OPIS PRZEDMIOTU ZAMÓWIENIA

Świadczenie usługi testów bezpieczeństwa w okresie 12 miesięcy

CPV:
79212000-3 – usługi audytu
72800000-8 – usługi audytu komputerowego

Przedmiotowe zamówienie podzielone jest na trzy części:

1. Część I - Testy bezpieczeństwa obszaru aplikacji Web,
2. Część II - Testy bezpieczeństwa obszaru aplikacji mobilnych,
3. Część III - Testy bezpieczeństwa infrastruktury.

Przedmiotem zamówienia w cz. I, II i III jest świadczenie usługi testów bezpieczeństwa zgodnie z wymaganiami określonymi w OPZ w okresie od dnia podpisania umowy przez 12 miesięcy lub do wyczerpania limitu kwotowego umowy, w zależności od tego które ze zdarzeń nastąpi wcześniej. Usługi w tym zakresie będą zlecane na podstawie zamówień składanych w miarę zapotrzebowania Zamawiającego (zwanych dalej „**Zleceniami**").

A. **Przedmiot usługi.**

1. Zakres testów bezpieczeństwa w poszczególnych częściach:

1.1. **Część I** - Testy bezpieczeństwa aplikacji Web:

1.1.1. Wykonawca przeprowadzi testy zgodnie z jednym ze standardów:

1.1.1.1. Open Web Application Security Project - Web Security Testing Guide (OWASP - WSTG),

1.1.1.2. The Open Source Security Testing Methodology Manual (OSSTMM),

1.1.1.3. The penetration testing execution standard (PTES).

1.1.2. Testy będą obejmowały wybrane lub wszystkie z wymienionych poniżej obszarów:

1.1.2.1. aplikację frontend zbudowaną np. w oparciu o cienkiego klienta (przeglądarka WWW),

1.1.2.2. Usługi backend udostępnianie poprzez API programowe,

1.1.2.3. Infrastrukturę, w ramach której uruchamiany jest system,

1.1.2.4. Analizę statyczną kodu źródłowego aplikacji, w tym elementy frontend i backend.

1.1.3. W celu potwierdzenia występowania podatności testy mogą obejmować analizę kodu źródłowego dla wskazanych komponentów lub funkcjonalności testowanego systemu.

1.2. **Część II** - Testy bezpieczeństwa aplikacji mobilnych:

1.2.1. Wykonawca przeprowadzi testy zgodnie z jednym ze standardów:

1.2.1.1. Open Web Application Security Project - Mobile Security Testing Guide (OWASP - MSTG),

1.2.1.2. The Mobile Application Penetration Testing Methodology (MAPTM),

1.2.1.3. The penetration testing execution standard (PTES).

1.2.2. Testy będą obejmowały wybrane lub wszystkie z wymienionych poniżej obszarów:

1.2.2.1. aplikację mobilną z uwzględnieniem platform Android i iOS,

1.2.2.2. usługi backend udostępnianie poprzez API programowe,

1.2.2.3. infrastrukturę, w ramach której uruchamiany jest system,

1.2.2.4. usługi wspierające (np. zapewniające konfigurację i zarządzanie) system i działające w oparciu o technologie web,

1.2.2.5. analizę statyczną kodu źródłowego aplikacji mobilnej dla platformy Android i iOS, usług backend udostępnianych przez API,

1.2.2.6. usługi komponentów zewnętrznych wchodzące w skład ekosystemu aplikacji mobilnych.

