

SOFTRONIC
SPÓŁKA ZOGRANICZONĄ
ODPOWIEDZIALNOŚĆ
CIĄ

★★★★☆ 4,3 / 5

197 ocen

Szkolenie SC-200T00 Microsoft Security Operations Analyst

Numer usługi 2026/07/15/142469/3690765

- 🏠 Usługa szkoleniowa
- 📄 zdalna w czasie rzeczywistym
- 👥 Zajęcia grupowe
- 🕒 28:00 h
- 📅 25.08.2026 do 28.08.2026

4 735,50 PLN brutto
3 850,00 PLN netto
169,13 PLN brutto/h
137,50 PLN netto/h
261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Małopolski Pociąg do kariery, Kierunek - Rozwój, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	Szkolenie jest skierowane do osób, które chcą zdobyć wiedzę z zakresu badania zagrożeń, odpowiadania na nie i ich wyszukowania za pomocą platformy Microsoft Azure Sentinel, Azure Defender i Microsoft 365 Defender. Kurs jest przeznaczony dla inżynierów IT, którzy będą odpowiedzialni na łagodzenie cyberzagrożeń za pomocą tych technologii, którzy będą zajmowali się konfiguracją i korzystaniem z Azure Sentinel, będą używali języka Kusto Query Language (KQL) do wykrywania, analizy i raportowania. Kurs został zaprojektowany z myślą o osobach, które pracują na stanowisku Security Operations i pomagają uczestnikom przygotować się do egzaminu SC-200: Microsoft Security Operations Analyst. Usługa adresowana również dla Uczestników projektu Kierunek – Rozwój oraz Małopolski Pociąg do Kariery – sezon 1 oraz projektu Zachodniopomorskie Bony Szkoleniowe
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	03-08-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Cel

Cel edukacyjny

Usługa przygotowuje Uczestnika do ograniczania zagrożeń przy wykorzystaniu z usługi Microsoft 365 Defender dla punktów końcowych oraz dla chmury, do tworzenia zapytań dla Microsoft Sentinel przy użyciu języka Kusto Query Language (KQL), konfigurowania środowiska Microsoft Sentinel, łączenia dzienników z Microsoft Sentinel, tworzenia, wykrywania i przeprowadzania dochodzenia za pomocą programu Microsoft Sentinel oraz do wyszukiwania zagrożeń w Microsoft Sentinel.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opisuje podstawowe zasady ochrony przed zagrożeniami na platformie MS365.	Definiuje kluczowe elementy ochrony przed zagrożeniami na platformie MS365. Wyjaśnia, jak Microsoft 365 Defender chroni przed incydentami. Identyfikuje podstawowe zagrożenia związane z tożsamością w Azure AD.	Test teoretyczny z wynikiem generowanym automatycznie
Ogranicza i eliminuje zagrożenia przy użyciu różnych usług Microsoft Defender.	Wdraża i konfiguruje Microsoft Defender for Office 365. Korzysta z Microsoft Defender for Identity do ochrony infrastruktury. Zabezpiecza aplikacje i usługi w chmurze za pomocą Microsoft Defender for Cloud Apps.	Test teoretyczny z wynikiem generowanym automatycznie
Reaguje na alerty i zarządza incydentami dotyczącymi bezpieczeństwa danych.	Konfiguruje i zarządza politykami DLP w Microsoft 365. Zarządza ryzykiem wewnętrznym przy użyciu Microsoft Purview. Wykorzystuje funkcje inspekcji do badania zagrożeń w Microsoft 365 Defender i Purview.	Test teoretyczny z wynikiem generowanym automatycznie
Wdraża i zarządza Microsoft Defender for Endpoint.	Konfiguruje ulepszenia zabezpieczeń systemu Windows. Przeprowadza badania i analizy urządzeń oraz podmiotów w Microsoft Defender for Endpoint. Zarządza automatyzacją i alertami bezpieczeństwa w Microsoft Defender for Endpoint.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Planuje i zabezpiecza obciążenia w chmurze przy użyciu Microsoft Defender for Cloud. Tworzy i analizuje zapytania przy użyciu języka KQL w Microsoft Sentinel.	Podłącza elementy Azure i spoza platformy Azure do Microsoft Defender for Cloud. Zarządza poziomem zabezpieczeń w chmurze. Koryguje alerty zabezpieczeń przy użyciu Microsoft Defender for Cloud. Tworzy instrukcje KQL dla Microsoft Sentinel. Analizuje wyniki zapytań KQL. Tworzy instrukcje wielu tabel przy użyciu języka KQL	Test teoretyczny z wynikiem generowanym automatycznie Test teoretyczny z wynikiem generowanym automatycznie
Zarządza danymi i analizami zagrożeń w Microsoft Sentinel.	Tworzy i zarządza obszarami roboczymi w Microsoft Sentinel. Używa obserwowanych list i rejestrów zapytań. Wykorzystuje analizę zagrożeń do identyfikacji i zarządzania incydentami bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Podłącza różne dane i źródła zagrożeń do Microsoft Sentinel.	Nawiązuje połączenia między usługami Microsoft a Microsoft Sentinel. Łączy hosty Windows i logi Common Event Format z Microsoft Sentinel. Integruje wskaźniki zagrożeń z Microsoft Sentinel.	Test teoretyczny z wynikiem generowanym automatycznie
Wykrywa zagrożenia i automatyzuje procesy bezpieczeństwa w Microsoft Sentinel.	Wykorzystuje zadania wyszukiwania i notesy do wyszukiwania zagrożeń. Automatyzuje procesy wykrywania i reagowania na zagrożenia. Zarządza zawartością i normalizacją danych w Microsoft Sentinel.	Test teoretyczny z wynikiem generowanym automatycznie
Przeprowadza zaawansowane badania i zarządza zagrożeniami w ekosystemie Microsoft 365.	Przeprowadza badania zagrożeń przy użyciu funkcji inspekcji w Microsoft 365 Defender. Korzysta z wyszukiwania zawartości w Microsoft Purview do badania zagrożeń. Wdraża zabezpieczenia i rozwiązuje problemy z bezpieczeństwem w ekosystemie Microsoft 365.	Test teoretyczny z wynikiem generowanym automatycznie
Współpracuje z innymi członkami zespołu w organizacji, korzystając z narzędzi do pracy grupowej w celu realizacji wyznaczonego celu lub projektu.	Identyfikuje wyzwania związane z wyznaczonym celem, planuje etapy ich realizacji, monitoruje ich wykonanie oraz ocenia ich efektywność. Współdzieli informacje z innym współpracownikami i wykorzystuje narzędzia do pracy nad danymi w ramach zespołów.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

