Numer sprawy**: DZ.22.58.2023.PP**

Załącznik nr 2 do zaproszenia

Opis przedmiotu zamówienia

Testy bezpieczeństwa platformy e-Konsylium

I. Zakres usługi

Etap I

1. Analiza architektury platformy pod kątem cyberbezpieczeństwa

   Celem analizy architektury będzie:
   a) wskazanie zagrożeń i ryzyk wynikających z braku zastosowania lub błędnego umiejscowienia technologii i systemów bezpieczeństwa,
   b) potwierdzenie obecności oraz ocena kompletności i adekwatności doboru zastosowanych technologii i mechanizmów bezpieczeństwa.
2. Audyt i testy bezpieczeństwa platformy e-Konsylium metodą „blackbox", obejmujące w szczególności:
   a) Przygotowanie scenariuszy testów
   b) Przeprowadzenie automatycznych testów podatności infrastruktury serwerowej i sieciowej
   c) Przeprowadzenie automatycznych testów modułów aplikacji e-Konsylium wytworzonych w ramach projektu tj.:
      • Moduł analityczny
      • Moduł obrazowania medycznego
      • Moduł wideo-konferencji
      • Moduł integracyjny.
      Testy winny objąć: front-end, back-end oraz API platformy.
   d) Przeprowadzenie manualnych testów penetracyjnych w/w modułów aplikacji e-Konsylium wytworzonych w ramach projektu.
   e) Weryfikacja zabezpieczeń kryptograficznych.
3. Przygotowanie raportu z wykonania w/w prac zawierającego rekomendacje działań zwiększających poziom bezpieczeństwa systemu.
4. Zaprezentowanie i omówienie raportu w formie warsztatów dla przedstawicieli Zamawiającego

Etap II

1. Retesty bezpieczeństwa platformy e-Konsylium w celu weryfikacji wprowadzonych zmian rekomendowanych w etapie I
2. Przygotowanie raportu z wykonania retestów
3. Zaprezentowanie i omówienie raportu w formie warsztatów dla przedstawicieli Zamawiającego

II. Metodyka testów

1. Zamawiający wymaga, że w ramach realizacji testów penetracyjnych przeprowadzonych zgodnie z metodykami

a) OWASP (Open Web Application Security Project) ASVS 4.0.2,
b) Open Source Security Testing Methodology Manual (OSSTMM 3),

2. Zamawiający wymaga, aby Wykonawca zakresem testów objął listę najpoważniejszych błędów występujących w aplikacjach webowych określoną w OWASP TOP10 z 2021 roku lub nowszą, aktualną na dzień rozpoczęcia audytu.

   Lista OWASP TOP10 2021

   a) Broken Access Control
   b) Cryptographic Failures
   c) Injection
   d) Insecure Design
   e) Security Misconfiguration
   f) Vulnerable and Outdated Components
   g) Identification and Authentication Failures
   h) Software and Data Integrity Failures
   i) Security Logging and Monitoring
   j) Server-Side Request Forgery

3. Zakres testów będzie obejmował testy wykonywane z sieci Zamawiającego oraz sieci publicznej
4. W trakcie prac prowadzonych przez Wykonawcę w ramach przedmiotu zamówienia, Zamawiający wymaga wykorzystania znanych baz danych o podatnościach i słabościach bezpieczeństwa systemów informatycznych (np. SANS Top 20 Critical Security Control, Common Vulnerabilities and Exposures).

III. Czas realizacji

Etap I czas realizacji wyniesie 8-10 tygodni od rozpoczęcia prac

Etap II czas realizacji wyniesie 3 - 5 tygodni od rozpoczęcia prac