

## Opis przedmiotu zamówienia (OPZ)

### I. Audyt, aktualizacja i dostosowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Celem zamówienia jest **zapewnienie zgodności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)** funkcjonującego u Zamawiającego, wdrożonego w 2023 roku i nieaktualizowanego od momentu wdrożenia, z obowiązującymi przepisami prawa oraz wymaganiami bezpieczeństwa informacji, w szczególności z:

- **Krajowymi Ramami Interoperacyjności (KRI),**
- **ustawą z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (UKSC),**
- **rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO).**

Zgodnie z § 20 ust. 2 rozporządzenia w sprawie KRI, **norma ISO/IEC 27001 stanowi metodykę i punkt odniesienia** do realizacji celu zamówienia, jako uznany międzynarodowy standard dobrych praktyk w zakresie zarządzania bezpieczeństwem informacji.

Zamawiający **nie wymaga certyfikacji SZBI**, a jedynie osiągnięcia stanu zgodności z obowiązującymi przepisami prawa, przy zastosowaniu metodyki ISO/IEC 27001 lub metodyki równoważnej.

#### 1. Wymagany rezultat zamówienia

Wymagany rezultat realizacji zamówienia jest:

- zaktualizowany, spójny i skutecznie wdrożony System Zarządzania Bezpieczeństwem Informacji,
- spełniający wymagania KRI, UKSC i RODO,
- potwierdzony kompletną i aktualną dokumentacją systemową,
- dostosowany do aktualnego stanu organizacyjnego i technicznego Zamawiającego.

#### 2. Metodyka realizacji

Osiągnięcie celu zamówienia nastąpi poprzez realizację przez Wykonawcę następujących, obowiązkowych etapów:

##### *Etap I – Audyt istniejącego SZBI*

Audyt obejmuje w szczególności: - analizę dokumentacji SZBI opracowanej w 2023 r., - ocenę aktualności dokumentacji w kontekście zmian prawnych, organizacyjnych i technicznych, - ocenę zgodności SZBI z KRI, UKSC i RODO, - ocenę SZBI w odniesieniu do metodyki ISO/IEC 27001, - ocenę zgodności praktyki operacyjnej z dokumentacją, - identyfikację niezgodności, luk i obszarów wymagających dostosowania.

##### *Etap II – Aktualizacja i dostosowanie SZBI*

Wykonawca zobowiązany jest do:

- a) aktualizacji dokumentacji SZBI, w tym: - polityki bezpieczeństwa informacji, - procedur i instrukcji bezpieczeństwa, - rejestru ryzyk oraz sposobów ich traktowania, - dokumentów wymaganych przez KRI i UKSC;
- b) dostosowania SZBI do aktualnej struktury organizacyjnej i systemów IT Zamawiającego;
- c) usunięcia stwierdzonych niezgodności; aktualizację Polityki Ochrony Danych Osobowych, zgodnej z RODO oraz spójnej z SZBI.

### *Etap III – Planowanie doskonalenia SZBI*

Wykonawca opracuje **mapę drogową utrzymania i doskonalenia SZBI na okres 3 lat**, odpowiadającą cyklowi ciągłego doskonalenia wynikającemu z metodyki ISO/IEC 27001.

#### **3. Rezultaty zamówienia**

Wykonawca dostarczy następujące, kompletne i wzajemnie spójne rezultaty realizacji zamówienia:

- a) **raport z audytu SZBI** – zawierający ocenę zgodności z KRI, UKSC i RODO oraz analizę SZBI w odniesieniu do metodyki ISO/IEC 27001.
- b) **zaktualizowaną dokumentację SZBI** – obejmującą wszystkie dokumenty systemowe niezbędne do prawidłowego funkcjonowania i utrzymania SZBI.
- c) **Polityka Ochrony Danych Osobowych (RODO)** – dostosowaną do aktualnych procesów przetwarzania danych osobowych i spójną z SZBI.
- d) **zestawienie wprowadzonych zmian** – w formie tabelarycznej, wskazujące zakres aktualizacji oraz dokumenty objęte zmianami.
- e) **plan utrzymania i doskonalenia SZBI na okres 3 lat** – stanowiącą koncepcję działań o charakterze organizacyjnym i systemowym, obejmujący w szczególności harmonogram przeglądów SZBI, audytów wewnętrznych, działań korygujących i doskonalących oraz kluczowe kamienie milowe wynikające z cyklu ciągłego doskonalenia, zgodnie z metodyką ISO/IEC 27001. Mapa drogową ma charakter planistyczny i nie stanowi zobowiązania Zamawiającego do realizacji przyszłych zamówień.
- f) **podsumowanie kierownicze** – przeznaczone dla kierownictwa Zamawiającego, prezentujące wnioski i rekomendacje w sposób syntetyczny.

