Możliwość dofinansowania

Szkolenie "Microsoft Cybersecurity Architect"

Numer usługi 2026/06/18/120967/3635978

3 198,00 PLN brutto
2 600,00 PLN netto
114,21 PLN brutto/h
92,86 PLN netto/h
332,00 PLN cena rynkowa

ALTKOM AKADEMIA SPÓŁKA AKCYJNA

4,4 / 5

2 715 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
28:00 h
15.09.2026 do 18.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Identyfikatory projektów	Kierunek - Rozwój
Grupa docelowa usługi	Usługa szkoleniowa adresowana jest do administratorów bezpieczeństwa i specjalistów IT z zaawansowanym doświadczeniem w inżynierii bezpieczeństwa, w szczególności do osób posiadających wiedzę w obszarach tożsamości i dostępu, ochrony platformy, operacji bezpieczeństwa, zabezpieczania danych oraz zabezpieczania aplikacji, a także do profesjonalistów z doświadczeniem we wdrożeniach hybrydowych i chmurowych. Wymagane przygotowanie uczestników: co najmniej 2-letnie doświadczenie w zakresie zarządzania infrastrukturą Active Directory, 2-letnie doświadczenie w zakresie zarządzania środowiskiem chmurowym, znajomość technologii zabezpieczeń i zgodności Microsoft, znajomość pojęć związanych z ochroną informacji, średniozaawansowaną znajomość systemu Windows 10/11 oraz umiejętność korzystania z anglojęzycznych materiałów.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	04-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestnika do projektowania architektury bezpieczeństwa na platformie Microsoft zgodnie z najlepszymi praktykami oraz priorytetami bezpieczeństwa.
Po szkoleniu Uczestnik identyfikuje proces projektowania strategii i architektury Zero Trust, rozróżnia elementy oceny strategii technicznych i operacji bezpieczeństwa w zakresie zarządzania ryzykiem, a także dobiera podstawowe założenia projektowania bezpieczeństwa dla infrastruktury, danych i aplikacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Uczestnik szkolenia identyfikuje podstawowe założenia architektury bezpieczeństwa Microsoft oraz modelu Zero Trust.	– Wskazuje filary technologii Zero Trust.	Test teoretyczny z wynikiem generowanym automatycznie
	– Rozróżnia znaczenie Cloud Adoption Framework i Well-Architected Framework w projektowaniu bezpieczeństwa.	Test teoretyczny
	– Identyfikuje podstawowe elementy strategii bezpieczeństwa.	Test teoretyczny
WIEDZA: Uczestnik szkolenia rozróżnia obszary projektowania bezpieczeństwa dla infrastruktury, tożsamości, aplikacji i danych.	– Wskazuje elementy projektowania rozwiązań do zarządzania tożsamością i dostępem.	Test teoretyczny
	– Rozróżnia wymagania bezpieczeństwa dla SaaS, PaaS i IaaS.	Test teoretyczny
	– Identyfikuje podstawowe elementy zabezpieczania aplikacji, Microsoft 365 i danych.	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik szkolenia dobiera podstawowe rozwiązania wspierające bezpieczeństwo tożsamości, dostępu i uprzywilejowanego administrowania.	– Wskazuje zasady projektowania rozwiązań dla sekretów, kluczy i certyfikatów.	Test teoretyczny
	– Rozróżnia strategie uwierzytelniania, autoryzacji i dostępu warunkowego.	Test teoretyczny
	– Identyfikuje elementy projektowania rozwiązań dla dostępu uprzywilejowanego i zarządzania tożsamością.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
UMIEJĘTNOŚCI: Uczestnik szkolenia analizuje podstawowe rozwiązania z zakresu operacji bezpieczeństwa, infrastruktury i ochrony punktów końcowych. KOMPETENCJE SPOŁECZNE: Uczestnik szkolenia dostrzega znaczenie spójnego podejścia do projektowania bezpieczeństwa oraz odpowiedzialności za odporność środowiska organizacji.	– Wskazuje elementy projektowania rozwiązań dla GRC, Microsoft Sentinel i Microsoft Defender XDR.	Test teoretyczny
	– Rozróżnia rozwiązania dotyczące środowisk hybrydowych, wielochmurowych i sieciowych.	Test teoretyczny
	– Identyfikuje podstawowe wymagania bezpieczeństwa dla punktów końcowych, urządzeń mobilnych, IoT i zdalnego dostępu.	Test teoretyczny
	– Wskazuje znaczenie wspierania odporności biznesowej i ochrony przed typowymi cyberzagrożeniami.	Test teoretyczny
	– Rozróżnia znaczenie bezpiecznych praktyk projektowych dla ochrony infrastruktury, aplikacji i danych.	Test teoretyczny
	– Identyfikuje potrzebę ciągłego doskonalenia stanu bezpieczeństwa i zgodności środowiska.	Test teoretyczny

