



ASSECO DATA
SYSTEMS SPÓŁKA
AKCYJNA

★★★★☆ 4,4 / 5

152 oceny

Cyber Security Foundation (S_52138) - TERMIN GWARANTOWANY

Numer usługi 2026/03/07/7629/3388102

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 24 h

📅 20.04.2026 do 22.04.2026

2 632,20 PLN brutto

2 140,00 PLN netto

109,68 PLN brutto/h

89,17 PLN netto/h

196,00 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Pracownicy działów IT Szefowie i pracownicy działów bezpieczeństwa (CISO /CSO) Audytorzy bezpieczeństwa IT Osoby odpowiedzialne za administrowanie sieciami i systemami IT Eksperti odpowiedzialni za ciągłość działania i zarządzanie kryzysowe Szefowie działów audytu Konsultanci i eksperci bezpieczeństwa informacji Menedżerowie i specjaliści z działów zarządzania ryzykiem Menedżerowie i dyrektorzy IT Eksperti IT Governance.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	13-04-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24

Cel

Cel edukacyjny

Celem szkolenia jest zapoznanie uczestników z podstawami zarządzania cyberbezpieczeństwem w organizacji, w tym z głównymi zagrożeniami, metodami cyberataków, technikami cyberobrony oraz podstawowymi regulacjami w obszarze bezpieczeństwa informacji. Uczestnicy poznają zasady organizacji systemu cyberbezpieczeństwa oraz rolę zarządzania ryzykiem i reagowania na incydenty w kontekście wymagań regulacyjnych i dobrych praktyk.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Uczestnik opisuje podstawowe pojęcia z zakresu cyberbezpieczeństwa oraz współczesne zagrożenia i techniki cyberataków.	Wyjaśnia pojęcia związane z cyberbezpieczeństwem (np. incydent, podatność, zagrożenie) Rozpoznaje podstawowe typy cyberataków Wskazuje przykłady zagrożeń dla systemów informatycznych i danych Opisuje podstawowe elementy SZBI	Test teoretyczny
WIEDZA: Uczestnik wyjaśnia zasady zarządzania cyberbezpieczeństwem w organizacji oraz rolę regulacji i standardów w tym obszarze.	Wskazuje rolę zarządzania ryzykiem i reagowania na incydenty Identyfikuje przykłady regulacji i dobrych praktyk w obszarze cyberbezpieczeństwa	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik identyfikuje podstawowe zagrożenia cyberbezpieczeństwa w organizacji.	Analizuje przykładowe scenariusze zagrożeń cybernetycznych Wskazuje potencjalne podatności w systemach lub procesach Określa możliwe skutki incydentów bezpieczeństwa	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik wskazuje podstawowe działania służące zapobieganiu incydentom cyberbezpieczeństwa.	Proponuje działania ograniczające ryzyko cyberzagrożeń Wskazuje przykłady środków organizacyjnych i technicznych zwiększających bezpieczeństwo Omawia podstawowe zasady reagowania na incydenty	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
KOMPETECJE SPOŁECZNE: Uczestnik dostrzega znaczenie cyberbezpieczeństwa dla funkcjonowania organizacji.	Wskazuje wpływ incydentów cyberbezpieczeństwa na działalność organizacji Uzasadnia potrzebę stosowania zasad bezpieczeństwa informacji Identyfikuje rolę pracowników w budowaniu bezpieczeństwa cyfrowego	Test teoretyczny
KOMPETECJE SPOŁECZNE: Uczestnik wykazuje odpowiedzialność za stosowanie zasad bezpieczeństwa informacji w swojej pracy.	Stosuje podstawowe zasady bezpiecznego korzystania z systemów informatycznych Identyfikuje sytuacje mogące prowadzić do naruszenia bezpieczeństwa informacji Proponuje działania wspierające budowanie kultury cyberbezpieczeństwa w organizacji	Test teoretyczny

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

- Wprowadzenie do kursu
- Podstawowe terminy stosowane w zarządzaniu cyberbezpieczeństwem
- Zarządzanie ryzykiem, zgodnością (compliance)
- Zapewnienie ciągłości działania i odtwarzanie po awarii
- Zarządzanie bezpieczeństwem zasobów i danych
- Bezpieczeństwo sieci i komunikacji