Pytanie 2. Czy dokument lub wyrażnie 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 wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie **SC-200T00 Microsoft Security Operations Analyst** jest przeznaczone dla analityków IT którzy chcą zdobyć wiedzę z zakresu badania zagrożeń, odpowiadania na nie oraz ich wyszukiwania za pomocą platformy Microsoft Azure Sentinel, Azure Defender i Microsoft 365 Defender. Kurs jest przeznaczony dla inżynierów IT, którzy będą odpowiedzialni na łagodzenie cyberzagrożeń za pomocą tych technologii, którzy będą zajmowali się konfiguracją i korzystaniem z Azure Sentinel, będą używali języka Kusto Query Language (KQL) do wykrywania, analizy i raportowania. Kurs został zaprojektowany z myślą o osobach, które pracują na stanowisku Security Operations i pomaga uczestnikom przygotować się do egzaminu SC-200: Microsoft Security Operations Analyst.

W celu przystąpienia do szkolenia Uczestnik powinien znać w stopniu podstawowym platformę Microsoft 365, produkty firmy Microsoft związane z zabezpieczeniami, zgodnością i tożsamością. Powinien również posiadać znajomość systemu Windows 10, usług platformy Azure, w szczególności Azure SQL Database i Azure Storage, maszyn wirtualnych platformy Azure i sieci wirtualnych. Uczestnik powinien również rozumieć podstawowe pojęcia związane ze skryptami.

Szkolenie składa się z wykładu wzbogaconego o prezentację. W trakcie szkolenia każdy Uczestnik wykonuje indywidualne ćwiczenia - laboratoria, dzięki czemu zyskuje praktyczne umiejętności. W trakcie szkolenia omawiane jest również studium przypadków, w którym Uczestnicy wspólnie wymieniają się doświadczeniami. Nad case-study czuwa autoryzowany Trener, który przekazuje informację na temat przydatnych narzędzi oraz najlepszych praktyk do rozwiązania omawianego zagadnienia.

Aby Uczestnik osiągnął zamierzony cel szkolenia niezbędne jest wykonanie przez niego zadanych laboratoriów.