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

Adresaci szkolenia

Usługa szkoleniowa adresowana jest do administratorów bezpieczeństwa i specjalistów IT z zaawansowanym doświadczeniem w inżynierii bezpieczeństwa, w szczególności do osób posiadających wiedzę w obszarach tożsamości i dostępu, ochrony platformy, operacji bezpieczeństwa, zabezpieczania danych oraz zabezpieczania aplikacji, a także do profesjonalistów z doświadczeniem we wdrożeniach hybrydowych i chmurowych.

Wymagane przygotowanie uczestników: co najmniej 2-letnie doświadczenie w zakresie zarządzania infrastrukturą Active Directory, 2-letnie doświadczenie w zakresie zarządzania środowiskiem chmurowym, znajomość technologii zabezpieczeń i zgodności Microsoft, znajomość pojęć związanych z ochroną informacji, średniozaawansowaną znajomość systemu Windows 10/11 oraz umiejętność korzystania z anglojęzycznych materiałów.

Warunki organizacyjne

- Szkolenie realizowane jest w formule **zdalnej w czasie rzeczywistym**, z wykorzystaniem platformy wideokonferencyjnej (Zoom).
- Grupa szkoleniowa liczy maksymalnie 12 uczestników, co pozwala na interaktywną pracę (dyskusje, prace w mniejszych grupach) w komfortowych warunkach.
- Każdy uczestnik powinien dysponować własnym stanowiskiem komputerowym z dostępem do Internetu – **dostawca usługi nie zapewnia sprzętu ani pomieszczenia do udziału w szkoleniu.**
- Materiały szkoleniowe (np. prezentacje) są udostępniane w formie elektronicznej na dedykowanej platformie Altkom Akademii (dostęp wysyłany mailowo uczestnikom przed rozpoczęciem szkolenia).
- Efekty uczenia się zostaną zweryfikowane poprzez walidację w formie testu teoretycznego, ostatniego dnia usługi tj. testu jednokrotnego wyboru.
- **Uwaga: Cena nie zawiera egzaminu SC-100.**

Szkolenie obejmuje:

- podręcznik w formie elektronicznej dostępny na platformie https://learn.microsoft.com/pl-pl/training/
- dostęp do portalu słuchacza Altkom Akademii
- szkolenie prowadzone w formie prezentacji
- demonstracje trenera
- ćwiczenia praktyczne w formie case studies

PROGRAM SZKOLENIA

1. Projektowanie rozwiązań zgodnych z najlepszymi praktykami i priorytetami w zakresie bezpieczeństwa
   - Wprowadzenie do Zero Trust i najlepszych praktyk
     - Inicjatywy Zero Trust RaMP
     - Filary technologii Zero Trust
     - Projektowanie rozwiązań zgodne z Cloud Adoption Framework (CAF) i Well-Architected Framework (WAF)
     - Definiowanie strategii bezpieczeństwa
   - Wprowadzenie do Cloud Adoption Framework
     - Cloud Adoption Framework — bezpieczna metodologia
     - Wprowadzenie do Azure Landing Zones
     - Projektowanie zabezpieczeń dzięki Azure Landing Zones
     - Wprowadzenie do Well Architected Framework
     - Well Architected Framework — filar bezpieczeństwa
     - Rozwiązania z CAF i WAF
   - Projektowanie rozwiązań zgodnych z Microsoft Cybersecurity Reference Architecture (MCRA) i Microsoft Cloud Security Benchmark (MCSB)
     - Wprowadzenie do MCRA i MCSB
     - Projektowanie rozwiązań z najlepszymi praktykami dotyczącymi możliwości i kontroli
     - Projektowanie rozwiązań z najlepszymi praktykami ochrony przed atakami
     - Strategia odporności na typowe cyberzagrożenia, takie jak ransomware
     - Typowe cyberzagrożenia i wzorce ataków
     - Wspieranie odporności biznesowej
     - Ochrona przed oprogramowaniem ransomware
     - Konfiguracje bezpiecznego tworzenia kopii zapasowych i przywracania
     - Aktualizacje zabezpieczeń

