



MASTER NIS2 kurs wideo - wdrożenie standardów cyberbezpieczeństwa w praktyce

Numer usługi 2025/07/15/7909/2881033

1 105,77 PLN brutto
899,00 PLN netto
184,30 PLN brutto/h
149,83 PLN netto/h

APEXNET SPÓŁKA
Z OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ SPÓŁKA
KOMANDYTOWA

★★★★★ 4,7 / 5

23 oceny

📍 zdalna

🏠 Usługa szkoleniowa

🕒 6 h

📅 06.08.2025 do 04.11.2025

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

1. osoby odpowiedzialne za wdrażanie i stosowanie Dyrektywy NIS2 w organizacji, w tym menedżerowie IT, ds. bezpieczeństwa informacji, audytorzy „compliance” menedżerowie;

2. wszyscy, którzy chcą zrozumieć, jak skutecznie wdrażać i stosować Dyrektywę NIS2.

Usługa również adresowana jest dla uczestników projektu Małopolski Pociąg do Kariery-sezon 1 realizowany przez WUP w Krakowie

Minimalna liczba uczestników

1

Maksymalna liczba uczestników

100

Data zakończenia rekrutacji

04-08-2025

Forma prowadzenia usługi

zdalna

Liczba godzin usługi

6

Podstawa uzyskania wpisu do BUR

Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Kurs przygotowuje uczestników do praktycznego wdrożenia wymagań Dyrektywy NIS2 w organizacji. Szkolenie skupia się na identyfikacji podmiotów objętych przepisami, zarządzaniu ryzykiem w kontekście łańcucha dostaw, wdrażaniu środków bezpieczeństwa informacji, reagowaniu na incydenty cyberbezpieczeństwa oraz zapewnianiu ciągłości działania usług kluczowych i istotnych zgodnie z wymaganiami NIS2.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje podmioty objęte Dyrektywą NIS2 oraz ich obowiązki	Uczestnik poprawnie wskazuje, które organizacje podlegają NIS2 i wymienia ich kluczowe obowiązki zgodnie z dyrektywą oraz projektem ustawy o KSC.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje wymagane normy i standardy w zakresie cyberbezpieczeństwa (ISO, NIST, MITRE)	Uczestnik poprawnie przyporządkowuje normy (np. ISO/IEC 27001, ISO 19011, NIST 800-53A) do etapów wdrażania NIS2 oraz podaje przykłady ich praktycznego zastosowania.	Test teoretyczny z wynikiem generowanym automatycznie
Ocenia ryzyko cyberbezpieczeństwa w organizacji, w tym w łańcuchu dostaw	Uczestnik potrafi wskazać zagrożenia i podatności, określić wpływ i prawdopodobieństwo oraz zaproponować działania zaradcze w kontekście dostawców usług i komponentów IT.	Test teoretyczny z wynikiem generowanym automatycznie
Planuje działania zgodne z NIS2 w zakresie zarządzania incydentami i zapewnienia ciągłości działania	Uczestnik tworzy schemat postępowania w przypadku incydentu oraz opisuje działania zapewniające ciągłość usług zgodnie z normą ISO 22301 i wymaganiami NIS2.	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

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?

Program

I Wstęp do Szkolenia

1. Cel Szkolenia
2. 3 kluczowe zagadnienia Szkolenia
3. Opis przebiegu Szkolenia
4. Dla kogo jest to Szkolenie
5. Prowadzący Szkolenie
6. Zasady: I.A.N.Y.L. i T.I.N.L.A.

II. LEKCJA 1: WPROWADZENIE DO NIS2D, CZYLI IGNORANTIA LEGIS NON EXCUSAT

1. Przyczyny uchwalenia NIS2D
2. Dyrektywa a Rozporządzenie w regulacjach UE
3. Motywy a artykuły w regulacjach EU
4. Główne założenia nowelizacji ustawy o KSC
5. Dyrektywa NIS2 a ochrona danych osobowych

III. LEKCJA 2: POWODY WDRAŻANIA NIS2D, CZYLI DLACZEGO ROBIMY POŻYTECZNĄ RZECZ

1. Korzyści z wdrożenia NIS2D
2. Harmonizacja wymagań bezpieczeństwa
3. Bezpieczeństwo a złożoność systemów
4. Rozwijanie kultury zarządzania ryzykiem
5. Inne regulacje UE powiązane z NIS2D
6. Rola nowych technologii w stosowaniu NIS2D

IV. LEKCJA 3: POJĘCIA I DEFINICJE, KTÓRE TRZEBA ZNAC, CZYLI NAUKA WYRAZÓW OBCYCH

1. Art. 6 Dyrektywy NIS2
2. Art. 2 projektu ustawy o Krajowym Systemie Cyberbezpieczeństwa
3. Norma PN-EN ISO/IEC 27000: Systemy zarządzania bezpieczeństwem informacji
4. Norma PN-EN ISO/IEC 19011: Wytyczne dot. audytowania systemów zarządzania

V. LEKCJA 4: STOSOWANIE PRZYJĘTYCH NORM I STANDARDÓW, CZYLI NAJLEPSZE PRAKTYKI BEZPIECZEŃSTWA

1. Norma ISO 19011
2. Norma ISO 27001
3. Norma ISO22301
4. Standard NIST 800-12
5. Standard NIST 800-37
6. Standard NIST 800-53A
7. Model MITRE Att@ck: Techniki, praktyki, procedury

