

Szczegółowy opis przedmiotu zamówienia

pn. „Merytoryczne prace rozwojowe podwykonawcy”

Projekt pn. „Technologia bezpiecznych aplikacji wykorzystujących inteligentną detekcję anomalii w zachowaniach użytkowników celem wczesnego wykrywania zagrożeń” (akronim IDA)

Projekt zostanie zgłoszony do dofinansowania w ramach Programu Operacyjnego Inteligentny Rozwój 2014-2020

Niniejsze postępowanie jest prowadzone w oparciu o „Regulamin udzielania zamówień przez Instytut Informatyki i Zarządzania na dostawy, usługi i roboty budowlane współfinansowanych ze środków zewnętrznych (publicznych)”, którego treść zamieszczona jest na stronie www.instytutiz.pl oraz jest do wglądu w siedzibie Instytutu Informatyki i Zarządzania.

1. Nazwa oraz adres Zamawiającego

95-200 Pabianice, ul. Szpitalna 15,
NIP 7272660642, REGON 100087765
KRS 0000242379
tel +48 42 201 13 00, fax +48 42 201 13 03
sekretariat@instytutiz.pl, <http://www.instytutiz.pl>

2. O projekcie

Celem projektu jest opracowanie nowej technologii ochrony aplikacji biznesowych. Istotę innowacyjności technologii stanowią opracowane i zintegrowane rozwiązania inteligentnych algorytmów wykrywania anomalii w zachowaniach użytkowników oraz procesach autentykacji i autoryzacji użytkowników. Takie połączenie zapewnia kompleksową detekcję potencjalnie szkodliwych działań, które mogą być objawem działań nieuprawnionych użytkowników prowadzących do kradzieży danych, naruszenia poufności czy też przełamania zabezpieczeń. Inteligentne algorytmy detekcji anomalii każdorazowo uwzględniają specyfikę dziedziny biznesowej aplikacji, co stanowi znaczącą przewagę nad rozwiązaniami działającymi tylko w dziedzinie sieci i systemów. Detekcja wcześniej nieznanych wzorców postępowania, czyli właśnie anomalii, przyczyni się znacznie do podniesienia bezpieczeństwa aplikacji biznesowych oferowanych przez LTC.

Prowadzi to uzyskania znacząco ulepszonych gwarancji poufności, autentyczności i integralności aplikacji biznesowych, a tym samym wysoką odporność na zagrożenia aktami cyberprzestępczości. Dzięki nowej technologii IDA wszelkie próby obejścia zabezpieczeń są wczesnie wykrywane.

Technologia wdrożona zostanie w działalności biznesowej LTC i posłuży to wytwarzania nowych i znacząco ulepszonych systemów informatycznych. Opracowane repozytorium wiedzy i procesów efektywne procedury opracowania i wdrażania nowych funkcjonalności aplikacji biznesowych w pełni wykorzystujących unikatowe rozwiązania środowiska IDA.

Przeprowadzone eksperymentalne prace rozwojowe, obejmujące również testy w środowisku demonstracyjnym oraz produkcyjnym, doprowadzą do powstania innowacyjnej co najmniej na skalę krajową i rynków

zagranicznych technologii, która umożliwi opracowanie nowych oraz rozwój istniejących produktów Wnioskodawcy.

Opracowane algorytmy oraz współpracujące z nimi moduły bezpieczeństwa zostaną równolegle przetestowane za pomocą instalacji demonstracyjnej oraz w warunkach rzeczywistych w celu potwierdzenia osiągnięcia zakładanych efektów.

Okres realizacji projektu: 1 grudnia 2022 – 31 grudnia 2023.