2. Projektowanie zabezpieczeń, tożsamości i zgodności
   - Projektowanie rozwiązania pod kątem zgodności z przepisami
     - Wprowadzenie do zgodności z przepisami
     - Przekształcanie wymagań dotyczących zgodności w rozwiązanie zabezpieczające
     - Spełnianie wymagań dotyczących zgodności z Purview
     - Spełnianie wymagań dotyczących prywatności z Priva
     - Użycie Azure Policy, aby spełnić wymagania dotyczące bezpieczeństwa i zgodności
     - Ocena zgodności infrastruktury za pomocą usługi Microsoft Defender for Cloud

   - Projektowanie rozwiązań do zarządzania tożsamością i dostępem
     - Projektowanie rozwiązania do zarządzania sekretami, kluczami i certyfikatami
     - Wprowadzenie do zarządzania tożsamością i dostępem
     - Projektowanie strategii dostępu do chmury, hybrydy i wielu chmur (w tym Azure AD)
     - Projektowanie rozwiązania dla tożsamości zewnętrznych
     - Projektowanie nowoczesnych strategii uwierzytelniania i autoryzacji
     - Dostosowywanie dostępu warunkowego i Zero Trust

   - Projektowanie rozwiązań zapewniających dostęp uprzywilejowany
     - Wprowadzenie do dostępu uprzywilejowanego
     - Model dostępu korporacyjnego
     - Projektowanie rozwiązania do zarządzania tożsamością
     - Projektowanie rozwiązania do zabezpieczenia administrowania tenantami
     - Projektowanie do zarządzania uprawnieniami do infrastruktury chmury (CIEM)
     - Projektowanie rozwiązania dla stacji roboczych z dostępem uprzywilejowanym i usługi bastion

   - Projektowanie rozwiązań dla operacji bezpieczeństwa
     - Wprowadzenie do operacji bezpieczeństwa (SecOps)
     - Projektowanie możliwości operacji bezpieczeństwa w środowiskach hybrydowych i wielochmurowych
     - Projektowanie scentralizowanego rejestrowania i inspekcji
     - Projektowanie rozwiązań SIEM
     - Projektowanie rozwiązania do wykrywania i reagowania
     - Projektowanie rozwiązania dla SOAR
     - Projektowanie przepływów pracy związanych z bezpieczeństwem
     - Projektowanie zasięgu wykrywania zagrożeń

3. Projektowanie rozwiązań zabezpieczających aplikacje i dane
   - Projektowanie rozwiązania do zabezpieczania platformy Microsoft 365
     - Zabezpieczenia dla Exchange, Sharepoint, OneDrive i Teams (M365)
     - Ocena stanu zabezpieczeń dla obciążeń związanych ze współpracą i produktywnością
     - Projektowanie rozwiązań Microsoft Defender 365
     - Projektowanie konfiguracji oraz praktyki operacyjne dla M365

   - Projektowanie rozwiązań do zabezpieczania aplikacji
     - Wprowadzenie do bezpieczeństwa aplikacji
     - Projektowanie i wdrażanie standardu w celu bezpiecznego rozwoju aplikacji
     - Ocena stanu zabezpieczeń istniejących aplikacji
     - Projektowanie strategii cyklu życia bezpieczeństwa dla aplikacji
     - Bezpieczny dostęp do tożsamości
     - Projektowanie rozwiązania do zarządzania API
     - Projektowanie rozwiązania zapewniającego bezpieczny dostęp do aplikacji

   - Projektowanie rozwiązania do zabezpieczania danych organizacji
     - Wprowadzenie do bezpieczeństwa danych
     - Projektowanie rozwiązania do wykrywania i klasyfikowania danych za pomocą Microsoft Purview
     - Projektowanie rozwiązania do ochrony danych w spoczynku, danych w ruchu i danych w użyciu
     - Bezpieczeństwo danych w obciążeniach platformy Azure
     - Zabezpieczenia usługi Azure Storage
     - Defender dla SQL i Defender dla pamięci masowej

4. Projektowanie rozwiązań bezpieczeństwa dla infrastruktury
   - Określanie wymagań dotyczących zabezpieczania usług SaaS, PaaS i IaaS
     - Zabezpieczanie SaaS, PaaS i Iaas (model współdzielonej odpowiedzialności)
     - Punkty bazowe bezpieczeństwa dla usług w chmurze
     - Określanie wymagań bezpieczeństwa dla obciążeń internetowych
     - Określanie wymagań bezpieczeństwa dla kontenerów i orkiestracji kontenerów

