

OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Utworzenie zespołów specjalistów cyberbezpieczeństwa działających lokalnie i wspierających podmioty krajowego systemu cyberbezpieczeństwa w obsłudze incydentów i odzyskiwaniu danych oraz prowadzenie działań podnoszących świadomość o cyberbezpieczeństwie		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	NASK-PIB		
Partnerzy	Komendant Główny Policji – zadania projektowe będą realizowane przez jednostki organizacyjne KGP (Komendy Głównej Policji) oraz CBZC (Centralnego Biura Zwalczania Cyberprzestępczości).		
Źródło finansowania	Krajowy Plan Odbudowy i Zwiększania Odporności, działanie C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo; budżet państwa, część budżetowa - w takcie ustaleń;		
Całkowity koszt projektu	44 143 026,21 zł		
Planowany okres realizacji projektu	11-2024 do 06-2026		
Osoba kontaktowa	Piotr Kozyra	piotr.kozyra@nask.pl	885910130

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Postępująca cyfryzacja usług Państwa to proces nieuchronny i nieodwracalny, przyspieszony dodatkowo przez pandemię, co zwiększyło znaczenie operowania na danych. Niezakłócony dostęp do zbiorów danych stanowi fundament współczesnych usług. Każdorazowe awarie, prace serwisowe lub ataki na środowiska przetwarzania danych prowadzą do zakłóceń w świadczeniu usług, generując rozległe skutki społeczne i ekonomiczne. W latach 2022-2024 podmioty publiczne raportowały do CSIRT NASK ataki na swoje środowiska przetwarzania danych: 24 razy w 2022, 37 razy w 2023 i 25 razy w 2024. Ataki te były przeprowadzane przez wyspecjalizowane grupy przestępcze, wykorzystujące szkodliwe oprogramowanie typu ransomware, żądając okupu za odzyskanie danych lub zaniechanie ich publikacji w Internecie. CSIRT NASK konsekwentnie rekomenduje niepłacenie przestępcom. Ataki ransomware stanowią globalny trend, który z dużym prawdopodobieństwem będzie się nasilał i ewoluował. Każde tego rodzaju zdarzenie wymaga skoordynowanych działań przywracających ciągłość usług, dogłębnej analizy incydentu i ustalenia sprawców. Presja medialna i społeczna dodatkowo utrudnia zarządzanie sytuacją. Ze względu na operowanie na danych ulotnych oraz możliwość celowego niszczenia artefaktów analitycznych, konieczna jest szybka i precyzyjna reakcja. Analitycy CSIRT i funkcjonariusze organów ścigania muszą ściśle współpracować, mając jasne procedury działania. Brak zunifikowanego systemu analizy incydentów skutkuje fragmentaryzacją danych, wydłużonym czasem reakcji i ograniczoną możliwością efektywnej współpracy. Utworzenie centralnego systemu preanalitycznego umożliwi automatyzację wnioskowania, ustrukturyzowaną analizę materiału dowodowego oraz szybsze podejmowanie decyzji operacyjnych, co znacząco podniesie skuteczność reakcji na incydenty cyberbezpieczeństwa.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Policja	<ul style="list-style-type: none"> • Brak niezbędnych narzędzi i procedur – Niedostatek specjalistycznych rozwiązań wsparcia analizy i obsługi incydentów, a także brak ujednoliconych metodyk postępowania. • Limity kompetencyjne i niewystarczające przeszkolenie – Niedostatek szkoleń oraz niedostosowane umiejętności personelu, co utrudnia sprawną reakcję na zaistniałe problemy. • Niedobory sprzętowe i infrastrukturalne – Brak zasobów technicznych pozwalających na efektywne zabezpieczanie danych oraz prowadzenie prac analitycznych w sytuacjach krytycznych. • Brak skutecznych mechanizmów komunikacji – Trudności w wymianie informacji i koordynacji działań między kluczowymi interesariuszami, co opóźnia proces decyzyjny. • Błędne adresowanie problemów w sytuacjach kryzysowych – Brak wypracowanych procedur i jasnych ścieżek eskalacji, co powoduje opóźnienia w reakcji na incydenty i wzrost ich skutków. • Nieoptymalna wymiana materiału analitycznego i dowodowego ze służbami – Brak wypracowanych procedur i kanałów przekazywania materiałów do Policji i Prokuratury powoduje utrudnienia w procesach dochodzeniowych i ogranicza możliwość skutecznego ścigania sprawców cyberprzestępstw. 	100 000
<p>Podmioty Publiczne (Każda instytucja publiczna posiadająca infrastrukturę / usługi sieciowe)</p> <p>https://www.gov.pl/web/cyfryzacja/podmioty-publiczne</p>	<ul style="list-style-type: none"> • Brak priorytetyzacji oraz koordynacji działań po wystąpieniu ataku - Brak klarownej kolejności postępowania, co skutkuje chaotyczną reakcją i opóźnia odzyskanie ciągłości działania. • Niewystarczający poziom wiedzy pracowników w zakresie incydentów cyberbezpieczeństwa - Personel nie dysponuje odpowiednimi informacjami ani umiejętnościami dotyczącymi rozpoznawania zagrożeń i stosowania procedur postępowania. • Nieprawidłowa identyfikacja źródła incydentu (nawracające incydenty) - Błędne określenie lub przeoczenie pierwotnej przyczyny ataku prowadzi do sytuacji, w której incydent (np. ransomware) może się powtórzyć po pewnym czasie. 	76000

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	<ul style="list-style-type: none"> • Utrata kluczowych danych ulotnych istotnych dla analizy - Brak mechanizmów do odpowiednio szybkiego i bezpiecznego zabezpieczania danych wrażliwych (m.in. logów, śladów systemowych) uniemożliwia przeprowadzenie całościowej analizy incydentu. 	
Podmioty KSC	<ul style="list-style-type: none"> • Niewystarczające rozpoznanie zagrożeń zmaterializowanych w obrębie danego sektora lub rynku - Brak efektywnej wymiany informacji oraz kompletnej wiedzy o występujących zagrożeniach, co utrudnia trafne wyciąganie wniosków i utwardzanie środowisk teleinformatycznych. • Niewłaściwy poziom utrzymania i zabezpieczenia usług oraz infrastruktury - Niedostateczne działania utrzymaniowe i prewencyjne, zwiększające podatność na ataki i skutkujące dłuższym czasem przywracania sprawności po incydencie. 	40 000 (Po implementacji NIS2)
NASK PIB / CSIRT NASK / CERT POLSKA	<ul style="list-style-type: none"> • Wydłużony czas realizacji analiz ze względu na brak jakościowego materiału analitycznego - Niedostateczne zabezpieczanie logów, obrazów dysków czy maszyn wirtualnych ogranicza możliwość sprawnego odtworzenia incydentu i powoduje znaczne opóźnienia w przygotowaniu kompleksowych raportów. • Wydłużony czas rozpoznania incydentu z powodu braku wypracowanej metodyki współpracy między zaatakowanym podmiotem a służbami - Brak jasno określonych procedur i odpowiedzialności przekłada się na nieefektywną wymianę informacji i utrudnia przeprowadzenie szybkich działań zaradczych. Może to skutkować błędnie obranymi priorytetami w obsługiwanym incydencie. • Brak standardowej metodyki komunikacji ze służbami w zakresie przyjmowania, wymiany i przekazywania materiału dowodowego oraz raportów - Niewypracowane kanały i formaty współpracy opóźniają przekazywanie kluczowych danych, prowadząc do przedłużenia całego procesu analitycznego i dochodzeniowego. 	1100
CSIRT MON, CSIRT GOV, CSIRTY Sektorowe	<ul style="list-style-type: none"> • Zbyt długi czas rozpoznania i analizy incydentów o wysokiej skali zagrożenia – opóźniona wymiana informacji pomiędzy CSIRT-ami i służbami powodują, że w przypadku poważnych incydentów proces 	50 (analitycy MON, GOV)

