Możliwość dofinansowania

Cyberbezpieczeństwo w praktyce – NIS2 / UoKSC, Cyber Resilience Act CRA, SZBI, ISO 27001 - wymagania dla podmiotów oraz produktów ICT na lata 2026 - 2028

Numer usługi 2026/06/01/204299/3601243

899,00 PLN brutto
899,00 PLN netto
112,38 PLN brutto/h
112,38 PLN netto/h
261,33 PLN cena rynkowa

LT MASTERY SZKOLENIA DLA BIZNESU PIOTR SZYMCZYK

Brak ocen dla tego dostawcy

- Usługa szkoleniowa
- zdalna w czasie rzeczywistym
- Zajęcia grupowe
- 08:00 h
- 16.06.2026 do 16.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Akademia HR, FELB.06.03-IZ.00-0003/24 ZIPH, FELB.06.08-IZ.00-0017/25, FELB.06.08-IZ.00-0083/24
Grupa docelowa usługi	Szkolenie skierowane jest do osób odpowiedzialnych za bezpieczeństwo informacji, zgodność z regulacjami oraz zarządzanie ryzykiem cybernetycznym w organizacji. Obejmuje zarówno aspekty prawno-organizacyjne, jak i techniczne, ze szczególnym uwzględnieniem ról decyzyjnych kadry kierowniczej i specjalistów IT/OT. Usługa adresowana jest do: • specjalistów ds. bezpieczeństwa informacji i IT (CISO, IT Manager, Security Officer) • kadry kierowniczej odpowiedzialnej za zgodność z przepisami (Compliance, Risk Manager, Prezes/Dyrektor) • inżynierów i architektów systemów odpowiedzialnych za produkty z elementami cyfrowymi (IoT, OT, systemy wbudowane, OZE) • pracowników działów prawnych i compliance obsługujących wdrożenie NIS2 / UoKSC / CRA • menedżerów projektów IT/OT realizujących projekty wymagające certyfikacji CE lub audytu bezpieczeństwa • uczestników projektów dofinansowanych: Kierunek-Rozwój, Bony Rozwojowe, MP Pociąg do Kariery, NSE i innych projektów EFS/FERS
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	15-06-2026

Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Celem szkolenia jest wyposażenie uczestników w wiedzę i praktyczne narzędzia niezbędne do wdrożenia i utrzymania zgodności z regulacjami NIS2 / UoKSC oraz CRA - Cyber Resilience Act. Szkolenie umożliwia samodzielne przeprowadzenie analizy ryzyka, opracowanie wymaganej dokumentacji (w tym Technical File i SZBI - ISO 27001), zaplanowanie działań audytowych, zarządzania łańcuchem dostaw, oraz reakcji na incydenty cyberbezpieczeństwa /podatności w organizacji lub dla produktu z elementami cyfrowymi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje obowiązki organizacji wynikające z UoKSC, NIS2 oraz Cyber Resilience Act w kontekście zarządzania cyberbezpieczeństwem.	Poprawnie przyporządkowuje obowiązki regulacyjne do właściwych przepisów i ról organizacyjnych.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik przeprowadza analizę ryzyka cybernetycznego dla systemu IT/OT lub produktu z elementami cyfrowymi z zastosowaniem metodyki threat modelling.	Prawidłowo identyfikuje zagrożenia, aktywa i środki zabezpieczające w przykładowym scenariuszu.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje wymagane elementy dokumentacji technicznej (Technical File) i SZBI zgodnej z wymogami CRA i NIS2.	Poprawnie wymienia i opisuje obowiązkowe składniki dokumentacji wymagane przez przepisy.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik opisuje proces zarządzania podatnościami i łańcuchem dostaw zgodnie z wymogami CRA, w tym obowiązki dotyczące SBOM/HBOM.	Prawidłowo wskazuje etapy procesu CVD/VDP oraz elementy rejestru komponentów.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik planuje działania reagowania na incydent bezpieczeństwa i raportowania zgodnie z art. 23 NIS2 oraz art. 14 CRA.	Poprawnie identyfikuje etapy procedury incydentowej, progi zgłoszeń i terminy raportowania.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik opracowuje założenia planu ciągłości działania (BCP/DRP) dla organizacji lub systemu krytycznego.	Prawidłowo definiuje metryki RTO/RPO i wskazuje kluczowe elementy planu odtworzenia.	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

