Ministerstwo Cyfryzacji

# Centrum Cyberbezpieczeństwa NASK (CCN)

Działanie FERC.02.02 Wzmocnienie krajowego systemu cyberbezpieczeństwa

Warszawa, 05 października 2023 r.

# Plan prezentacji

- Cel projektu
- CSIRT NASK
- Zakres Projektu
- Adresowane wyzwania i potrzeby
- Budżet i okres projektu
- Harmonogram realizacji projektu
- Harmonogram prac
- Efekty wdrożenia / rezultaty projektu

# Cel Projektu

**Celem strategicznym projektu jest *wzmocnienie krajowego systemu cyberbezpieczeństwa* poprzez utworzenie**
**Centrum Cyberbezpieczeństwa NASK [CCN]**

**Beneficjent projektu:** NASK

CSIRT NASK Ministerstwo Cyfryzacji

# CSIRT NASK

- Podstawą działającego w NASK CSIRT (Computer Security Incident Response Team) jest ustawa o krajowym systemie cyberbezpieczeństwa implementująca do polskiego prawa dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. dyrektywę NIS).
- Na mocy ustawy role CSIRT'ów poziomu krajowego przyjęły na siebie Agencja Bezpieczeństwa Wewnętrznego (CSIRT GOV), NASK – Państwowy Instytut Badawczy (CSIRT NASK) oraz resort obrony narodowej (CSIRT MON).
- Współpracują one ze sobą oraz z organami właściwymi do spraw cyberbezpieczeństwa.
- Razem zapewniają spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów.