3. Opis przedmiotu zamówienia

1. Przedmiotem zapytania jest realizacja zamówienia pn. „**Merytoryczne prace rozwojowe podwykonawcy**” w ramach planowanego do realizacji projektu pn. „**Technologia bezpiecznych aplikacji wykorzystujących inteligentną detekcję anomalii w zachowaniach użytkowników celem wczesnego wykrywania zagrożeń**” (akronim IDA) .
2. Zlecenia mają charakter eksperymentalnych prac rozwojowych, wykonanych przez własną kadrę naukową Wykonawcy w oparciu o aparaturę/infrastrukturę Wykonawcy i udostępnioną instalację demonstracyjną przez IIZ.
3. Przedmiot zamówienia obejmuje:
 - a. Merytoryczne prace rozwojowe podwykonawcy Zlecenie 1 – dotyczy Etapu 2
 - b. Merytoryczne prace rozwojowe podwykonawcy Zlecenie 2 – dotyczy Etapu 4

3.1. Merytoryczne prace rozwojowe podwykonawcy Zlecenie 1 – dotyczy Etapu 2

Kluczowym problemem do rozwiązania jest uzyskanie modelu danych wejściowych oraz szkieletowych algorytmów uczenia maszynowego dla wykrywania anomalii w zachowaniach użytkowników (UBA).

Model danych wejściowych musi uwzględniać wielowymiarowość danych pochodzących z komponentów detekcji, identyfikacji i analizy zachowań użytkowników realizowanych w interfejsie użytkownika aplikacji typu SPA (ang. Single Page Application), jak i danych pochodzących z usług, w szczególności z systemu autentykacji i autoryzacji użytkowników. Co do zasady dane wejściowe będą to dane sekwencyjne. Docelowa wymiarowość danych wejściowych musi zapewniać możliwość przeprowadzenia uczenia wybranego dla rozwiązania problemu mechanizmu uczenia maszynowego.

Szkieletowe algorytmy uczenia maszynowego dla wykrywania anomalii w zachowaniach użytkowników (UBA) muszą określać wykorzystane elementy składowe (np. CNN, RNN, autoencoder) oraz topologię. Powinny również wskazywać techniki konieczne do zastosowania w celu zapewnienia zbieżności procesu uczenia się (np. LSTM, GRU).

Oczekiwane kryteria jakości: zbieżność procesu uczenia się algorytmu wykrywania anomalii w zachowaniach użytkowników (UBA).

3.2. Merytoryczne prace rozwojowe podwykonawcy Zlecenie 2 – dotyczy Etapu 4

Kluczowym problemem do rozwiązania jest optymalizacja modelu wejściowych oraz szkieletowych algorytmów uczenia maszynowego dla wykrywania anomalii w zachowaniach użytkowników (UBA).

Optymalizacja ma zapewnić szybszą zbieżność procesów uczenia poszczególnych elementów składowych (optymalizacja uczenia) oraz wyższą jakość uzyskiwanych wyników.

Oczekiwane kryteria jakości: średni odsetek false-positive dla algorytmów uczenia maszynowego dla wykrywania anomalii w zachowaniach użytkowników UBA na poziomie nie większym niż 20%.

4. Wymagane zasoby kadrowe podwykonawcy

Do wykonania przedmiotu prac rozwojowych specjaliści B+R (specjalista uczenia maszynowego, programista systemów bezpieczeństwa) Podwykonawcy będą do dyspozycji Wnioskodawcy, w każdym kolejnym miesiącu etapu, w łącznym wymiarze czasu w Zleceniu nr 1 i 2, odpowiadającym 1,25 etatu (zakłada się tolerancję na poziomie 0,25 etatu, przy czym w całym okresie podwykonawstwa średniomiesięczny wymiar nie może być niższy niż 1,25 etatu.

Specjaliści powinni posiadać ugruntowaną wiedzę przedmiotową, doświadczenie i wysokie umiejętności w zakresie:

- wszystkich zaplanowanych metod naukowych realizacji projektu,
- realizacji projektów B+R z zaplanowaną komercjalizacją wyników,
- złożonych systemów informatycznych wykorzystanych w pracach projektowych, programistycznych, instalacyjnych, konfiguracyjnych i wdrożeniowych oraz przeprowadzaniu testów,
- inteligentnych algorytmów uczenia maszynowego,
- systemów sterowania biznesowego,
- zasad budowy i modelowania interakcji człowiek-komputer za pomocą graficznych interfejsów użytkownika.