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	rozpoznania i neutralizacji zagrożenia jest znacząco wydłużony.	
PROKURATURA	<ul style="list-style-type: none"> • Brak ujednoliconej metodyki postępowania w sprawach cyberprzestępczości – Różnice w podejściu do analizy i klasyfikacji incydentów pomiędzy jednostkami prokuratury skutkują niespójnością działań i wydłużeniem procesów dochodzeniowych. • Ograniczona wiedza specjalistyczna w zakresie analizy incydentów cyberbezpieczeństwa – Niski poziom wyspecjalizowania prokuratorów w obszarze kompetencji dot. Informatyki śledczej utrudnia efektywną współpracę z zespołami CSIRT oraz służbami, co może prowadzić do błędnej kwalifikacji czynów lub trudności w zabezpieczaniu materiału dowodowego. • Brak efektywnego systemu wymiany informacji z CSIRT-ami i służbami – Niedostateczne mechanizmy przekazywania analiz, raportów technicznych i materiałów dowodowych powodują, że postępowania są wydłużone, a ich skuteczność ograniczona. • Problemy w zakresie zabezpieczania i przechowywania dowodów cyfrowych – Brak wypracowanych standardów dotyczących ochrony materiałów pochodzących z cyberprzestępstw prowadzi do ryzyka ich utraty, niewłaściwego przechowywania lub kwestionowania ich integralności w procesach sądowych. 	5000

1.2. Opis stanu obecnego

Artykuł 34.1 UoKSC mówi: CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezp. oraz podmioty świadczące usługi z zakresu cyberbezp. współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań. Począwszy od 2018 roku funkcjonujący w ramach NASK PIB zespół CERT Polska rozpoczął systemowe budowanie relacji na rzecz współpracy przy incydentach teleinformatycznych w sektorze publicznym dla których zaistniało przestępstwo zdefiniowane w Kodeksie Karnym (Art.269 KK). W celu doskonalenia systemu przeprowadzono szereg inicjatyw na rzecz rozwoju obszaru styku NASK PIB oraz Policji. Poza częścią warsztatową (CyberPOL, inicjatywa NASK PIB w latach 2018-2019), identyfikującą luki kompetencyjno-proceduralne dla tego typu spraw, dnia 26.05.2022 podpisano porozumienia kierunkowe pomiędzy jednostkami, dające podwaliny pod uruchomienie szerszego wymiaru współpracy, w tym na rzecz rozwoju szeroko rozumianych systemów. Ze względu na rosnącą liczbę obsługiwanych przez CSIRT NASK spraw tego typu, a także na ich złożony charakter wymagający zaangażowania i koordynacji wielu interesariuszy krajowego systemu cyberbezp., od 08.2022, nawiązano stałą współpracę operacyjną z Sekcją Obsługi Całodobowej WWK CBZC. W ramach tej współpracy prowadzona jest bieżąca

komunikacja w przedmiocie występujących na terenie RP spraw tego typu. W ramach kanału następuje koordynacja działań podejmowanych we współpracy z policją operującą lokalnie. Zaznaczyć należy, że sprowadza się to do ustalenia przedstawicieli organów ścigania, a także przedstawicieli CSIRT NASK, którzy będą prowadzić działania na miejscu w podmiocie. Dalsze kroki w ramach prowadzonych działań są przedmiotem każdorazowych ustaleń pomiędzy stronami. Raport przedstawiający wyniki przeprowadzonych przez CSIRT NASK prac analitycznych jest przekazywany do jednostki prowadzącej lub prokuratury nadzorującej postępowanie w formie elektronicznej, w końcowej fazie obsługi incydentu

2. EFEKTY PROJEKTU

2.1. Cele i korzyści wynikające z projektu

Cel - 1	Modernizacja i ujednolicenie metodyki postępowania przy atakach typu ransomware (lub innych wyczerpujących znamiona przestępstwa (Art.269 KK) w podmiotach krajowego systemu cyberbezpieczeństwa, w celu szybszego przywracania ciągłości usług oraz ograniczenia strat finansowych i społecznych.
Cel strategiczny	Wpisuje się w realizację celu szczegółowego nr 2 Strategii Cyberbezpieczeństwa RP (2019–2024), zakładającego podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego. Strategii Cyberbezpieczeństwa RP na lata 2019–2024, w tym w cel strategiczny nr 2: „Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty”.
Korzyść:	<ul style="list-style-type: none"> - Skrócenie czasu reakcji na incydenty. - Zwiększenie skuteczności w ustalaniu sprawców oraz zabezpieczaniu materiału dowodowego. - Podniesienie poziomu zaufania społecznego do zdolności organów ścigania w zakresie zwalczania cyberprzestępczości.
KPI:	<p>KPI 1: Opracowanie ujednoliconych metodyki oraz skonfigurowanie odpowiedniego zaplecza systemowego, pozwalających na kompleksową, powtarzalną i szybką reakcję na incydenty typu ransomware (i inne poważne zdarzenia)</p> <p>KPI 2: Liczba podmiotów krajowego systemu cyberbezpieczeństwa (KSC) wdrażających nową metodykę postępowania przy atakach ransomware.</p>
Wartość aktualna i docelowa KPI:	<p>KPI 1: - wartość aktualna: 0</p> <p>KPI 2: - wartość aktualna: 0</p> <p>KPI 1: - wartość docelowa: 1 (Wytworzono kompletną nową metodykę do końca I kw. 2026 r.</p> <p>KPI 1: - wartość docelowa: Minimum 2 podmioty podlegające pod KSC wdrożyły nową metodykę do końca II kw. 2026 r.</p>