Dokumentacja zostanie przekazana w formie elektronicznej (PDF oraz format edytowalny).

#### **4. Termin realizacji**

Termin realizacji zamówienia: **do 60 dni kalendarzowych od dnia zawarcia umowy.**

### **Warunki udziału w postępowaniu**

#### **1. Zdolność techniczna lub zawodowa**

##### **a) doświadczenie Wykonawcy**

Zamawiający wymaga, aby Wykonawca wykazał, że w okresie ostatnich 3 lat wykonał należycie co najmniej 2 usługi polegające na audytach bezpieczeństwa informacji lub audytach i aktualizacji SZBI dla jednostek sektora finansów publicznych, obejmujące obszar KRI, UKSC lub RODO.

##### **b) potencjał kadrowy**

Zamawiający wymaga, aby Wykonawca skierował do realizacji zamówienia co najmniej 2 osoby, z których każda: - posiada co najmniej jeden ważny certyfikat z obszaru bezpieczeństwa informacji lub audytu bezpieczeństwa, wskazany w § 20 ust. 2 rozporządzenia w sprawie KRI (np. CISA, CISM, CISSP, ISO/IEC 27001 Lead Auditor, ISO/IEC 27001 Lead Implementer lub równoważny), - posiada co najmniej 2 lata doświadczenia zawodowego w obszarze bezpieczeństwa informacji, audytów IT lub SZBI.



**Kryteria oceny ofert**

Zamawiający dokona oceny ofert na podstawie następujących kryteriów:

1. Cena – 60%
2. Doświadczenie zespołu audytowego – 40%

Wyliczenia dotyczące ceny

Cena najniższa / Cena badanej oferty × 60 pkt

Doświadczenie zespołu audytowego (40%)

Punkty przyznawane będą za doświadczenie osób skierowanych do realizacji zamówienia w realizacji audytów SZBI / KRI / UKSC / RODO dla jednostek sektora publicznego: -

- 2 - 3 usługi - 20 pkt;
- 4–5 usług - 30 pkt;
- powyżej 5 usług - 40 pkt;

Oferta, która uzyska najwyższą liczbę punktów, zostanie uznana za najkorzystniejszą.

## **II. Szkolenie pracowników i kadry kierowniczej z zakresu cyberbezpieczeństwa z wykorzystaniem platformy Security Awareness Training (SAT) - program budowania świadomości bezpieczeństwa**

Celem zamówienia jest zakup i uruchomienie okresowych szkoleń z zakresu cyberbezpieczeństwa dla pracowników i kadry kierowniczej, wraz z udostępnieniem platformy Security Awareness Training umożliwiającej prowadzenie kampanii edukacyjnych, symulacji socjotechnicznych oraz testów wiedzy przez okres 12 miesięcy. Program ma wspierać mierzalną zmianę zachowań użytkowników (redukcję podatności na phishing, wzrost zgłaszalności incydentów oraz wzrost poziomu wiedzy pracowników urzędu).

### **1. Zakres przedmiotu zamówienia**

- a) dostarczenie platformy SAT w modelu SaaS (licencje per użytkownik) wraz z konfiguracją i uruchomieniem programu,
- b) realizacja szkoleń okresowych (online lub stacjonarnie) dla: pracowników i kadry kierowniczej,
- c) dostarczenie materiałów wspierających kampanie edukacyjne (pakiety komunikacyjne, alerty),
- d) przeprowadzenie testów wiedzy oraz symulacji phishing mailowy, a także raportowanie i przeglądy okresowe KPI,
- e) wsparcie operacyjne programu przez zespół wykonawcy (planowanie kampanii, rekomendacje).