Podwykonawca musi przedstawić wiarygodne referencje dotyczące specjalistów, z których co najmniej 3 powinno wykazać się wyższym stopniem naukowym. Specjalistów nie powinno być więcej niż 8.

Każdy ze specjalistów musi być wykonawcą prac rozwojowych o okresie nie krótszym niż 1 rok, a przedmiot prac musi być zbieżny z celami i przedmiotem niniejszego projektu.

4.1. Kadra – Zlecenie 1 – dotyczy Etapu 2

Specjaliści Podwykonawcy muszą posiadać ugruntowaną wiedzę przedmiotową, doświadczenie i wysokie umiejętności w zakresie:

- wszystkich zaplanowanych metod naukowych realizacji projektu,
- realizacji projektów B+R z zaplanowaną komercjalizacją wyników,
- złożonych systemów informatycznych wykorzystanych w pracach projektowych, programistycznych, instalacyjnych, konfiguracyjnych i wdrożeniowych oraz przeprowadzaniu testów,
- inteligentnych algorytmów,
- systemów sterowania biznesowego,
- zasad budowy i modelowania interakcji człowiek-komputer za pomocą graficznych interfejsów użytkownika.

Każdy ze specjalistów musi być wykonawcą prac rozwojowych o okresie nie krótszym niż 1 rok, a przedmiot prac był zbieżny z celami i przedmiotem niniejszego projektu.

4.2. Kadra – Zlecenie 2 – dotyczy Etapu 4

Specjaliści Podwykonawcy muszą posiadać ugruntowaną wiedzę przedmiotową, doświadczenie i wysokie umiejętności w zakresie:

- wszystkich zaplanowanych metod naukowych realizacji projektu,
- realizacji projektów B+R z zaplanowaną komercjalizacją wyników,
- złożonych systemów informatycznych wykorzystanych w pracach projektowych, programistycznych, instalacyjnych, konfiguracyjnych i wdrożeniowych oraz przeprowadzaniu testów,
- inteligentnych algorytmów,

- systemów sterowania biznesowego,
- zasad budowy i modelowania interakcji człowiek-komputer za pomocą graficznych interfejsów użytkownika.

Każdy ze specjalistów musi być wykonawcą prac rozwojowych o okresie nie krótszym niż 1 rok, a przedmiot prac był zbieżny z celami i przedmiotem niniejszego projektu.

5. Wymagane zasoby podwykonawcy

Podwykonawca musi posiadać co najmniej niżej wymienione zasoby, które są niezbędne do realizacji powierzonych prac rozwojowych. Aparatura B+R i wyposażenie laboratorium pozwolą na wykonanie wszechstronnych prac rozwojowych zadeklarowanej liczbie specjalistów naukowych w zakresie zaprojektowania, opracowania i optymalizacji prototypów – inteligentnych algorytmów oraz umożliwią symulacje komputerowe testujące przedmiotowe algorytmy.

Wymagania dotyczą Zlecenia nr 1 i 2.

Wymagane zasoby:

1. LABORATORIUM SIECIOWYCH SYSTEMÓW OPERACYJNYCH I TECHNOLOGII SIECI KOMPUTEROWYCH

Specjalizuje się w technologiach: wirtualizacji sieci predestynowanych dla centrów przetwarzania danych, syst. bezpieczeństwa (firewalle), technologii routingu i przełączania, transmisji multimed. (VoIP i IPTV) wraz z komunikacją z sieciami tradycyjnymi (POTS i DVB-T), sieciami radiowymi (WiFi do standardu 802.11ac wave 1 w wersji dostępowej i jako „ostatnia mila” oraz 3G/4G w części dostępowej).

2. LABORATORIUM SYSTEMÓW ROZPROSZONYCH, wyposażone m.in.

- w KLASZTER OBLICZENIOWY, specjalizujące się w przetwarzaniu danych w systemach rozproszonych, przetwarzaniu równoległym czy przetwarzaniu w chmurze włączając w to środowiska wirtualizacji oraz programowania równoległego.

- LABORATORIUM BEZPIECZEŃSTWA SIECI KOMPUTEROWYCH