Moduł I: Regulacje CRA, NIS2 i UoKSC – ramy prawne i obowiązki organizacji

- Przegląd regulacji: NIS2, UoKSC (nowelizacja 2024), Cyber Resilience Act – zakres stosowania, powiązania i różnice
- Kto jest podmiotem kluczowym i podmiotem waznym wg UoKSC – klasyfikacja i kryteria
- Definicja "producenta" w CRA – producent, integrator, dostawca komponentów: odpowiedzialność za produkt jako całość
- Obowiązki organizacji w 12 kluczowych obszarach NIS2: zarządzanie ryzykiem, incydenty, ciągłość, łańcuch dostaw, szyfrowanie, kontrola dostępu
- Obowiązki producenta w CRA: 40 wymagań bezpieczeństwa i 10 obowiązków eksploatacyjnych w cyklu życia produktu
- Powiązanie CRA z oznakowaniem CE – kiedy i jak wymagania cyberbezpieczeństwa wpływają na certyfikację
- Harmonogram wdrażania przepisów – terminy wejścia w życie i priorytety działania

Efekt modułu: uczestnik rozumie, które regulacje dotyczą jego organizacji lub produktu, zna zakres obowiązków i potrafi określić punkt startowy wdrożenia.

Moduł II: Analiza ryzyka cybernetycznego i Security by Design

- Metodyka analizy ryzyka dla systemów IT i OT – threat modelling, STRIDE, DREAD w praktyce
- Identyfikacja aktywów, zagrożeń i podatności – macierz ryzyka i dokumentowanie wyników
- Security by Design: zasady minimalizacji powierzchni ataku, kontroli dostępu i bezpiecznych aktualizacji od fazy projektowania
- Analiza ryzyka IT/OT dla fizycznych urządzeń (IoT, systemy wbudowane, OZE/SCADA) – punkty wejścia i środki zaradcze
- Segmentacja sieci i środowisk – topologie VLAN, strefy bezpieczeństwa, oddzielenie OT od IT
- Higiena technologiczna: MFA, zarządzanie uprzywilejowanymi kontami, patch management
- Dokumentacja oceny ryzyka jako fundament Technical File i SZBI – wymagana zawartość i powiązania

Efekt modułu: uczestnik potrafi przeprowadzić i udokumentować analizę ryzyka wymaganą przez CRA i NIS2 oraz zaprojektować podstawowe zabezpieczenia.

Moduł III: Zarządzanie dokumentacją techniczną i łańcuchem dostaw

- Struktura i zawartość Technical File (CRA) – analiza ryzyka, opis zabezpieczeń, komponenty, SBOM/HBOM, deklaracja zgodności
- SBOM i HBOM w praktyce – jak tworzyć i aktualizować rejestr komponentów, w tym open source
- Supply Chain Risk Management (SCRM) – identyfikacja ryzyk u dostawców hardware i software
- Weryfikacja bezpieczeństwa dostawców – checklista techniczna, klauzule umowne, audyt dostawcy
- Zarządzanie podatnościami (CVD/VDP) – procedura od wykrycia po zamknięcie podatności
- Reaktywna polityka bezpieczeństwa komponentów open source w DevSecOps

- Dokumentacja SZBI jako podstawa Technical File – powiązanie polityk, procedur i dowodów zgodności

Efekt modułu: uczestnik potrafi opracować wymaganą dokumentację techniczną i zarządzać ryzykiem w łańcuchu dostaw.