# Zakres projektu

**Zadanie 1 UTWORZENIE CENTRUM CYBERBEZPIECZEŃSTWA NASK (CCN)**

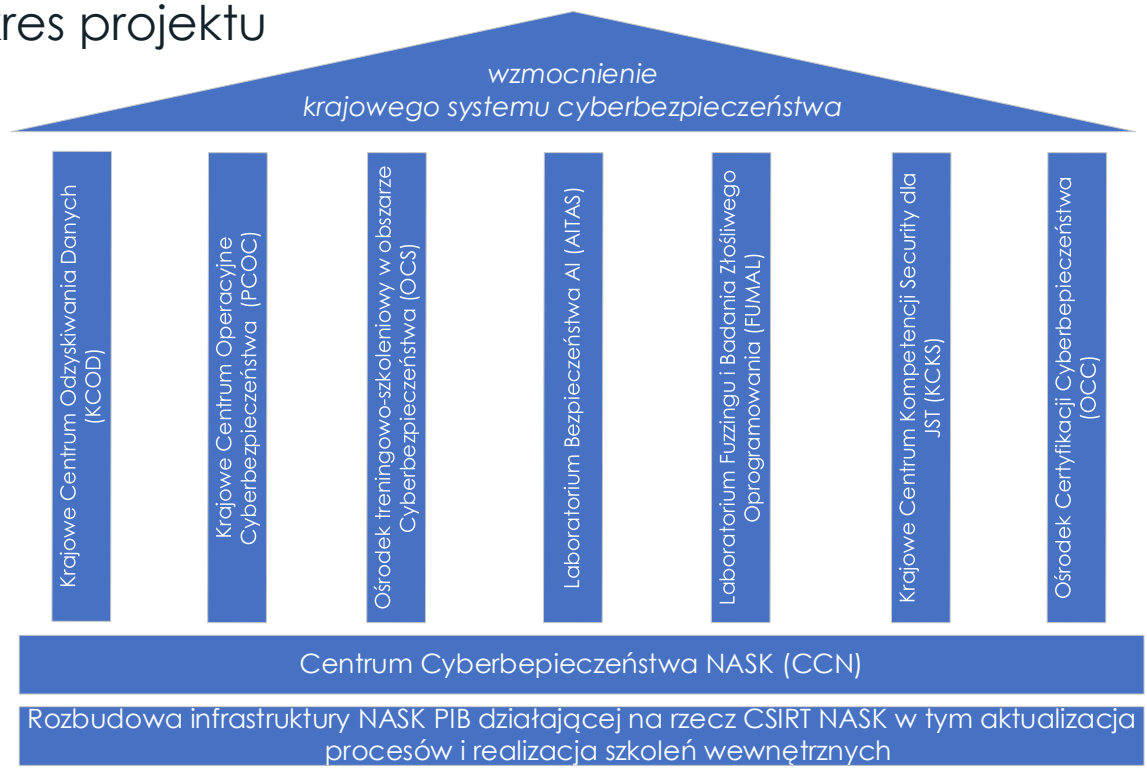
**Podzadanie 1 Utworzenie obiektu CCN**

**Podzadanie 2 Utworzenie specjalistycznych centrów i laboratoriów**

- *Działanie 2.1 Utworzenie Krajowego Centrum Odzyskiwania Danych (KCOD)*
- *Działanie 2.2 Utworzenie Krajowego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC)*
- *Działanie 2.3 Utworzenie modelowego Ośrodka treningowo – szkoleniowego w obszarze Cyberbezpieczeństwa (OSC)*
- *Działanie 2.4 Utworzenie Laboratorium Bezpieczeństwa AI (AITAS)*
- *Działanie 2.5 Utworzenie Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania (FUMAL)*
- *Działanie 2.6 Utworzenie Krajowego Centrum Kompetencji Security dla JST (KCKS)*
- *Działanie 2.7 Utworzenie Ośrodka Certyfikacji Cyberbezpieczeństwa (OCC)*

**Podzadanie 3 Rozbudowa infrastruktury NASK PIB działającej na rzecz CSIRT NASK w tym aktualizacja procesów i realizacja szkoleń wewnętrznych**

# Zakres projektu




CSIRT NASK

Ministerstwo Cyfryzacji

# Adresowane wyzwania i potrzeby
## Utworzenie obiektu CCN

- Potrzeba utworzenia obiektu dającego możliwości utworzenia i zlokalizowania w jednym miejscu niezbędnych centrów i laboratoriów (stanowiące podzadanie 2), które będą istotnie zwiększać poziom bezpieczeństwa informacji poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych państwa oraz podmiotach mających kluczowe znaczenie dla gospodarki, co przełoży się na wzmocnienie krajowego sytemu cyberbezpieczeństwa

# Adresowane wyzwania i potrzeby
## Krajowe Centrum Odzyskiwania Danych (KCOD)

- Potrzeba utworzenia i rozwoju profesjonalnej oraz rozpoznawalnej w skali kraju jednostki stanowiącej odpowiedź na problemy związane z ciągłością funkcjonowania podmiotów po skutecznym ataku, w którym zniszczeniu uległy dane w formie cyfrowej
- Kompetencje KCOD stanowiłyby istotny element dla planowania obsługi incydentu, w tym przywracania ciągłości działania w podmiocie dotkniętym incydentem, a także niezbędny element uzupełnienia procesu informatyki śledczej, w tym na potrzeby organów ścigania, dla których odzyskanie niezbędnych śladów cyfrowych może stanowić o kierunkach prowadzonego dochodzenia/śledztwa lub postępowania karnego.

# Adresowane wyzwania i potrzeby
## Krajowe Centrum Operacyjne Cyberbezpieczeństwa (PCOC)

- Brak wspólnego miejsca pracy adekwatnego do potrzeb CSIRT'ów, a także rozwiązań umożliwiających ich współpracę np. w zakresie dzielenia się większymi zbiorami/strumieniami danych
- Potrzeba stworzenia  miejsca umożliwiającego efektywną współpracę pomiędzy krajowymi CSIRT'ami w obszarze analizy aktywności zorganizowanych grup przestępczych i aktorów państwowych oraz rozwoju narzędzi służących do monitorowania bezpieczeństwa, zbierania, analizy i wymiany informacji o zagrożeniach, podatnościach i incydentach, w tym do zaawansowanego rozpoznawania zagrożeń w cyberprzestrzeni - Cyber Threat Intelligence (CTI)

# Adresowane wyzwania i potrzeby
## Ośrodek treningowo – szkoleniowy w obszarze Cyberbezpieczeństwa (OSC)

- Brak wykwalifikowanej kadry specjalistów, którzy będą w stanie skutecznie reagować na nowe rodzaje ataków i zabezpieczać systemy
- Brak wyspecjalizowanego ośrodka pozwalającego na organizację warsztatów scenariuszy cyberzagrożeń i reakcji na nie – szczególnie w domenie publicznej (sale treningowe SOC, red/blue/... team, OT itp.)
- Potrzeba utworzenia modelowego ośrodka treningowo – szkoleniowego:
  - ✓ integrującego szkolenia i treningi specjalistyczne
  - ✓ propagującego cyberbezpieczeństwo w kontekście społecznym (przez kampanie, e-learning  oraz z wykorzystaniem innych nowoczesnych narzędzi)
  - ✓ działającego na bazie aktualnych trendów i doświadczeń CSIRT