- Projektowanie rozwiązania do zarządzania stanem bezpieczeństwa w środowiskach hybrydowych i wielochmurowych
  - Wprowadzenie do środowisk hybrydowych i wielochmurowych
  - Ocena postawy za pomocą MCSB
  - Projektowanie zarządzania postawą i ochroną obciążeń w środowiskach hybrydowych i wielochmurowych
  - Omówienie oceny postawy za pomocą Defender for Cloud
  - Ocena postawy za pomocą bezpiecznego wyniku usługi Microsoft Defender for Cloud
  - Projektowanie rozwiązania do ochrony obciążeń w chmurze, które korzystają z usługi Microsoft Defender for Cloud
  - Projektowanie rozwiązania do integracji środowisk hybrydowych i wielochmurowych przy użyciu usługi Azure Arc
  - Zarządzanie zewnętrzną powierzchnią ataku
- Projektowanie rozwiązań do zabezpieczania punktów końcowych serwerów i klientów
  - Wprowadzenie do bezpieczeństwa punktów końcowych
  - Określanie wymagań bezpieczeństwa serwera i linii bazowych
  - Określanie wymagań dotyczących urządzeń mobilnych i klientów
  - Określanie wymagań dotyczących bezpieczeństwa IoT i urządzeń wbudowanych
  - Microsoft Defender dla IoT
  - Określanie linii bazowych zabezpieczeń dla punktów końcowych serwera i klienta
  - Projektowanie rozwiązania dla bezpiecznego zdalnego dostępu
- Projektowanie rozwiązań dla bezpieczeństwa sieci
  - Projektowanie rozwiązań segmentacji sieci
  - Projektowanie rozwiązania do filtrowania ruchu z sieciowymi grupami zabezpieczeń
  - Projektowanie rozwiązań do zarządzania stanem sieci
  - Projektowanie rozwiązań do monitorowania sieci

5. Projektowanie rozwiązań zgodnych z najlepszymi praktykami i priorytetami w zakresie bezpieczeństwa
   - Studium przypadku
6. Projektowanie operacji zabezpieczeń, tożsamości i możliwości zgodności
   - Studium przypadku
7. Projektowanie rozwiązań zabezpieczających aplikacje i dane
   - Studium przypadku
8. Projektowanie rozwiązań bezpieczeństwa dla infrastruktury
   - Studium przypadku