- Zarządzanie tożsamością i użytkownikami
- Kryptografia i PKI
- Malware i bezpieczeństwo stacji końcowej (end-point security)
- Zarządzanie podatnościami (Vulnerability management)
- Bezpieczeństwo fizyczne i regulacyjne
- Polityki, procedury, standardy i rekomendacje bezpieczeństwa
- Szkolenia i podnoszenie świadomości cyberbezpieczeństwa
- Ataki i inżynieria socjalna (social engineering)
- Bezpieczeństwo urządzeń mobilnych
- Podsumowanie szkolenia

Harmonogram

Liczba przedmiotów/zajęć: 16

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Wprowadzenie do kursu	academy@assecods.pl	20-04-2026	09:00	09:15	00:15
2 z 16 Podstawowe terminy stosowane w zarządzaniu cyberbezpieczeństwem	academy@assecods.pl	20-04-2026	09:15	10:30	01:15
3 z 16 Zarządzanie ryzykiem, zgodnością (compliance)	academy@assecods.pl	20-04-2026	10:30	11:45	01:15
4 z 16 Zapewnienie ciągłości działania i odtwarzanie po awarii	academy@assecods.pl	20-04-2026	11:45	13:00	01:15
5 z 16 Zarządzanie bezpieczeństwem zasobów i danych	academy@assecods.pl	20-04-2026	13:00	14:15	01:15
6 z 16 Bezpieczeństwo sieci i komunikacji	academy@assecods.pl	20-04-2026	14:15	15:30	01:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 16 Zarządzanie tożsamością i użytkownikami	academy@assec ods.pl	21-04-2026	09:00	10:15	01:15
8 z 16 Kryptografia i PKI	academy@assec ods.pl	21-04-2026	10:15	11:30	01:15
9 z 16 Malware i bezpieczeństwo stacji końcowej (end-point security)	academy@assec ods.pl	21-04-2026	11:30	12:45	01:15
10 z 16 Zarządzanie podatnościami (Vulnerability management)	academy@assec ods.pl	21-04-2026	12:45	14:00	01:15
11 z 16 Bezpieczeństwo fizyczne i regulacyjne	academy@assec ods.pl	21-04-2026	14:00	15:30	01:30
12 z 16 Polityki, procedury, standardy i rekomendacje bezpieczeństwa	academy@assec ods.pl	22-04-2026	09:00	10:30	01:30
13 z 16 Szkolenia i podnoszenie świadomości cyberbezpieczeństwa	academy@assec ods.pl	22-04-2026	10:30	12:00	01:30
14 z 16 Ataki i inżynieria socjalna (social engineering)	academy@assec ods.pl	22-04-2026	12:30	14:00	01:30
15 z 16 Bezpieczeństwo urządzeń mobilnych	academy@assec ods.pl	22-04-2026	14:00	15:15	01:15
16 z 16 Podsumowanie szkolenia	academy@assec ods.pl	22-04-2026	15:15	15:30	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 632,20 PLN
Koszt przypadający na 1 uczestnika netto	2 140,00 PLN
Koszt osobogodziny brutto	109,68 PLN
Koszt osobogodziny netto	89,17 PLN

Prowadzący

Liczba prowadzących: 2



1 z 2

academy@assecods.pl

Trener z co najmniej 5 letnim doświadczeniem w prowadzeniu szkoleń, w tym z obszaru merytorycznego, którego dotyczy. W przypadku szkoleń akredytowanych i autoryzowanych nasi trenerzy posiadają stosowne uprawnienia do ich prowadzenia.



2 z 2

Koordinator walidacji efektów uczenia się

Pracownik Asseco Academy, który przeprowadza i zarządza procesem walidacji efektów uczenia w oparciu o przygotowane narzędzia diagnostyczne

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

W cenie uczestnik otrzymuje

- Udział w 3-dniowym szkoleniu #cyberSecurity Foundation prowadzonym na żywo przez trenera eksperta ds. cyberbezpieczeństwa
- Komplet materiałów szkoleniowych #cyberSecurity Foundation w wersji elektronicznej
- Zaświadczenie Asseco Academy o ukończeniu szkolenia.

