Możliwość dofinansowania

NTG.pl Sp. z o.o.

★★★★☆

Szkolenie: SC 200 Microsoft Security Operations Analyst

Numer usługi 2025/02/10/5395/2550465

3 200,00 PLN brutto
3 200,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
32 h
22.04.2025 do 25.04.2025

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	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	17-04-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	32
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
: Zapobieganie 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
Zapobieganie zagrożeniom przy użyciu Microsoft 365 Defender Zapobieganie zagrożeniom przy użyciu Azure Defender	Uczestnik potrafi wykorzystać Microsoft 365 Defender do zapobiegania zagrożeniom.Uczestnik potrafi wdrożyć i skonfigurować Azure Defender.	Test teoretyczny z wynikiem generowanym automatycznie
Konfigurowanie 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
Tworzenie wykryć i przeprowadzanie śledztw za pomocą Azure Sentinel	Uczestnik potrafi tworzyć reguły analityczne i modelować ataki. Uczestnik potrafi tworzyć skoroszyty w Azure Sentinel do analizy danych.	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, dokument zawiera opis efektów uczenia się.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak, test w oparciu o zawarte w karcie efekty uczenia się (test teoretyczny).

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak, dokument zawiera informacje o rozdzielności szkolenia i walidacji.

Program

Całe szkolenie będzie prowadzone zamiennie: część praktyczna (laboratoria) z częścią teoretyczną. Szkolenie prowadzone w czasie rzeczywistym.

Szkolenie jest realizowane w godzinach dydaktycznych.

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.

Harmonogram

Liczba przedmiotów/zajęć: 4

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 Dzień 1: Zapobieganie zagrożeniom przy użyciu Microsoft Defender dla Endpoint.;Zapobieganie zagrożeniom przy użyciu Microsoft 365 Defender.	Wojciech Szymański	22-04-2025	09:00	15:00	06:00
2 z 4 Dzień 2: Zapobieganie zagrożeniom przy użyciu Azure Defender.;Tworzenie zapytań dla Azure Sentinel za pomocą języka Kusto Query Language (KQL).	Wojciech Szymański	23-04-2025	09:00	15:00	06:00
3 z 4 Dzień 3: Konfigurowanie środowiska Azure Sentinel; Podłączanie dzienników do Azure Sentinel.	Wojciech Szymański	24-04-2025	09:00	15:00	06:00
4 z 4 Dzień 4: Tworzenie wykryć i przeprowadzanie śledztw za pomocą Azure Sentinel; Wykrywanie zagrożeń w Azure Sentinel.	Wojciech Szymański	25-04-2025	09:00	15:00	06:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 200,00 PLN

Koszt przypadający na 1 uczestnika netto	3 200,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Wojciech Szymański

Ponad 15 lat doświadczenia w realizacji szkoleń IT jako Microsoft Certified Trainer. Prowadzenie autoryzowanych szkoleń Microsoft, dotyczących tematów związanych z SQL, Security oraz programowaniem w środowisku .NET.Wykształcenie:wyższe

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 wszystkie Twoje pytania.

Pełna oferta szkoleń dostępna na stronie: www.ntg.pl

Warunki techniczne

Zalecamy korzystanie z dodatkowego monitora, aby móc swobodnie wykonywać ćwiczenia wraz z trenerem.

Szkolenie będzie realizowane za pośrednictwem aplikacji Microsoft Teams. Link do spotkania można otworzyć za pomocą przeglądarki, nie jest wymagana instalacja aplikacji.

Do poprawnego udziału w usłudze uczestnik powinien posiadać komputer z kamerą, mikrofonem, dostępem do Internetu; szybkością pobierania i przesyłania 500 kb/s; aktualną wersje przeglądarki Microsoft Edge, Internet Explorer, Safari lub Chrome. Zalecamy posiadanie systemu operacyjnego Windows 10 oraz min. 2 GB RAM pamięci.

Kontakt

NTG.pl sp. z o.o.

E-mail ntg@ntg.edu.pl

Telefon (+48) 609 009 742