Moduł IV: Reagowanie na incydenty, monitoring i zgłaszanie zdarzeń

- Definicja incydentu wg NIS2 / UoKSC – progi istotności, kategorie i obowiązkowe zgłoszenia
- Raportowanie incydentów: Early Warning (24h), powiadomienie właściwe (72h), raport końcowy (30 dni) – art. 23 NIS2 / art. 14 CRA
- Procedura zarządzania incydentami – identyfikacja, analiza, ograniczenie, przywrócenie, wnioski
- Macierz RACI dla incydentów: role decyzyjne, techniczne i komunikacyjne
- Monitoring i detekcja: architektura SIEM, źródła telemetrii (logi, EDR, NDR), reguły korelacji i ML
- Kluczowe pola logów i formaty – co zbierać i dlaczego z perspektywy dowodów zgodności
- Integracja logów operacyjnych z Technical File i dokumentacją SZBI
- KPI i raportowanie: mierniki skuteczności procesu reagowania dla zarządu i organu nadzoru

Efekt modułu: uczestnik wie, jak wykrywać, klasyfikować, reagować i raportować incydenty zgodnie z wymogami regulacyjnymi.

Moduł V: Ciągłość działania, audyt i certyfikacja

- Plan ciągłości działania (BCP) i odtwarzania po katastrofie (DRP) – metodyka i kluczowe metryki RTO/RPO
- Kopie zapasowe i strategie odtwarzania – zasada 3-2-1, testy odtwarzania, rola backupu w kontekście ransomware
- Przegląd wymogów audytowych NIS2 / UoKSC – co będzie sprawdzane przez CSIRT Polska i organy nadzoru sektorowego
- Zakres weryfikacji technicznej przed oznakowaniem CE w CRA – metodyki testowania odporności
- Red Team vs. Pentest vs. Ocena zgodności – kiedy stosować i jak dokumentować wyniki
- Praktyczne przygotowanie do audytu: listy kontrolne, artefakty dowodowe, najczęstsze braki dokumentacyjne
- Nadzór po certyfikacji – monitorowanie ryzyk, zarządzanie aktualizacjami i obowiązki raportowania po wdrożeniu
- Podsumowanie: plan działań - quick wins: co wdrożyć w pierwszej kolejności

Efekt modułu: uczestnik rozumie wymagania audytowe i potrafi przygotować organizację lub produkt do pomyślnego przejścia weryfikacji.

Całkowity czas trwania szkolenia : 8 godzin zegarowych (5 godzin zegarowych przekazywania wiedzy + 1,5 godziny warsztatów + 30 min walidacji wiedzy + 60 min przerw)

Czas nauki oraz warsztatów: 6,5 godziny

Czas walidacji wiedzy: 30 min

Czas przerw: 4 x 15 minut (razem 60 min)

· Egzamin wewnętrzny / walidacja jest wliczona w czas trwania szkolenia.

· Przerwy nie są wliczone w czas trwania szkolenia

Harmonogram

Liczba pozycji harmonogramu: 13

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 Regulacje CRA, NIS2 i UoKSC – ramy prawne i obowiązki organizacji	Zajęcia	Piotr Szymczyk	16-06-2026	08:00	08:45	00:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 13 Obowiązki producenta w CRA oraz znak CE	Zajęcia	Piotr Szymczyk	16-06-2026	08:45	09:45	01:00
3 z 13 -	Przerwa	-	16-06-2026	09:45	10:00	00:15
4 z 13 Analiza ryzyka cybernetycznego i Security by Design	Zajęcia	Piotr Szymczyk	16-06-2026	10:00	10:45	00:45
5 z 13 Metodyka analizy ryzyka w systemach IT / OT	Zajęcia	Piotr Szymczyk	16-06-2026	10:45	11:45	01:00
6 z 13 -	Przerwa	-	16-06-2026	11:45	12:00	00:15
7 z 13 Zarządzanie dokumentacją techniczną i łańcuchem dostaw	Zajęcia	Piotr Szymczyk	16-06-2026	12:00	12:45	00:45
8 z 13 S-BOM / H-BOM; Zarządzanie podatnościami (CVD/VDP)	Zajęcia	Piotr Szymczyk	16-06-2026	12:45	13:30	00:45
9 z 13 -	Przerwa	-	16-06-2026	13:30	13:45	00:15
10 z 13 Reagowanie na incydenty, monitoring i zgłaszanie zdarzeń	Zajęcia	Piotr Szymczyk	16-06-2026	13:45	14:30	00:45
11 z 13 Ciągłość działania, audyt i certyfikacja	Zajęcia	Piotr Szymczyk	16-06-2026	14:30	15:15	00:45
12 z 13 -	Przerwa	-	16-06-2026	15:15	15:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 13 -	Walidacja	Piotr Szymczyk	16-06-2026	15:30	16:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00
w tym suma godzin zajęć	06:30
w tym suma godzin walidacji	00:30
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	09:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	899,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 113 ust. 1 ustawy o VAT ze względu na wartość sprzedaży	
Koszt przypadający na 1 uczestnika netto	899,00 PLN
Koszt osobogodziny brutto	112,38 PLN
Koszt osobogodziny netto	112,38 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	08:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Piotr Szymczyk

