

Julia Onisk
NCC-PL

Program Cyfrowa Europa: Nowe Nabory

Nowe perspektywy finansowania
w cyberbezpieczeństwie

Kim jesteśmy?

- Krajowe Centrum Kompetencji Cyberbezpieczeństwa (NCC-PL) działające w strukturach Ministerstwa Cyfryzacji.
- Jesteśmy częścią europejskiej sieci zarządzanej przez ECCCC (Europejskie Centrum Kompetencji w Bukareszcie).

Jak pomagamy?

- Informujemy o otwartych naborach i harmonogramach konkursów.
- Wyjaśniamy zasady aplikowania i wymogi (np. Cyber Resilience Act, NIS2).
- Wspieramy w poszukiwaniu partnerów do konsorcjów międzynarodowych.



NCC-PL

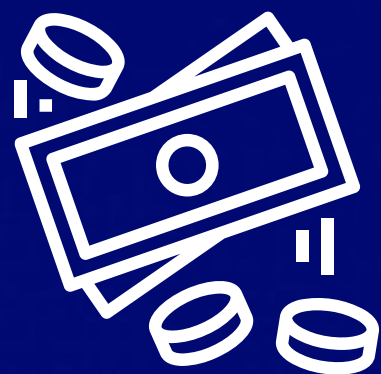
Krajowe Centrum Kompetencji
Cyberbezpieczeństwa



Nasza misja

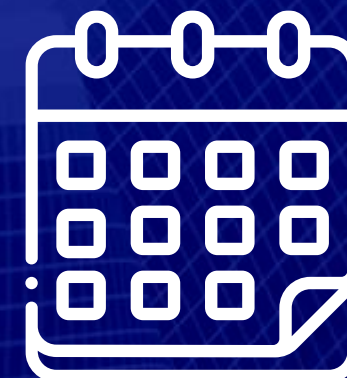
- Wspieranie polskich firm, jednostek badawczych i podmiotów publicznych w pozyskiwaniu środków z UE (programy: Cyfrowa Europa, Horyzont Europa).
- Budowanie krajowej społeczności cyberbezpieczeństwa i łączenie partnerów do projektów.
- Działanie jako punkt kontaktowy i informacyjny dla podmiotów działających w obszarze cyberbezpieczeństwa oraz zapewnienie informacji o inicjatywach europejskich

Kluczowe informacje o naborze



50 MLN €

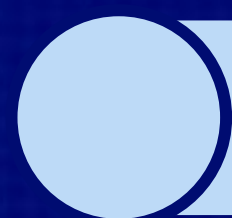
Łączna alokacja budżetowa



31 MARCA 2026

Termin składania wniosków

Złożony proces budowania konsorcjum -
rozpocznij już dziś



Teraz



31.03.2026



NCC-PL
Krajowe Centrum Kompetencji
Cyberbezpieczeństwa



**Ministerstwo
Cyfryzacji**

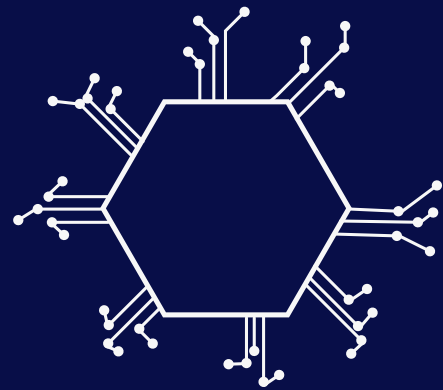


ECCCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Co-funded by
the European Union

4 kluczowe obszary naboru



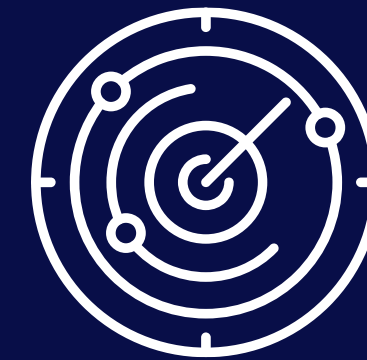
1. AI w cyberbezpieczeństwie

- Automatyzacja procesów
- Zwiększenie efektywności wykrywania zagrożeń



2. Wsparcie dla MŚP

- Absorpcja innowacyjnych rozwiązań
- Ułatwienie spełnienia wymogów regulacyjnych



3. Testy gotowości i odporności

- Dla operatorów usług kluczowych
- Zaawansowane symulacje ataków
- Weryfikacja zabezpieczeń

