Możliwość dofinansowania

Szkolenie SC-300T00 Microsoft Identity And Access Administrator

Numer usługi 2024/06/24/142469/2195365

4 120,50 PLN brutto
3 350,00 PLN netto
147,16 PLN brutto/h
119,64 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
28 h
16.09.2024 do 19.09.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
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.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	02-09-2024
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

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.

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
Konfiguruje podstawowe ustawienia Microsoft Entra ID.	Przeprowadza wstępną konfigurację Microsoft Entra ID. Integruje Microsoft Entra ID z innymi systemami.	Test teoretyczny
Tworzy, konfiguruje i zarządza tożsamościami w Microsoft Entra ID.	Tworzy nowe tożsamości użytkowników. Konfiguruje ustawienia tożsamości. Zarządza cyklem życia tożsamości.	Test teoretyczny
Implementuje i zarządza tożsamościami zewnętrznymi.	Wdraża tożsamości zewnętrzne w Microsoft Entra ID. Zarządza dostępem użytkowników zewnętrznych.	Test teoretyczny
Integruje i zarządza tożsamościami hybrydowymi.	Konfiguruje tożsamości hybrydowe. Monitoruje synchronizację tożsamości hybrydowych.	Test teoretyczny
Wdraża uwierzytelnianie wieloskładnikowe dla użytkowników.	Konfiguruje uwierzytelnianie wieloskładnikowe (MFA). Zarządza politykami MFA.	Test teoretyczny
Planuje, wdraża i zarządza dostępem warunkowym.	Tworzy zasady dostępu warunkowego. Monitoruje i modyfikuje zasady dostępu.	Test teoretyczny
Implementuje zarządzanie dostępem do zasobów Azure.	Konfiguruje role i uprawnienia w Azure. Monitoruje dostęp do zasobów platformy Azure.	Test teoretyczny
Planuje i wdraża zarządzanie uprawnieniami oraz przeglądy dostępu.	Tworzy i zarządza politykami uprawnień. Przeprowadza przeglądy dostępu.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Monitoruje i utrzymuje Microsoft Entra ID.	Konfiguruje narzędzia monitorujące. Analizuje logi i raporty w Microsoft Entra ID. Wdraża poprawki i aktualizacje systemu.	Test teoretyczny

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 4. Czy dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w danej branży/sektorze (czy certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów)?

Certyfikaty Microsoft cieszą się globalnym uznaniem, potwierdzając umiejętności w obszarze powszechnie używanych technologii. Ich wartość wynika z rozległości produktów Microsoft, uznawalności w branży, wymagań praktycznych i regularnych aktualizacji. To kwalifikacje cenione na poziomie globalnym.

Pytanie 5. Czy dokument jest certyfikatem, dla którego wypracowano system walidacji i certyfikowania efektów uczenia się na poziomie międzynarodowym?

Tak, certyfikat Microsoft dla którego wypracowano system walidacji i certyfikacji na poziomie międzynarodowym.

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnionych do wydawania dokumentów potwierdzających uzyskanie kwalifikacji, w tym w zawodzie
Nazwa/Kategoria Podmiotu prowadzącego walidację	Pearson VUE
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie
Nazwa/Kategoria Podmiotu certyfikującego	Microsoft
Podmiot certyfikujący jest zarejestrowany w BUR	Nie

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. Pomocne będzie również ugruntowanie wiedzy i wykonywanie ćwiczeń po zakończonej usłudze. Każdy Uczestnik dysponuje dostępem do laboratoriów przez okres 180 dni.

Który egzamin potwierdza zdobyte umiejętności?

Zdaj 1 egzamin:

- **Exam SC-300: Microsoft Identity and Access Administrator**

Zdobądź certyfikat:

- **Microsoft Certified: Identity and Access Administrator Associate**

Szkolenie trwa 28 godzin zegarowych i jest realizowane w ciągu 4 dni (po 7 godzin zegarowych dzinnie, wliczając w to przerwy - dwie przerwy kawowe po 15 minut i jedna lanchowa po 30 minut).

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	4 120,50 PLN
Koszt przypadający na 1 uczestnika netto	3 350,00 PLN
Koszt osobogodziny brutto	147,16 PLN
Koszt osobogodziny netto	119,64 PLN
W tym koszt walidacji brutto	553,50 PLN
W tym koszt walidacji netto	450,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 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 dostępami przekazywanymi Uczestnikowi, w trakcie szkolenia, Trener przedstawia i omawia autoryzowaną prezentację.

Warunki uczestnictwa

W celu przystąpienia do szkolenia Uczestnik powinien znać najlepsze praktyki w zakresie bezpieczeństwa oraz 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.

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, ktory potwierdzi swój udziałw 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/glosniki 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