



CloudTeam Spółka z ograniczoną odpowiedzialnością



SC-100 Microsoft Cybersecurity Architect - szkolenie

Numer usługi 2023/11/22/15086/2023005

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 28 h

📅 03.06.2024 do 03.06.2024

5 535,00 PLN brutto

4 500,00 PLN netto

197,68 PLN brutto/h

160,71 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
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 przeszli 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 z wdrożeniami hybrydowymi i chmurowymi. Początkujący studenci powinni zamiast tego wziąć udział w kursie SC-900: Microsoft Security, Compliance, and Identity Fundamentals.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	16
Data zakończenia rekrutacji	27-05-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	28
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Ten kurs dostarcza IT Identity and Access Professional, wraz z IT Security Professional, wiedzy i umiejętności potrzebnych do wdrożenia rozwiązań zarządzania tożsamością opartych na Microsoft Azure AD, oraz powiązanych z nim technologii tożsamości. Kurs ten przygotowuje studentów do projektowania i oceny strategii cyberbezpieczeństwa w następujących obszarach: Zero Trust, Governance Risk Compliance (GRC), operacje bezpieczeństwa (SecOps) oraz dane i aplikacje. Studenci dowiedzą się również, jak

Efekty uczenia się

Uczestnik, który ukończył szkolenie:

- buduje strategię i tworzy architekturę bezpieczeństwa
- projektuje strategię operacji bezpieczeństwa
- projektuje strategię bezpieczeństwa tożsamości
- ocenia strategię zgodności z przepisami i stan bezpieczeństwa
- projektuje strategię zabezpieczania punktów końcowych serwera i klienta
- projektuje strategię zabezpieczania usług Pass, IaaS i SaaS
- projektuje strategię bezpieczeństwa dla aplikacji
- projektuje strategię bezpieczeństwa dla danych

Uczestnik będzie również znał najlepsze praktyki dotyczące architektury strategii bezpieczeństwa i ich zmian w chmurze.

Sposób weryfikacji efektów uczenia się

W celu określenia przyrostu wiedzy uczestnik wypełni test przed usługą i po zrealizowanej usłudze (pre i post test).

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Program

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

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	5 535,00 PLN
Koszt przypadający na 1 uczestnika netto	4 500,00 PLN
Koszt osobogodziny brutto	197,68 PLN
Koszt osobogodziny netto	160,71 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma w pierwszym dniu szkolenia dostęp do materiałów szkoleniowych:

- Autoryzowany podręcznik Microsoft w wersji elektronicznej (przesłany na maila uczestnika)
- Dostęp do środowiska Azure

Informacje dodatkowe

Po szkoleniu uczestnik otrzyma zaświadczenie o ukończeniu usługi.

Szkolenie realizujemy codziennie w godzinach 9.00-16.00.

Przerwy:

10.30-10.45 - I przerwa kawowa

12.00-13.00 - przerwa obiadowa

14.30-14.45 - II przerwa kawowa

Godzinowy harmonogram usługi ma charakter orientacyjny - trener, w zależności od potrzeb uczestników, może zmienić długość poszczególnych modułów (przy zachowaniu łącznego wymiaru 28 godz.).

Podczas szkolenia, w zależności od potrzeb uczestników, będą robione krótkie przerwy. Trener ustali z uczestnikami konkretne godziny przerw.

Warunki techniczne

Aby poprawnie podłączyć się do szkolenia potrzebne będą:

Komputer/laptop z dowolnym systemem np. Windows 10

Słuchawki lub głośniki

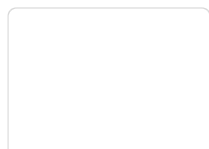
Mikrofon

Dostęp do Internetu

Dostęp do przeglądarki internetowej

Uczestnicy tydzień przed szkoleniem na podany adres mailowy otrzymają zaproszenie wraz z linkiem i hasłem do platformy Zoom. Link będzie aktywny przez cały okres trwania kursu.

Kontakt



Angelika Wiącek-Suska

E-mail angelika.wiacek@cloudteam.pl



Telefon (+48) 726 225 455