# Adresowane wyzwania i potrzeby
## Laboratorium Bezpieczeństwa AI (AITAS)

- Potrzeba badania cyberbezpieczeństwa AI. Rozwój rozwiązań AI napotyka obecnie na problemy z dziedziny bezpieczeństwa, etyki i prawa. Zadbanie o cyberbezpieczeństwo rozwiązań AI jest więc teraz znaczącym wyzwaniem, mającym wpływ na to jak te technologie będą funkcjonowały w cyfrowym świecie.
- Brak zaufanie do rozwiązań AI. Obawa o bezpieczeństwo AI może powstrzymać ich rozwój w kluczowych dziedzinach życia. Powstała więc potrzeba określania narzędzi, procedur i metod osiągania cyberbezpieczeństwa systemów i aplikacji opartych na działaniu samouczących się algorytmów. Propagowanie takich działań może wspomóc uzyskiwanie zaufania do tego typu rozwiązań.
- Potrzeba utworzenie specjalistycznej komórki zajmującej się procesem implementacji narzędzi, procedur i reguł dbania o cyberbezpieczeństwo AI (a w tym monitorowaniem, badaniami, analizami, raportowaniem i propagowaniem najlepszych rozwiązań) - AITAS (ang. Artificial intelligence Trust And Security)

# Adresowane wyzwania i potrzeby
## Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania (FUMAL)

**Obszar FUZZINGU**

- Potrzeba utworzenia podmiotu, który będzie badał możliwe podatności różnych projektów (np. aplikacji, oprogramowania, autonomicznych modeli samodecyzyjnych) zgodnie z wymaganiami bieżącej pracy CISRT
- Potrzeba wykorzystywania metody fuzzingu na poziomie krajowym
- Potrzebna możliwości doboru (wspólnie z partnerami krajowymi) projektów poddawanych testowaniu (jako domena krajowa nie mamy wpływu na dobór projektów testowanych tą metodą przez światowych graczy (np. google))

**Obszar Badania złośliwego oprogramowania**

- Brak skutecznego udostępniania baz CERT Polska dla badaczy, podmiotów KSC oraz obywateli RP
- Konieczność zwiększenia skali analizy złośliwego oprogramowania
- Potrzeba powiększania zestawu informacji z analizy statycznej i behawioralnej, włączenie obszarów zagrożeń mobilnych oraz zwiększenie możliwości przeszukiwania bazy
- Rozbudowa bazy MWDB (Malware Data Base) i nauka pozyskiwania z niej użytecznych informacji dla profesjonalistów niezwiązanych ściśle z analizą złośliwego oprogramowania, w tym organów ścigania

# Adresowane wyzwania i potrzeby
## Krajowe Centrum Kompetencji Security dla JST (KCKS)

- Potrzeba utworzenia rozpoznawalnego w skali kraju miejsca, które umożliwi jednostkom JST skorzystanie ze specjalistycznych konsultacji w obszarze reagowania na incydenty (takie jak pre-testy, analizy, konfiguracje zabezpieczające) w celu wzmocnienia ich odporności i zdolności do podejmowania skutecznych działań zapobiegawczych przed wystąpieniem potencjalnych incydentów oraz skutecznego reagowania na nie
- Potrzeba inicjowania operacji threat huntingowych wspólnie z JST lub grupą JST
- Potrzeba większej otwartości na współpracę JST z odpowiednim CSIRT'em w zakresie adresowania konkretnych problemów

# Adresowane wyzwania i potrzeby
## Ośrodek Certyfikacji Cyberbezpieczeństwa (OCC)

- Potrzeba stworzenia fundamentów pod rozwój krajowego systemu certyfikacji cyberbezpieczeństwa:
  - ✓ potrzeba zapewnienia systemowego podejścia do analizy produktów, usług i procesów (w tym dla rozwiązań chmurowych, IOT,CSAM)
  - ✓ potrzeba opracowania dokumentacji, procedur oraz programów certyfikacji cyberbezpieczeństwa
  - ✓ potrzeba przygotowania, utrzymania i doskonalenia kadry certyfikującej posiadającej niepodważalne w skali kraju kompetencje
  - ✓ potrzeba wzmocnienia NASK jako jednostki certyfikującej w obszarze cyberbezpieczeństwa, a także mającej realny wpływ na podnoszenie poziomu usług krajowych w zakresie zwalczania cyberzagrożeń

