26.11.2026

Fundusze Europejskie

EDIH CyberSEC Krajowe Centrum Bezpiecznej Transformacji Cyfrowej – Twój Partner w cyfrowej transformacji

Gerard Frankowski EDIH CyberSec / PCSS

Fundusze Europejskie dla Nowoczesnej Gospodarki
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR

Krótka agenda

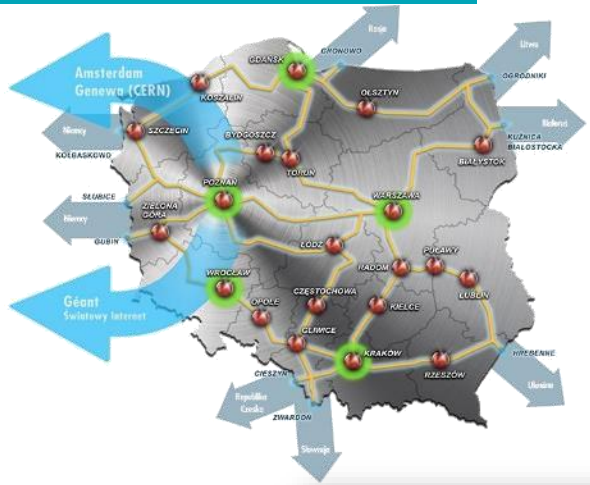
26.11.2026

- Przywitanie
- CyberSec EDIH – Krajowe Centrum Bezpiecznej Transformacji Cyfrowej
- Wsparcie ze strony CyberSec EDIH 2.0 dla procesu aplikacji o pożyczkę
- Zaproszenie na szkolenie CyberSec EDIH dla Przedsiębiorców



Poznańskie Centrum Superkomputerowo-Sieciowe

- Jednostka naukowo-badawcza, afiliowana przy IChB PAN
- Operator krajowej sieci naukowej PIONIER
- 2 centra danych
- 4 lokalizacje, ponad 500 pracowników
- Główne obszary zainteresowań
  - Zastosowania technologii HPC
  - Sztuczna inteligencja (AI)
  - Internet Rzeczy z usługami aplikacyjnymi
  - Usługi oraz infrastruktury sieciowe
  - Informatyka kwantowa
  - Bezpieczeństwo sieci i systemów (reprezentuję Dział Bezpieczeństwa ICT PCSS)
- Certyfikaty ISO 27001 oraz ISO 9001
- Więcej – np. https://www.pcss.pl, https://www.pcss.pl/raport/











CyberSec EDIH – Krajowe Centrum Bezpiecznej Transformacji Cyfrowej

- Europejski Hub Innowacji Cyfrowych (EDIH) koordynowany przez PCSS
  - EDIH-y stymulują rozwój innowacji i wzrost dojrzałości cyfrowej organizacji (aspekty cyberbezpieczeństwa są elementem oceny DMA)
- Jedyny polski EDIH specjalizowany w obszarze cyberbezpieczeństwa
  - 2024-2026 (CybeSec EDIH 2.0: 2027-2029)
- Bezpłatne usługi cyberbzpieczeństwa dla sektora SME, m.in.:
  - Audyty bezpieczeństwa systemów i usług (także systemów AI)
  - Szkolenia cyberbezpieczeństwa (użytkownicy, audytorzy, programiści)
- Budowa systemów zarządzania bezpieczeństwem informacji oraz jakością (w tym wsparcie certyfikacji)
- Analiza dojrzałości cyfrowej z rekomendacjami cyberbezpieczeństwa
- (Od 2027) Budowa strategii cyfryzacji z poszukiwaniem źródeł finansowania
- (Od 2027) Wspieranie osiągania autonomii cyfrowej i technologicznej
- (Od 2027) Wsparcie w tworzeniu rozwiązań AI

Najważniejsze usługi CyberSec EDIH 2.0

- Opracowanie strategii digitalizacji, uwzględniającej dostęp do finansowania - :DIGIT
- Audyty cyberbezpieczeństwa (zgodności i techniczne – w tym testy penetracyjne) – np. PCSS:TCA
- Szkolenia dla Programistów, Administratorów, „Bezpieczników”, świadomościowe – np. PCSS:SECTR
- Określanie poziomu zgodności organizacji z regulacjami cyberbezpieczeństwa
- Wdrożenie lub konsultacja bezpiecznego cyklu życia oprogramowania (SDLC)
- Ocena dojrzałości cyfrowej organizacji i zgodności z dyrektywą NIS2
- Usługi eksperckie w zakresie autonomii cyfrowej
- Wsparcie procesów zarządczych – ITTI:SMP
- Wsparcie w tworzeniu systemów AI
- Ćwiczenia w zakresie obsługi incydentów
- Organizacja wydarzenia współpracy sieciowej



Jak wygląda współpraca z hubami EDIH?



