

Załącznik nr 1 do Zaproszenia – Opis Przedmiotu Zamówienia

Konkurs Ofert Nr 5/2024

CPV: 73100000-3– Usługi badawcze i eksperymentalno-rozwojowe.

Przedmiotem zamówienia jest **realizacja dwóch zadań zleconych przez Zamawiającego, w ramach projektu TAMAbbox – wirtualne i fizyczne urządzenia chroniące przed atakami typu DDoS (Distributed Denial of Service) współfinansowanego ze środków Europejskiego Funduszu Dla Nowoczesnej Gospodarki w ramach Programu Fundusze Europejskie Dla Nowoczesnej Gospodarki 2021-2027 (FENG) (Umowa o dofinansowanie nr: FENG.01.01-IP.01-0013/23-00). Okres realizacji projektu: 01.10.2023 – 30.09.2025”**

Zamawiający przewiduje następujące zadania dla Wykonawcy w związku z realizacją Przedmiotu Zamówienia:

LP. 1 - Zadanie nr 1

Tytuł Zadania: Stworzenie i opracowanie rozwiązania analitycznego opartego na metodach uczenia maszynowego lub równoważnych, realizującego funkcjonalności związane z wykrywaniem, reagowaniem i informowaniem o atakach typu Denial of Service/Distributed Denial of Service wraz systemem do utrzymywania i aktualizowania.

W ramach realizacji zadania nr 1 Zamawiający oczekuje od Wykonawcy następujących działań:

- 1) Zaproponowanie i zaimplementowanie rozwiązań algorytmicznych opartych na uczeniu maszynowym lub równoważnych dla następujących przypadków ataków
 - a. ataki DDoS w warstwie sieciowej, transportowej oraz aplikacyjnej o krótkim czasie trwania, ale o dużym wolumenie ruchu na jednostkę czasu.
 - b. ataki DDoS w warstwie aplikacyjnej oparte na działaniach automatów i botów, które podszywając swoje zachowanie pod działania użytkowników, powodując tym samym, że podstawowe mechanizmy cyberbezpieczeństwa uznają taki ruch za dopuszczalny.
 - c. złożone i hybrydowe ataki DDoS łączące w logice ataku działania wolumetryczne i niewolumetryczne w przekroju warstw sieciowej, transportowej i aplikacyjnej, a także doprowadzając do manipulacji zasobami informatycznymi w kierunku doprowadzenia do odmowy usługi.
- 2) Zaproponowanie rozwiązań oraz procesów związanych z utrzymaniem opracowanych w 1) algorytmów oraz ich aktualizacją, dostrajaniem oraz interpretowaniem sposobu działania, zgodnie z domeną problemu (cyberbezpieczeństwo, ataki sieciowe, ataki DDoS). Proponowane rozwiązanie powinno wspierać możliwość dobudowania komponentów wspierających zaproponowane procesy.
- 3) Proponowane rozwiązanie powinno przyjmować formę, która pozwoli Zamawiającemu na integrację rozwiązania z istniejącym, a rozwijanym w projekcie system anty-DDoS TAMA.

- 4) Proponowane rozwiązanie powinno być przystosowane do skalowalnego wdrażania.
- a. Dla ustalenia uwagi należy rozpatrzyć następujące środowiska wdrożeniowe:
- Maszyna wirtualna o parametrach 8vCPU, 16GB RAM, 100GB dysku
 - Lekkie urządzenie fizyczne biurkowe lub do zamontowania w szafie Rack, CPU 4 rdzenie/8 wątków, 16GB RAM, 500GB dysku
 - Urządzenie fizyczne w postaci urządzenia serwerowego wielkości maksymalnej do 2U, 2xCPU (w sumie 16 rdzeni), 32GB RAM, 1TB dysku
 - Klaster urządzeń fizycznych z punktu iii. – co najmniej 3 urządzenia spięte razem ze wspólną warstwą wykorzystania zasobów obliczeniowych
 - Kombinacja środowisk z punktów i. – iv.
- b. Wykonawca może wskazywać własne propozycje co do wymaganych zasobów obliczeniowych w proponowanych scenariuszach wdrożenia.
- c. W ramach rozważań wdrożenia należy rozpatrzyć także akcelerację obliczeń z wykorzystaniem rozwiązań jak np. FPGA, GPU lub inne rozwiązania sprzętowe. Oczekujemy w tym obszarze wsparcia i konsultacji Dostawcy.

LP. 2 - Zadanie 2

Tytuł Zadania: Stworzenie i opracowanie rozwiązania operacyjnego do przeprowadzania działań związanych z utrzymywaniem, aktualizacją i dostrajaniem algorytmów wykrywania oraz reagowania na ataki DDoS opartych na uczeniu maszynowym.