Przed rozpoczęciem szkolenia Uczestnik rozwiązuje pre-test badający poziom wiedzy na wstępie.

Walidacja: Na koniec usługi Uczestnik wykonuje post-test w celu dokonania oceny wzrostu poziomu wiedzy. Test teoretyczny z wynikiem generowanym automatycznie.

STRUKTURA KURSU:

Kurs trwa 28 godzin i jest realizowany w ciągu 4 dni, na platformie Microsoft Teams, na żywo z trenerem.

Program szkolenia:

Wprowadzenie do ochrony przed zagrożeniami na platformie Microsoft 365

Ograniczanie incydentów przy użyciu usługi Microsoft 365 Defender

Ochrona tożsamości za pomocą usługi Azure AD Identity Protection

Eliminowanie zagrożeń za pomocą usługi Microsoft Defender dla usługi Office 365

Ochrona infrastruktury dzięki usłudze Microsoft Defender for Identity

Zabezpieczanie aplikacji i usług w chmurze dzięki usłudze Microsoft Defender w Cloud Apps

Reagowanie na alerty dotyczące zapobiegania utracie danych przy użyciu platformy Microsoft 365

Zarządzanie ryzykiem wewnętrznym w usłudze Microsoft Purview

Badanie zagrożeń przy użyciu funkcji inspekcji w usługach Microsoft 365 Defender i Microsoft Purview Standard

Badanie zagrożeń przy użyciu inspekcji w usługach Microsoft 365 Defender i Microsoft Purview (Premium)

Badanie zagrożeń za pomocą funkcji wyszukiwania zawartości w usłudze Microsoft Purview

Ochrona przed zagrożeniami za pomocą usługi Microsoft Defender for Endpoint

Wdrażanie Microsoft Defender dla punktów końcowych

Wdrażanie ulepszeń zabezpieczeń systemu Windows za pomocą programu Microsoft Defender Endpoint

Przeprowadzanie badań urządzenia w programie Microsoft Defender w Endpoint

Wykonywanie działań na urządzeniu przy użyciu usługi Microsoft Defender w Endpoint

Wykonywanie analiz elementów i podmiotów przy użyciu usługi Microsoft Defender for Endpoint

Konfigurowanie automatyzacji i zarządzanie nią przy użyciu programu Microsoft Defender for Endpoint

Konfigurowanie alertów i wykrywania w usłudze Microsoft Defender w Microsoft Defender for Endpoint

Wykorzystanie zarządzania podatnościami na zagrożenia w usłudze Microsoft Defender Endpoint

Planowanie ochrony obciążeń w chmurze przy użyciu usługi Microsoft Defender for Cloud

Podłączanie elementów Azure do usługi Microsoft Defender for Cloud

Łączenie elementów spoza platformy Azure z usługą Microsoft Defender for Cloud

Zarządzanie poziomem zabezpieczeń w chmurze

Wyjaśnienie ochrony obciążeń w chmurze w usłudze Microsoft Defender for Cloud

Korygowanie alertów zabezpieczeń przy użyciu usługi Microsoft Defender for Cloud

Konstruowanie instrukcji KQL dla usługi Microsoft Sentinel

Analizowanie wyników zapytań przy użyciu języka KQL

Tworzenie instrukcji wielu tabel przy użyciu języka KQL

Praca z danymi w usłudze Microsoft Sentinel przy użyciu języka zapytań Kusto

Wprowadzenie do Microsoft Sentinel

Tworzenie obszarów roboczych Microsoft Sentinel i zarządzanie nimi

Rejestry zapytań w Microsoft Sentinel

Używanie obserwowanych list w Microsoft Sentinel

Wykorzystywanie analizy zagrożeń w usłudze Microsoft Sentinel

Podłączanie danych do platformy Microsoft Sentinel przy użyciu łączników danych

Nawiązywanie połączeń między usługami firmy Microsoft a usługą Microsoft Sentinel

Nawiązywanie połączenia między usługą Microsoft 365 Defender a usługą Microsoft Sentinel