### **3. Definicje**

- a) SAT - program budowania świadomości bezpieczeństwa obejmujący szkolenia, symulacje oraz pomiar zachowań,
- b) kampania - zestaw działań edukacyjnych w określonym czasie,
- c) baseline - pomiar stanu wyjściowego (wyniki testów wiedzy),

- d) KPI programu - m.in. click rate, report rate, completion rate, wyniki testów, trend w czasie.

#### 4. Wymagania funkcjonalne platformy

Platforma SAT musi spełniać wymagania funkcjonalne określone w Załączniku nr 1 (matryca wymagań platformy). W szczególności obejmuje to:

- a) symulacje phishing,
- b) moduł treningowy z treściami w języku polskim, quizami i certyfikatami,
- c) landing pages i obsługę wielu domen/HTTPS,
- d) mechanizmy raportowania, metryk na poziomie grup/działów, role-based access,

#### 5. Wymagania нефunkcjonalne i bezpieczeństwa

- a) model SaaS, dostęp przez przeglądarkę; brak potrzeby instalacji komponentów po stronie serwerów Zamawiającego,
- b) wsparcie 2FA,
- c) możliwość integracji SSO (SAML) z katalogiem tożsamości Zamawiającego,
- d) zgodność z RODO (przetwarzanie danych osobowych użytkowników - dane identyfikacyjne i metryki postępów),
- e) możliwość eksportu raportów (CSV/PDF) i przechowywania historii kampanii.

#### 6. Wdrożenie i konfiguracja

Wykonawca zapewni konfigurację i uruchomienie programu obejmujące co najmniej:

- a) warsztat startowy i uzgodnienie KPI, grup użytkowników oraz polityki kampanii,
- b) konfigurację administracji, ról i uprawnień oraz mechanizmów 2FA,
- c) integrację użytkowników (import) i budowę grup (działy/oddziały),
- d) uruchomienie baseline: pierwsza symulacja phishing + test wiedzy,
- e) konfigurację landing pages, domen symulacji, harmonogramów kampanii i automatycznych przypisań szkoleń,
- f) przygotowanie pakietu komunikacji wewnętrznej i planu rocznego kampanii.

#### 7. Szkolenia okresowe

Wymagany jest podział programu szkoleniowego na role. Minimalny zakres obejmuje:

- a) szkolenie podstawowe dla pracowników (min. 2 godziny),
- b) szkolenie dla kadry kierowniczej (min. 2 godziny) obejmujące aspekty zarządcze i ryzyk BEC/fraud,
- c) materiały poszkoleniowe oraz możliwość potwierdzenia udziału (imienny certyfikat/dyplom).

#### 8. Materiały wspierające kampanie edukacyjne

W ramach kampanii edukacyjnych wykonawca zapewni co najmniej:

- a) pakiety komunikacyjne (plakaty, infografiki, krótkie komunikaty e-mail/intranet) wspierające bieżący temat kampanii,
- b) microlearning / "teachable moments" uruchamiane po interakcji z symulacją phishingu,
- c) materiały dla kadry kierowniczej (1-2 stronicowe briefy KPI/ryzyka do przeglądu okresowego).



**9. Raportowanie i przeglądy programu**

- a) raport baseline (stan wyjściowy) - do 10 dni roboczych od zakończenia pierwszej kampanii,
- b) raporty okresowe (co najmniej kwartalne) obejmujące KPI, trend, rekomendacje działań oraz propozycje tematów kolejnych kampanii,
- c) raport roczny podsumowujący wraz z rekomendacjami na kolejny okres.

**10. Wsparcie i utrzymanie**

- a) wsparcie administracyjne platformy (konfiguracja kampanii, użytkownicy, raporty),
- b) wsparcie merytoryczne (dobór tematów kampanii, dostosowanie treści, konsultacje).

**11. Wymagania dotyczące zespołu wykonawcy**

Wykonawca zapewni minimum 2-osobowy zespół realizacyjny obejmujący:

- a) eksperta audytowo-systemowego posiadającego certyfikaty: (a) Audytor Wiodący SZBI wg PN-EN ISO/IEC 27001:2023 oraz (b) Audytor Wiodący SZCD wg PN-EN ISO 22301:2020.
- b) ekspert merytoryczny musi wykazać przeprowadzenie 2 szkoleń security awareness w roku 2025 – jedno dla administracji publicznej i jedno dla podmiotu komercyjnego.
- c) wykonawca musi posiadać ważny certyfikat ISO/IEC 27001 obejmujący usługi bezpieczeństwa informacji.