Metoda pomiaru KPI	<p>KPI 1: Ćwiczenia tabletop z wykorzystaniem wytworzonego systemu (jednorazowo)</p> <p>KPI 2: Raport z zastosowania metodyki w analizie incydentów (na koniec projektu)</p>
Cel - 2	Stworzenie i wdrożenie centralnego systemu preanalitycznego służącego do bezpiecznego transferu i analizy danych dowodowych, umożliwiającej sprawną współpracę pomiędzy Policją (CBZC), Prokuraturą oraz CSIRT NASK.
Cel strategiczny	<p>Wpisuje się w zadania wskazane w KPO (Komponent C3.1.1. Cyberbezpieczeństwo – CyberPL), zmierzające do optymalizacji i cyfryzacji współpracy służb państwowych odpowiedzialnych za bezpieczeństwo.</p> <p>Wpisuje się w realizację Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), Komponent C3.1.1. Cyberbezpieczeństwo – CyberPL, w tym w cel strategiczny: „Zwiększenie skuteczności krajowego systemu cyberbezpieczeństwa poprzez cyfryzację procesów współpracy służb odpowiedzialnych za bezpieczeństwo”.</p>
Korzyść:	<ul style="list-style-type: none"> - Usprawniona koordynacja międzyinstytucjonalna. - Krótszy czas obsługi incydentu dzięki szybkiemu udostępnianiu materiałów i raportów. - Zwiększenie skuteczności postępowań karnych dzięki lepszemu zabezpieczaniu dowodów cyfrowych.
KPI:	<p>KPI 1: Liczba uruchomionych platform wspierających współpracę międzyinstytucjonalną</p> <p>KPI 2: Uśredniony czas obsługi incydentów wymagających współpracy międzyinstytucjonalnej</p> <p>KPI 3: Liczba spraw, w których nowy system został wykorzystany w analizie materiałów dowodowych</p>
Wartość aktualna i docelowa KPI:	<p>KPI 1:</p> <ul style="list-style-type: none"> - wartość aktualna: 0 <p>KPI 2:</p> <ul style="list-style-type: none"> - wartość aktualna: 90 dni (średni czas obsługi w 2024 r.). <p>KPI 3:</p> <ul style="list-style-type: none"> - wartość aktualna: 0 <p>KPI 1:</p> <ul style="list-style-type: none"> - wartość docelowa: 1 <p>KPI 2:</p> <ul style="list-style-type: none"> - wartość docelowa: 30 dni (średni czas obsługi w 2026 r. po wdrożeniu platformy). <p>KPI 3:</p> <ul style="list-style-type: none"> - wartość docelowa: 30 spraw rocznie
Metoda pomiaru KPI	<p>KPI 1:</p> <p>Wdrożenie systemu</p> <ul style="list-style-type: none"> • Sposób pomiaru: Notatka z wdrożenia • Źródło pomiaru: Repozytorium kodu • Termin pomiaru: Wdrożenie systemu w wersji produkcyjnej

	<p>KPI 2:</p> <ul style="list-style-type: none"> • Sposób pomiaru: Analiza danych operacyjnych • Źródło danych: System zgłoszeń incydentów, raporty podsumowujące działania międzyinstytucjonalne • Częstotliwość pomiaru: Półroczne raportowanie + pomiar końcowy <p>KPI 3:</p> <ul style="list-style-type: none"> • Sposób pomiaru: Ewaluacja ilościowa – liczba spraw wykorzystujących system • Źródło danych: Raporty z użytkowania systemu, dane operacyjne CBZC i CSIRT • Częstotliwość pomiaru: Pomiar kwartalny + końcowy
Cel - 3	Modernizacja i rozwój stanowisk sprzętowych w tym oprogramowania, w komórkach Policji (CBZC), zajmujących się zwalczaniem cyberprzestępczości, ze szczególnym uwzględnieniem narzędzi do zabezpieczania danych ulotnych i odzyskiwania informacji.
Cel strategiczny	Realizuje założenia Strategii Cyberbezpieczeństwa RP w obszarze zwiększania zdolności operacyjnych organów ścigania. Wpisuje się w realizację Strategii Cyberbezpieczeństwa RP na lata 2019–2024, w tym w cel strategiczny nr 3: „Zwiększenie zdolności operacyjnych organów ścigania, administracji i sektora prywatnego do zwalczania cyberzagrożeń”.
Korzyść:	<ul style="list-style-type: none"> - Skrócenie czasu analizy incydentu dzięki wyspecjalizowanym narzędziom. - Poprawa jakości zabezpieczanego materiału dowodowego (minimalizacja ryzyka utraty danych). - Możliwość szybszego identyfikowania i neutralizowania zagrożeń.
KPI:	<p>KPI 1: Liczba zmodernizowanych komórek organizacyjnych Policji (CBZC) dysponujących nowym sprzętem.</p> <p>KPI 2: Liczba zmodernizowanych komórek organizacyjnych Policji (CBZC) dysponujących nowym oprogramowaniem.</p>
Wartość aktualna i docelowa KPI:	<p>KPI 1:</p> <ul style="list-style-type: none"> - wartość aktualna: 0 <p>KPI 2:</p> <ul style="list-style-type: none"> - wartość aktualna: 0 <p>KPI 1:</p> <ul style="list-style-type: none"> - wartość docelowa: 18 zmodernizowanych komórek organizacyjnych Policji do końca II kw. 2026 r. <p>KPI 2:</p> <ul style="list-style-type: none"> - wartość docelowa: 18
Metoda pomiaru KPI	<p>KPI 1:</p> <p>Zakończona procedura zakupowa i wykonanie odbiorów sprzętu</p> <ul style="list-style-type: none"> • Sposób pomiaru: Protokół odbioru • Źródło danych: Dokumentacja projektowa / protokół odbioru • Częstotliwość pomiaru: Jednorazowo w dniu zakończenia projektu <p>KPI 2:</p> <p>Zakończona procedura zakupowa i wykonanie odbiorów</p> <ul style="list-style-type: none"> • Sposób pomiaru: Protokół odbioru • Źródło danych: Dokumentacja projektowa / protokół odbioru