Zamawiający przewiduje następujące zadania dla Wykonawcy w związku z realizacją Przedmiotu Zamówienia:

- Zaproponowanie i zaimplementowanie rozwiązań uzupełniających rezultaty Zadania 1, a realizujących w praktyce zaproponowany w Zadaniu 1 model utrzymywania, aktualizowania, dostrajania i interpretowania sposobu działania.
 - Dostarczenie wyników badawczych z doboru algorytmów do działania w obszarze monitorowania jakości stosowanych algorytmów ML oraz w obszarze wytłumaczalności
 - Proponowane rozwiązanie powinno przyjmować formę, która pozwoli Zamawiającemu na integrację rozwiązania z istniejącym, a rozwijanym w projekcie system anty-DDoS TAMA.
 - Proponowane rozwiązanie ma posiadać interfejs do wykorzystania lub zintegrowania z interfejsami użytkownika w środowisku operacyjnym Zamawiającego w obszarze monitorowania i reagowania na incydenty (SOC, konsola systemu anty-DDoS TAMA).
- 5) Proponowane rozwiązanie powinno być przystosowane do skalowalnego wdrażania:
- a. Dla ustalenia uwagi należy rozpatrzyć następujące środowiska wdrożeniowe:
- Maszyna wirtualna o parametrach 8vCPU, 16GB RAM, 100GB dysku

- ii. Lekkie urządzenie fizyczne biurkowe lub do zamontowania w szafie Rack, CPU 4 rdzenie/8 wątków, 16GB RAM, 500GB dysku
 - iii. Urządzenie fizyczne w postaci urządzenia serwerowego wielkości maksymalnej do 2U, 2xCPU (w sumie 16 rdzeni), 32GB RAM, 1TB dysku
 - iv. Klaster urządzeń fizycznych z punktu iii. – co najmniej 3 urządzenia spięte razem ze wspólną warstwą wykorzystania zasobów obliczeniowych
 - v. Kombinacja środowisk z punktów i. – iv.
- b. Wykonawca może wskazywać własne propozycje co do wymaganych zasobów obliczeniowych w proponowanych scenariuszach wdrożenia.
- c. W ramach rozważań wdrożenia należy rozpatrzyć także akcelerację obliczeń z wykorzystaniem rozwiązań jak FPGA lub GPU. Zamawiający oczekuje w tym obszarze wsparcia i konsultacji Wykonawcy.

Ogólne warunki realizacji Zadań:

- a) Zamawiający oczekuje realizacji Zadania 1 przy założonych na etapie negocjacji wskaźników oceny jakości i parametrów technicznych, właściwości funkcjonalnych, poziomu innowacyjności do 30 września 2024 roku.
- b) Zamawiający oczekuje realizacji Zadania 2 przy założonych na etapie negocjacji wskaźników oceny jakości i parametrów technicznych, właściwości funkcjonalnych, poziomu innowacyjności do 30 listopada 2024 roku.
- c) Wykonawca udostępni dokumentację rozwiązania, Zamawiającemu.
- d) Zamawiający oczekuje przeniesienia praw związanych z tworzonymi dziełami i utworami na Zamawiającego.
- e) Wykonawca w ramach współpracy, będzie dzielił się regularnie wiedzą z obszaru data science oraz uczenia maszynowego z Zamawiającym, co najmniej w zakresie:
 - Seminariów projektowych co najmniej raz na miesiąc w trakcie trwania współpracy;
 - Przeprowadzenia co najmniej 2 warsztatów szkoleniowych.

Dodatkowy opis projektów TAMA oraz ARFA

Przy planowaniu zakresu oferty, należy założyć, że rozwijane algorytmy i moduły realizujące rozwiązania dla wskazanych zadań w Zamówieniu mają docelowo stać się elementem działającego produkcyjnie systemu anty-DDoS TAMA opracowanego przez Exatel w ostatnich latach w ramach projektów TAMA i ARFA. Integracja ta obejmie zarówno:

- zasilenie opracowywanych algorytmów i modułów za pomocą danych dostępnych w systemie
- konsumpcję wygenerowanych danych przez opracowywane algorytmy i moduły w założony sposób

Oficjalny opis systemu znajduje się na stronie publicznej Exatel: <https://exatel.pl/badania-i-rozwoj/exatel-tama/>

Warto zwrócić uwagę, że rozwiązanie TAMA to aktualnie dwie główne linie produktowe:

- TAMA – główny system chroniący łączy klientów Exatel
- TAMA Pro7 – stanowiące rozszerzenie głównego systemu TAMA w zakresie ochrony przed atakami aplikacyjnymi, nowymi atakami wolumetrycznymi, atakami na serwery oraz atakami na BGP.

