Możliwość dofinansowania

Szkolenie SC 200 Microsoft Security Operations Analyst

Numer usługi 2026/06/01/5395/3602141

3 200,00 PLN brutto
3 200,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h
332,00 PLN cena rynkowa

NTG.pl Sp. z o.o.

4,4 / 5

5 666 ocen

Łódź
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
32:00 h
29.09.2026 do 02.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Identyfikatory projektów	Małopolski Pociąg do kariery, Nowy start w Małopolsce z EURESEM, Zachodniopomorskie Bony Szkoleniowe, Kierunek - Rozwój
Grupa docelowa usługi	Kurs przeznaczony dla specjalistów IT, którzy chcą pogłębić swoją wiedzę w zakresie operacji bezpieczeństwa. Uczestnicy nauczą się wykorzystywać narzędzia takie jak Microsoft Defender for Endpoint, Microsoft Defender for Cloud oraz Microsoft Sentinel.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	24-09-2026
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

Celem kursu jest nabycie umiejętności w zakresie badania, reagowania, śledzenia zagrożeń przy użyciu Microsoft Sentinel, Microsoft Defender XDR oraz Microsoft Defender for Cloud.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik potrafi identyfikować i eliminować zagrożenia przy użyciu rozwiązań Microsoft Defender XDR, Microsoft Defender for Endpoint oraz Microsoft Sentinel.	Uczestnik potrafi wskazać odpowiednie narzędzia Microsoft służące do wykrywania, analizy i reagowania na incydenty bezpieczeństwa w środowisku Microsoft 365 i Azure. Uczestnik zna mechanizmy zapobiegania atakom za pomocą Defender dla Endpoint.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozumie możliwości Microsoft Sentinel w zakresie analizy danych, wykrywania zagrożeń oraz automatyzacji działań bezpieczeństwa.	Uczestnik potrafi tworzyć i analizować podstawowe zapytania KQL oraz opisać proces konfiguracji i obsługi incydentów w Microsoft Sentinel.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik zna możliwości Microsoft Purview w zakresie ochrony danych, zgodności i analizy ryzyka wewnętrznego.	Uczestnik potrafi opisać mechanizmy DLP, eDiscovery, inspekcji oraz zarządzania ryzykiem poufnym w Microsoft Purview.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozumie zastosowanie Microsoft Copilot for Security oraz mechanizmów AI wspierających operacje bezpieczeństwa.	Uczestnik potrafi wskazać funkcje Microsoft Copilot for Security oraz opisać zastosowanie generatywnej AI w analizie zagrożeń i wsparciu zespołów SOC.	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: Eliminowanie zagrożeń przy użyciu usługi Microsoft Defender XDR

- Wprowadzenie do ochrony przed zagrożeniami XDR w usłudze Microsoft Defender
- Eliminowanie zdarzeń przy użyciu usługi Microsoft 365 Defender
- Ochrona tożsamości za pomocą Ochrona tożsamości Microsoft Entra
- Korygowanie ryzyka przy użyciu Ochrona usługi Office 365 w usłudze Microsoft Defender
- Sejf guard your environment with Microsoft Defender for Identity (Ochrona środowiska za pomocą usługi Microsoft Defender for Identity)
- Zabezpieczanie aplikacji i usług w chmurze za pomocą usługi Microsoft Defender dla Chmury App

Moduł 2: Eliminowanie zagrożeń przy użyciu rozwiązania Microsoft Copilot for Security

- Podstawy generowania sztucznej inteligencji
- Opis rozwiązania Microsoft Copilot for Security
- Opis podstawowych funkcji rozwiązania Microsoft Copilot for Security
- Opis osadzonych środowisk rozwiązania Microsoft Copilot for Security

Moduł 3: Eliminowanie zagrożeń przy użyciu usługi Microsoft Purview

- Reagowanie na alerty ochrony przed utratą danych przy użyciu platformy Microsoft 365
- Zarządzanie ryzykiem poufnym w usłudze Microsoft Purview
- Wyszukiwanie i badanie za pomocą Inspekcja w Microsoft Purview
- Badanie zagrożeń za pomocą funkcji wyszukiwania zawartości w usłudze Microsoft Purview

Moduł 4: Eliminowanie zagrożeń przy użyciu Ochrona punktu końcowego w usłudze Microsoft Defender