Walidacja

Język

- Szkolenie: polski
- Materiały: angielski

Harmonogram

Liczba pozycji harmonogramu: 29

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 29 **Projektowanie rozwiązań zgodnych z najlepszymi praktykami i priorytetami w zakresie bezpieczeństwa_wykład**	Zajęcia	Norbert Blonkowski	15-09-2026	09:00	10:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 29 -	Przerwa	-	15-09-2026	10:30	10:45	00:15
3 z 29 Zero Trust, Cloud Adoption Framework, Well-Architected Framework i strategia bezpieczeństwa_wykład + ćwiczenia praktyczne	Zajęcia	Norbert Blonkowski	15-09-2026	10:45	12:45	02:00
4 z 29 -	Przerwa	-	15-09-2026	12:45	13:15	00:30
5 z 29 Strategia odporności, ransomware, kopie zapasowe i aktualizacje zabezpieczeń _wykład + ćwiczenia praktyczne	Zajęcia	Norbert Blonkowski	15-09-2026	13:15	15:00	01:45
6 z 29 -	Przerwa	-	15-09-2026	15:00	15:15	00:15
7 z 29 Ocena stanu zabezpieczeń i zgodności infrastruktury _wykład	Zajęcia	Norbert Blonkowski	15-09-2026	15:15	16:00	00:45
8 z 29 Projektowanie rozwiązań do zarządzania tożsamością i dostępem_wykład	Zajęcia	Norbert Blonkowski	16-09-2026	09:00	10:30	01:30
9 z 29 -	Przerwa	-	16-09-2026	10:30	10:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 29 Sekrety, klucze, certyfikaty, strategie dostępu i tożsamości zewnętrzne_wykład + ćwiczenia praktyczne	Zajęcia	Norbert Blonkowski	16-09-2026	10:45	12:45	02:00
11 z 29 -	Przerwa	-	16-09-2026	12:45	13:15	00:30
12 z 29 Uwierzytelnianie, autoryzacja, dostęp warunkowy i Zero Trust_wykład + ćwiczenia praktyczne	Zajęcia	Norbert Blonkowski	16-09-2026	13:15	15:00	01:45
13 z 29 -	Przerwa	-	16-09-2026	15:00	15:15	00:15
14 z 29 Dostęp uprzywilejowany i zabezpieczenie administrowania tenantami_wykład	Zajęcia	Norbert Blonkowski	16-09-2026	15:15	16:00	00:45
15 z 29 Projektowanie rozwiązań dla operacji bezpieczeństwa_wykład	Zajęcia	Norbert Blonkowski	17-09-2026	09:00	10:30	01:30
16 z 29 -	Przerwa	-	17-09-2026	10:30	10:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 29 Strategie GRC, Microsoft Sentinel, Defender XDR oraz wykrywanie i reagowanie_wykład + ćwiczenia praktyczne	Zajęcia	Norbert Blonkowski	17-09-2026	10:45	12:45	02:00
18 z 29 -	Przerwa	-	17-09-2026	12:45	13:15	00:30
19 z 29 SOAR, przepływy pracy bezpieczeństwa i zasięg wykrywania zagrożeń_wykład + ćwiczenia praktyczne	Zajęcia	Norbert Blonkowski	17-09-2026	13:15	15:00	01:45
20 z 29 -	Przerwa	-	17-09-2026	15:00	15:15	00:15
21 z 29 Projektowanie rozwiązań zabezpieczających aplikacje i dane_wykład	Zajęcia	Norbert Blonkowski	17-09-2026	15:15	16:00	00:45
22 z 29 Zabezpieczanie platformy Microsoft 365, aplikacji oraz danych_wykład + ćwiczenia praktyczne	Zajęcia	Norbert Blonkowski	18-09-2026	09:00	10:30	01:30
23 z 29 -	Przerwa	-	18-09-2026	10:30	10:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
24 z 29 Bezpieczeństwo infrastruktury SaaS, PaaS i IaaS oraz środowisk hybrydowych i wielochmurowych_wykład + ćwiczenia praktyczne	Zajęcia	Norbert Blonkowski	18-09-2026	10:45	12:45	02:00
25 z 29 -	Przerwa	-	18-09-2026	12:45	13:15	00:30
26 z 29 Bezpieczeństwo punktów końcowych, IoT i rozwiązań sieciowych_wykład + ćwiczenia praktyczne	Zajęcia	Norbert Blonkowski	18-09-2026	13:15	15:00	01:45
27 z 29 -	Przerwa	-	18-09-2026	15:00	15:15	00:15
28 z 29 Podsumowanie materiału i przygotowanie do walidacji_test_wykład	Zajęcia	Norbert Blonkowski	18-09-2026	15:15	15:30	00:15
29 z 29 -	Walidacja	-	18-09-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	28:00
w tym suma godzin zajęć	23:30
w tym suma godzin walidacji	00:30
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	3 198,00 PLN
Koszt przypadający na 1 uczestnika netto	2 600,00 PLN
Koszt osobogodziny brutto	114,21 PLN
Koszt osobogodziny netto	92,86 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	28:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Norbert Blonkowski

"Trener posiada wykształcenie wyższe techniczne w zakresie informatyki oraz systemów komputerowych, zdobyte na Wydziale Techniki Morskiej Politechniki Szczecińskiej. Od wielu lat specjalizuje się w prowadzeniu szkoleń z technologii Microsoft, w szczególności w zakresie infrastruktury, bezpieczeństwa oraz rozwiązań chmurowych. Jako certyfikowany trener Microsoft (MCT) oraz posiadacz licznych certyfikatów branżowych, m.in. Microsoft Certified Azure Administrator Associate, prowadzi szkolenia techniczne dla administratorów, inżynierów i specjalistów IT.

Od 2017 roku współpracuje z Altkom Akademią, gdzie realizuje szkolenia z zakresu Microsoft Azure,

Active Directory, Windows Server, SCCM, Microsoft 365, PKI i zabezpieczeń IT. Posiada wieloletnie doświadczenie w realizacji szkoleń dla partnerów i dystrybutorów IT oraz firm z różnych branż, zarówno komercyjnych, jak i publicznych. Wspiera również projekty wdrożeniowe i konsultacyjne związane z infrastrukturą IT i cyberbezpieczeństwem. Dodatkowo, posiada poświadczenia bezpieczeństwa umożliwiające dostęp do informacji niejawnych, także na poziomie UE i NATO. Jego praktyczne doświadczenie, ugruntowane certyfikacjami i pracą projektową, przekłada się na wysoką jakość prowadzonych szkoleń. W ciągu ostatnich 5 lat przeszkolił z Altkom Akademią ponad 1000 osób."