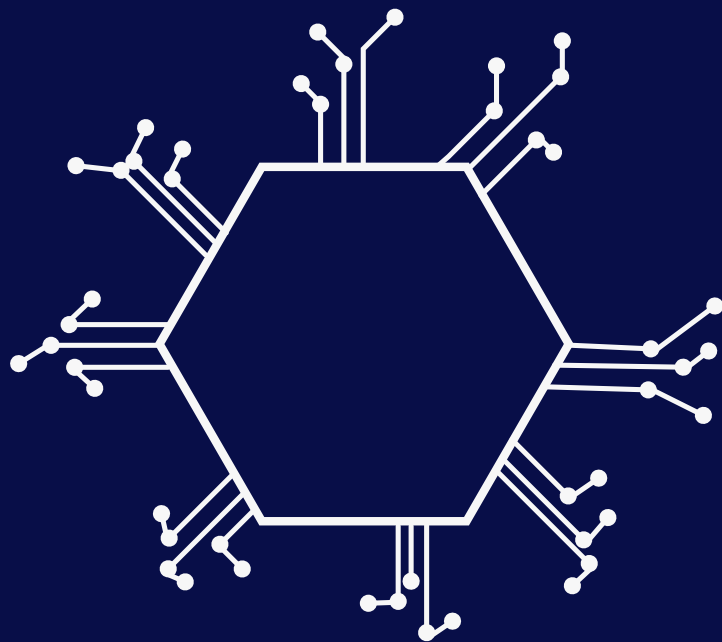


4. Ochrona infrastruktury podmorskiej

- Zabezpieczenie kabli (telko/energetyka)
- Ścisła koordynacja transgraniczna

1. Cybersecure tools, technologies and services relying on AI

Cel i zastosowanie



- Wdrożenie i walidacja narzędzi AI
- Automatyzacja procesów detekcji i reakcji
- Szybsze przetwarzanie dużych wolumenów danych
- Wykrywanie anomalii (wsparcie dla analitów)

Rozwój rozwiązań opartych na AI

Kto może aplikować Budżet i finansowanie

- Dostawcy technologii i rozwiązań cyberbezpieczeństwa
- Operatorzy usług kluczowych i ważnych (NIS2)
- Instytucje badawcze i naukowe (wsparcie wdrożenia)



Łączny budżet:
15 MLN

Dofinansowanie:
50% kosztów kwalifikowanych
3-5 MLN € na projekt

2. Uptake of innovative cybersecurity solutions for SMEs

Cel i zastosowanie



- Zwiększenie absorpcji innowacyjnych rozwiązań cyberbezpieczeństwa
- Dostosowanie do wymogów rynkowych i prawnych
- Wdrożenie dyrektywy NIS2 oraz Cyber Resilience Act (CRA)

Unikalna szansa na rozwój i zgodność

Kto może aplikować Budżet i finansowanie

- Mikro, małe i średnie przedsiębiorstwa (MŚP)
- Startupy oferujące innowacyjne technologie
- Podmioty publiczne/prywatne



Łączny budżet:
15 MLN

Dofinansowanie dla MŚP:
75% kosztów kwalifikowanych
50% dla pozostałych podmiotów
3 MLN € na projekt

3. Coordinated preparedness testing and other preparedness actions

Cel i zastosowanie

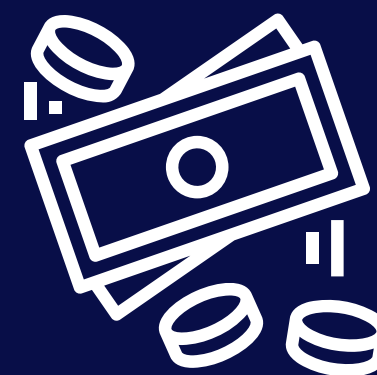


**Nie tylko
teoria**

- Bezpośrednia weryfikacja stanu zabezpieczeń
- Skoordynowane działania testowe
- Praktyczne sprawdzenie odporności infrastruktury krytycznej na incydenty
- Realizacja zaawansowanych testów penetracyjnych
- Opracowywanie scenariuszy zagrożeń i audyty podatności IT/OT

Kto może aplikować Budżet i finansowanie

- Zespoły reagowania na incydenty (CSIRT)
- Podmioty publiczne działające jako właściwe organy ds. cyberbezpieczeństwa
- Podmioty publiczne objęte dyrektywą NIS2