1.3. **Część III** - Testy bezpieczeństwa infrastruktury, a w tym:

1.3.1. Wykonawca przeprowadzi testy zgodnie z jednym ze standardów:

1.3.1.1. Open Web Application Security Project - Web Security Testing Guide (OWASP),

1.3.1.2. The Open Source Security Testing Methodology Manual (OSSTMM),

1.3.1.3. The penetration testing execution standard (PTES).

1.3.2. Testy będą obejmowały wybrane lub wszystkie z wymienionych poniżej obszarów:

1.3.2.1. Weryfikację konfiguracji komponentów programowo-sprzętowych w zakresie zapewnienia bezpieczeństwa, np. w oparciu o międzynarodowe standardy zgodne z wytycznymi producenta,

1.3.2.2. Weryfikację konfiguracji aplikacji i systemów uruchamianych na infrastrukturze programowo-sprzętowej w zakresie zapewnienia bezpieczeństwa,

1.3.2.3. Identyfikację podatności w komponentach sprzętowo-programowych infrastruktury, działania aktywne mające na celu potwierdzenie występowania podatności.

2. Usługi dla wszystkich części realizowane będą z uwzględnieniem poniższych warunków:

2.1. Testy i analizy odbywać się będą w zależności od możliwości technicznych: stacjonarnie (w siedzibie Zamawiającego w Warszawie) w infrastrukturze Zamawiającego, bądź zdalnie – poza siedzibą Zamawiającego. Wykonawca nie ma możliwości podłączenia własnego sprzętu do sieci Zamawiającego. Niezbędne dedykowane środowisko pracy będzie przygotowane na sprzęcie Zamawiającego we współpracy z Wykonawcą. Decyzja o sposobie realizacji testów należy do Zamawiającego.

2.2. Niedopuszczalne jest stosowanie przez Wykonawcę w testach obejmujących infrastrukturę wewnętrzną oraz przy statycznej analizę kodu źródłowego narzędzi wykorzystujących rozwiązania chmurowe, SaaS, itp..

2.3. Analiza statyczna kodu źródłowego będzie się odbywać w Dni Robocze i Godziny Robocze, lokalnie (w biurze Centralnego Ośrodka Informatyki w Warszawie) – w infrastrukturze Zamawiającego. Wykonawca nie ma możliwości podłączenia własnego sprzętu do sieci Zamawiającego. Niezbędne dedykowane środowisko pracy będzie przygotowane na sprzęcie Zamawiającego we współpracy z Wykonawcą.

2.4. Zamawiający na potrzeby wykonania usług może wymagać wykorzystania będącej w posiadaniu Zamawiającego:

2.4.1. stacji roboczej,
2.4.2. maszyny wirtualnej,
2.4.3. przestrzeni dyskowej,
2.4.4. oprogramowania i licencji na narzędzia zainstalowane na stacji roboczej Zamawiającego.

2.5. Wykonawca na potrzeby wykonania usług musi zapewnić:
2.5.1. stację roboczą do realizacji usług w trybie zdalnym,
2.5.2. możliwość wykonania usług w siedzibie Zamawiającego,
2.5.3. niezbędne narzędzia, oprogramowanie, licencje.

2.6. Wykonawca zapewni wsparcie w interpretacji wyników testów i analiz przedstawianych w przygotowanym raporcie (poprzez przeprowadzenie warsztatów celem omówienia i wyjaśnienia wątpliwości Zamawiającego w formie zdalnej lub stacjonarnej w siedzibie Zamawiającego, w zależności od decyzji Zamawiającego).

2.7. Wykonawca będzie zobowiązany do zachowania niezmienności składu osobowego zespołu audytowego realizującego prace zlecane przez Zamawiającego. Wszelkie zmiany będą wymagały akceptacji Zamawiającego oraz weryfikacji dokumentów potwierdzających kompetencje, doświadczenie i certyfikaty wskazane w części C (poniżej). Wykonawca będzie informował Zamawiającego o wszelkich zmianach w zespole audytowym Wykonawcy realizującym prace objęte przedmiotem umowy z wyprzedzeniem 4 dni roboczych przed wykonaniem przez nowego członka zespołu audytowego czynności w ramach Umowy.

2.8. Roboczodzień oznacza dzień pracy jednego członka zespołu audytowego wynoszący 8 godzin.

2.9. Dla części I, II i III podstawą obliczenia wynagrodzenia Wykonawcy za realizację Zlecenia będzie stawka za jeden roboczodzień realizacji Zlecenia przemnożona przez liczbę roboczodni określoną w Zleceniu.