Organizacja szkolenia

- Rodzaj szkolenia: otwarte lub dla grup zamkniętych
- Forma realizacji: stacjonarnie lub zdalnie
- Język szkolenia: polski
- Język materiałów: polski
- Wielkość grupy: do 20 uczestników

Organizacja szkolenia w Wirtualnej Klasie

- Szkolenie jest realizowane w godz. 9:00-15:30
- Każdy uczestnik powinien dokonać rejestracji do zdalnej sesji szkoleniowej w godz. 8:30-8:50
- W trakcie dnia szkoleniowego przewidujemy kilka przerw, w tym 60-minutową na lunch, a także po każdej godzinie szkolenia 10-minutowe przerwy; szczegółowy rozkład przerw każdy trener ustala indywidualnie z grupą
- Jedna godzina lekcyjna to 45 minut
- Komplet akredytowanych materiałów szkoleniowych dystrybuowany jest w formie elektronicznej.

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową <https://academy.assecod.pl/szkolenie/cyber-security-foundation/> w celu rezerwacji miejsca.

UWAGA! Dla usług z dofinansowaniem powyżej 70% istnieje możliwość wystawienia faktury ZW VAT. Prosimy o kontakt z Biurem Assecod Academy academy@assecods.pl. Natomiast w przypadku dofinansowania usługi poniżej 70% ze środków publicznych, usługa nie jest zwolniona z podatku VAT. Należy wówczas doliczyć do usługi szkoleniowej należny VAT w wysokości 23%.

Warunki techniczne

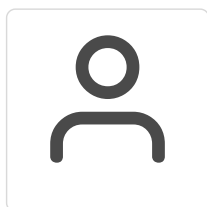
Szkolenie prowadzone jest w formie zdalnej na żywo za pośrednictwem aplikacji Webex Meeting. Aby wziąć udział, konieczne jest posiadanie urządzenia takiego jak komputer stacjonarny, laptop wyposażonego w stabilne połączenie internetowe oraz mikrofon i kamerę. Przed rozpoczęciem szkolenia uczestnicy będą mieli możliwość przetestowania swojego sprzętu podczas sesji próbnej, aby upewnić się, że połączenie internetowe, mikrofon i kamera/słuchawki działają poprawnie.

Minimalne wymagania sprzętowo-systemowe:

- Komputer PC z systemem Windows 7 lub nowszym, Mac OS 10.13 lub nowszym. Istnieje możliwość korzystania z innych systemów, w tym Linux. Szczegółowe informacje można uzyskać pod adresem: <https://help.webex.com/en-us/nki3xrq/Webex-Meetings-Suite-SystemRequirements>.
- Przeglądarka internetowa (zalecamy korzystanie z Chrome lub Firefox).
- Karta LAN: min. 100 MBPS lub stabilne połączenie WiFi (zalecamy połączenie do sieci „kablem”). Nie dopuszcza się udziału w szkoleniu za pośrednictwem łącz GSM/LTE. Zalecane pasmo, to przynajmniej 2 MB/s (download i upload). W przypadku spadku przepustowości łącza poniżej 1,2 MB/s należy liczyć się z istotnym obniżeniem jakości połączenia.
- Mikrofon i głośniki (zalecamy korzystanie z zestawu typu headset).
- Kamera internetowa.

Przed szkoleniem każdy uczestnik otrzyma na podany adres email link do platformy, gdzie odbędzie się szkolenie. Uczestnictwo w szkoleniu umożliwia aktywne uczestnictwo w zajęciach, w tym komunikację z trenerem oraz pozostałymi uczestnikami. Umożliwia to wymianę doświadczeń oraz aktywny kontakt zarówno z grupą, jak i prowadzącym. Dodatkowo, uczestnicy mają dostęp do funkcji czatu online, co jeszcze bardziej ułatwia interakcję.

Kontakt



Alicja Kozłowska

E-mail bur-szkolenia@assecods.pl

Telefon (+48) 801 303 030