	<ul style="list-style-type: none"> • Częstotliwość pomiaru: Jednorazowo w dniu zakończenia projektu
Cel - 4	Rozwój kompetencyjny funkcjonariuszy Policji (CBZC), Prokuratury oraz pracowników podmiotów krajowego systemu cyberbezpieczeństwa (KSC) w zakresie prewencji, detekcji i reakcji na ataki ransomware poprzez zintegrowany system szkoleń.
Cel strategiczny	<p>Odpowiada wytycznym Strategii Cyberbezpieczeństwa RP, ukierunkowanym na rozwój kompetencji cyfrowych pracowników administracji oraz służb publicznych.</p> <p>Wpisuje się w realizację Strategii Cyberbezpieczeństwa RP na lata 2019–2024, w tym w cel strategiczny nr 5: „Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów IT oraz pracowników administracji publicznej”.</p>
Korzyść:	<ul style="list-style-type: none"> - Rozwój kompetencyjny uczestników KSC. - Wyższy poziom świadomości wśród pracowników i funkcjonariuszy (ograniczenie ryzyka ludzkich błędów). - Wzmocnienie autorytetu służb państwowych dzięki skuteczniejszym działaniom i transparentnym procedurom.
KPI:	<p>KPI 1: Liczba funkcjonariuszy i pracowników podmiotów KSC objętych szkoleniami</p> <p>KPI 2: Liczba przeprowadzonych seminariów</p>
Wartość aktualna i docelowa KPI:	<p>KPI 1:</p> <ul style="list-style-type: none"> - wartość aktualna: 0 <p>KPI 2:</p> <ul style="list-style-type: none"> - wartość aktualna: 0 <p>KPI 1:</p> <ul style="list-style-type: none"> - wartość docelowa: 1900 przeszkolonych uczestników (łącznie suma) do końca II kw. 2026 r. <p>KPI 2:</p> <ul style="list-style-type: none"> - wartość docelowa: 1
Metoda pomiaru KPI	<p>KPI 1:</p> <ul style="list-style-type: none"> • Sposób pomiaru: Realizacja szkoleń • Źródło danych: Lista obecności i/lub protokół odbioru • Częstotliwość pomiaru: Po zakończonym szkoleniu <p>KPI 2:</p> <ul style="list-style-type: none"> • Sposób pomiaru: Realizacja seminarium • Źródło danych: Dokumentacja seminarium, raporty organizatorów • Częstotliwość pomiaru: Pomiar jednorazowy na koniec projektu

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi
1	Zgłoszenie incydentu i przekazanie materiału do wspólnej analizy	A2B A2A	Policja Podmioty Publiczne	Dwustronna interakcja

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi
	(Uploader)		Podmioty KSC NASK PIB / CSIRT NASK / CERT POLSKA CSIRT MON, CSIRT GOV, CSIRTY Sektorowe PROKURATURA (rocznie ok 100 transakcji)	
2	Dostęp do wyników analiz i raportów końcowych	A2A	Policja NASK PIB / CSIRT NASK / CERT POLSKA PROKURATURA CSIRT MON, CSIRT GOV, CSIRTY Sektorowe (rocznie ok 50 transakcji)	Dwustronna interakcja
3	Dostęp do repozytorium wiedzy o incydentach i rekomendacjach postępowania	A2A	Policja NASK PIB / CSIRT NASK / CERT POLSKA PROKURATURA CSIRT MON, CSIRT GOV, CSIRTY Sektorowe (rocznie ok 100 transakcji)	Jednostronna interakcja

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
Materiały informacyjno-promocyjne zwiększające świadomość interesariuszy na temat projektu i jego efektów	09-2025
Materiały szkoleniowe – materiały dydaktyczne wspierające proces podnoszenia kompetencji	03-2026
Raport z testu prywatności	05-2026
CROPT - System teleinformatyczny wspierający analizę danych dowodowych, wymianę materiałów międzyinstytucjonalnych oraz wsparcie zarządzania incydentami cyberbezpieczeństwa	06-2026
Raport z testów bezpieczeństwa – dokumentacja dotycząca weryfikacji zabezpieczeń wdrożonych systemów i infrastruktury	06-2026

Nazwa produktu	Planowana data wdrożenia
Raport z testów wydajności – analiza obciążenia i skalowalności systemów w kontekście przetwarzania danych dowodowych	06-2026
Raport WCAG - WCAG (Web Content Accessibility Guidelines) to zestaw międzynarodowych wytycznych opracowanych przez W3C, które definiują techniczne i projektowe kryteria zapewnienia dostępności treści internetowych dla osób z różnymi ograniczeniami, koncentrując się na czterech filarach: postrzegalności, funkcjonalności, zrozumiałości i solidności	06-2026

3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
- Ukończone prace koncepcyjno-programistyczne	2025-04-30
- Uruchomiony prototyp narzędzia do współdzielenia materiału (Wdrożenie wersji testowej platformy w środowisku testowym oraz rozpoczęcie testów funkcjonalnych)	2025-09-30
- Zakupione kluczowe elementy infrastruktury IT (serwery, stacje robocze, urządzenia do analizy incydentów teleinformatycznych)	2025-12-31
- Uruchomiona wersja produkcyjna narzędzia do współdzielenia materiału (Wdrożony system w środowisku operacyjnym).	2026-05-29
- Przeprowadzono inicjalny test prywatności	2026-05-29
- Zakończone testy bezpieczeństwa, wydajności, WCAG podsumowane raportami.	2026-06-30
- Zmodernizowana infrastruktura sprzętowa i oprogramowanie CBZC (Zakupiony, zainstalowany i skonfigurowany sprzęt dla CBZC (m.in. narzędzia do odzyskiwania danych, sprzęt perymetryczny)).	2026-06-30
- Zakończony proces zakupowy, komplet sprzętu projektowego znajduje się w siedzibie zamawiającego (NASK-PIB) i jest wykorzystywany operacyjnie.	2026-06-30

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

Całkowity koszt projektu (netto oraz brutto), w tym	Netto 37 500 000,00 zł Brutto 44 143 026,21 zł	
Procent dofinansowania ze środków UE (brutto)	85%	
Procent środków z budżetu państwa (brutto)	15%	
Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto)	2024	Netto 0,00 zł Brutto 0,00 zł
	2025	Netto 35 114 331,35 zł Brutto 41 743 557,56 zł
	2026	Netto 2 385 668,65 zł Brutto 2 399 468,65 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Koszt wytworzenia oprogramowania specjalistycznego – prace analityczne, programistyczne, wytwarzanie, testowanie, wdrożenie	9 090 528,06 zł	Wytworzenie specjalistycznego oprogramowania jest niezbędny do wdrożenia nowych narzędzi analitycznych i systemów raportowania incydentów. Brak tych rozwiązań uniemożliwiłby sprawną obsługę zgłoszeń oraz szybką analizę incydentów. W efekcie ograniczyłoby to możliwość skutecznego zabezpieczania i odzyskiwania danych dotkniętych atakiem
Infrastruktura	Zakup urządzeń i wyposażenia technicznego, koszty wynagrodzeń personelu projektującego i wdrażającego elementy infrastruktury	23 943 082,42 zł	„Modernizacja sprzętowa obejmująca serwery, macierze dyskowe i zestawy kryminalistyczne pozwala na wytworzenie i utrzymanie platformy do zarządzania incydentami i wymiany danych. Inwestycja jest kluczowa w kontekście realizacji kamieni milowych projektu.
Koszty UX i grafiki	Koszty wynagrodzeń personelu wytwarzającego makiety systemu, projektującego i	104 393,59 zł	Przejrzysty interfejs oraz czytelna warstwa graficzna zwiększają efektywność pracy użytkowników, zwłaszcza przy wieloetapowych procesach obsługi incydentów. Dzięki intuicyjnemu UX możliwe