2.10. Dla części I, II i III cena brutto określona w stawce za roboczodzień obejmuje wszystkie koszty Wykonawcy, w tym podatek VAT oraz wynagrodzenie za przeniesienie autorskich praw majątkowych oraz prawa do wykonywania praw zależnych do utworów powstałych w związku z realizacją usług Wykonawcy w ramach umowy.

2.11. Dla części I, II i III, umowa zobowiązuje Wykonawcę do realizacji zlecanych przez Zamawiającego usług w łącznym wymiarze nieprzekraczającym maksymalnej liczby roboczodni członków zespołu audytowego:
a) 90 roboczodni dla części I – Testy bezpieczeństwa obszaru aplikacji Web;
b) 45 roboczodni dla części II- Testy bezpieczeństwa obszaru aplikacji mobilnych;
c) 45 roboczodni dla części III - Testy bezpieczeństwa infrastruktury.

Umowa będzie obowiązywała przez okres 12 miesięcy od dnia zawarcia. W całym okresie obowiązywania Umowy, prace będą zlecane wg potrzeb Zamawiającego, ze wskazaniem terminu realizacji.

2.12. Dla części I, II, III Wykonawca rozpocznie realizację zleconych prac w terminie nie dłuższym niż 5 dni roboczych od złożenia Zlecenia przez Zamawiającego.

2.13. Podstawą wystawienia faktury za dane Zlecenie będzie dokonanie odbioru zleconych prac i podpisanie protokołu zdawczo-odbiorczego do Zlecenia.

3. Usługi dla części I, II realizowane będą z uwzględnieniem poniższych warunków:

3.1. Zakres zlecanych prac będzie określony poprzez wskazanie:
3.1.1. nazwy systemu/aplikacji poddawanego testom,
3.1.2. podejściu do testów (black box, gray box, white box),
3.1.3. wskazaniu czy testy obejmują cały system czy tylko wybrane funkcjonalności/moduły (załączana jest lista funkcjonalności/modułów poddawanych testom),
3.1.4. przewidywane okno czasowe, w którym testy mają zostać przeprowadzone,
3.1.5. dane dostępowe (adresy IP, nazwy domen) wraz z loginami i hasłami,
3.1.6. w przypadki testów API specyfikacja interfejsów API.

4. Usługi dla części III realizowane będą z uwzględnieniem poniższych warunków:

4.1. Zakres zlecanych prac będzie określony poprzez wskazanie:
4.1.1. nazwy systemu/infrastruktury poddawanego testom,
4.1.2.wskazaniu czy testy obejmują cały system czy tylko wybrane serwery/urządzenia sieciowe (załączana jest lista serwerów/urządzeń poddawanych testom),
4.1.3. przewidywanego okna czasowego, w którym testy mają zostać przeprowadzone,
4.1.4.dane dostępowe (adresy IP, nazwy domen) wraz z loginami i hasłami,

B. Wymagania dotyczące produktów.

1. W ramach każdego Zlecenia w zakresie cz. I, II i III, Wykonawca zobowiązany jest do przedstawienia Zamawiającemu raportu (w formacie docx oraz pdf), zgodnego z szablonem dostarczonym przez Zamawiającego, zawierającego co najmniej:

1.1. Podsumowanie dla Zamawiającego (streszczenie ogólne), a w nim informacje opisujące jakościowo wyniki usługi, przy czym podsumowanie nie może zawierać informacji, które w przypadku ujawnienia zmniejszają bezpieczeństwo badanego obszaru lub systemu.

