Możliwość dofinansowania

szkolenie SC-100T00 Microsoft Cybersecurity Architect

Numer usługi 2024/04/24/142469/2134338

4 489,50 PLN brutto
3 650,00 PLN netto
160,34 PLN brutto/h
130,36 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
28 h
15.07.2024 do 18.07.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
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.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	01-07-2024
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

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
Projektuje rozwiązania zgodne z ramami CAF i WAF.	Planuje architekturę zgodną z CAF. Projektuje systemy zgodne z WAF.	Test teoretyczny
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
Opracowuje strategie ochrony przed typowymi cyberzagrożeniami.	Projektuje mechanizmy ochrony przed ransomware. Implementuje strategie odzyskiwania danych po atakach.	Test teoretyczny
Projektuje rozwiązania zgodne z regulacjami prawnymi.	Stosuje przepisy dotyczące ochrony danych w projektowanych rozwiązaniach. Monitoruje zgodność z przepisami.	Test teoretyczny
Projektuje i implementuje zarządzanie tożsamością oraz dostępem uprzywilejowanym	Konfiguruje mechanizmy zarządzania tożsamością. Projektuje systemy kontroli dostępu uprzywilejowanego.	Test teoretyczny
Tworzy rozwiązania dla operacji bezpieczeństwa.	Implementuje narzędzia do monitorowania bezpieczeństwa. Konfiguruje systemy do analizy incydentów.	Test teoretyczny
Projektuje zabezpieczenia dla MS365 i aplikacji.	Konfiguruje zabezpieczenia w MS365. Implementuje zabezpieczenia aplikacji webowych.	Test teoretyczny

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
Projektuje zabezpieczenia sieci.	Konfiguruje zapory sieciowe. Implementuje rozwiązania do monitorowania i analizy ruchu sieciowego.	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 **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.

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

Szkolenie trwa 32 godziny zegarowych, realizowane w ciągu 4 następujących po sobie dni.
W trakcie każdego dnia szkolenia przewidziane są dwie krótkie przerwy "kawowe" oraz przerwa lunchowa.

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

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.)

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