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	wdrażającego rozwiązania.		jest skrócenie czasu potrzebnego do poznania platformy i ograniczenie błędów ludzkich. Usprawnia to również współpracę międzyinstytucjonalną, gdy różne służby korzystają z jednego narzędzia.
Bezpieczeństwo	Zakup urządzeń oraz wynagrodzenia personelu konfigurujuącego elementy infrastruktury – sprzęt i usługi wytworzone w ramach projektu. Przeprowadzenie testów bezpieczeństwa, koszty utwardzania systemu i realizacji rekomendacji wynikających z przeprowadzonych testów.	332 765,42 zł	Środki na podniesienie poziomu bezpieczeństwa pozwalają uniknąć wycieku danych i nieautoryzowanego dostępu. W kontekście incydentów ransomware, a także krytycznych danych przetwarzanych w systemie, zabezpieczenie kluczowych systemów jest absolutnym priorytetem. Te inwestycje obniżają ryzyko strat finansowych i wizerunkowych. Środki na przeprowadzenie testów bezpieczeństwa.
Wydajność rozwiązań	Wynagrodzenie personelu odpowiadającego za optymalizacji wydajności wprowadzanych rozwiązań oraz przeprowadzenie testów wydajności	201 240,65 zł	Zapewnienie wydajności wdrażanych systemów (poprzez zapewnienie odpowiedniej mocy obliczeniowej) gwarantuje szybką sprawne działanie systemu zarządzania i współdzielenia incydentów i sprawniejszą reakcję na zagrożenia. Bez odpowiednich parametrów pracy narzędzi, podmioty nie będą w stanie obsłużyć rosnącej liczby zgłoszeń. Skalowalna architektura zapobiega utrudnieniom i utrzymuje stabilność usług w sytuacjach krytycznych. Środki na przeprowadzenie testów wydajności.
Szkolenia	Zaawansowane kursy dla specjalistów zajmujących się cyberbezpieczeństwem.	6 477 785,65 zł	Rozwój kompetencji personelu w zakresie nowoczesnych technik analizy incydentów i odzyskiwania danych stanowi klucz do skutecznej reakcji na ataki i zapewnienia ciągłości

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	Przygotowanie materiałów szkoleniowych.		działania systemów. Szkolenia m.in. BTL oraz SANS to rozpoznawalny standard branżowy, gwarantujący wysoki poziom wiedzy specjalistycznej. Materiały szkoleniowe.
Działania informacyjno-promocyjne	Promocja i informacja (materiały i koszty inne)	669 484,09 zł	Prezentacje i wystąpienia poszerzające świadomość o zagrożeniach cyberbezpieczeństwa wśród interesariuszy (instytucje publiczne, sektor biznesowy), a także wymiana doświadczeń z innymi krajowymi i międzynarodowymi ekspertami.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Wyjazdy służbowe związane z realizacją projektu (np. spotkania koordynacyjne, wizyty w innych jednostkach oraz wynagrodzenie personelu zarządzającego i wspomagającego. Zawiera również koszty pośrednie w wysokości 6% od wszystkich kosztów bezpośrednich.	3 323 746,33 zł	Prawidłowe zarządzanie projektem wymaga koordynacji działań między różnymi interesariuszami (Policja, Prokuratura, CSIRT NASK), co wiąże się z koniecznością odbywania delegacji. Dzięki temu możliwe jest ustalenie spójnych procedur i skoordynowanie planu wdrożenia nowych rozwiązań. Koszty pośrednie, w tym m.in. koszty personelu obsługowego, koszty utrzymania powierzchni biurowych, opłaty za energię i wodę, koszty materiałów biurowych, prowadzenia rachunków, ochrony czy sprzątania.

4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania (okres 5 lat)

Całkowity koszt utrzymania trwałości projektu (brutto)	6 473 814,67 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz	2026	504 949,78 zł (brutto) (488 849,78 zł netto)	krajowe środki publiczne - budżet państwa
	2027	1 110 889,51 zł (brutto) (1 075 469,51 zł netto)	krajowe środki publiczne - budżet

brutto)			państwa
	2028	1 221 978,46 zł (brutto) (1 183 016,46 zł netto)	krajowe środki publiczne - budżet państwa
	2029	1 344 176,31 zł (brutto) (1 301 318,11 zł netto)	krajowe środki publiczne - budżet państwa
	2030	1 478 593,94 zł (brutto) (1 431 449,92 zł netto)	krajowe środki publiczne - budżet państwa
	2031	813 226,67 zł (brutto) (787 297,45 zł netto)	krajowe środki publiczne - budżet państwa

4.4. Planowane koszty ogólne realizacji (w przypadku projektu współfinansowanego – wkład krajowy z budżetu państwa) oraz koszty utrzymania projektu:

- zostaną pokryte w ramach budżetów odpowiednich dysponentów części budżetowych bez konieczności występowania o dodatkowe środki z budżetu państwa
- będą powodować konieczność przyznania dodatkowych kwot

5. GŁÓWNE RYZYKA

5.1. Ryzyka wpływające na realizację projektu

Nazwa ryzyka	Siła oddziaływania		Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Brak możliwości zatrudnienia osób o odpowiednich kompetencjach	Duża		Średnie	Współpraca z uczelniami technicznymi i ośrodkami szkoleniowymi, dostosowanie polityki wynagrodzeń do konkurencyjnych stawek rynkowych.
Brak wystarczających zasobów kadrowych do realizacji projektu	Duża		Średnie	Przesunięcie wewnętrznych zasobów, outsourcing części zadań, uwzględnienie elastycznych form współpracy (np. umowy eksperckie, kontrakty krótkoterminowe).
Przekroczenie harmonogramu realizacji projektu	Duża		Średnie	Monitorowanie postępów w cyklach kwartalnych, wprowadzenie buforów czasowych, zapewnienie dodatkowego wsparcia kadrowego w kluczowych momentach projektu.
Nieosiągnięcie wskaźników	Duża		Niskie	Bieżąca kontrola postępów i raportowanie w odniesieniu do KPI,