1.2. Opracowanie szczegółowe, które będzie zawierać:
1.2.1. W części ogólnej:
a) streszczenie, w tym w zależności od zakresu Zlecenia ogólną opinię nt. bezpieczeństwa, przeciwskazań do produkcyjnego wdrożenia, zgodności z określonymi standardami i regulacjami wewnętrznymi i zewnętrznymi, zakres analizy lub koncepcji;
b) główne ustalenia, zalecenia lub założenia – odpowiednio do zakresu Zlecenia;
1.2.2. W części szczegółowej:
a) Opis konfiguracji, nr wersji i stanu testowanego obszaru;
b) Szczegółowy opis dat przeprowadzenia testów, użytych narzędzi, konfiguracji środowiska testowego;
c) Zakres przeprowadzonych testów i sposób ich przeprowadzenia;
d) Wyniki testów i ich interpretację;
e) Listę zidentyfikowanych podatności opisanych poziomem krytyczności, szacowaniem zgodnym z CVSSv3 oraz opatrzonych komentarzem przedstawiciela zespołu audytowego Wykonawcy;
f) Wnioski z testów bezpieczeństwa;
g) Zalecenia i rekomendacje;
h) Zakres czynności niezbędnych do weryfikacji i odtworzenia zidentyfikowanych podatności;
i) Zakres czynności niezbędnych do zaimplementowania rekomendacji po wykonanych testach bezpieczeństwa;

j) W przypadku konieczności wykonania zmian konfiguracyjnych lub instalacji uaktualnień/poprawek, Wykonawca przedstawi opis konfiguracji lub instalacji;
k) Opracowanie wyników w zakresie bezpieczeństwa na poziomie procesu biznesowego obsługiwanego przez badany system.

1.3. Załączniki zawierające wyniki pracy narzędzi wykorzystanych podczas testów bezpieczeństwa.

2. Oczekiwany zakres prac wykonywanych w ramach testów bezpieczeństwa:

Dla części I, II:

2.1. Zapoznanie się z zakresem i przedmiotem testów.
2.2. Skonfigurowanie narzędzi, w celu przeprowadzenia testów.
2.3. Przeprowadzenie testów i analiz, zgodnie ze specyfikacją zawartą w opisie przedmiotu usługi w części A pkt 1 Zakres testów bezpieczeństwa w poszczególnych częściach, mających na celu wskazanie zagrożeń i ryzyk wynikających z:
2.3.1. Zastosowanych technologii i standardów zabezpieczeń,
2.3.2. Błędów oprogramowania,
2.3.3. Poprawnej konfiguracji komponentów systemowych, aplikacyjnych i sieciowych,
2.3.4. Istniejących / wykrytych styków sieci o różnym charakterze (np. styku z siecią Internet, styku sieci systemów utrzymywanych / budowanych u Zamawiającego z innymi sieciami,
2.3.5. Potencjalnych zagrożeń ze strony sieci wewnętrznej (LAN/WAN/WLAN) i zewnętrznej (Internet),
2.3.6. Zastosowanych rozwiązań na poziomie architektury i ich wpływu na bezpieczeństwo systemu,
2.3.7. Prawidłowości wyboru rozwiązania sprzętowego dla aplikacji pod kątem bezpieczeństwa.
2.4. Testy powinny obejmować poniższe rodzaje testów, w przypadku, gdy wykonanie, któregoś z testów nie będzie możliwe bądź nie będzie zasadne dla danej aplikacji należy poinformować Zamawiającego przekazując stosowne uzasadnienie:
2.4.1. Weryfikację mechanizmów uwierzytelniania, autoryzacji i kontroli dostępu,
2.4.2. Weryfikację mechanizmów zarządzania sesją,
2.4.3. Weryfikację mechanizmów kontroli dostępu,
2.4.4. Weryfikację walidacji danych wejściowych oraz wyjściowych,
2.4.5. Weryfikacje mechanizmów kryptograficznych,
2.4.6. Weryfikację mechanizmów ochrony danych,
2.4.7. Weryfikacje komunikacji pomiędzy poszczególnymi komponentami systemu,
2.4.8. Weryfikację prawidłowej obsługi błędów,
2.4.9. Weryfikację konfiguracji poszczególnych komponentów systemu (serwery, urządzenia sieciowe),
2.4.10. Weryfikacja mechanizmów ochrony przed złośliwym oprogramowaniem.
2.5. W przypadku zlecenia statycznej analizy kodu źródłowego, zakres prac powinien obejmować:
2.5.1. Weryfikację podatności w obszarach:
a) Walidacji danych wejściowych,
b) Autentykacji i autoryzacji,
c) Podatności na ataki odmowy usługi,