**12. Odbiór i kryteria akceptacji**

Za zakończony etap uznaje się w szczególności:

- a) uruchomienie platformy i integracji użytkowników (konto admin, role, import/SSO, grupy),
- b) uruchomienie pierwszej kampanii baseline i testu wiedzy,
- c) przekazanie planu kampanii na 12 miesięcy oraz pakietów komunikacyjnych,
- d) realizację szkoleń zgodnie z harmonogramem i przekazanie certyfikatów uczestnikom,
- e) przekazanie raportów okresowych i rocznego.

**13. Kryteria oceny ofert**

- 1. Cena – 60%
- 2. Doświadczenie zespołu audytowego – 40%

Wyliczenia dotyczące ceny

Cena najniższa / Cena badanej oferty × 60 pkt

W tym kryterium można uzyskać maksymalnie 60 punktów.

„Doświadczenie zawodowe eksperta merytorycznego skierowanego do realizacji zamówienia” – waga 40%.

Dla porównania i oceny ofert, pod uwagę brana będzie wskazana w Formularzu oferty liczba wykonanych szkoleń security awareness w których brała udział osoba skierowana do realizacji zamówienia - ekspert merytoryczny.

Punkty w ramach tego kryterium zostaną przyznane w następujący sposób:

- za wykazanie 2 usług - 0 punktów,
- za wykazanie 4 usług – 40 punktów,

W tym kryterium można uzyskać maksymalnie 40 punktów.

**Załącznik nr 1. Matryca wymagań platformy SAT (wymagania Zamawiającego)**

Poniższe tabele stanowią wymagania minimalne dotyczące platformy. Kolumny "Tak/Nie" pozostają do wypełnienia przez wykonawcę w ofercie.

**A. Wymagania ogólne platformy (symulacje i kampanie)**

Lp.	Platforma szkoleniowa powinna posiadać	Tak / Nie	ilość
1	Gotowe szablony symulacji phishingowej dostępne w wielu językach min. angielski, polski, niemiecki, czeski, ukraiński, hiszpański, włoski.		1000
2	Możliwość dostosowania szablonów do potrzeb organizacji		x
3	Symulacja technik ataku spearphishing		x
4	Symulacja technik ataku BEC (Business Email Compromise)		x
5	Automatyczne kampanie – z możliwością planowania (harmonogram)		x
6	Funkcjonalność automatycznego grupowania użytkowników		x
7	Funkcjonalność nadawania i indeksowania metryk na poziomie działów i grup		x
8	Predefiniowany pulpit nawigacyjny obrazujący stan systemu		x
9	Predefiniowany pulpit nawigacyjny z dostępem opartym o uprawnienia (podział)		x
10	Predefiniowany pulpit nawigacyjny z podziałem funkcji pracownik/dział/oddział		x
11	Możliwość integracji z AD		x
12	Możliwość integracji z Microsoft Azure (Entra ID)		x
13	Możliwość prowadzenia symulacji opartej o wyniki użytkowników		x
14	Możliwość dostosowania nazw domen w symulacjach		x
15	Funkcjonalność automatycznego kierowania treningów do odbiorców		x
16	Wsparcie procesu symulacji oparte o procesy behawioralne – badanie emocji i wrażliwości na phishing		x
17	Możliwość dynamicznego tworzenia symulacji zagrożeń – na podstawie zewnętrznych informacji, aktualnych ataków, kampanii itp		x
18	Możliwość tworzenia kampanii opartych na badaniu ryzyka		x
19	Możliwość tworzenia kampanii wyrównanych dla poszczególnych grup		x
20	Predefiniowany system powiadomień dotyczących kampanii np. dla kierowników		x
21	Możliwość tworzenia kampanii phishingowych na nośnikach USB		x



22	Możliwość tworzenia kampanii z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji		x
----	---	--	---

## B. Landing pages

Lp	Landing pages	Tak/nie	ilość
1	Gotowe szablony stron phishingowych		20
2	Obsługę HTTPS		x
3	Obsługę wielu domen		5
4	Możliwość dostosowania strony docelowej		x
5	Możliwość dostosowania domeny		x
6	Możliwość stosowania niestandardowych formularzy internetowych		x

