Możliwość dofinansowania

NTG.pl Sp. z o.o.

4,4 / 5

5 458 ocen

Szkolenie: SC 200 Microsoft Security Operations Analyst

Numer usługi 2025/08/19/5395/2947231

Łódź / stacjonarna

Usługa szkoleniowa

28 h

09.09.2025 do 12.09.2025

2 800,00 PLN brutto

2 800,00 PLN netto

100,00 PLN brutto/h

100,00 PLN netto/h

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	Osoby odpowiedzialne za zarządzanie zagrożeniami, monitorowanie i reagowanie, korzystając z różnych rozwiązań bezpieczeństwa w całym środowisku IT.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	05-09-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	28
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Celem kursu jest nabycie umiejętności w zakresie zapobiegania zagrożeniom i zarządzania bezpieczeństwem IT przy użyciu narzędzi Microsoft, takich jak Microsoft Defender dla Endpoint, Microsoft 365 Defender, Azure Defender oraz Azure Sentinel.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zapobiega zagrożeniom przy użyciu Microsoft Defender dla Endpoint	Uczestnik potrafi wdrożyć Microsoft Defender dla Endpoint w organizacji. Uczestnik zna mechanizmy zapobiegania atakom za pomocą Defender dla Endpoint.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik zapobiega zagrożeniom przy użyciu Microsoft 365 Defender; Azure Defender.	Uczestnik potrafi wykorzystać Microsoft 365 Defender do zapobiegania zagrożeniom.Uczestnik potrafi wdrożyć i skonfigurować Azure Defender.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik konfiguruje środowiska Azure Sentinel.	Uczestnik potrafi utworzyć przestrzeń roboczą w Azure Sentinel. Uczestnik potrafi skonfigurować listy obserwowanych i wskaźniki zagrożeń.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik tworzy skoroszyty w Azure Sentinel do analizy danych.	Uczestnik potrafi tworzyć reguły analityczne i modelować ataki.	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 realizowane w godzinach dydaktycznych.

📘 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: Zapobieganie zagrożeniom przy użyciu Microsoft Defender dla Endpoint:

- Wdrażanie Microsoft Defender dla Endpoint.
- Zapobieganie atakom za pomocą Defender dla Endpoint.

Moduł 2: Zapobieganie zagrożeniom przy użyciu Microsoft 365 Defender:

- Zapobieganie atakom za pomocą Microsoft 365 Defender.

Moduł 3: Zapobieganie zagrożeniom przy użyciu Azure Defender:

- Wdrożenie Azure Defender.

Moduł 4: Tworzenie zapytań dla Azure Sentinel za pomocą języka Kusto Query Language (KQL).

- Tworzenie podstawowych zapytań KQL.
- Analiza wyników zapytań za pomocą KQL.
- Tworzenie zapytań wielotabelowych za pomocą KQL.
- Praca z danymi tekstowymi za pomocą zdań KQL.

Moduł 5: Konfigurowanie środowiska Azure Sentinel:

- Utworzenie przestrzeni roboczej Azure Sentinel.
- Utworzenie listy obserwowanych.
- Utwórzenie wskaźnika zagrożenia.

Moduł 6: Podłączanie dzienników do Azure Sentinel:

- Usługi Microsoft do Azure Sentinel.
- Hosty Windows do Azure Sentinel.
- Hosty Linux do Azure Sentinel.

Moduł 7: Tworzenie wykryć i przeprowadzanie śledztw za pomocą Azure Sentinel:

- Tworzenie reguł analitycznych.
- Modelowanie ataków w celu zdefiniowania logiki reguły.
- Zapobieganie atakom za pomocą Azure Sentinel.
- Tworzenie skoroszytów w Azure Sentinel.

Moduł 8: Neutralizacja zagrożeń w usłudze Azure Sentinel:

- Wykrywanie zagrożeń w Azure Sentinel.
- Wykrywanie zagrożeń za pomocą notatników.

Test z wynikiem generowanym automatycznie.

Harmonogram

Liczba przedmiotów/zajęć: 5

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 5 Dzień 1: Zapobieganie zagrożeniom przy użyciu Microsoft Defender dla Endpoint.;Zapobieganie zagrożeniom przy użyciu Microsoft 365 Defender	Tomasz Skurniak	09-09-2025	09:00	15:15	06:15
2 z 5 Dzień 2: Zapobieganie zagrożeniom przy użyciu Azure Defender.;Tworzenie zapytań dla Azure Sentinel za pomocą języka Kusto Query Language (KQL).	Tomasz Skurniak	10-09-2025	09:00	15:15	06:15
3 z 5 Dzień 3: Konfigurowanie środowiska Azure Sentinel	Tomasz Skurniak	11-09-2025	09:00	15:15	06:15
4 z 5 Dzień 4: Podłączanie dzienników do Azure Sentinel.	Tomasz Skurniak	12-09-2025	09:00	15:00	06:00
5 z 5 Test z wynikiem generowanym automatycznie	Tomasz Skurniak	12-09-2025	15:00	15:15	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 800,00 PLN
Koszt przypadający na 1 uczestnika netto	2 800,00 PLN

Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

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.

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.

Dlaczego wybrać firmę NTG Sp. z o.o.?

- Realizujemy szkolenia od 2002 roku.
- Mamy wyspecjalizowaną kadrę szkoleniową.
- Przeprowadzimy Ciebie przez cały proces pozyskania dofinansowania.
- Bezpłatnie pomożemy w uzyskaniu dofinansowania.
- Zaproponujemy szkolenia dopasowane do potrzeb Twojej firmy.
- Dostarczymy dokumentację szkoleniową, niezbędną do rozliczenia.
- Odpowiemy na Twoje pytania.

Adres

ul. Pomorska 65
90-218 Łódź
woj. łódzkie

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