Możliwość dofinansowania

szkolenie SC-100T00 Microsoft Cybersecurity Architect

Numer usługi 2025/11/25/142469/3169485

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
10.03.2026 do 13.03.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Ten kurs jest przeznaczony dla doświadczonych inżynierów bezpieczeństwa w chmurze, którzy uzyskali wcześniejszą certyfikację w zakresie bezpieczeństwa, zgodności i tożsamości. W szczególności studenci powinni mieć zaawansowane doświadczenie i wiedzę w szerokim zakresie obszarów inżynierii bezpieczeństwa, w tym tożsamości i dostępu, ochrony platformy, operacji bezpieczeństwa, zabezpieczania danych i zabezpieczania aplikacji. Powinni również mieć doświadczenie we wdrożeniach hybrydowych i chmurowych. Początkujący studenci powinni zamiast tego wziąć udział w kursie SC-900: Microsoft Security, Compliance and Identity Fundamentals. Usługa adresowana również dla Uczestników *projektu* ***Małopolski Pociąg do Kariery - sezon 1,*** *oraz projektu* ***Zachodniopomorskie Bony Szkoleniowe.***
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	10-02-2026
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

Ten kurs przygotowuje studentów do samodzielnego projektowania i oceny strategii cyberbezpieczeństwa w następujących obszarach: Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps) oraz dane i aplikacje. Studenci dowiedzą się również, jak projektować i architektować rozwiązania z wykorzystaniem zasad zerowego zaufania oraz określać wymagania bezpieczeństwa dla infrastruktury chmurowej w różnych modelach usług (SaaS, PaaS, IaaS).

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje i charakteryzuje zasady modelu Zero Trust oraz struktur najlepszych praktyk.	Wyjaśnia koncepcje modelu Zero Trust. Charakteryzuje elementy struktury najlepszych praktyk.	Test teoretyczny z wynikiem generowanym automatycznie
Projektuje rozwiązania zgodne z ramami CAF i WAF.	Planuje architekturę zgodną z CAF. Projektuje systemy zgodne z WAF.	Test teoretyczny z wynikiem generowanym automatycznie
Projektuje rozwiązania zgodne z MCRA i Microsoft Cloud Security Benchmark.	Analizuje i implementuje wytyczne MCRA. Stosuje benchmarki Microsoft Cloud Security do projektowania zabezpieczeń.	Test teoretyczny z wynikiem generowanym automatycznie
Opracowuje strategie ochrony przed typowymi cyberzagrożeniami.	Projektuje mechanizmy ochrony przed ransomware. Implementuje strategie odzyskiwania danych po atakach.	Test teoretyczny z wynikiem generowanym automatycznie
Projektuje rozwiązania zgodne z regulacjami prawnymi.	Stosuje przepisy dotyczące ochrony danych w projektowanych rozwiązaniach. Monitoruje zgodność z przepisami.	Test teoretyczny z wynikiem generowanym automatycznie
Projektuje i implementuje zarządzanie tożsamością oraz dostępem uprzywilejowanym	Konfiguruje mechanizmy zarządzania tożsamością. Projektuje systemy kontroli dostępu uprzywilejowanego.	Test teoretyczny z wynikiem generowanym automatycznie
Tworzy rozwiązania dla operacji bezpieczeństwa.	Implementuje narzędzia do monitorowania bezpieczeństwa. Konfiguruje systemy do analizy incydentów.	Test teoretyczny z wynikiem generowanym automatycznie
Projektuje zabezpieczenia dla MS365 i aplikacji.	Konfiguruje zabezpieczenia w MS365. Implementuje zabezpieczenia aplikacji webowych.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Tworzy i zarządza rozwiązaniami zabezpieczającymi w hybrydowych i wielochmurowych środowiskach oraz na punktach końcowych.	Monitoruje i zarządza stanem zabezpieczeń w hybrydowych środowiskach. Implementuje zabezpieczenia punktów końcowych.	Test teoretyczny z wynikiem generowanym automatycznie
Projektuje zabezpieczenia sieci.	Konfiguruje zapory sieciowe. Implementuje rozwiązania do monitorowania i analizy ruchu sieciowego.	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-100T00 Microsoft Cybersecurity Architect** przeznaczone jest dla doświadczonych inżynierów bezpieczeństwa w chmurze, którzy uzyskali wcześniejszą certyfikację w zakresie bezpieczeństwa, zgodności i tożsamości. W szczególności studenci powinni mieć zaawansowane doświadczenie i wiedzę w szerokim zakresie obszarów inżynierii bezpieczeństwa, w tym tożsamości i dostępu, ochrony platformy, operacji bezpieczeństwa, zabezpieczania danych i zabezpieczania aplikacji. Powinni również mieć doświadczenie we wdrożeniach hybrydowych i chmurowych. Początkujący studenci powinni zamiast tego wziąć udział w kursie SC-900: Microsoft Security, Compliance and Identity Fundamentals.