d) Nieautoryzowanego dostępu, umożliwiającego naruszenie bezpieczeństwa danych.
e) Obsługi błędów i wyjątków,
f) Weryfikacja mechanizmów kryptograficznych,
g) Weryfikacja implementacji funkcji uznawanych za niebezpieczne.

2.5.2. Weryfikację jakości kodu źródłowego z punktu widzenia bezpieczeństwa aplikacji – weryfikacja, czy kod spełnia dobre wzorce projektowe oraz praktyki, mające na celu minimalizację ryzyka związanego z potencjalnymi lukami bezpieczeństwa.
2.5.3. Analizę wykorzystywanych zewnętrznych bibliotek pod kątem znanych podatności.

2.6. Sporządzenie i dostarczenie Zamawiającemu raportu z przeprowadzonych prac, zgodnie z wymaganiami zdefiniowanymi powyżej w części B pkt 1.
2.7. Zamawiający zastrzega sobie prawo, że na jego zgłoszenie Wykonawca, bez dodatkowych opłat, usunie zidentyfikowane nieprawidłowości, wyjaśni nieścisłości i/lub przeprowadzi warsztaty celem omówienia i wyjaśnienia informacji przedstawionych w produktach prac na zasadach zawartych w umowie.

Dla części III:

2.8. Zapoznanie się z zakresem i przedmiotem testów.
2.9. Skonfigurowanie narzędzi, w celu przeprowadzenia testów.
2.10. Przeprowadzenie testów i analiz, zgodnie ze specyfikacją zawartą w opisie przedmiotu usługi w części A pkt 1 Zakres testów bezpieczeństwa w poszczególnych częściach, mających na celu wskazanie zagrożeń i ryzyk wynikających z:
2.10.1. Zastosowanych technologii i standardów zabezpieczeń,
2.10.2. Błędów oprogramowania,
2.10.3. Poprawnej konfiguracji komponentów systemowych, aplikacyjnych i sieciowych,
2.10.4. Istniejących / wykrytych styków sieci o różnym charakterze (np. styku z siecią Internet, styku sieci systemów utrzymywanych / budowanych u Zamawiającego z innymi sieciami,
2.10.5. Potencjalnych zagrożeń ze strony sieci wewnętrznej (LAN/WAN/WLAN) i zewnętrznej (Internet),
2.10.6. Zastosowanych rozwiązań na poziomie architektury i ich wpływu na bezpieczeństwo systemu,
2.10.7. Prawidłowości wyboru rozwiązania sprzętowego dla aplikacji pod kątem bezpieczeństwa.
2.11. Przeprowadzone w ramach realizacji części III testy infrastruktury pod kątem bezpieczeństwa powinny uwzględniać specyfikę testowanego rozwiązania, a w szczególności podatności systemów (wynikające z błędów w aplikacji i oprogramowania, z którymi aplikacja się komunikuje np. bazy danych, serwery proxy, etc.) na znane ataki,
2.12. Sporządzenie i dostarczenie Zamawiającemu raportu z przeprowadzonych prac, zgodnie z wymaganiami zdefiniowanymi powyżej w części B pkt 1.
2.13. Zamawiający zastrzega sobie prawo, że na jego zgłoszenie Wykonawca, bez dodatkowych opłat, usunie zidentyfikowane nieprawidłowości w wytworzonych produktach przez Wykonawcę, wyjaśni nieścisłości i/lub przeprowadzi warsztaty celem omówienia i wyjaśnienia informacji przedstawionych w produktach prac na zasadach zawartych w umowie.