## C. Moduł treningowy (LMS)

Lp	Niezbędne funkcjonalności modułu treningowego:		
1	Możliwość dostarczenia interaktywnych szablonów treningowych – w chwili wymagania ( w samą porę)		x
2	Możliwość dostarczenia statycznych materiałów – w chwili kiedy konieczne		x
3	LSM – system zarządzania nauką		x
4	Interaktywne szkolenia z zakresu bezpieczeństwa		x
5	Firmowane - interaktywne szkolenia z zakresu bezpieczeństwa		x
6	Indywidualne interaktywne mikro szkolenia		x
7	Indywidualne materiały szkoleniowe		x
8	Spersonalizowane ścieżki nauki		x
9	Możliwość automatycznego powiadamiania LMS		x
10	Planowanie powiadomień związanych ze szkoleniami		x
11	Powiadamianie o postępach szkoleniowych np. do kierownika działu		x
12	Powiadomienia o stanie prowadzonej kampanii np. dla kadry zarządzającej		x

13	Quizy indywidualne		x
14	Możliwość importowania własnych szkoleń w formacie SCORM 1.2		x
15	Szkolenia dostępne w wielu językach min. angielski, polski, niemiecki, czeski, ukraiński, hiszpański, włoski.		x
16	Automatyczne generowanie certyfikatu po ukończeniu szkolenia.		x

#### D. Moduł phishing / zgłaszanie podejrzanych wiadomości

lp	Niezbędne funkcjonalności modułu phishingowe:	Tak/nie	
1	Dodatek – (wtyczka) do klientów Office 365 / Outlook/ Gmail		x
2	Możliwość Kontroli adresów URL / linków/ załączników		x
3	Dynamiczną listę nadawców zaufanych		x
4	Moduł analizy podejrzanych wiadomości (email clustering analysis)		x
5	Możliwość automatycznego wyzwalania – zadań treningowych		x
6	Ujednolicony pulpit nawigacyjny		x
7	Automatyczny system raportujący o problemach w konkretnych obszarach		x
8	Możliwość modelowania scenariuszy w odpowiedzi na działania użytkowników		x
9	System inteligentnej dystrybucji materiałów		x

#### E. Wymagania niefunkcjonalne

lp	Platforma powinien zapewniać:		
1	Możliwość pracy w modelu SAAS		x
2	Mechanizmy wspierające 2FA		x
3	Dostęp do pulpitu oparty prawa dostępu ( stopniowanie praw)		x



### III. Świadczenie usług testów bezpieczeństwa

Celem zamówienia jest świadczenie usług testów bezpieczeństwa obejmujące:

1. Testy bezpieczeństwa infrastruktury sieciowej,
2. Testy bezpieczeństwa serwisów internetowych,
3. Testy bezpieczeństwa aplikacji (w tym API),

w celu identyfikacji podatności technicznych i logicznych, oceny ryzyka oraz przekazania rekomendacji naprawczych zgodnych z obowiązującymi standardami i regulacjami bezpieczeństwa informacji.

#### 1. Zakres zamówienia

##### 1.1. Testy bezpieczeństwa infrastruktury sieciowej (model Gray-Box)

Zakres obejmuje automatyczne i kompleksowe skany podatności oraz manualne testy penetracyjne dla poniższych komponentów:

- serwery fizyczne i wirtualne,
- hosty systemowe,
- urządzenia sieciowe,
- usługi udostępniane wewnętrznie i zewnętrznie.

W ramach testów Wykonawca przeprowadzi m.in.:

- automatyczne skany podatności infrastruktury sieciowej w modelu GrayBox,
- manualne testy penetracyjne komponentów infrastruktury sieciowej w modelu GrayBox:
  - manualny rekonesans i enumerację,
  - weryfikację i analizę błędów konfiguracyjnych,
  - weryfikację i analizę podatności systemów operacyjnych i usług sieciowych,
  - weryfikację i ocenę odporności na ataki typu Brute-Force,
  - identyfikację możliwości eskalacji uprawnień,
  - identyfikację możliwości przeprowadzenia Lateral Movement,
  - analizę aktualności poprawek bezpieczeństwa.

