Załącznik nr 1 do rozeznania cenowego

Opis przedmiotu zamówienia

Opis przedmiotu zamówienia:

1. Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa aplikacji internetowej o statusie rejestru państwowego.
2. Przedmiot zamówienia musi obejmować realizację następujących działań:
   2.1. Testowanie aplikacji webowej z wykorzystaniem testów penetracyjnych od strony wewnętrznej i zewnętrznej, wraz z rekomendacjami dotyczącymi ich usunięcia w różnych warstwach obronnych Zamawiającego (UTM, izolacja, aplikacja);
   2.2. Testowanie warstwy API przewidywanej do udostępnienia dla systemów obcych do realizacji funkcjonalności aplikacji (https/JSON);
   2.3. Audyt bezpieczeństwa kodu źródłowego aplikacji;
   2.4. Audyt bezpieczeństwa bezpośredniego otoczenia aplikacji (architektura rozwiązania, konfiguracja komponentów sprzętowych, środowisk, topologii sieci, systemów zintegrowanych z aplikacją) pod kątem możliwości skompromitowania aplikacji rejestru;
   2.5. Ponowna weryfikacja środowiska po usunięciu błędów przez Wykonawcę.
3. Architektura aplikacji obejmuje dwie aplikacje webowe (obejmujące dedykowaną stronę www oraz API dla klientów zewnętrznych, stronę www dla klientów wewnętrznych), oraz dedykowaną aplikację egzaminacyjną w formie strony www, dostępną wyłącznie przez sieć zlokalizowaną w Centrum Egzaminowania i Monitorowania Maszynistów.
4. Całość systemu będzie dostępna dla Wykonawcy w modelu whitebox, wraz z kompletną wytworzoną dokumentacją oraz konfiguracją usług.
5. Dane systemu do oceny złożoności testowania:
   5.1. Objętość kodu: ok. 480 000 linii kodu;
   5.2. Liczba unikalnych formatek WWW (ekranów): ok. 250;
   5.3. Przeprowadzenie testów wraz z ich dokumentacją powinno zakończyć się nie później niż w terminie 1 miesiąca od dnia udostepnienia środowiska przez Zamawiającego dla Wykonawcy;
   5.4. Przeprowadzenie retestów oraz dostarczenie ich dokumentacji powinno zakończyć się nie później niż w terminie 2 tygodni od udostepnienia przez Zamawiającego dla Wykonawcy poprawionej wersji aplikacji przez jej dostawcę.
6. Testy odbędą się na kompletnym środowisku Zamawiającego, Zamawiający udostępni VPN i/lub lokalizację na potrzeby wykonania testów.
7. Usługi zewnętrzne od których zależny jest system: ADFS, systemy wewnętrzne na poziomie baz danych, systemy i rejestry państwowe na poziomie ich API.
8. Zamawiający oczekuje raportów z testów oraz retestów, z naniesionymi wynikami analizy osoby weryfikującej (po skanowaniu automatycznym, oczekujemy weryfikacji specjalisty w zakresie oceny rzeczywistego zagrożenia w testowanym systemie).