Warszawa, dn. 04.09.2025 r.

Odpowiedzi na zadane pytania

Pytania formalne:

1. W odniesieniu do warunku dotyczącego kwalifikacji członków zespołu audytowego, tj. obowiązku posiadania certyfikatów wskazanych w SWZ (m.in. CASP, CEH, CSFA, OSCP, OSWE, GSEC lub równoważne z rodziny GIAC), zwracamy się z prośbą o doprecyzowanie:

Czy Zamawiający uzna za równoważne certyfikaty eWPT (eLearnSecurity Web Application Penetration Tester) oraz eJPT (eLearnSecurity Junior Penetration Tester), jako potwierdzające wiedzę i umiejętności w obszarze testów penetracyjnych oraz bezpieczeństwa aplikacji webowych, odpowiadające zakresem wymaganiom stawianym dla certyfikatów OSCP/OSWE?

Tak zostaną uznane.

2. W odniesieniu do warunku udziału w postępowaniu wskazanego w pkt b) Specyfikacji: „posiadać doświadczenie: w ciągu ostatnich 3 lat brał udział w minimum 3 projektach polegających na wykonaniu testów bezpieczeństwa, audytów systemów informatycznych i testów penetracyjnych, każdy o wartości nie mniejszej niż 25 000 zł”, prosimy o doprecyzowanie:

Czy Zamawiający uzna spełnienie warunku, jeżeli Wykonawca wykaże doświadczenie w realizacji osobnych projektów obejmujących poszczególne wskazane usługi (np. jeden projekt – testy bezpieczeństwa, drugi – audyt systemów informatycznych, trzeci – testy penetracyjne), czy też wymagane jest, aby każdy z wykazanych projektów obejmował łącznie wszystkie trzy rodzaje usług?

Tak.

Pytania dotyczące treści zapytania:

1. Czy wszystkie wymienione systemy (SODiR, e-PFRON2, NEO, SOW, SOF2, iPFRON+, portale) mają osobne środowiska testowe, czy testy muszą być prowadzone na produkcji?

Wszystkie systemy posiadają instancje testowe. Portale internetowe nie posiadają środowisk testowych.

2. Ile jest ról użytkowników w każdym systemie (np. użytkownik, admin, operator, integrator)?

Użytkownik, administrator - zazwyczaj występują te dwie role. Użytkownik występuje w roli użytkownika wewnętrznego i zewnętrznego.

3. Czy otrzymamy dokumentację funkcjonalną i/lub architektoniczną aplikacji?

Tak, po podpisaniu umowy.

4. Czy aplikacje korzystają z zewnętrznych integracji (API, SSO, płatności), które też mają być objęte testami?

Tak, aplikacje komunikują się z zewnętrznymi systemami i rejestrami. Audytowi podlegają tylko API po stronie systemów Zamawiającego.

5. Ile dokładnie jest API i ile mają endpointów.

Liczba API nie przekracza łącznie liczby 20.

6. Czy otrzymamy dokumentację API (Swagger/OpenAPI itp.)

Tak, po podpisaniu umowy. Dokumentacja API jest częścią dokumentacji technicznej systemów dziedzinowych.

7. Czy testy obejmują tylko webaplikacje czy tez aplikacje mobilne, desktopowe itp.?

W przypadku systemu SOF2, badanie obejmie aplikację napisaną w technologii Oracle Forms. Pozostałe aplikacje są wyłacznie webowe.

8. Czy w testach CI/CD chodzi o przegląd procesów i repozytoriów kodu, czy tylko testy bezpieczeństwa pipeline'u na poziomie wdrożenia?

Przegląd repozytoriów kodu źródłowego, procesów CI/CD.

9. Jak rozumieć testy wydajnościowe i odpornościowe – czy mamy je prowadzić na środowisku testowym, czy dopuszczacie ograniczone testy na produkcji w oknach serwisowych?

Dopuszczalne są testy w oknach serwisowych w niewielkim zakresie. Pozostałe testy będą prowadzone na środowiskach PREPROD i TEST.

10. Czy DoS/DDoS testujemy na własnej infrastrukturze Zamawiającego, czy w symulowanym środowisku testowym dostarczonym przez Wykonawcę?

Testy mają być wykonane z wykorzystaniem narzędzi i generatorów ruchu Wykonawcy.

11. Jak duże jest środowisko Active Directory – ile domen/kontenerów/serwerów?

Posiadamy jedną domenę i około 1500 użytkowników. Wykorzystujemy również usługę Azure AD.

12. Czy przewidziane są testy wewnętrzne (LAN) czy tylko zewnętrzne (Internet, DMZ)?

Tylko zewnętrzne.

13. Jakie urządzenia sieciowe (firewalle, routery, VPN) są objęte zakresem – czy wszystkie, czy wybrane punkty styku z Internetem?

Wybrane punkty styku z Internetem i urządzenia brzegowe.

14. Czy jakieś urządzenia są wyłączone z testów?

Tak, dla sieci LAN.

15. Jakie systemy bazodanowe są używane (Oracle, MSSQL, PostgreSQL, MySQL)?

Oracle, PostgreSQL, MySQL, MSSQL.

16. Czy testy mają obejmować tylko konfigurację i uprawnienia, czy również próby eksploatacji podatności w aplikacjach korzystających z baz?

Tylko konfigurację i uprawnienia.

17. Czy w zakresie są tylko komputery pracowników IT, czy również stacje końcowe zwykłych użytkowników?

Zwykłych użytkowników również.

18. Czy testy socjotechniczne mają obejmować tylko phishing mailowy, czy również vishing/USB drop/fizyczne wejście do lokalizacji?

Phishing oraz testy fizycznego podłączenia urządzenia zewnętrznego do komputera użytkownika.

19. Ile lokalizacji PFRON ma być objętych testami fizycznymi?

Zamawiający rezygnuje z przeprowadzenia testów fizycznych, o których mowa w Załączniku 1a sekcja „Audyt bezpieczeństwa aplikacji" lit e) tiret d oraz w Załączniku 1b sekcja „Audyt bezpieczeństwa aplikacji" lit. e) lit. d).

20. Czy Zamawiający chce raport tylko z wyników (ile osób kliknęło), czy również pełne analizy i szkolenia?

Raport z testów bez szkoleń.

21. Jak wygląda okno czasowe testów – czy możemy prowadzić testy w godzinach nocnych/weekendy, czy tylko w godzinach pracy?

Jeśli nie będzie potrzebny udział pracowników Zamawiającego to testy mogą być prowadzone w godzinach nocnych i w weekendy.