



Szkolenie SC 100 Microsoft Cybersecurity Architect

Numer usługi 2026/06/02/5395/3604239

3 200,00 PLN brutto
3 200,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h
261,33 PLN cena rynkowa ⓘ

NTG.pl Sp. z o.o.

★★★★☆ 4,4 / 5

5 667 ocen

📍 Łódź

🏢 Usługa szkoleniowa

📄 stacjonarna

👥 Zajęcia grupowe

🕒 32:00 h

📅 24.11.2026 do 27.11.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie jest skierowane do profesjonalistów IT, architektów bezpieczeństwa i administratorów systemów, którzy chcą wzmocnić swoje umiejętności w zakresie cyberbezpieczeństwa.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	19-11-2026
Forma prowadzenia usługi	stacjonarna
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 do projektowania i wdrażania kompleksowych strategii cyberbezpieczeństwa w środowiskach chmurowych, hybrydowych i lokalnych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozumie podstawowe pojęcia związane z bezpieczeństwem, zgodnością i zarządzaniem tożsamością w środowisku Microsoft. Uczestnik zna możliwości Microsoft Entra w zakresie uwierzytelniania, autoryzacji oraz zarządzania dostępem do zasobów.	Uczestnik potrafi wyjaśnić pojęcia związane z bezpieczeństwem, zgodnością oraz tożsamością i wskazać ich zastosowanie w usługach Microsoft. Uczestnik potrafi wskazać funkcje Microsoft Entra ID oraz dobrać odpowiednie mechanizmy kontroli dostępu do przykładowego scenariusza biznesowego.	Test teoretyczny z wynikiem generowanym automatycznie Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozpoznaje podstawowe rozwiązania zabezpieczeń Microsoft wykorzystywane do ochrony infrastruktury, użytkowników i danych. Uczestnik rozumie możliwości Microsoft Purview w zakresie zgodności, ochrony informacji i zarządzania ryzykiem organizacji.	Uczestnik potrafi opisać zastosowanie usług Microsoft Sentinel, Microsoft Defender XDR oraz mechanizmów zabezpieczeń Azure. Uczestnik potrafi wskazać funkcje Microsoft Purview związane z ochroną danych, zgodnością, eDiscovery oraz zarządzaniem cyklem życia informacji.	Test teoretyczny z wynikiem generowanym automatycznie Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Jak wygląda szkolenie?

Szkolenie prowadzone jest w sposób uporządkowany i praktyczny - składa się z trzech etapów:

- Wprowadzenie teoretyczne
- Ćwiczenia wspólne z trenerem – wykonujemy zadania krok po kroku, ucząc się na konkretnych przykładach.
- Zadania do samodzielnego wykonania – utrwalenie wiedzy.

Opieka poszkoleniowa

Po zakończeniu szkolenia zapewniamy pełną opiekę poszkoleniową:

- kontakt z trenerem
- wsparcie techniczne i merytoryczne po szkoleniu
- dodatkowe materiały i wskazówki, które pomogą wracać do kluczowych zagadnień.

Program szkolenia:

Moduł 1: Projektowanie rozwiązań, które są zgodne z najlepszymi rozwiązaniami i priorytetami zabezpieczeń

- Wprowadzenie do platform Zero Trust i najlepszych rozwiązań
- Projektowanie rozwiązań zabezpieczeń dostosowanych do struktury Cloud Adoption Framework (CAF) i dobrze zaprojektowanej struktury (WAF)
- Projektowanie rozwiązań, które są zgodne z architekturą referencyjną cyberbezpieczeństwa firmy Microsoft (MCRA) i testem porównawczym zabezpieczeń chmury firmy Microsoft (MCSB)
- Projektowanie strategii odporności oprogramowania wymuszającego okup i innych ataków w oparciu o najlepsze rozwiązania w zakresie zabezpieczeń firmy Microsoft
- Analiza przypadku: Projektowanie rozwiązań, które są zgodne z najlepszymi rozwiązaniami i priorytetami zabezpieczeń

Moduł 2: Projektowanie operacji zabezpieczeń, tożsamości i możliwości zgodności:

- Projektowanie rozwiązań pod kątem zgodności z przepisami
- Projektowanie rozwiązań do zarządzania tożsamościami i dostępem
- Projektowanie rozwiązań do zabezpieczania uprzywilejowanego dostępu
- Projektowanie rozwiązań dla operacji zabezpieczeń
- Analiza przypadku: Projektowanie operacji zabezpieczeń, tożsamości i możliwości zgodności