Na wskazanej stronie zaprezentowano ideową architekturę głównego systemu wraz ze wskazaniem podstawowych komponentów składających się na to rozwiązanie. Zamawiający oczekuje, że Wykonawca dostarczy rozwiązania, które będzie można integrować z komponentami systemu TAMA oraz TAMA Pro7, w szczególności w ramach rozwijanych wersji Box dla obu tych linii produktowych.

Zakres i sposób integracji na poziomie składania oferty należy założyć ideowo wraz z propozycjami zgodnymi z istniejącymi sposobami technologicznymi. Założenia dotyczące integracji zostaną wypracowane we wcześniejszych etapach projektu, aby właściwa realizacja integracji i jej elementów (poziom danych, implementacja technologii) będą wykonywane w ramach dalszych etapów wypełniania kontraktu przez Wykonawcę.

Publicznie dostępne materiały szczegółowe dotyczące systemu TAMA można znaleźć na blogu R&D Exatel, m.in.:

- <https://exatel.pl/wiedza/materialy/video/tama-pro7-sztama-z-cyberbezpieczenstwem/>
- <https://exatel.pl/wiedza/materialy/artykuly/misja-tama-do-sforsowania-dzien-pierwszy-rozpoznanie/>
- <https://exatel.pl/wiedza/materialy/artykuly/jak-wygladaja-ataki-ddos-na-przykladzie-romeo-i-julia/>
- <https://exatel.pl/wiedza/materialy/podcast/podcast-tama-nie-zwalniamy-kroku-w-rozwoju-autorskiego-systemu-anty-ddos/>
- <https://exatel.pl/wiedza/materialy/artykuly/wybrane-mechanizmy-przeciwdzialania-atakam-ddos-mitygacja/>
- <https://exatel.pl/wiedza/materialy/artykuly/wybrane-mechanizmy-przeciwdzialania-atakam-ddos-czesc-1-wykrywanie-ataku/>
- <https://exatel.pl/wiedza/materialy/artykuly/portal-do-tama/>
- <https://exatel.pl/wiedza/materialy/podcast/podcast-jak-powstaja-rozwiazania-anty-ddos/>
- <https://exatel.pl/wiedza/materialy/video/ataki-ddos-a-bezpieczenstwo-biznesu/>
- <https://exatel.pl/wiedza/materialy/artykuly/arfa-jak-spolka-skarbu-panstwa-przesiewa-zwir/>
- <https://exatel.pl/wiedza/materialy/artykuly/pierwotna-informatyka-w-systemie-tama/>

Nagrania nt. TAMA dostępne w serwisie YouTube:

- <https://www.youtube.com/watch?v=5KGTepGLKPQ>
- https://www.youtube.com/watch?v=pWh_U-j_UzI

Produkty końcowe zamówienia

Zadanie 1 – warunki odbiorcze

1. Dostarczenie opisu rozwiązania analitycznego opisanego w zadaniu 1 w tym:
 - a) Opis rozwiązań algorytmicznych opartych na uczeniu maszynowym dla opisanych przypadków ataków;
 - b) Opis propozycji rozwiązań i procesów związanych z utrzymaniem opracowanych w zadaniu 1 algorytmów oraz ich aktualizacją, dostrajaniem oraz interpretowaniem sposobu działania, zgodnie z domeną problemu (cyberbezpieczeństwo, ataki sieciowe, ataki DDoS). Rozwiązanie powinno wspierać możliwość dobudowania komponentów wspierających zaproponowane procesy;
 - c) Opis rozwiązania przystosowane do skalowalnego wdrażania wraz z wnioskami dla wszystkich środowisk wdrożeniowych wymienionych w opisie przedmiotu zamówienia
 - d) Opis rozważań wdrożenia akceleracji obliczeń z wykorzystaniem rozwiązań jak np. FPGA, GPU lub innych rozwiązań sprzętowych;
 - e) Dokumentacja rozwiązania analitycznego wraz z wykazem wszystkich potrzebnych narzędzi programowych, bibliotek, systemów operacyjnych wraz z ich wersjami.
2. Wersje rozwojowe kodu, skryptów, notatników i innych obiektów, które Wykonawca wytworzy w ramach prac badawczych w zakresie zadania. Preferowane jest przekazanie kopii wszystkich repozytoriów systemu kontroli wersji typu Git wykorzystywanych przez Wykonawcę wraz z historią aktualizacji (commitów do repozytorium)
3. Kod źródłowy rozwiązania pozwalający na wykonanie testów weryfikujących poprawność wykonania zadań wraz z testami automatycznymi
4. Raport obejmujący
 - wyniki testów systemowych (jakościowe testy oprogramowania, testy modeli AI/ML, testy bezpieczeństwa, testy wydajności, testy pomiaru parametrów pracy) Wykonawcy potwierdzających realizację wymagań,
 - wykaz potrzebnego sprzętu do przeprowadzenia pełnych testów funkcjonalności zrealizowanej przez Wykonawcę,
 - instrukcję konfiguracji środowiska testowego zawierająca szczegółowy opis środowiska testowego,
 - instrukcję uruchomienia testów (jakościowe testy oprogramowania, testy modeli AI/ML, testy bezpieczeństwa, testy wydajności, testy pomiaru parametrów pracy) sprawdzających zaimplementowane funkcjonalności,
 - opis w jaki sposób otrzymane wyniki powinny być interpretowane wraz z analizą przykładowych, oczekiwanych, wyników testów,
 - Instrukcje użytkownika,
 - Instrukcje rozwojowe rozwiązania końcowego (rozwój rozumiany jako m.in. rozszerzanie, skalowanie, zmiana technologii).
5. Raport podsumowujący wykonanie prac z wykorzystanego przez Wykonawcę systemu zarządzania zadaniami, który pozwoli udokumentować zrealizowane: zadania, grupy zadań, historie użytkownika, epiki i wersje wydawcze na przestrzeni realizacji zamówienia. Raport ma zawierać zarówno wymiar ilościowy, jak i jakościowy. (po zakończeniu realizacji zadania nr 1)
6. Przygotowanie wkładu do raportu z realizacji prac związanych z realizacją projektu TAMAbOX dla NCBR.