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
produktu oraz celu projektu			dostosowanie działań projektowych w razie ryzyka nieosiągnięcia założeń.
Przekroczenie budżetu projektu	Duża	Niskie	Ścisła kontrola kosztów, bufor finansowy, monitorowanie kluczowych wydatków na bieżąco.
Opóźnienia w pozyskaniu sprzętu i oprogramowania wynikające z utrudnień procesu zakupowego w PZP, ryzyka odwołań do KIO, chwilowego braku dostępności wybranego sprzętu.	Średnia	Średnie	Ujęcie w harmonogramie dodatkowego czasu na dostawę sprzętu. Przydzielenie dodatkowych zasobów do realizacji procesów zakupowych
Opóźnienie we wdrożeniu metodyki przez CBZC / Policję oraz innych partnerów / podmioty KSC	Duża	Średnie	Wyznaczenie koordynatora: Osoby odpowiedzialnej za przepływ informacji między wszystkimi zaangażowanymi instytucjami.
Brak możliwości pełnej realizacji projektu w planowanych ramach czasowych Ograniczenia wynikające z czasu trwania projektu i kwalifikowalności wydatkowania środków	Duża	Średnie	Zapewnić kontynuację przedsięwzięcia z innego źródła finansowania
Zmiany regulacyjne i prawne	Duża	Niskie	Monitoring legislacyjny: Wyznaczenie osoby lub zespołu śledzącego na bieżąco zmiany w prawie krajowym i unijnym. Elastyczne zapisy w dokumentacji projektowej: Umieszczenie klauzul o możliwej modyfikacji zakresu w razie istotnych zmian przepisów. Konsultacje z ekspertami prawnymi:

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
			Regularna weryfikacja projektu pod kątem zgodności z nowymi regulacjami (np. NIS2/ Nowelizacja KSC).

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Zmiana kształtu KSC (np. ograniczenie kompetencji CSIRT NASK)	Duża	Znikome	<ul style="list-style-type: none"> - Ustanowienie dedykowanego zespołu lub koordynatora do bieżącego śledzenia prac nad ustawą o KSC (w tym potencjalnych nowelizacji) oraz analizowania ich konsekwencji dla projektu. - Regularne konsultacje z przedstawicielami administracji rządowej i innych interesariuszy (np. Ministerstwo Cyfryzacji, KPRM), aby jak najwcześniej uzyskać informacje o proponowanych zmianach w kompetencjach CSIRT NASK. - Wprowadzenie do umów klauzul o utrzymaniu i rozwoju rozwiązań w zakresie cyberbezpieczeństwa niezależnie od modyfikacji przepisów regulujących status jednego uczestnika systemu.
Brak możliwości zatrudnienia osób o odpowiednich kompetencjach niezbędnych do utrzymania efektów projektu	Duża	Średnie	Utworzenie długoterminowej ścieżki kariery dla kluczowych ekspertów, współpraca z ośrodkami edukacyjnymi, programy szkoleniowe dla pracowników.
Brak wystarczających zasobów kadrowych do utrzymania efektów projektu	Duża	Średnie	Zabezpieczenie etatów w ramach budżetu operacyjnego, elastyczne modele zatrudnienia, rotacja pracowników w ramach różnych zespołów.
Brak wystarczających środków na	Duża	Średnie	Opracowanie długoterminowego planu finansowania, zabezpieczenie środków w budżecie państwa lub w ramach

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
utrzymanie efektów projektu			funduszy UE.
Niska adopcja nowego systemu przez użytkowników końcowych	Średnia	Średnie	Intensywne szkolenia dla użytkowników, uproszczona dokumentacja, wsparcie techniczne po wdrożeniu.
Nieosiągnięcie wszystkich zaplanowanych korzyści	Duża	Niskie	Regularna ewaluacja rezultatów projektu, wdrożenie planu optymalizacji i doskonalenia wypracowanych narzędzi.

6. OTOCZENIE PRAWNE

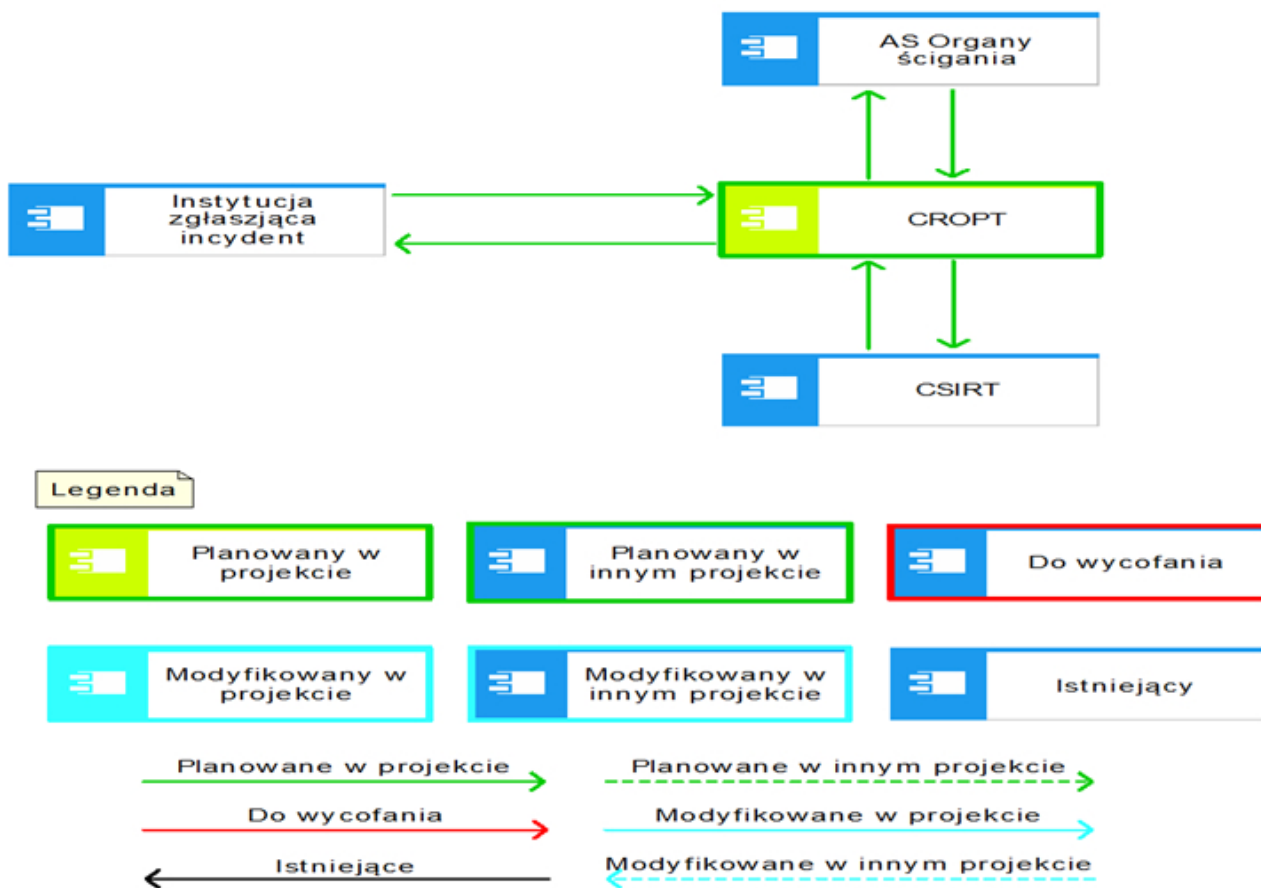
Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC)	TAK/NIE		
2	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (Dyrektywa NIS 2)	TAK/NIE		
3	Uchwała Rady Ministrów w sprawie przyjęcia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (uchwała nr 125/2019)	TAK/NIE		
4	Ustawa z dnia 6 kwietnia 1990 r. o Policji	TAK/NIE		
5	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne	TAK/NIE		
6	Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).	TAK/NIE		
7	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oraz Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781)	TAK/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
8	Krajowy Plan Odbudowy i Zwiększania Odporności (KPO), Komponent C3.1.1 – „Cyberbezpieczeństwo – CyberPL”	TAK/NIE		
9	Ustawa z dnia 11 września 2019 r. – Prawo zamówień publicznych	TAK/NIE		
10	Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46)	TAK/NIE		
11	Rozporządzenie Prezesa Rady Ministrów z dnia 26 kwietnia 2023 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego • Dz. U. z 2023 r. poz. 789	TAK/NIE		
12	Rozporządzenie Prezesa Rady Ministrów z dnia 14 października 2023 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych • Dz. U. z 2023 r. poz. 1023	TAK/NIE		
13	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO)	TAK/NIE		
14	Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych • Tekst jednolity: Dz. U. z 2024 r. poz. 1769 • Ostatnia nowelizacja: Dz. U. z 2024 r. poz. 1254	TAK/NIE		
15	Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego • Tekst jednolity: Dz. U. z 2023 r. poz. 1524 • Ostatnia nowelizacja: Dz. U. z 2022 r. poz. 1700	TAK/NIE		
16	Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych • Tekst jednolity: Dz. U. z 2020 r. poz. 344 • Ostatnia nowelizacja: Dz. U. z 2022 r. poz. 1264	TAK/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
17	Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych <ul style="list-style-type: none"> • Tekst jednolity: Dz. U. z 2021 r. poz. 777 • Ostatnia nowelizacja: Dz. U. z 2023 r. poz. 1234 	TAK /NIE		
18	Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych <ul style="list-style-type: none"> • Tekst jednolity: Dz. U. z 2020 r. poz. 2320 • Ostatnia nowelizacja: Dz. U. z 2023 r. poz. 567 	TAK /NIE		
19	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej <ul style="list-style-type: none"> • Tekst jednolity: Dz. U. z 2019 r. poz. 162 • Ostatnia nowelizacja: Dz. U. z 2022 r. poz. 987 	TAK /NIE		
20	Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie profilu zaufanego i podpisu zaufanego <ul style="list-style-type: none"> • Dz. U. z 2018 r. poz. 1938 	TAK /NIE		
21	Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników <ul style="list-style-type: none"> • Dz. U. z 2018 r. poz. 1780 	TAK /NIE		
22	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych <ul style="list-style-type: none"> • Tekst jednolity: Dz. U. z 2019 r. poz. 1781 • Ostatnia nowelizacja: Dz. U. z 2023 r. poz. 456 	TAK /NIE		
23	Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych <p>Tekst jednolity: Dz. U. z 2019 r. poz. 742</p> <p>Ostatnia nowelizacja: Dz. U. z 2022 r. poz. 1111</p>	TAK /NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



