami. Pewne doświadczenie z systemami operacyjnymi Windows i Linux oraz językami skryptowymi jest pomocne, ale nie jest wymagane.

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. zmieniające 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**;

Zawarto umowę z WUP w Szczecinie na świadczenie usług rozwojowych w ramach **Projektu Zachodniopomorskie Bony Szkoleniowe.**

Usługa jest skierowana do Uczestników Projektu MP.

Kompetencja związana z cyfrową transformacją.

UWAGA! Przed dokonaniem zgłoszenia / złożeniem wniosku o dofinansowanie prosimy o kontakt z SOFTRONIC w celu potwierdzenia terminu szkolenia oraz dostępności miejsc: **e-mail: softronic@softronic.pl**

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 obywa 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