- Złożenie przez MŚP dokumentów aplikacyjnych oraz ich weryfikacja przez EDIH
- Podpisanie umowy NDA
- Ustalenie zakresu działań, listy i wartości usług, pochodzących z katalogu EDIH
  - Wartości **średnie** usług można znaleźć w cenniku usług EDIH – wartość konkretnej usługi najczęściej zależy od kontekstu i wielkości organizacji oraz charakteru zapotrzebowania
- Podpisanie umowy na realizację usług po weryfikacji statusu MŚP i limitu pomocy *de minimis* (300 tys. EUR w ciągu 3 lat)
- Realizacja usług EDIH – **bezpłatna dla MŚP**
  - W CyberSec EDIH 2.0 ok. 4,5% kwoty wartości usług stanowi dotację z Komisji Europejskiej, ok. 95,5% - stanowi pomoc publiczną udzielaną przez hub EDIH
  - W przypadku pozostałych polskich EDIH kwoty rozkładają się po połowie
  - Przedsiębiorstwa inne niż MŚP albo instytucje mogą skorzystać z usług na zasadach komercyjnych
- Wynik realizacji usługi jest w całości własnością MŚP; EDIH raportuje tylko wskaźniki pochodne
- Ankiety dojrzałości cyfrowej DMA: T0, T1, T2, ankieta kontentacyjna

Cyberbezpieczeństwo jako niezbędny element transformacji cyfrowej przedsiębiorstwa

- Cyberbezpieczeństwo należy traktować jako **integralny element transformacji cyfrowej** przedsiębiorstwa
- Wskazuje się na uwzględnienie wymagań zawartych w **UoKSC / CRA**
- W przypadku przeprowadzania transformacji cyfrowej w dziedzinie cyberbezpieczeństwa Odbiorca może wdrożyć jedynie technologie cyfrowe wynikające z rekomendacji wydanych po **przeprowadzonych testach penetracyjnych lub audytach bezpieczeństwa**
- Przy etapie wnioskowania o pożyczkę na innym obszarze audyty i testy penetracyjne nie są obowiązkowe, ale mogą być elementem **niezbędnej analizy ryzyka**
- Więcej: „Przewodnik dla Partnerów Finansujących i Ostatecznych Odbiorców Instrumentu Finansowego…”, https://feng.parp.gov.pl/storage/publications/pdf/2_FE-Publikacja-A4-srodek_przewodnik.pdf

Przykładowy zakres wsparcia CyberSec EDIH w obszarze audytu / analizy transformacji cyfrowej (1/2)

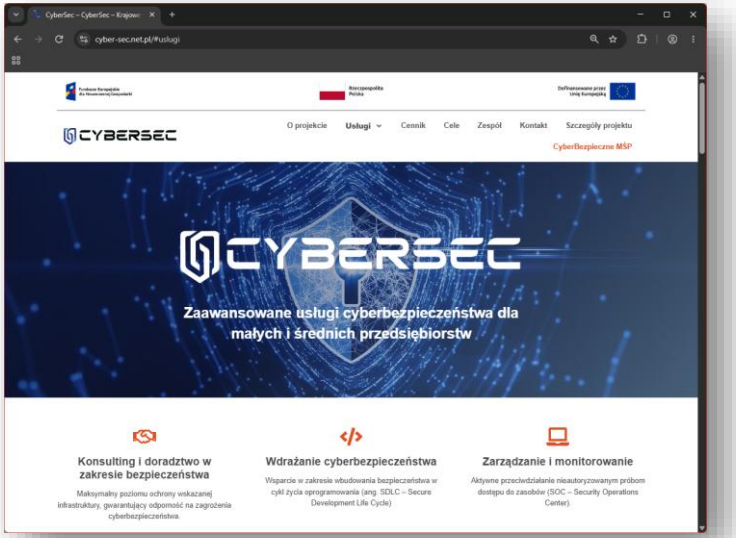
Obszar	Zakres wsparcia	Uwagi
Opis przebiegu i wyników samooceny przedsiębiorstwa w zakresie gotowości do wdrażania rozwiązań z zakresu Przemysłu 4.0.	Wsparcie w wykonaniu ankiety ADMA oraz opracowaniu dokumentacji	W ramach usługi :DIGIT
Opis kompleksowego planu transformacji przedsiębiorstwa w kierunku przemysłu 4.0	Analiza technologiczna procesów, analiza infrastruktury i narzędzi informatycznych, analiza kompetencji	Usługi :DIGIT, PCSS:TCSA lub PCSS:AIEVL w przypadku rozwiązań AI; szczegółowe analizy w obszarze cyberbezpieczeństwa – możliwość poprawy kompetencji dzięki usługom szkoleniowym
Analiza ryzyka - zidentyfikowanie ryzyk związanych z realizacją Inwestycji Końcowej	Przeprowadzenie analizy ryzyka, przeszkolenie kadry, = samodzielna realizacja analiz w przyszłości	Usługi w obszarze potwierdzania zgodności, także elementy :DIGIT, PCSS:TCSA; koncentracja na ryzykach (cyber)bezpieczeństwa