Lista systemów wykorzystywanych w projekcie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	CROPT	CSIRT	Centralny system preanalityczny do współdzielenia materiałów związanych z postępowaniami prowadzonymi przez zespoły reagowania i analityków. Ma on umożliwić szybkie i bezpieczne przekazywanie zabezpieczonego materiału związanego z prowadzonymi działaniami mających na celu analizę zaistniałego incydentu. Umożliwia współdzielenie materiału	Planowany	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			oraz wymianę informacji dotyczących ustaleń i wyników analiz. Posiada możliwość zarządzania rolą i uprawnieniami w dostępie do wspomnianego materiału, jak i do ustaleń związanych z prowadzoną analizą. System ma obejmować kilka komponentów: CORE – zarządzanie systemem, CASE – zarządzanie incydem, UPLOADER – transfer materiałów, Baza wiedzy - moduł pomagający użytkownikowi przejść przez zabezpieczanie materiału, dostarczający informacji jak korzystać z systemu.		
2	CSIRT	Ministerstwo Spraw Wewnętrznych i Administracji / Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Zespół oraz system wspomagający prace CSIRT poziomu krajowego odpowiadający za proces reagowania na incydenty komputerowe występujące w obszarze wskazanym w ustawie z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U.2018 poz.1560)	Istniejący	
3	AS Organy Ścigania	Ministerstwo Spraw Wewnętrznych i Administracji / AS Organy Ścigania	Zespół oraz system wspomagający pracę organów ścigania w zakresie cyberprzestępczości, odpowiadający za proces zbierania, analizy i zabezpieczania materiałów dowodowych w sprawach przestępstw popełnionych z wykorzystaniem	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			systemów teleinformatycznych, zgodnie z ustawą z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. 2023 poz. 1234) oraz ustawą z dnia 6 kwietnia 1990 r. o Policji (Dz.U. 2024 poz. 567).		
4	Instytucja zgłaszająca incydent	Właściwe dla instytucji ministerstw o / Instytucja zgłaszająca incydent	Podmiot zgłaszający incydent (poszkodowany), czyli instytucja publiczna, przedsiębiorstwo lub inny podmiot wskazany w ustawie z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 923), zobowiązany do identyfikacji, zgłaszania oraz współpracy w zakresie obsługi incydentów komputerowych, w tym dostarczania niezbędnych informacji umożliwiających ich analizę i skuteczne przeciwdziałanie skutkom naruszeń bezpieczeństwa teleinformatycznego.	Istniejący	

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	AS Organy Ścigania	CROPT	Opracowane dane - wskaźniki aktywności atakującego Opracowane dane - wyniki analizy Opracowane	Online, interfejs CROPT, tryb odwołań bezpośrednich (§13 ust. 2) i kopiowanie danych (§13 ust. 3)	krytyczny dla sukcesu projektu	Usługa WWW oraz protokół SFTP

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			<p>dane – informacja o elementach niezbędnych do zabezpieczenia</p> <p>Dane dot. incydentu - Obrazy maszyn wirtualnych (małe wolumeny)</p> <p>Dane dot. incydentu - Obrazy maszyn wirtualnych (duże wolumeny)</p> <p>Dane dot. incydentu - Dyski fizyczne</p> <p>Dane dot. incydentu - Serwery fizyczne</p>			
2	CROPT	AS Organy Ścigania	<p>Raport dot. incydentu - podsumowanie analizy incydentu</p> <p>Informacje o zgłaszającym - Dane kontaktowe</p> <p>Informacje o zgłaszającym - informacje wstępne o incydencie</p> <p>Informacje o zgłaszającym - Osoba decyzyjna / upoważniona</p> <p>Informacje o zgłaszającym -</p>	Online, interfejs CROPT, tryb odwołań bezpośrednich (§13 ust. 2)	krytyczny dla sukcesu projektu	USŁUGA WWW