- Ochrona przed zagrożeniami za pomocą Ochrona punktu końcowego w usłudze Microsoft Defender
- Wdrażanie środowiska Ochrona punktu końcowego w usłudze Microsoft Defender
- Implementowanie ulepszeń zabezpieczeń systemu Windows za pomocą Ochrona punktu końcowego w usłudze Microsoft Defender
- Przeprowadzanie badań urządzeń w usłudze Ochrona punktu końcowego w usłudze Microsoft Defender
- Wykonywanie akcji na urządzeniu przy użyciu Ochrona punktu końcowego w usłudze Microsoft Defender
- Przeprowadzanie badań dowodów i jednostek przy użyciu Ochrona punktu końcowego w usłudze Microsoft Defender
- Konfigurowanie automatyzacji i zarządzanie nią przy użyciu Ochrona punktu końcowego w usłudze Microsoft Defender
- Konfigurowanie alertów i wykrywania w Ochrona punktu końcowego w usłudze Microsoft Defender
- Korzystanie z zarządzania lukami w zabezpieczeniach w Ochrona punktu końcowego w usłudze Microsoft Defender

Moduł 5: Ograniczanie zagrożeń przy użyciu Microsoft Defender dla Chmury

- Planowanie ochrony obciążeń w chmurze przy użyciu Microsoft Defender dla Chmury
- Połączenie zasobów platformy Azure do Microsoft Defender dla Chmury
- Połączenie zasobów spoza platformy Azure do Microsoft Defender dla Chmury
- Zarządzanie stanem zabezpieczeń w chmurze
- Wyjaśnienie ochrony obciążeń w chmurze w Microsoft Defender dla Chmury
- Korygowanie alertów zabezpieczeń przy użyciu Microsoft Defender dla Chmury

Moduł 6: Tworzenie zapytań dla usługi Microsoft Sentinel przy użyciu język zapytań Kusto (KQL)

- Konstruowanie instrukcji KQL dla usługi Microsoft Sentinel
- Analizowanie wyników zapytania przy użyciu języka KQL
- Tworzenie instrukcji z wieloma tabelami przy użyciu języka KQL
- Praca z danymi w usłudze Microsoft Sentinel przy użyciu język zapytań Kusto

Moduł 7: Konfigurowanie środowiska usługi Microsoft Sentinel

- Wprowadzenie do usługi Microsoft Sentinel
- Tworzenie obszarów roboczych usługi Microsoft Sentinel i zarządzanie nimi
- Wykonywanie zapytań dotyczących dzienników w usłudze Microsoft Sentinel
- Korzystanie z list obserwowanych w usłudze Microsoft Sentinel
- Korzystanie z analizy zagrożeń w usłudze Microsoft Sentinel

Moduł 8: Dzienniki Połączenie do usługi Microsoft Sentinel

- Połączenie danych do usługi Microsoft Sentinel przy użyciu łączników danych
- Połączenie usługi firmy Microsoft do usługi Microsoft Sentinel
- Połączenie usługi Microsoft Defender XDR do usługi Microsoft Sentinel
- Połączenie hostów systemu Windows do usługi Microsoft Sentinel
- Połączenie dzienniki common event format do usługi Microsoft Sentinel
- Połączenie źródła danych dziennika systemu do usługi Microsoft Sentinel
- Połączenie wskaźniki zagrożeń do usługi Microsoft Sentinel

Moduł 9: Tworzenie wykryć i przeprowadzanie badań przy użyciu usługi Microsoft Sentinel

- Wykrywanie zagrożeń za pomocą analizy usługi Microsoft Sentinel
- Automatyzacja w usłudze Microsoft Sentinel
- Reagowanie na zagrożenia za pomocą podręczników usługi Microsoft Sentinel
- Zarządzanie zdarzeniami zabezpieczeń w usłudze Microsoft Sentinel
- Identyfikowanie zagrożeń za pomocą analizy behawioralnej
- Normalizacja danych w usłudze Microsoft Sentinel
- Wykonywanie zapytań, wizualizowanie i monitorowanie danych w usłudze Microsoft Sentinel
- Zarządzanie zawartością w usłudze Microsoft Sentinel

Moduł 10: Wykonywanie wyszukiwania zagrożeń w usłudze Microsoft Sentinel

- Wyjaśnienie pojęć związanych z wyszukiwaniem zagrożeń w usłudze Microsoft Sentinel
- Wyszukiwanie zagrożeń za pomocą usługi Microsoft Sentinel
- Korzystanie z zadań wyszukiwania w usłudze Microsoft Sentinel
- Wyszukiwanie zagrożeń za pomocą notesów w usłudze Microsoft Sentinel