C. Wymagania dotyczące zespołu audytowego wykonującego testy bezpieczeństwa.

1. Wymaga się, aby Wykonawca dysponował jednocześnie dla:

1.1. **Część I** – zespołem audytowym składającym się z 6 osób, przy czym każda z nich musi posiadać co najmniej jeden z poniższych certyfikatów, z zastrzeżeniem, że zespół audytowy musi posiadać co najmniej dwa różne certyfikaty spośród niżej wymienionych:

1.1.1. aktualny certyfikat Offensive Security Certified Professional (OSCP) lub równoważny, który pokrywa obszary:

1.1.1.1. Bezpieczeństwo ofensywne,

1.1.1.2. Techniki przełamywania zabezpieczeń sieciowych, systemów operacyjnych oraz oprogramowania,

1.1.1.3. Narzędzia bezpieczeństwa,

1.1.1.4. Techniki wykrywania błędów oprogramowania,

1.1.2. Aktualny certyfikat eLearnSecurity Web application Penetration Tester (EWPT) lub równoważny, który pokrywa obszary:

1.1.2.1. Procesy i metodologie testów penetracyjnych,

1.1.2.2. Analiza i inspekcja aplikacji WEB,

1.1.2.3. Gromadzenie informacji,

1.1.2.4. Zarządzanie podatnościami WEB aplikacji,

1.1.2.5. OWASP Testing Guide / OWASP Top 10,

1.1.2.6. Manualne potwierdzenie podatności XSS, SQLi itd.,

1.1.2.7. Zaawansowana raportowanie i remediacja,

1.1.3. Aktualny certyfikat eLearn Security Web application Penetration Tester eXtreme (EWPTX) lub równoważny, który pokrywa obszary:

1.1.3.1. Procesy i metodologie testów penetracyjnych,

1.1.3.2. Analiza i kontrola aplikacji WEB,

1.1.3.3. Zaawansowane umiejętności raportowania i działań naprawczych,

1.1.3.4. Zaawansowana wiedza i umiejętności omijania podstawowych oraz zaawansowanych filtrów XSS, SQLi itd.,

1.1.3.5. Zaawansowana znajomość różnych systemów zarządzania bazami danych,

1.1.3.6. Umiejętność przygotowania własnego exploita, gdy gotowe narzędzia zawodzą,

1.1.4. Aktualny certyfikat Offensive Security Certified Expert (OSCE) lub równoważny, który pokrywa obszary:

1.1.4.1. Ataki na aplikacje webowe (min. XSS/LFI),

1.1.4.2. Analiza i wstrzykiwanie kodu złośliwego w pliki wykonywalne PE,

1.1.4.3. Omijanie systemów antywirusowych,

1.1.4.4. Omijanie mechanizmów zabezpieczenia pamięci,

1.1.4.5. Fuzzing, konstruowanie exploitów 0-day,

1.1.4.6. Obchodzenie zabezpieczeń,

1.1.4.7. Atakowanie infrastruktury sieciowej,

1.1.5. Aktualny certyfikat Certified Ethical Hacker (CEH) lub równoważny, który pokrywa obszary:

1.1.5.1. Analiza oraz ocena ryzyka danych oraz systemów,
1.1.5.2. Kontrola bezpieczeństwa, wykrywanie oraz zapobieganie atakom,
1.1.5.3. Znajomość narzędzia, systemów, programów,
1.1.5.4. Znajomość procedur oraz metodologii,
1.1.5.5. Znajomość Regulacji i polityk.