Moduł 3: Projektowanie rozwiązań zabezpieczeń dla aplikacji i danych:

- Projektowanie rozwiązań do zabezpieczania platformy Microsoft 365
- Projektowanie rozwiązań do zabezpieczania aplikacji
- Projektowanie rozwiązań do zabezpieczania danych organizacji
- Analiza przypadku: Projektowanie rozwiązań zabezpieczeń dla aplikacji i danych

Moduł 4: Projektowanie rozwiązań zabezpieczeń dla infrastruktury:

- Określanie wymagań dotyczących zabezpieczania usług SaaS, PaaS i IaaS
- Projektowanie rozwiązań do zarządzania stanem zabezpieczeń w środowiskach hybrydowych i wielochmurowych
- Projektowanie rozwiązań do zabezpieczania punktów końcowych serwera i klienta
- Projektowanie rozwiązań na potrzeby zabezpieczeń sieci
- Analiza przypadku: Projektowanie rozwiązań zabezpieczeń dla infrastruktury

Test z wynikiem generowanym automatycznie.

Harmonogram

Liczba pozycji harmonogramu: 29

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 29 Wprowadzenie do platform Zero Trust, Projektowanie rozwiązań zabezpieczeń dostosowanych do struktury Cloud Adoption Framework (CAF) i dobrze zaprojektowanej struktury (WAF)	Zajęcia	Tomasz Skurniak	24-11-2026	08:00	10:00	02:00
2 z 29 -	Przerwa	-	24-11-2026	10:00	10:15	00:15
3 z 29 Projektowanie rozwiązań, które są zgodne z architekturą referencyjną cyberbezpieczeństwa firmy Microsoft (MCRA) i testem porównawczym zabezpieczeń chmury firmy Microsoft (MCSB)	Zajęcia	Tomasz Skurniak	24-11-2026	10:15	12:15	02:00
4 z 29 -	Przerwa	-	24-11-2026	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 29 Projektowanie strategii odporności oprogramowania wymuszającego okup i innych ataków w oparciu o najlepsze rozwiązania w zakresie zabezpieczeń firmy Microsoft	Zajęcia	Tomasz Skurniak	24-11-2026	12:45	14:15	01:30
6 z 29 -	Przerwa	-	24-11-2026	14:15	14:30	00:15
7 z 29 Analiza przypadku: Projektowanie rozwiązań, które są zgodne z najlepszymi rozwiązaniami i i priorytetami zabezpieczeń	Zajęcia	Tomasz Skurniak	24-11-2026	14:30	16:00	01:30
8 z 29 Projektowanie rozwiązań pod kątem zgodności z przepisami Projektowanie rozwiązań do zarządzania tożsamością i i dostępem	Zajęcia	Tomasz Skurniak	25-11-2026	08:00	10:00	02:00
9 z 29 -	Przerwa	-	25-11-2026	10:00	10:15	00:15
10 z 29 Projektowanie rozwiązań do zabezpieczania uprzywilejowanego dostępu	Zajęcia	Tomasz Skurniak	25-11-2026	10:15	12:15	02:00
11 z 29 -	Przerwa	-	25-11-2026	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 29 Projektowanie rozwiązań dla operacji zabezpieczeń	Zajęcia	Tomasz Skurniak	25-11-2026	12:45	14:15	01:30
13 z 29 -	Przerwa	-	25-11-2026	14:15	14:30	00:15
14 z 29 Analiza przypadku: Projektowanie operacji zabezpieczeń, tożsamości i możliwości zgodności	Zajęcia	Tomasz Skurniak	25-11-2026	14:30	16:00	01:30
15 z 29 Projektowanie rozwiązań do zabezpieczani a platformy Microsoft 365 Projektowanie rozwiązań do zabezpieczani a aplikacji	Zajęcia	Tomasz Skurniak	26-11-2026	08:00	10:00	02:00
16 z 29 -	Przerwa	-	26-11-2026	10:00	10:15	00:15
17 z 29 Projektowanie rozwiązań do zabezpieczani a aplikacji	Zajęcia	Tomasz Skurniak	26-11-2026	10:15	12:15	02:00
18 z 29 -	Przerwa	-	26-11-2026	12:15	12:45	00:30
19 z 29 Projektowanie rozwiązań do zabezpieczani a danych organizacji	Zajęcia	Tomasz Skurniak	26-11-2026	12:45	14:15	01:30
20 z 29 -	Przerwa	-	26-11-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 29 Analiza przypadku: Projektowanie rozwiązań zabezpieczeń dla aplikacji i danych	Zajęcia	Tomasz Skurniak	26-11-2026	14:30	16:00	01:30
22 z 29 Określanie wymagań dotyczących zabezpieczania usług SaaS, PaaS i IaaS Projektowanie rozwiązań do zarządzania stanem zabezpieczeń w środowiskach hybrydowych i wielochmurowych	Zajęcia	Tomasz Skurniak	27-11-2026	08:00	10:00	02:00
23 z 29 -	Przerwa	-	27-11-2026	10:00	10:15	00:15
24 z 29 Projektowanie rozwiązań do zabezpieczania punktów końcowych serwera i klienta	Zajęcia	Tomasz Skurniak	27-11-2026	10:15	12:15	02:00
25 z 29 -	Przerwa	-	27-11-2026	12:15	12:45	00:30
26 z 29 Projektowanie rozwiązań na potrzeby zabezpieczeń sieci	Zajęcia	Tomasz Skurniak	27-11-2026	12:45	14:15	01:30
27 z 29 -	Przerwa	-	27-11-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 29 Analiza przypadku: Projektowanie rozwiązań zabezpieczeń dla infrastruktury	Zajęcia	Tomasz Skurniak	27-11-2026	14:30	15:30	01:00
29 z 29 -	Walidacja	Tomasz Skurniak	27-11-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	32:00
w tym suma godzin zajęć	27:30
w tym suma godzin walidacji	00:30
w tym suma przerw	04:00
Suma godzin dydaktycznych bez przerw	37:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 200,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	3 200,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Liczba godzin usługi