Zadanie 2 - warunki odbiorcze

1. Dostarczenie opisu rozwiązania operacyjnego opisanego w zadaniu 2 w tym:
 - a) Opis rozwiązań uzupełniających rezultaty zadania ;
 - b) Wyniki badawcze z doboru algorytmów do działania w obszarze monitorowania jakości stosowanych algorytmów ML oraz w obszarze wytłumaczalności wraz z opisem;
 - c) Opis rozwiązania przystosowane do skalowalnego wdrażania wraz z wnioskami dla wszystkich środowisk wdrożeniowych wymienionych w opisie przedmiotu zamówienia;
 - d) Opis rozważań wdrożenia akceleracji obliczeń z wykorzystaniem rozwiązań jak np. FPGA, GPU lub innych rozwiązań sprzętowych;
 - e) Dokumentacja rozwiązania operacyjnego wraz z wykazem wszystkich potrzebnych narzędzi programowych, bibliotek, systemów operacyjnych wraz z ich wersjami.
2. Wersje rozwojowe kodu, skryptów, notatników i innych obiektów, które Wykonawca wytworzy w ramach prac badawczych w zakresie zadania. Preferowane jest przekazanie kopii wszystkich repozytoriów systemu kontroli wersji typu Git wykorzystywanych przez Wykonawcę wraz z historią aktualizacji (commitów do repozytorium)
3. Kod źródłowy rozwiązania pozwalający na wykonanie testów weryfikujących poprawność wykonania zadań wraz z testami automatycznymi
4. Raport obejmujący
 - wyniki testów systemowych (jakościowe testy oprogramowania, testy modeli AI/ML, testy bezpieczeństwa, testy wydajności, testy pomiaru parametrów pracy) Wykonawcy potwierdzających realizację wymagań,
 - wykaz potrzebnego sprzętu do przeprowadzenia pełnych testów funkcjonalności zrealizowanej przez Wykonawcę,
 - instrukcję konfiguracji środowiska testowego zawierająca szczegółowy opis środowiska testowego,
 - instrukcję uruchomienia testów (jakościowe testy oprogramowania, testy modeli AI/ML, testy bezpieczeństwa, testy wydajności, testy pomiaru parametrów pracy) sprawdzających zaimplementowane funkcjonalności,
 - opis w jaki sposób otrzymane wyniki powinny być interpretowane wraz z analizą przykładowych, oczekiwanych, wyników testów,
 - Instrukcje użytkownika- Instrukcje rozwojowe rozwiązania końcowego (rozwój rozumiany jako m.in. rozszerzanie, skalowanie, zmiana technologii).
5. Raport podsumowujący wykonanie prac z wykorzystanego przez Wykonawcę systemu zarządzania zadaniami, który pozwoli udokumentować zrealizowane: zadania, grupy zadań, historie użytkownika, epiki i wersje wydawcze na przestrzeni realizacji zamówienia. Raport ma zawierać zarówno wymiar ilościowy, jak i jakościowy.
6. Przygotowanie wkładu do raportu z realizacji prac związanych z realizacją projektu TAMAbbox dla NCBR.