##### 1.2. Testy bezpieczeństwa serwisów internetowych (zewnętrzne aplikacje webowe) (model BlackBox/GrayBox)

Zakres obejmuje automatyczne i kompleksowe skany podatności oraz manualne testy penetracyjne serwisów internetowych (zewnętrzne aplikacje webowe). Testy bezpieczeństwa obejmują m.in.:

- automatyczne skany podatności serwisów internetowych w modelu BlackBox,
- manualne testy penetracyjne serwisów internetowych w modelu GrayBox:
  - manualny rekonesans i enumerację,
  - weryfikację mechanizmów uwierzytelniania i autoryzacji,
  - analizę zarządzania sesją (cookies, timeout, CSRF),
  - weryfikację autoryzacji i uwierzytelniania,
  - ocenę odporności na ataki typu Brute-Force,
  - identyfikację możliwości eskalacji uprawnień,
  - analizę nagłówków bezpieczeństwa (m.in. HSTS, X-Frame-Options, CSP).

Analiza wyników obejmuje podatności z obszaru framework OWASP Top 10, w tym m.in.:

XSS, SQL Injection, RCE, Broken Authentication, IDOR, oraz błędy konfiguracyjne i nieaktualne komponenty.

### 1.3. Testy bezpieczeństwa aplikacji (w tym API) (wewnętrzne aplikacje webowe) (model Gray-Box),

Zakres obejmuje automatyczne i kompleksowe skany podatności oraz manualne testy penetracyjne wewnętrznych aplikacji webowych w tym poczty webowej oraz API stanowiącego część aplikacji.

Testy obejmują m.in.:

- automatyczne skany podatności wewnętrznych aplikacji webowych w modelu BlackBox,
- manualne testy wewnętrznych aplikacji webowych w modelu GrayBox:
  - weryfikację mechanizmów uwierzytelniania i autoryzacji,
  - analizę logiki biznesowej (obejścia walidacji, nadużycia procesów),
  - weryfikację autoryzacji i uwierzytelniania,
  - identyfikację możliwości eskalacji uprawnień i dostępu do danych innych użytkowników,
  - analizę bezpieczeństwa API (walidacja wejść, JWT, kontrola ról),
  - ocenę odporności na ataki typu Brute-Force,
  - analizę nagłówków bezpieczeństwa (m.in. HSTS, X-Frame-Options, CSP).

Analiza wyników obejmuje podatności z obszaru framework OWASP Top 10, w tym m.in.:

XSS, SQL Injection, RCE, Broken Authentication, IDOR, oraz błędy konfiguracyjne i nieaktualne komponenty.

## 2. Warunki realizacji testów

Testy będą realizowane na środowiskach produkcyjnych lub przedprodukcyjnych, zgodnie z ustaleniami z Zamawiającym.

Wykonawca wykorzysta konta testowe udostępnione przez Zamawiającego (model GrayBox).

Zakres testów w modelu GrayBox obejmuje:

- 10 hostów (ok. 40 maszyn wirtualnych),
- dodatkowo 4 hosty (ok. 10 maszyn wirtualnych).

## 3. Oczekiwane rezultaty

W ramach realizacji zamówienia Wykonawca dostarczy:

1. Raport techniczny, zawierający:
  - listę wykrytych podatności,
  - klasyfikację wg CVSS, CWE oraz OWASP Top 10,
  - dowody techniczne (PoC),
  - szczegółowe rekomendacje naprawcze.
2. Raport zarządczy, zawierający:
  - syntetyczne podsumowanie ryzyk,
  - ocenę wpływu na działalność Zamawiającego,
  - priorytety działań naprawczych.
3. Rekomendacje naprawcze dla każdej podatności o poziomie CRITICAL, HIGH oraz MEDIUM.
4. Dokumentacja przygotowana w zgodności z:
  - NIST,
  - ISO/IEC 27001,
  - RODO.



## 5. Raporty w formatach:

- PDF (obowiązkowo),
- CSV i/lub JSON (opcjonalnie).

**4. Wymagania dotyczące narzędzi i zespołu**

Wykonawca zobowiązany jest do wykorzystania:

- Skanera podatności Nessus Professional,
- Systemu operacyjnego Kali Linux lub równoważnego,

Konieczność zestawienia tunelu VPN do infrastruktury Zamawiającego. Zamawiający zapewni dedykowane środowisko w postaci np. maszyny wirtualnej wewnątrz infrastruktury do przeprowadzenia testów (pivot) oraz konta testowego.