VI. LEKCJA 5: NOWE ZAGADNIENIA W NIS2D A ICH WPLYW NA WDROŻENIE I STOSOWANIE DYREKTYWY

1. Cyberhigiena i szkolenia
2. Zarządzanie łańcuchem dostaw
3. Ryzyko łańcucha dostaw i dostawcy usług cybersec
4. Nowy zakres podmiotowy
5. Potrzeby "Małych i Średnich" przedsiębiorstw w zakresie cyberbezpieczeństwa

VII. LEKCJA 6: PRZYGOTOWANIE DO WDROŻENIA DYREKTYWY NIS2, CZYLI DOBRY PLAN TERAZ JEST LEPSZY NIŻ NAJLEPSZY PLAN ZA PÓŹNO

1. Inwentaryzacja zasobów
2. Klasyfikacja informacji
3. Audyt zgodnie z ISO19011

VIII. LEKCJA 7: WSPIERANIE I ROZWIJANIE KULTURY ZARZĄDZANIA RYZYKIEM, CZYLI „RÓŻNE ODCIENIE SZAROŚCI”

1. Identyfikacja ryzyka :Podatności, zagrożenia, zabezpieczenia
2. Ocena ryzyka: Ustalenie prawdopodobieństwa i wpływu
3. Postępowanie z ryzykiem: Wynik analizy ma „różne odcienie szarości”

IX. LEKCJA 8: MONITOROWANIE CIĄGŁOŚCI DZIAŁANIA I ZGODNOŚCI Z NIS2, CZYLI PROCES CIĄGŁY

1. Ciągłość działania: ISO 22301, ITIL
2. Monitorowanie skuteczności zabezpieczeń: Analiza i raportowanie
3. Monitorowanie zgodności z NIS2D: Audyty i kontrole

X. LEKCJA 9: ZARZĄDZANIE INCYDENTAMI, CZYLI DLACZEGO TRZEBA BYĆ PRZYGOTOWANYM NA NAJGORSZE SCENARIUSZE

1. Rodzaje ataków: sieciowe, aplikacyjne, systemowe
2. Obsługa incydentów
3. Kultura zgłaszania podatności

XI. LEKCJA 10: Omówienie „Szablону sprawozdania z audytu zgodnego z ustawą o krajowym systemie cyberbezpieczeństwa”

1. Metryka dokumentu
2. Poziom istotności niezgodności
3. 10 obszarów audytu
4. Wybrane listy kontrolne: Gotowe przepisy na zgodność

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 105,77 PLN
Koszt przypadający na 1 uczestnika netto	899,00 PLN
Koszt osobogodziny brutto	184,30 PLN
Koszt osobogodziny netto	149,83 PLN

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Dostępność materiałów:

- Materiały dostępne są 24 godziny na dobę przez cały okres trwania dostępu.
- Uczestnik może wielokrotnie odtwarzać poszczególne lekcje w ramach przyznanego okresu dostępu.
- Na platformie dostępne są materiały szkoleniowe w formie nagrań wideo, plików PDF, prezentacji lub innych materiałów dydaktycznych, w zależności od lekcji.

Uczestnik otrzymuje:

- EduBox, czyli paczkę materiałów wysłaną pocztą
- Roczny dostęp do EduStrefy
- Certyfikat ukończenia szkolenia

Warunki uczestnictwa

ZGŁOSZENIE NA USŁUGĘ

Rezerwacji miejsca szkoleniowego można dokonać za pośrednictwem BUR.

Informacje dodatkowe

zaakceptowano Regulamin dla instytucji szkoleniowych.

Egzamin/Test weryfikujący nabycie kwalifikacji – w cenie szkolenia (brak dodatkowej opłaty).

Koszt wydania certyfikatu/zaświadczenia – wliczony w cenę szkolenia.

Po zakończeniu usługi uczestnik otrzyma certyfikat.

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa prawna stawki zwolnionej: Rozporządzenie Ministra finansów z 20 grudnia 2013 w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2020r.poz.1983 z 10.11.2020) § 3 pkt 1 ust. 14

Warunki techniczne

Kurs realizowany jest w formie **zdalnej (e-learningowej)** za pośrednictwem platformy szkoleniowej **EduStrefa**.

Organizacja dostępu:

- W dniu nadania dostępu generowany jest indywidualny link aktywacyjny z danymi logowania.
- Dane dostępowe przekazywane są uczestnikowi drogą elektroniczną na wskazany adres e-mail.
- Uczestnik ma możliwość rozpoczęcia nauki w dowolnym momencie w okresie aktywnego dostępu.

Warunki techniczne:

- Dostęp do platformy EduStrefa odbywa się przez przeglądarkę internetową.
- Wymagania techniczne po stronie uczestnika:
 - urządzenie umożliwiające połączenie z Internetem (komputer, laptop, tablet lub smartfon),
 - aktualna wersja przeglądarki internetowej (zalecane: Google Chrome, Mozilla Firefox, Microsoft Edge, Safari),
 - stałe i stabilne połączenie internetowe o minimalnej prędkości 5 Mb/s,
 - aktywny adres e-mail do przesłania danych logowania.

Dostępność materiałów:

- Materiały dostępne są 24 godziny na dobę przez cały okres trwania dostępu.
- Uczestnik może wielokrotnie odtwarzać poszczególne lekcje w ramach przyznanego okresu dostępu.
- Na platformie dostępne są materiały szkoleniowe w formie nagrań wideo, plików PDF, prezentacji lub innych materiałów dydaktycznych, w zależności od lekcji.

Wsparcie techniczne:

- W przypadku problemów technicznych uczestnik ma zapewnione wsparcie techniczne drogą mailową lub telefoniczną (dane kontaktowe przekazywane są wraz z danymi dostępowymi).

Kontakt

Aleksandra Wlazło



E-mail aleksandra.wlazlo@apexnet.pl

Telefon (+48) 222 058 902