Dynamiczny menedżer i trener z wieloletnim doświadczeniem w sektorze IT oraz usługach bezpieczeństwa dla globalnych korporacji (blue-chip). Specjalizuje się w budowaniu odporności cyfrowej organizacji, optymalizacji procesów serwisowych oraz wdrażaniu standardów zgodnych z najnowszymi dyrektywami unijnymi (w tym NIS2). Jako praktyk biznesu, Piotr nie tylko przekazuje wiedzę teoretyczną, ale uczy, jak zarządzać zmianą w środowisku wysokiej zmienności i niepewności (VUCA). Jego szkolenia charakteryzują się wysokim poziomem merytorycznym, ścisłą orientacją na cele biznesowe oraz praktycznym podejściem do technologii, co pozwala uczestnikom na natychmiastowe wdrożenie zdobytych umiejętności.
OBSZARY EKSPERTYZY SZKOLENIOWEJ
• Cyberbezpieczeństwo i Zgodność: Kompleksowe wdrażanie dyrektywy NIS2, nowelizacja UoKSC, implementacja SZBI, audyt systemów informatycznych zgodnie z normami ISO 27001
• Zarządzanie Usługami IT (ITIL): Optymalizacja procesów dostarczania usług, zarządzanie incydentami oraz planowanie ciągłości działania (BCP/DRP)
• Change Management: Prowadzenie organizacji przez procesy transformacji cyfrowej i przełamywanie oporu wobec zmian technologicznych
• Przywództwo w IT: Budowanie i szkolenie wielokulturowych zespołów technicznych, coaching menedżerski oraz strategiczne zarządzanie talentami
Certyfikaty: AgilePM® Foundation & Practitioner, Change Management® Foundation, ISO 27001 Audytor Wewnętrzny, Akademia Bezpieczeństwa Informacji (EITCA/IS), ITIL® 4 Foundation

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- prezentację ze szkolenia (w formacie PDF)
- zestaw szablonów i narzędzi: checklista wymagań NIS2/CRA, wzór rejestru ryzyka, przykładowa struktura Technical File, wzór procedury reagowania na incydent
- zaświadczenie / certyfikat o ukończeniu szkolenia - roczny obowiązkowy wymóg nakładany przez ustawę o KSC
- ponad 60 wzorów dokumentów takich jak polityki / instrukcje / raporty / rejestry zgodne z SZBI oraz CRA

Warunki uczestnictwa

- Podstawowa wiedza w zakresie kompetencji cyfrowych
- Logowanie się pełnym imieniem i nazwiskiem
- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80%–100% zajęć usługi rozwojowej (w zależności od programu dofinansowania i podpisanej umowy z Operatorem)
- W ramach realizacji usług szkoleniowych Organizator utrwala wizerunek Uczestników w formie nagrań wideo, fotografii lub innych materiałów audiowizualnych wyłącznie w celach archiwizacyjnych, kontrolnych oraz dokumentacyjnych związanych z projektem dofinansowanym
- Uczestnik zapisując się na szkolenie wyraża zgodę na utrwalenie i wykorzystanie jego wizerunku w wyżej wymienionych celach

Informacje dodatkowe

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: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług orazszczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Całe szkolenie jest rejestrowane w celach kontroli oraz audytu.

Wykorzystanie nagrania w innym celu niż kontrola czy audyt wymaga zgody trenera oraz uczestników.

Uczestnicy otrzymają zaświadczenie / certyfikat, potwierdzające ukończenie szkolenia.