1.2. **Część II** – zespołem audytowym składającym się z 3 osób, przy czym każda z nich musi posiadać co najmniej jeden z poniższych certyfikatów, z zastrzeżeniem, że zespół audytowy musi posiadać co najmniej dwa różne certyfikaty spośród niżej wymienionych:

1.2.1. aktualny certyfikat Offensive Security Certified Professional (OSCP) lub równoważny, który pokrywa obszary:
1.2.1.1. Bezpieczeństwo ofensywne,
1.2.1.2. Techniki przełamywania zabezpieczeń sieciowych, systemów operacyjnych oraz oprogramowania,
1.2.1.3. Narzędzia bezpieczeństwa,
1.2.1.4. Techniki wykrywania błędów oprogramowania,

1.2.2. Aktualny certyfikat eLearnSecurity Mobile Application Penetration Tester (eMAPT) lub równoważny, który pokrywa obszary:
1.2.2.1. Zbieranie informacji,
1.2.2.2. Inżynieria wsteczna dla aplikacji Android,
1.2.2.3. Wykorzystanie podatności w systemie Android,
1.2.2.4. Stosowanie zasad bezpieczeństwa,
1.2.2.5. Wady logiczne,
1.2.2.6. Szyfrowanie i kryptografia,
1.2.2.7. Identyfikacja podatnych implementacji,

1.2.3. Aktualny certyfikat eLearnSecurity Web application Penetration Tester (EWPT) lub równoważny, który pokrywa obszary:
1.2.3.1. Procesy i metodologie testów penetracyjnych,
1.2.3.2. Analiza i inspekcja aplikacji WEB,
1.2.3.3. Gromadzenie informacji,
1.2.3.4. Zarządzanie podatnościami WEB aplikacji,
1.2.3.5. OWASP Testing Guide / OWASP Top 10,
1.2.3.6. Manualne potwierdzenie podatności XSS, SQLi itd.,
1.2.3.7. Zaawansowana raportowanie i remediacja,

1.2.4. Aktualny certyfikat eLearn Security Web application Penetration Tester eXtreme (EWPTX) lub równoważny, który pokrywa obszary:
1.2.4.1. Procesy i metodologie testów penetracyjnych,
1.2.4.2. Analiza i kontrola aplikacji WEB,
1.2.4.3. Zaawansowane umiejętności raportowania i działań naprawczych,
1.2.4.4. Zaawansowana wiedza i umiejętności omijania podstawowych oraz zaawansowanych filtrów XSS, SQLi itd.,
1.2.4.5. Zaawansowana znajomość różnych systemów zarządzania bazami danych,
1.2.4.6. Umiejętność przygotowania własnego exploita, gdy gotowe narzędzia zawodzą,

1.2.5. Aktualny certyfikat Offensive Security Certified Expert (OSCE) lub równoważny, który pokrywa obszary:

1.2.5.1. Ataki na aplikacje webowe (min. XSS/LFI),
1.2.5.2. Analiza i wstrzykiwanie kodu złośliwego w pliki wykonywalne PE,
1.2.5.3. Omijanie systemów antywirusowych,
1.2.5.4. Omijanie mechanizmów zabezpieczenia pamięci,
1.2.5.5. Fuzzing, konstruowanie exploitów 0-day,
1.2.5.6. Obchodzenie zabezpieczeń,
1.2.5.7. Atakowanie infrastruktury sieciowej,

1.2.6. Aktualny certyfikat Certified Ethical Hacker (CEH) lub równoważny, który pokrywa obszary:
1.2.6.1. Analiza oraz ocena ryzyka danych oraz systemów,
1.2.6.2. Kontrola bezpieczeństwa, wykrywanie oraz zapobieganie atakom,
1.2.6.3. Znajomość narzędzia, systemów, programów,
1.2.6.4. Znajomość procedur oraz metodologii,
1.2.6.5. Znajomość Regulacji i polityk.

1.3. **Część III** – zespołem audytowym składającym się z 3 osób, przy czym każda z nich musi posiadać co najmniej jeden z poniższych certyfikatów, z zastrzeżeniem, że zespół audytowy musi posiadać co najmniej dwa różne certyfikaty spośród niżej wymienionych:

1.3.1. Aktualny certyfikat Offensive Security Certified Professional (OSCP) lub równoważny, który pokrywa obszary:
1.3.1.1. Bezpieczeństwo ofensywne,
1.3.1.2. Techniki przełamywania zabezpieczeń sieciowych, systemów operacyjnych oraz oprogramowania,
1.3.1.3. Narzędzia bezpieczeństwa,
1.3.1.4. Techniki wykrywania błędów oprogramowania,