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			<p>adres siedziby</p> <p>Informacje o zgłaszającym - powiązanie infrastruktury z innymi podmiotami/ placówkami</p> <p>Informacje o zgłaszającym - informacje o architekturze infrastruktury</p> <p>Dane dot. incydentu - Wskaźniki aktywności atakującego</p> <p>Opracowane dane - wskaźniki aktywności atakującego</p> <p>Opracowane dane - wyniki analizy</p> <p>Opracowane dane – informacja o elementach niezbędnych do zabezpieczenia</p> <p>Udostępnione dane dot. incydentu - materiał w postaci zaszyfrowanej</p> <p>Dane dot. incydentu - Dyski fizyczne</p> <p>Dane dot. incydentu – Serwery fizyczne</p>			
3	Instytucja zgłaszając	CROPT	Informacje o zgłaszającym -	Online, interfejs	krytyczny dla sukcesu	USŁUGA WWW

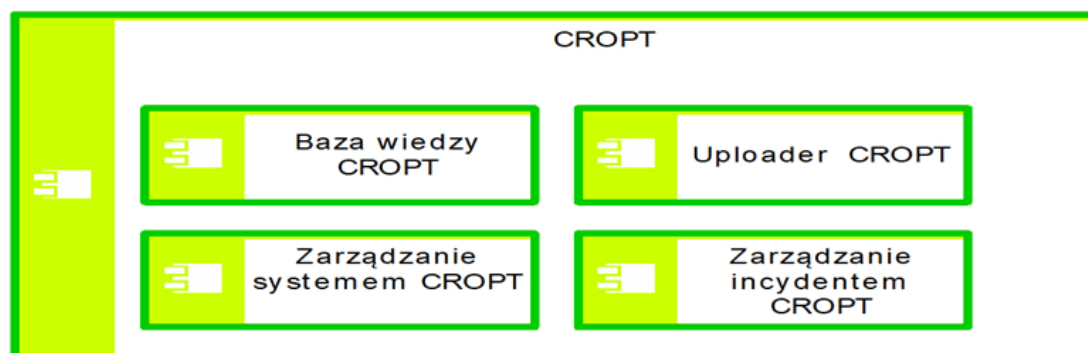
Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
	a incydent		Dane kontaktowe Informacje o zgłaszającym - informacje wstępne o incydencie Informacje o zgłaszającym - Osoba decyzyjna / upoważniona Informacje o zgłaszającym - adres siedziby Informacje o zgłaszającym - powiązanie infrastruktury z innymi podmiotami/ placówkami Informacje o zgłaszającym - informacje o architekturze infrastruktury Dane dot. incydentu - Wskaźniki aktywności atakującego Dane dot. incydentu - Logi z urządzeń instytucji Dane dot. incydentu - Pliki powiązane z atakującym Dane dot. incydentu - Obrazy maszyn wirtualnych Dane dot. incydentu - Dyski fizyczne	CROPT, tryb odwołań bezpośrednich (§13 ust. 2)	projektu	

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			Dane dot. incydentu - Serwery fizyczne			
4	CSIRT	CROPT	Raport dot. incydentu - podsumowanie analizy incydentu Opracowane dane - wskaźniki aktywności atakującego Opracowane dane - wyniki analizy Opracowane dane – informacja o elementach niezbędnych do zabezpieczenia a Opracowanie metodyk postępowania – zabezpieczenia materiałów Dane dot. incydentu - Obrazy maszyn wirtualnych Dane dot. incydentu - Dyski fizyczne Dane dot. incydentu - Serwery fizyczne	interfejs CROPT, tryb odwołań bezpośrednich (§13 ust. 2) i kopiowanie danych (§13 ust. 3)	krytyczny dla sukcesu projektu	USŁUGA WWW oraz protokół SFTP
5	CROPT	CSIRT	Informacje o zgłaszającym - Dane kontaktowe Informacje o zgłaszającym -	Online, interfejs CROPT, tryb odwołań bezpośrednich (§13 ust. 2)	krytyczny dla sukcesu projektu	USŁUGA WWW

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			informacje wstępne o incydencie Informacje o zgłaszającym - Osoba decyzyjna / upoważniona Informacje o zgłaszającym - adres siedziby Informacje o zgłaszającym - powiązanie infrastruktury z innymi podmiotami/ placówkami Informacje o zgłaszającym - informacje o architekturze infrastruktury Dane dot. incydentu - Wskaźniki aktywności atakującego Dane dot. incydentu - Logi z urządzeń instytucji Dane dot. incydentu - Pliki powiązane z atakującym Dane dot. incydentu - Obrazy maszyn wirtualnych Dane dot. incydentu - Dyski fizyczne Dane dot. incydentu - Serwery fizyczne			

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			Opracowane dane – wyniki analizy Opracowane dane – wskaźniki aktywności atakującego Udostępnione dane dot. incydentu - materiał w postaci zaszyfrowanej			
6	CROPT	Instytucja zgłaszająca incydent	Instrukcje postępowania - zabezpieczenie materiałów Raport dot. incydentu - podsumowanie analizy incydentu Opracowane dane - wskaźniki aktywności atakującego Opracowane dane - wyniki analizy Opracowane dane – informacja o elementach niezbędnych do zabezpieczenia Dane dot. incydentu - Dyski fizyczne Dane dot. incydentu - Serwery fizyczne	Online, interfejs CROPT, tryb odwołań bezpośrednich (§13 ust. 2) i kopiowanie danych (§13 ust. 3)	krytyczny dla sukcesu projektu	USŁUGA WWW oraz protokół SFTP

7.2. Kluczowe komponenty architektury rozwiązania



Legenda



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Wirtualizacja oparta o KVM, kubectl, docker
2.	Sieć i bezpieczeństwo	UTM, WAF, Firewall
3.	Standardy wymiany danych	Rest-api
4.	Systemy operacyjne serwerowe	Linux
5.	Bazy danych	Postgressql
6.	Serwery aplikacji	Python
7.	Portale	Python
8.	Inne	

7.4. Opis zasobów danych przetwarzanych w planowanym rozwiązaniu

Czy nowy system będzie tworzył zasoby danych o charakterze rejestru publicznego?
TAK/NIE

Czy nowy system będzie przetwarzał (używał, zmieniał) zawartość innych rejestrów publicznych?
TAK/NIE

7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności [...]) (Dz. U. 2012, poz. 526 z późn. zm.) w zakresie dot. systemu zarządzania bezpieczeństwem informacji:

- ~~-system nie podlega rygorom KRI – należy wyjaśnić czy istnieją inne normy bezpieczeństwa,~~
- ~~które będą spełnione przez system zgodnie z wymogami KRI~~
- ~~-dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie~~