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 Moduł 1: Eliminowanie zagrożeń przy użyciu usługi Microsoft Defender XDR - teoria	Zajęcia	Tomasz Skurniak	29-09-2026	08:00	10:00	02:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 29 -	Przerwa	-	29-09-2026	10:00	10:15	00:15
3 z 29 Moduł 1: Eliminowanie zagrożeń przy użyciu usługi Microsoft Defender XDR - praktyka	Zajęcia	Tomasz Skurniak	29-09-2026	10:15	12:15	02:00
4 z 29 -	Przerwa	-	29-09-2026	12:15	12:45	00:30
5 z 29 Moduł 2: Eliminowanie zagrożeń przy użyciu rozwiązania Microsoft Copilot for Security - teoria	Zajęcia	Tomasz Skurniak	29-09-2026	12:45	14:15	01:30
6 z 29 -	Przerwa	-	29-09-2026	14:15	14:30	00:15
7 z 29 Moduł 2: Eliminowanie zagrożeń przy użyciu rozwiązania Microsoft Copilot for Security - praktyka	Zajęcia	Tomasz Skurniak	29-09-2026	14:30	16:00	01:30
8 z 29 8 z 29 Moduł 3: Eliminowanie zagrożeń przy użyciu usługi Microsoft Purview	Zajęcia	Tomasz Skurniak	30-09-2026	08:00	10:00	02:00
9 z 29 -	Przerwa	-	30-09-2026	10:00	10:15	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 29 Moduł 4: Eliminowanie zagrożeń przy użyciu Ochrona punktu końcowego w usłudze Microsoft Defender	Zajęcia	Tomasz Skurniak	30-09-2026	10:15	12:15	02:00
11 z 29 -	Przerwa	-	30-09-2026	12:15	12:45	00:30
12 z 29 Moduł 5: Ograniczanie zagrożeń przy użyciu Microsoft Defender dla Chmury-teoria	Zajęcia	Tomasz Skurniak	30-09-2026	12:45	14:15	01:30
13 z 29 -	Przerwa	-	30-09-2026	14:15	14:30	00:15
14 z 29 Moduł 5: Ograniczanie zagrożeń przy użyciu Microsoft Defender dla Chmury - praktyka	Zajęcia	Tomasz Skurniak	30-09-2026	14:30	16:00	01:30
15 z 29 Moduł 6: Tworzenie zapytań dla usługi Microsoft Sentinel przy użyciu język zapytań Kusto (KQL)	Zajęcia	Tomasz Skurniak	01-10-2026	08:00	10:00	02:00
16 z 29 -	Przerwa	-	01-10-2026	10:00	10:15	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 29 Moduł 7: Konfigurowanie środowiska usługi Microsoft Sentinel - teoria	Zajęcia	Tomasz Skurniak	01-10-2026	10:15	12:15	02:00
18 z 29 -	Przerwa	-	01-10-2026	12:15	12:45	00:30
19 z 29 Moduł 7: Konfigurowanie środowiska usługi Microsoft Sentinel - praktyka	Zajęcia	Tomasz Skurniak	01-10-2026	12:45	14:15	01:30
20 z 29 -	Przerwa	-	01-10-2026	14:15	14:30	00:15
21 z 29 Moduł 8: Dzienniki Połączenie do usługi Microsoft Sentinel	Zajęcia	Tomasz Skurniak	01-10-2026	14:30	16:00	01:30
22 z 29 Moduł 9: Tworzenie wykryć i przeprowadzanie badań przy użyciu usługi Microsoft Sentinel - teoria	Zajęcia	Tomasz Skurniak	02-10-2026	08:00	10:00	02:00
23 z 29 -	Przerwa	-	02-10-2026	10:00	10:15	00:15
24 z 29 Moduł 9: Tworzenie wykryć i przeprowadzanie badań przy użyciu usługi Microsoft Sentinel - praktyka	Zajęcia	Tomasz Skurniak	02-10-2026	10:15	12:15	02:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
25 z 29 -	Przerwa	-	02-10-2026	12:15	12:45	00:30
26 z 29 Moduł 10: Wykonywanie wyszukiwania zagrożeń w usłudze Microsoft Sentinel - teoria	Zajęcia	Tomasz Skurniak	02-10-2026	12:45	14:15	01:30
27 z 29 -	Przerwa	-	02-10-2026	14:15	14:30	00:15
28 z 29 Moduł 10: Wykonywanie wyszukiwania zagrożeń w usłudze Microsoft Sentinel- praktyka	Zajęcia	Tomasz Skurniak	02-10-2026	14:30	15:30	01:00
29 z 29 -	Walidacja	Tomasz Skurniak	02-10-2026	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.

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 dofinasowania.
- Krok 4: Zapisanie na szkolenie poprzez platformę BUR.

Adres

ul. Pomorska 65

90-218 Łódź

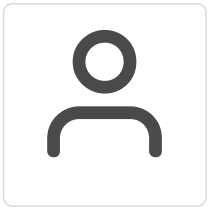
woj. łódzkie

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