1.3.2. Aktualny certyfikat eLearnSecurity Web application Penetration Tester (EWPT) lub równoważny, który pokrywa obszary:
1.3.2.1. Procesy i metodologie testów penetracyjnych,
1.3.2.2. Analiza i inspekcja aplikacji WEB,
1.3.2.3. Gromadzenie informacji,
1.3.2.4. Zarządzanie podatnościami WEB aplikacji,
1.3.2.5. OWASP Testing Guide / OWASP Top 10,
1.3.2.6. Manualne potwierdzenie podatności XSS, SQLi itd.,
1.3.2.7. Zaawansowana raportowanie i remediacja,

1.3.3. Aktualny certyfikat eLearn Security Web application Penetration Tester eXtreme (EWPTX) lub równoważny, który pokrywa obszary:
1.3.3.1. Procesy i metodologie testów penetracyjnych,
1.3.3.2. Analiza i kontrola aplikacji WEB,
1.3.3.3. Zaawansowane umiejętności raportowania i działań naprawczych,
1.3.3.4. Zaawansowana wiedza i umiejętności omijania podstawowych oraz zaawansowanych filtrów XSS, SQLi itd.,
1.3.3.5. Zaawansowana znajomość różnych systemów zarządzania bazami danych,
1.3.3.6. Umiejętność przygotowania własnego exploita, gdy gotowe narzędzia zawodzą,

1.3.4. Aktualny certyfikat Offensive Security Certified Expert (OSCE) lub równoważny, który pokrywa obszary:
1.3.4.1. Ataki na aplikacje webowe (min. XSS/LFI),
1.3.4.2. Analiza i wstrzykiwanie kodu złośliwego w pliki wykonywalne PE,
1.3.4.3. Omijanie systemów antywirusowych,
1.3.4.4. Omijanie mechanizmów zabezpieczenia pamięci,
1.3.4.5. Fuzzing, konstruowanie exploitów 0-day,
1.3.4.6. Obchodzenie zabezpieczeń,
1.3.4.7. Atakowanie infrastruktury sieciowej,

1.3.5. Aktualny certyfikat Certified Ethical Hacker (CEH) lub równoważny, który pokrywa obszary:
1.3.5.1. Analiza oraz ocena ryzyka danych oraz systemów,
1.3.5.2. Kontrola bezpieczeństwa, wykrywanie oraz zapobieganie atakom,
1.3.5.3. Znajomość narzędzia, systemów, programów,
1.3.5.4. Znajomość procedur oraz metodologii,
1.3.5.5. Znajomość Regulacji i polityk.

2. Osoby wchodzące w skład zespołu audytowego, realizującego testy po stronie Wykonawcy dla części I, II, III:

2.1. Będą bezstronne i niezależne, w zakresie wykonywanych prac od:
2.1.1. Kancelarii Prezesa Rady Ministrów (KPRM),
2.1.2. Ministerstwa Spraw Wewnętrznych i Administracji,
2.1.3. NASK PIB,
2.1.4. NASK S.A.,
2.1.5. PWPW S.A.,
2.1.6. Ministerstwa Cyfryzacji.

2.2. Za bezstronne i niezależne od wyżej wymienionych podmiotów Zamawiający rozumie osoby, które na dzień składania ofert, w czasie trwania postępowania o udzielenie zamówienia publicznego oraz przez cały okres obowiązywania umowy nie realizowały prac na rzecz COI w okresie ostatnich 12 miesięcy, na dowód czego złożą, przed podpisaniem umowy, stosowne oświadczenia. Przyjmuje się, że pracami wytwórczymi i/lub utrzymaniowymi nie są testy bezpieczeństwa. Zamawiający zastrzega sobie prawo do weryfikacji i zmian składu osobowego zespołu audytowego prowadzącego testy na zasadach określonych w Umowie.