Usługa zdalna w czasie rzeczywistym - prowadzona na żywo.

Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej na formularzu reklamacji i odsyłając na adres: biuro@legacyturn.com

Warunki techniczne

Poniżej opisane są minimalne wymagania techniczne dotyczące uczestnictwa w szkoleniu przy pomocy platformy ZOOM:

1. Parametry urządzenia: komputer / laptop / tablet

- Procesor dwurdzeniowy 1–2 GHz minimalnie; zalecany dual-core 2 GHz lub lepszy (Intel i3/i5 lub równoważny)
- 2 GB pamięci RAM (zalecane 4 GB lub więcej).
- System operacyjny: Windows 10/11, macOS 10.13+ (lub nowsze), Linux (nowsze dystrybucje wspierane), iOS 13+/Android 8+
    - zainstalowany **Zoom Desktop Client** (najświeższa wersja) lub najnowsza wersja Chrome/Edge/Firefox;

1. Kamera i mikrofon

- Zoom współpracuje z wbudowanymi kamerami w laptopach oraz większością kamer internetowych.
    - słuchawki z mikrofonem zalecane dla lepszej jakości dźwięku.
    - zaawansowane lub profesjonalne kamery/mikrofony, mogą wymagać zainstalowanie dodatkowego oprogramowania .

1. Urządzenia mobilne

- Jeżeli łączysz się z urządzenia mobilnego, pobierz i zainstaluj aplikację Zoom z App Store (Apple) lub Google Play
- Aby korzystać z dźwięku i obrazu, użyj zestawu słuchawkowego z mikrofonem lub głośników podłączonych do urządzenia.
- Przed rozpoczęciem szkolenia sprawdź, czy urządzenie rozpoznaje wybrane urządzenie audio oraz czy nie jest ono jednocześnie zajęte przez inną aplikację
- Upewnij się, że aplikacja ma przyznane uprawnienia do korzystania z mikrofonu i kamery.

1. Wymagania dla łącza internetowego:

- *min. 1,5 Mbps download i upload* dla podstawowego udziału
- zalecane 3 Mbps+ dla stabilnego wideo HD i udostępniania ekranu
- najnowsza wersja używanej przeglądarki internetowej

1. Link do szkolenia oraz warunki / wymagania dodatkowe:
    - Link do szkolenia zostanie dosłany drogą elektroniczną przed rozpoczęciem usługi na adres email podany przez uczestnika szkolenia.

- Link do szkolenia będzie ważny w dniach i godzinach określonych w harmonogramie usługi.

1. Podczas szkolenia online zapewniamy:
    - Wygodną formę szkolenia, gdzie wystarczy dostęp do urządzenia z internetem (komputer, tablet, telefon), słuchawki lub głośniki.

- Szkolenie zdalne w czasie rzeczywistym w wirtualnym pokoju konferencyjnym, w niewielkiej grupie uczestników.
- Możliwość pełnej interakcji z trenerem, który prowadzi zajęcia "na żywo" z włączoną kamerą w czasie trwania całego szkolenia.
- Możliwości zadawania pytań, omawiania indywidulanych zagadnień oraz aktywny udział w ćwiczeniach.

Przed szkoleniem:

- Upewnij się, że masz stabilne połączenie internetowe, które spełnia minimalne wymagane prędkości dla transmisji audio oraz wideo.
- Przetestuj dostęp i uruchomienie aplikacji ZOOM w wykorzystaniem kamery oraz mikrofonu.
- Rekomenduje się przygotowanie zapasowego zestawu awaryjnego sprzętu w celu zapewnienia ciągłości realizacji szkolenia. Powinien on obejmować kluczowe komponenty: komputer, kamerę, mikrofon/głośnik, klawiaturę, myszkę oraz alternatywne źródło dostępu do Internetu (np. modem Hot-Spot).

Podstawą do rozliczenia usługi jest wygenerowanie z systemu raportu, umożliwiającego identyfikację wszystkich uczestników oraz zastosowanego narzędzia.

Kontakt

PIOTR SZYMCZYK

E-mail szyplodz@yahoo.com
Telefon (+48) 501 435 131