# Adresowane wyzwania i potrzeby

## Rozbudowa infrastruktury NASK PIB działającej na rzecz CSIRT NASK

- Potrzeba wzmocnienia i rozwój infrastruktury NASK PIB działającej na rzecz CSiRT NASK wynikająca z bardzo szybkiego rozwoju NASK PIB, co spowodowało dużą różnorodnością infrastruktury wewnętrznej, w tym w zakresie bezpieczeństwa. Taka sytuacja zagraża sprawnemu działaniu CSIRT NASK
- Brak jest spójnego podejścia do korzystania z usług chmurowych - w tym chmury publicznej - co prowadzi do zagrożenia działania wszystkich komórek NASK PIB - w tym CSIRT NASK
- Zasoby obliczeniowe chmur prywatnych NASK PIB, konieczne w szczególności do realizacji zadań laboratoriów CCN, są niewystarczające i wymagają dużego wzmocnienia
- Potrzeba sukcesywnego przeszkolenia z zasad cyberhigieny wszystkich pracowników NASK PIB wynika z konieczności ograniczenia ryzyka ataków (np. socjotechnicznych) na pracowników NASK PIB, a w konsekwencji możliwego ataku na infrastrukturę używaną przez CSIRT NASK

# Budżet i okres realizacji projektu

| | |
|---|---|
| **Szacowana wartość projektu** | **ok. 310 000 000,00* zł** |
| **Szacowany wkład UE** | **247 101 000,00 zł**<br>**(79.71% całkowitej wartości projektu)** |
| **Wkład własny** | **62 899 000,00 zł**<br>**dofinansowany z budżetu Państwa** |
| **Okres realizacji projektu** | **IV kw. 2023 r. – IV kw. 2029 r.** |

* wartość wyliczona przy kursie EUR 4,57 PLN i może ulec zmianie

# Harmonogram realizacji projektu

- Opracowanie założeń projektu: Q3 2023
- Utworzenie obiektu CCN: 2023 – 2027
- Utworzenie centrów, laboratoriów oraz rozbudowa infrastruktury NASK PIB: 2024 – 2029
- Monitorowanie realizacji projektu: 2023 – 2029
- Ewaluacja, rozliczenie projektu: 2030
- Okres trwałości rezultatów projektu: 5 lat (2030-2034)

# Harmonogram realizacji projektu

| | 2023 | | 2024 | | | | 2025 | | | | 2026 | | | | 2027 | | | | 2028 | | | | 2029 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 | Q1 | Q2 | Q3 | Q4 |
| **PRZYGOTOWANIE** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przygotowanie założeń projektowych | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przyjęcie kryteriów przez KM | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przyjęcie projektu przez MFiPR i wpisanie na listę | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Opracowanie studium wykonalności | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Wezwanie do złożenia WoD | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Złożenie WoD | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Ocena WoD | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Podpisanie UoD | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **REALIZACJA** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Faza A:** Utworzenie obiektu CCN (podzadanie 1) | | decyzja w zakresie lokalizacji, pozyskanie zgód i pozwoleń, opracowanie projektów z uwzględnieniem wymogów związanych ze specjalnymi strefami bezpieczeństwa, realizacja budowy, odbiór budynku | | | | | | | | | | | | | | | | | | | | | | | | |
| **Faza B:** Utworzenie centrów, laboratoriów (podzadanie 2) oraz rozbudowa infrastruktury NASK PIB (podzadanie 3) | | | przygotowanie i realizacja postepowań zakupowych, zakup sprzętu , przygotowanie procedur i procesów, szkoleń | | | | | | | | | | | | | | | | | | | | | | | |

# Efekty realizacji projektu 1/2

Wzmocnienie krajowego systemu bezpieczeństwa poprzez:

- Utworzenie Centrum Cyberbezpieczeństwa NASK z nowoczesnymi centrami i laboratoriami badawczymi w obszarze cyberbezpieczeństwa
- Istotne inwestycje zwiększające m.in. poziom bezpieczeństwa informacji poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych państwa oraz podmiotów mających kluczowe znaczenie dla gospodarki
- Budowę i rozwój narzędzi służących do monitorowania bezpieczeństwa, zbierania, analizy i wymiany informacji o zagrożeniach, podatnościach i incydentach, w tym do zaawansowanego rozpoznawania zagrożeń cyberprzestrzeni

# Efekty realizacji projektu 2/2

Wzmocnienie krajowego systemu bezpieczeństwa poprzez:

- Wzmocnienie krajowego systemu certyfikacji cyberbezpieczeństwa produktów, usług i procesów  poprzez opracowanie procedur badawczych oraz metod i technik oceny  oraz opracowywania programów certyfikacji cyberbezpieczeństwa
- Stymulowanie rozwoju innowacyjnych rozwiązań w obszarze cyberbezpieczeństwa poprzez zapewnienie procesu implementacji narzędzi, procedur i reguł dbania o cyberbezpieczeństwo procesów uczenia maszynowego (systemów wykorzystujących AI)
- Optymalizacja i zwiększenie bezpieczeństwa środowiska działania CSIRT NASK
- Zapewnienie możliwości kształcenie kadr w zakresie cyberbepieczeństwa

# Dziękujemy za uwagę