Łączenie hostów Windows z usługą Microsoft Sentinel

- Połączenie logów Common Event Format z usługą Microsoft Sentinel
 - Możliwość łączenia źródeł danych syslog z usługą Microsoft Sentinel
 - Łączenie z programem Microsoft Sentinel wskaźników zagrożeń
 - Wykrywanie zagrożeń za pomocą analizy Microsoft Sentinel
 - Automatyzacja w Microsoft Sentinel
 - Zarządzanie incydentami bezpieczeństwa w Microsoft Sentinel
 - Identyfikowanie zagrożeń za pomocą analizy behawioralnej
 - Normalizacja danych w usłudze Microsoft Sentinel
 - Zapytania, wizualizacja i monitorowanie danych w usłudze Microsoft Sentinel
 - Zarządzanie zawartością w usłudze Microsoft Sentinel
 - Wyjaśnienie koncepcji wykrywania zagrożeń w usłudze Microsoft Sentinel
 - Wykrywanie zagrożeń za pomocą Microsoft Sentinel
 - Używanie zadań wyszukiwania w usłudze Microsoft Sentinel
 - Wyszukiwanie zagrożeń przy użyciu notesów w usłudze Microsoft Sentinel
- SOFTRONIC Sp. z o. o. zastrzega sobie prawo do zmiany terminu szkolenia lub jego odwołania w przypadku niezebrania się minimalnej liczby Uczestników tj. 3 osób.*

Harmonogram

Liczba pozycji harmonogramu: 29

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 29 Ograniczanie zagrożeń przy użyciu usługi Microsoft 365 Defender (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	25-08-2026	09:00	10:30	01:30
2 z 29 -	Przerwa	-	25-08-2026	10:30	10:45	00:15
3 z 29 Ograniczanie zagrożeń przy użyciu usługi Microsoft 365 Defender (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	25-08-2026	10:45	12:15	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 29 -	Przerwa	-	25-08-2026	12:15	12:45	00:30
5 z 29 Ograniczanie zagrożeń przy użyciu usługi Microsoft Defender for Endpoint (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	25-08-2026	12:45	14:15	01:30
6 z 29 -	Przerwa	-	25-08-2026	14:15	14:30	00:15
7 z 29 Ograniczanie zagrożeń przy użyciu usługi Microsoft Defender for Endpoint (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	25-08-2026	14:30	16:00	01:30
8 z 29 Ograniczanie zagrożeń przy użyciu usługi Microsoft Defender for Cloud (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	26-08-2026	09:00	10:30	01:30
9 z 29 -	Przerwa	-	26-08-2026	10:30	10:45	00:15
10 z 29 Ograniczanie zagrożeń przy użyciu usługi Microsoft Defender for Cloud (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	26-08-2026	10:45	12:15	01:30
11 z 29 -	Przerwa	-	26-08-2026	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 29 Tworzenie zapytań dla Microsoft Sentinel przy użyciu języka Kusto Query Language (KQL)(on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	26-08-2026	12:45	14:15	01:30
13 z 29 -	Przerwa	-	26-08-2026	14:15	14:30	00:15
14 z 29 Tworzenie zapytań dla Microsoft Sentinel przy użyciu języka Kusto Query Language (KQL) (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	26-08-2026	14:30	16:00	01:30
15 z 29 Konfigurowanie środowiska MS Sentinel (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	27-08-2026	09:00	10:30	01:30
16 z 29 -	Przerwa	-	27-08-2026	10:30	10:45	00:15
17 z 29 Konfigurowanie środowiska MS Sentinel (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	27-08-2026	10:45	12:15	01:30
18 z 29 -	Przerwa	-	27-08-2026	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 29 Łącznie dzienników z MS Sentinel (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	27-08-2026	12:45	14:15	01:30
20 z 29 -	Przerwa	-	27-08-2026	14:15	14:30	00:15
21 z 29 Łącznie dzienników z MS Sentinel (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	27-08-2026	14:30	16:00	01:30
22 z 29 Wykrywanie i badanie zagrożeń przy użyciu usługi Microsoft Sentinel (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	28-08-2026	09:00	10:30	01:30
23 z 29 -	Przerwa	-	28-08-2026	10:30	10:45	00:15
24 z 29 Wykrywanie i badanie zagrożeń przy użyciu usługi Microsoft Sentinel (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	28-08-2026	10:45	12:15	01:30
25 z 29 -	Przerwa	-	28-08-2026	12:15	12:45	00:30
26 z 29 Neutralizacja zagrożeń w usłudze Microsoft Sentinel (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	28-08-2026	12:45	14:15	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
27 z 29 -	Przerwa	-	28-08-2026	14:15	14:30	00:15
28 z 29 Neutralizacja zagrożeń w usłudze Microsoft Sentinel (online, na żywo, wykład + ćwiczenia)	Zajęcia	Tomasz Skurniak	28-08-2026	14:30	15:45	01:15
29 z 29 -	Walidacja	-	28-08-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	28:00
w tym suma godzin zajęć	23:45
w tym suma godzin walidacji	00:15
w tym suma przerw	04:00
Suma godzin dydaktycznych bez przerw	32:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 735,50 PLN
Koszt przypadający na 1 uczestnika netto	3 850,00 PLN