Łączny budżet:
10 MLN

Dofinansowanie:
50% kosztów kwalifikowanych
Do 1,5 MLN € na projekt

4. Regional Cable Hubs

Cel i zastosowanie

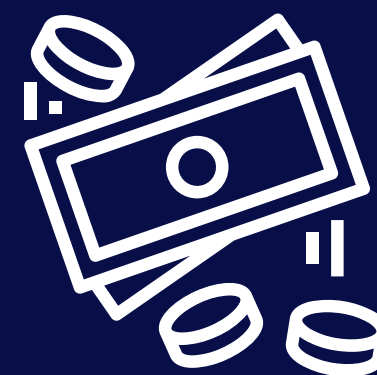


Strategia w obliczu zagrożeń hybrydowych

- Zabezpieczenie fizycznej warstwy przesyłu (dane/energia)
- Utworzenie i operacjonalizacja Regional Cable Hubs
- Monitorowanie zagrożeń i koordynacja działań naprawczych/konserwacyjnych
- Skrócenie czasu reakcji na awarie lub sabotaż

Kto może aplikować Budżet i finansowanie

- Organy administracji państwowej
- Podmioty zarządzające infrastrukturą krytyczną i operatorzy kabli
- Podmioty posiadające zdolności obronne i nadzoru morskiego.



Łączny budżet:
10 MLN

Dofinansowanie:
70% kosztów kwalifikowanych
Do 3 MLN € na projekt

Planowane nabory z zakresu cyberbezpieczeństwa na 2026 rok

- Cybersecure tools, technologies and services relying on AI
- Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions
- Mutual assistance
- Regional Cable Hubs
- Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements
- Dual-use technologies
- Preparedness support
- SECURE

Kontakt



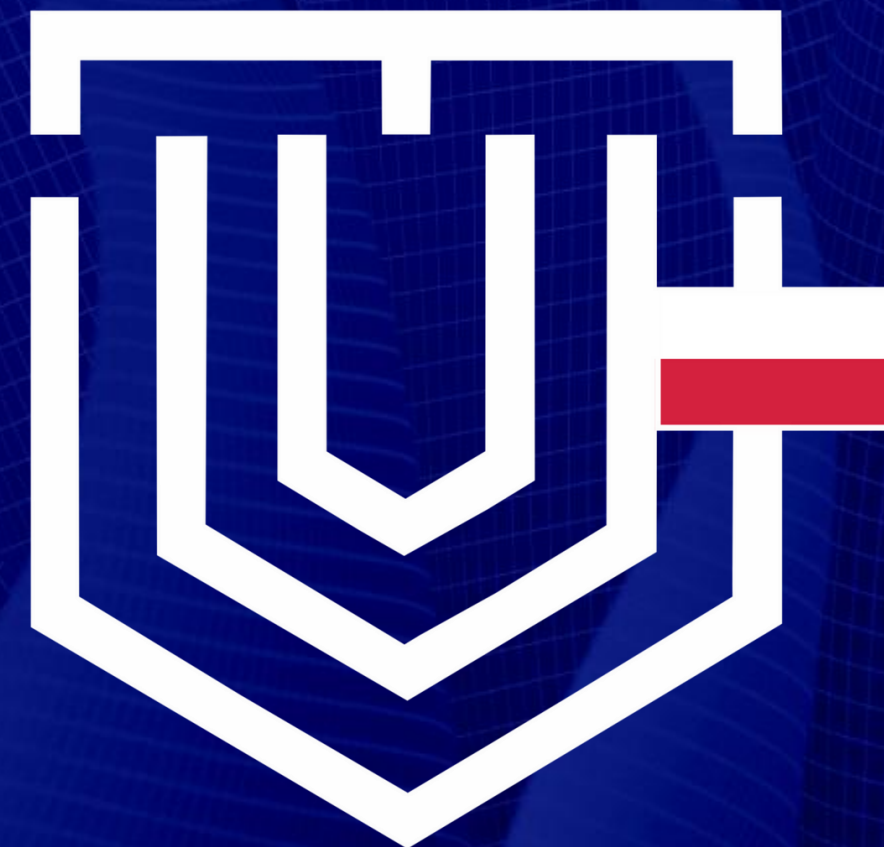
www.gov.pl/web/cyber-nccpl



ncc@cyfra.gov.pl



www.linkedin.com/company/ncc-pl



NCC-PL