Ten kurs przygotowuje studentów do samodzielnego projektowania i oceny strategii cyberbezpieczeństwa w następujących obszarach: Zero Trust, Governance Risk Compliance (GRC), security operations (SecOps) oraz dane i aplikacje. Studenci dowiedzą się również, jak projektować i architektować rozwiązania z wykorzystaniem zasad zerowego zaufania oraz określać wymagania bezpieczeństwa dla infrastruktury chmurowej w różnych modelach usług (SaaS, PaaS, IaaS).

W celu przystąpienia do szkolenia Uczestnik powinien posiadać zaawansowane doświadczenie i wiedzę w zakresie tożsamości i dostępu, ochrony platform, operacji bezpieczeństwa, zabezpieczania danych i zabezpieczania aplikacji. Potrzebne będzie również doświadczenie we wdrożeniach hybrydowych i chmurowych. Zdecydowanie zaleca się również posiadanie i zdanie jednego z certyfikatów poziomu stowarzyszonego w zakresie bezpieczeństwa, zgodności i tożsamości (takich jak AZ-500, SC-200 lub SC-300)

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. P

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

Szkolenie trwa **32 godziny dydaktyczne** (1 godz. dydaktyczna = 45 minut) i jest realizowane w ciągu 4 dni.

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

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

Szkolenie jest prowadzone na żywo (on-line), na platformie Microsoft Teams.

Program szkolenia:

Wprowadzenie do Zero Trust i struktur najlepszych praktyk

Projektowanie rozwiązań zgodnych z ramami Cloud Adoption Framework (CAF) i Well-Architected Framework (WAF)

Projektowanie rozwiązań zgodnych z Microsoft Cybersecurity Reference Architecture (MCRA) i Microsoft Cloud Security Benchmark

Projektowanie strategii zapewniającej odporność na typowe cyberzagrożenia, takie jak oprogramowanie ransomware.

Analiza przykładów: Projektowanie rozwiązań zgodnych z najlepszymi praktykami i priorytetami w zakresie zabezpieczeń

Tworzenie rozwiązań zapewniających zgodność z przepisami

Opracowanie rozwiązań do zarządzania tożsamością i dostępem

Projektowanie rozwiązań zabezpieczających dostęp uprzywilejowany

Projektowanie rozwiązań dla operacji związanych z bezpieczeństwem

Analiza przykładów: Projektowanie operacji zabezpieczeń, tożsamości i zgodności z przepisami

Projektowanie rozwiązań zabezpieczających platformę Microsoft 365

Tworzenie rozwiązań do zabezpieczania aplikacji

Projektowanie rozwiązań zabezpieczających dane organizacji

Analiza przykładów: Projektowanie rozwiązań zabezpieczających aplikacje i dane

Określanie wymagań dotyczących zabezpieczania usług SaaS, PaaS i IaaS

Opracowanie rozwiązań do zarządzania stanem zabezpieczeń w środowiskach hybrydowych i wielochmurowych

Projektowanie rozwiązań zabezpieczających punkty końcowe serwerów i klientów

Projektowanie rozwiązań dla bezpieczeństwa sieci

Analiza przykładów: Projektowanie rozwiązań bezpieczeństwa dla infrastruktury

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.

Warunki uczestnictwa

W celu przystąpienia do szkolenia uczestnik powinien posiadać zaawansowane doświadczenie i wiedzę w zakresie tożsamości i dostępu, ochrony platform, operacji bezpieczeństwa, zabezpieczania danych i zabezpieczania aplikacji. Potrzebne będzie również doświadczenie we wdrożeniach hybrydowych i chmurowych. Zdecydowanie zaleca się również posiadanie i zdanie jednego z certyfikatów poziomu stowarzyszonego w zakresie bezpieczeństwa, zgodności i tożsamości (takich jak AZ-500, SC-200 lub SC-300)

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

Ewa Kasprzak

E-mail ewa.kasprzak@softronic.pl
Telefon (+48) 618 658 840