Koszt osobogodziny brutto	169,13 PLN
---------------------------	------------

Koszt osobogodziny netto	137,50 PLN
--------------------------	------------

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
---------------	---------------

Liczba godzin zegarowych usługi	28:00
---------------------------------	-------

Prowadzący

Liczba prowadzących: 1



1 z 1

Tomasz Skurniak

Certyfikowany trener Microsoft (MCT). Specjalizuje się w szkoleniach z zakresu Baz Danych, Programowania w języku .NET oraz C#, Azur, Windows Server oraz Power BI. Jest twórcą szkoleń z zakresu Baz danych MS SQL oraz Oracle. Posiada ponad 20-letnie doświadczenie w prowadzeniu autoryzowanych szkoleń dla specjalistów IT. Ukończył studia wyższe na Politechnice Poznańskiej zdobywając dyplom magistra inżyniera. Zrealizował szkolenia dla setek Klientów z sektora publicznego oraz prywatnego co potwierdzają liczne referencje.

Doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat przed datą wprowadzenia szczegółowych danych dotyczących oferowanej usługi.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu uczestnikowi zostaną przekazane autoryzowane materiały szkoleniowe, które są dostępne na koncie uczestnika na dedykowanym portalu. Uczestnik uzyskuje również dostęp do laboratoriów Microsoft.

Warunki uczestnictwa

W celu przystąpienia do szkolenia Uczestnik powinien znać w stopniu podstawowym platformę Microsoft 365, produkty firmy Microsoft związane z zabezpieczeniami, zgodnością i tożsamością. Powinien również posiadać znajomość systemu Windows 10, usług platformy Azure, w szczególności Azure SQL Database i Azure Storage, maszyn wirtualnych platformy Azure i sieci wirtualnych. Uczestnik powinien również rozumieć podstawowe pojęcia związane ze skryptami.

Informacje dodatkowe

Istnieje możliwość zastosowania zwolnienia z podatku VAT dla szkoleń mających charakter kształcenia zawodowego lub służących przekwalifikowaniu zawodowemu pracowników, których poziom dofinansowania ze środków publicznych wynosi co najmniej 70% (na podstawie § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. zmieniające rozporządzenie w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r. poz. 1722 ze zm.))

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój;

Zawarto umowę z WUP w Szczecinie na świadczenie usług rozwojowych z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu Zachodniopomorskie Bony Szkoleniowe

Usługa skierowana również o Uczestników Projektu MP.

kompetencja związana z cyfrową transformacją;

UWAGA! Przed dokonaniem zgłoszenia / złożeniem wniosku o dofinansowanie prosimy o kontakt z SOFTRONIC w celu potwierdzenia terminu szkolenia: softtronic@softtronic.pl

Warunki techniczne

Szkolenie realizowane jest w formule distance learning - szkolenie **on-line w czasie rzeczywistym**, w którym możesz wziąć udział z każdego miejsca na świecie.

Szkolenie odbywa się za pośrednictwem platformy **Microsoft Teams**, która umożliwia transmisję dwukierunkową, dzięki czemu Uczestnik może zadawać pytania i aktywnie uczestniczyć w dyskusji. Uczestnik, który potwierdzi swój udział w szkoleniu, przed rozpoczęciem szkolenia, drogą mailową, otrzyma link do spotkania wraz z hasłami dostępu.

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 20Mb/s.
- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/głośniki oraz mikrofon i **kamerę**.
- zainstalowana przeglądarka internetowa - Microsoft Edge/ Internet Explorer 10+ / **Google Chrome** 39+ (sugerowana) / Safari 7+
- aplikacja MS Teams może zostać zainstalowana na komputerze lub można z niej korzystać za pośrednictwem przeglądarki internetowej

Kontakt



AGATA WOJCIECHOWSKA

E-mail agata.wojciechowska@softtronic.pl

Telefon (+48) 618 658 840