Przykładowe zakresy wsparcia CyberSec EDIH w obszarze audytu / analizy transformacji cyfrowej (2/2)

Obszar	Zakres wsparcia	Uwagi
Propozycja harmonogramu realizacji inwestycji z zakresu transformacji przedsiębiorstwa	Podniesienie kompetencji kadry w zakresie procesów transformacji/innowacyjnych	Zaplanowanie realizacji niezbędnych szkoleń przy udziale usług *Skills and training* CyberSec EDIH
Rekomendacje działań towarzyszących, w tym w zakresie działań przygotowawczych	Przygotowanie mapy drogowej w zakresie cyberbezpieczeństwa	Może być to dodatkowy efekt realizacji usługi audytorskiej takiej jak PCSS:TCSA lub ITTI:CA
Pozostałe obszary	Wsparcie konsultacyjne, tworzenie dokumentacji, propozycje rozwiązań alternatywnych, dostarczenie wiedzy dziedzinowej	Duża część obszarów oparta jest na specyfice działalności MŚP i wymaga wiedzy leżącej po jego stronie. Najważniejsze obszary dziedzinowe CyberSec EDIH: cyberbezpieczeństwo, sztuczna inteligencja, systemy zarządzania bezpieczeństwem informacji, zgodność z regulacjami prawnymi w obszarze cybersec/AI

A jeżeli zakres usług CyberSec EDIH wydaje się nie pokrywać Państwa zapotrzebowania?

- Należy pamiętać, że konkretne usługi są projektowane **w oparciu o potrzeby** MŚP; mamy również możliwość zatrudnienia dodatkowych ekspertów w razie potrzeby
- Szczegółowe informacje o usługach będą dostępne **po rozpoczęciu projektu** na stronie CyberSec EDIH: https://cyber-sec.net.pl/
- Można **równolegle nawiązać współpracę** z innym hubem albo hubami EDIH na analogicznych zasadach
  - CyberSec EDIH świadomie pełni funkcję **hubu specjalistycznego**, uzupełniając ofertę pozostałych (regionalnych) hubów w Polsce
- W CyberSec EDIH istnieje ścieżka tzw. *entity referral* , pozwalająca rozszerzyć współpracę na **dalsze podmioty ekosystemu innowacji**, np. fabryki AI



Zapraszamy na szkolenie „CyberBezpieczne MŚP”
Poznań (PCSS – CBPIO), 2 grudnia 2026 r. godz. 9:30-16:45

- Wystąpią zaproszeni Goście (m.in. Unicredit) oraz Partnerzy Konsorcjum
- Odpowiedź na wyzwania cyberbezpieczeństwa, stojące dziś przed MŚP – m.in.:
  - Wycieki danych i zagrożenia – jak przeciwdziałać i reagować?
  - Najczęstsze metody ataków na MŚP
  - Przegląd systemów i zabezpieczeń przed cyberatakami
  - Bezpieczeństwo i cyberataki w usługach finansowych dla MŚP
  - Jak wygląda cyberatak na sieć produkcyjną?
  - Zarządzanie ryzykiem w małej firmie
  - Czy należy bać się sztucznej inteligencji?
- Przybliżymy również portfolio usługowe CyberSec EDIH 2.0 na lata 2027-2029
- Więcej: https://cyber-sec.net.pl/cyberbezpiecznemsp/





Fundusze Europejskie

Dziękuję za uwagę!

email: gerard@man.poznan.pl, contact@cyber-sec.net.pl

Fundusze Europejskie dla Nowoczesnej Gospodarki

Rzeczpospolita Polska

Dofinansowane przez Unię Europejską

PARP Grupa PFR