Usługa musi być realizowana przez zespół typu red team.

Zespół musi obejmować co najmniej 2 pentesterów zatrudnionych na umowach o pracę posiadających poniższe certyfikaty (każdy z pentesterów co najmniej cztery certyfikaty z poniższych):

OSCP, OSCP+, OSCP, PNPT, eJPT, C|EH, C|EH Master, C|EH Practical.

Wykonawca musi posiadać ważny certyfikat ISO/IEC 27001 obejmujący usługi bezpieczeństwa informacji oraz ISO 9001.

**5. Zakres SLA, retesty i wsparcie po realizacji testów.****5.1. SLA**

Wykonawca zapewni następujące poziomy SLA:

- rozpoczęcie realizacji testów: do 5 dni roboczych od podpisania umowy,
- dostarczenie raportów:
  - technicznego: do 10 dni roboczych od zakończenia testów,
  - zarządczego: do 10 dni roboczych od zakończenia testów.

Dokumentacja techniczna z przeprowadzonych testów zostanie udostępniona w języku angielskim wraz z rekomendacjami w języku polskim. Dokumentacja zarządcza zostanie udostępniona w języku polskim.

**5.2. Retesty**

Wykonawca zobowiązany jest do przeprowadzenia jednego retestu podatności o poziomie CRITICAL i HIGH w formie GrayBox.

Retest zostanie wykonany po wdrożeniu poprawek przez Zamawiającego, w terminie uzgodnionym przez strony.

Wyniki retestu zostaną udokumentowane w formie raportu technicznego uzupełniającego.

**5.3. Wsparcie po realizacji testów**

W ramach zamówienia Wykonawca zapewni spotkanie podsumowujące (online), obejmujące:

- omówienie wyników testów,
- prezentację kluczowych ryzyk,
- wyjaśnienie rekomendacji naprawczych,
- sesję pytań i odpowiedzi dla zespołów technicznych i zarządczych.
- Czas trwania spotkania: minimum 2 godziny.

- Spotkanie zostanie zrealizowane zdalnie po przekazaniu raportów końcowych i uzgodnieniu dogodnego terminu przez obie strony.

## 6. Terminy realizacji

Termin realizacji zamówienia: do 21 dni od dnia podpisania umowy.

Wykonawca w ofercie wskaże:

- cenę za realizację zamówienia
- doświadczenie zespołu audytowego,
- termin realizacji retestu,

## 7. Kryteria oceny ofert

1. Cena – 60%
2. Doświadczenie i kompetencje zespołu wykonawczego – 30%
3. Zakres wsparcia po usunięciu podatności przez Zamawiającego - waga 10%

### Wyliczenia dotyczące ceny

Cena najniższa / Cena badanej oferty × 60 pkt

W tym kryterium można uzyskać maksymalnie 60 punktów.

### Doświadczenie i kompetencje zespołu wykonawczego

W tym kryterium ocenie podlegać będzie doświadczenie i kompetencje zespołu wykonawczego skierowanego do realizacji zamówienia - o którym mowa w pkt. 4 OPZ.

Dla porównania i oceny ofert, pod uwagę brana będzie wskazana w formularzu ofertowym liczba posiadanych certyfikatów przez każdego z dwóch członków zespołu wykonawczego - pentestera.

Punkty w ramach tego kryterium zostaną przyznane w następujący sposób:

- po 1 certyfikacie – 0%
- po 2 certyfikaty – 10%
- po 3 certyfikaty – 20%
- po 4 i więcej certyfikatów – 30%

W tym kryterium można uzyskać maksymalnie 30 punktów.

**Do oferty należy załączyć skany certyfikatów (Zamawiający zastrzega sobie prawo do weryfikacji legalności przesłanych certyfikatów).**

### Zakres wsparcia po usunięciu podatności przez Zamawiającego

Dla porównania i oceny ofert, pod uwagę brany będzie czas wskazany w formularzu ofertowym gotowości do przeprowadzenia retestu od dnia zgłoszenia przez Zamawiającego:

- 1 dzień roboczy od daty zgłoszenia – 10%
- więcej niż jeden dzień – 0 %

W tym kryterium można uzyskać maksymalnie 10 punktów.