Możliwość dofinansowania

Cyberbezpieczeństwo w przedsiębiorstwie

Numer usługi 2026/05/21/47095/3575383

2 000,00 PLN brutto
2 000,00 PLN netto
125,00 PLN brutto/h
125,00 PLN netto/h
284,58 PLN cena rynkowa

ADN AKADEMIA spółka z ograniczoną odpowiedzialnością spółka komandytowa

4,6 / 5

385 ocen

Usługa szkoleniowa
zdalna
16:00 h
10.07.2026 do 19.07.2026

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Grupa docelowa usługi	Odbiorcami szkolenia są osoby kluczowe dla bezpieczeństwa informacji w organizacjach, w tym: • Menedżerowie i właściciele firm dążący do zwiększenia odporności organizacji na cyberzagrożenia. • Dyrektorzy IT oraz administratorzy systemów odpowiedzialni zaochronę infrastruktury. • Specjaliści ds. compliance, bezpieczeństwa i ryzyka. • Kierownicy działów operacyjnych, HR i marketingu pracujący z danymiwrażliwymi klientów. • Przedsiębiorcy i startupowcy wdrażający nowoczesne rozwiązania cyfrowe.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	09-07-2026
Forma prowadzenia usługi	zdalna
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Celem szkolenia jest nabycie przez uczestników praktycznej wiedzy i umiejętności w zakresie identyfikowania oraz przeciwdziałania cyberzagrożeniom w środowisku biznesowym. Uczestnik przygotuje się do aktywnego podejmowania decyzji w sytuacjach kryzysowych oraz wdrożenia skutecznych polityk bezpieczeństwa w przedsiębiorstwie przy wykorzystaniu nowoczesnych narzędzi e-learningowych

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje rodzaje zagrożeń i potrafi ocenić ryzyko cyberataków w swojej branży	Poprawne zidentyfikowanie min. 80%przedstawionych w case studyschematów ataków oraz wskazanie ryzyk specyficznych dla sektora działalności firmy.	Test teoretyczny z wynikiem generowanym automatycznie
Zna metody ochrony infrastruktury IT oraz danych wrażliwych	Wskazanie właściwych narzędzi i technologii zabezpieczających infrastrukturę (firewalle, szyfrowanie, systemy backupu) adekwatnych do zadanych scenariuszy	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje zasady bezpiecznej pracy w sieci i korzystania z urządzeń mobilnych	Poprawne rozwiązanie symulacji zachowania pracownika w publicznej sieci Wi-Fi oraz konfiguracja zabezpieczeń urządzenia mobilnego	Test teoretyczny z wynikiem generowanym automatycznie
Integruje bezpieczeństwo z procesami biznesowymi i łańcuchem dostaw	Prawidłowe wskazanie punktów styku procesów biznesowych z wymogami bezpieczeństwa w analizowanym modelu firmy	Test teoretyczny z wynikiem generowanym automatycznie
Tworzy procedury reagowania na incydenty i plan ciągłości działania	Opracowanie (w formie wyboru gotowych komponentów) poprawnej sekwencji działań w przypadku wystąpienia incydentu ransomware.	Test teoretyczny z wynikiem generowanym automatycznie
Rozumie obowiązki prawne dotyczące ochrony danych i raportowania incydentów	Wykazanie się znajomością terminów raportowania incydentów orazpodmiotów odpowiedzialnych zgodnie z aktualnymi regulacjami (np. RODO, KSC)	Test teoretyczny z wynikiem generowanym automatycznie
Buduje kulturę cyberbezpieczeństwa wśród pracowników	Zaproponowanie co najmniej trzech działań edukacyjnych dla personelu podnoszących świadomość zagrożeń	Test teoretyczny z wynikiem generowanym automatycznie
Potrafi wdrożyć polityki bezpieczeństwa i monitorować ich skuteczność	Uzyskanie pozytywnego wyniku z testu końcowego obejmującego zagadnienia monitoringu i wdrażania polityk	Test teoretyczny z wynikiem generowanym automatycznie

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

1.Wprowadzenie do cyberbezpieczeństwa w biznesie (2h):

Podstawowe pojęcia, znaczenie bezpieczeństwa dla ciągłości biznesu.

2.Identyfikacja i klasyfikacja zagrożeń (2h):

Przegląd aktualnych metod ataków (phishing, vishing, socjotechnika).

3.Ochrona infrastruktury IT i danych (2h):

Techniczne aspekty zabezpieczeń serwerów, baz danych i stacji roboczych.

4.Bezpieczne korzystanie z sieci i urządzeń (2h):

Zasady pracy zdalnej, higiena haseł, bezpieczeństwo urządzeń mobilnych.

5.Cyberbezpieczeństwo w zarządzaniu procesami biznesowymi (2h):

Bezpieczeństwo w relacjach z dostawcami i wewnątrz procesówfirmowych.

6.Reagowanie na incydenty i plan ciągłości działania (2h):

Procedury po wystąpieniu ataku, minimalizacja strat, backupy.

7.Aspekty prawne i regulacyjne (2h):

Obowiązki przedsiębiorcy wynikające z przepisów krajowych i unijnych.

8.Budowanie kultury bezpieczeństwa w organizacji (2h):

Szkolenie pracowników, polityki „clean desk”, rola czynnika ludzkiego.

Szkolenie realizowane jest w modelu e-learningowym, co pozwala uczestnikowi na elastyczne zarządzanie czasem nauki. Średni czas potrzebny na realizację programu to 16 godzin.

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 000,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	2 000,00 PLN
Koszt osobogodziny brutto	125,00 PLN
Koszt osobogodziny netto	125,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

skrypty PDF, karty pracy, szablony BPMN-lite, checklisty wdrożeniowe, mini-poradniki narzędzi, quizy

Warunki uczestnictwa

podstawowa obsługa komputera; doświadczenie w prowadzeniu działalności/organizacji — rekomendowane, nieobowiązkowe

Informacje dodatkowe

Usługa Szkoleniowa została stworzona na podstawie licencji pełnej Edu Narzędzia zakupionej z dofinansowaniem projektu "USŁUGIROZWOJOWE 4.0 – wsparcie podmiotów BUR w obszarze tworzenia, rozwoju i sprzedaży nowych form usług rozwojowych lub wykorzystaniu nowych technologii" nr FERS.01.03-IP.09-0015/23.

Warunki techniczne

- Komputer lub laptop z dostępem do stabilnego łącza internetowego.
- Sprawna kamera internetowa oraz mikrofon (wymagane do aktywnego uczestnictwa w warsztatach).
- Przeglądarka internetowa obsługująca środowisko chmurowe EduNarzędzia.
- Dostęp do konta e-mail w celu otrzymania linków do wersji demo narzędzi AI.

Kontakt

Marta Michalak

E-mail marta.michalak@adn.pl

Telefon (+48) 509 358 891