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na platformie Wirtualna Klasa Altkom Akademii udostępnione zostaną bezterminowo materiały szkoleniowe (tj. np. podręczniki/prezentacje/materiały dydaktyczne niezbędne do odbycia szkolenia/ebooki itp.), zasoby bazy wiedzy portalu oraz dodatkowe informacje od trenera. Uczestnicy zachowują bezterminowy dostęp do zasobów Mojej Akademii i materiałów szkoleniowych zgromadzonych w Wirtualnej Klasie szkolenia. Platforma do kontaktu z trenerami, grupą i całą społecznością absolwentów jest portal Moja Akademia.

Warunki uczestnictwa

1. Niezbędnym warunkiem uczestnictwa w szkoleniach dofinansowanych z funduszy europejskich jest założenie konta w Bazie Usług Rozwojowych, zapis na szkolenie za pośrednictwem Bazy oraz spełnienie warunków przedstawionych przez danego Operatora, dysponenta funduszy publicznych.
2. Przez uczestnictwo w usłudze rozwojowej rozumie się aktywny udział Uczestnika w szkoleniu wyłącznie przy włączonej kamerze skierowanej na osobę uczestniczącą i umożliwiającej jej identyfikację.
3. Warunkiem uznania uczestnictwa w szkoleniu jest obecność podczas co najmniej 80% czasu trwania szkolenia (lub zgodnie z warunkami określonymi w umowie z Operatorem). Uczestnik, który nie spełni tego wymagania, traktowany jest jako nieobecny.
4. Frekwencja będzie potwierdzana na podstawie raportów logowań z platformy Zoom oraz bieżącej obserwacji uczestnika przez trenera.
5. Ogólne warunki uczestnictwa w szkoleniach Altkom Akademii zamieszczone są na stronie: https://www.altkomakademia.pl/ogolne-warunki-uczestnictwa-w-szkoleniach/

Informacje dodatkowe

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

Kompetencja związana z cyfrową transformacją

Po szkoleniu uczestnik otrzyma zaświadczenie o ukończeniu szkolenia.

Uwaga! W przypadku, gdy liczba zapisów na szkolenie nie osiągnie minimalnej liczby Uczestników, usługa może zostać niezrealizowana.

Informacja dot. podatku VAT:

Zwolnienie z podatku VAT może mieć zastosowanie wyłącznie w przypadku spełnienia przesłanek określonych w art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług – w przypadku finansowania usługi w całości ze środków publicznych – albo w § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień – w przypadku finansowania usługi w co najmniej 70% ze środków publicznych. W przypadku zastosowania zwolnienia obowiązuje cena netto, a w pozostałych przypadkach doliczany jest VAT 23%.

Warunki techniczne

Wymagania ogólne realizacji szkolenia w formule distance learning (online):

Komputer stacjonarny lub notebook wyposażony w mikrofon, głośniki i kamerę internetową z przeglądarką internetową z obsługą HTML 5. Monitor o rozdzielczości FullHD. Szerokopasmowy dostęp do Internetu o przepustowości co najmniej 25/5 (download/upload) Mb/s. W przypadku szkoleń z laboratoriami zalecamy: sprzęt wyposażony w dwa ekrany o rozdzielczości minimum HD (lub dwa komputery), kamerę internetową USB, zewnętrzne głośniki lub słuchawki.

Informacje oraz wymagania dotyczące uczestniczenia w szkoleniach w formule zdalnej dostępne na: https://www.altkomakademia.pl/distance-learning/#FAQ

Platforma komunikacji – ZOOM

Oprogramowanie – zdalny pulpit, aplikacja ZOOM

Link do szkolenia zgodnie z regulaminem zostanie wysłany na 2 dni przed rozpoczęciem usługi.

Link do szkolenia jest ważny w trakcie trwania całej usługi szkoleniowej.

Kontakt

AGNIESZKA SIPURA

E-mail agnieszka.sipura@altkom.pl
Telefon (+48) 609 191 281