Rodzaj godzin

Liczba godzin

Liczba godzin zegarowych usługi

32:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Tomasz Skurniak

Ponad 15 lat doświadczenia w realizacji szkoleń IT jako Microsoft Certified Trainer. Prowadzenie autoryzowanych szkoleń Microsoft (w tym obszarów Microsoft Security). Doskonała znajomość praktyczna i teoretyczna środowiska informatycznego opartego o systemy operacyjne MS Windows, Netware oraz Unix. Bardzo dobra znajomość środowiska programistycznego .NET (najnowsze wersje) w tym języków: C# oraz VB. Umiejętność tworzenia aplikacji WinForms jak i WebForms (w tym Ajax, SilverLight, WebServices – WCF, WPF, MVC, MVVM). Trener posiada doświadczenie zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Autoryzowane materiały Microsoft w formie elektronicznej. Laboratorium on-line niezbędne do wykonywania ćwiczeń / symulacji dostępne będą dla uczestnika przez 6 miesięcy od zakończenia szkolenia.

Warunki uczestnictwa

Kursant powinien posiadać zaawansowane doświadczenie i wiedzę w szerokim zakresie dziedzin inżynierii bezpieczeństwa, w tym tożsamość i dostęp, ochrona platformy, operacje bezpieczeństwa, zabezpieczanie danych i aplikacji. Zaleca się również doświadczenie w implementacjach hybrydowych i chmurowych. Jest to kurs na poziomie zaawansowanym, więc kursanci powinni wcześniej uzyskać certyfikat na poziomie stowarzyszonym z portfolio bezpieczeństwa, zgodności i tożsamości, takie jak AZ-500, SC-200 lub SC-300.

Dla osób początkujących zalecane jest wzięcie udziału w kursie SC-900: Microsoft Security, Compliance, and Identity Fundamentals.

Informacje dodatkowe

Po ukończeniu szkolenia uczestnik otrzymuje certyfikat Microsoft potwierdzający zdobyte umiejętności.

Uczestnik powinien uzyskać frekwencje w min. 80% zajęć.

Podczas szkoleń istnieje możliwość przeprowadzenia kontroli/audytu usługi przez osoby do tego upoważnione przez PARP.

Jak skorzystać z usług dofinansowanych?

- Krok 1: Założenie konta indywidualnego/instytucjonalnego w Bazie Usług Rozwojowych.
- Krok 2: Złożenie wniosku do Operatora, który rozdziela środki w Twoim województwie.
- Krok 3: Uzyskanie dofinansowania.
- Krok 4: Zapisanie na szkolenie poprzez platformę BUR.

Adres

ul. Pomorska 65

90-218 Łódź

woj. łódzkie

Piętro 3

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt



NTG.pl Sp. z o.o.

E-mail ntg@ntg.edu.pl

Telefon (+48) 609 009 742