

Załącznik nr 1 do zaproszenia do szacowania

Znak sprawy: BDG-WI.....2026

## OPIS PRZEDMIOTU ZAMÓWIENIA

(opis przedmiotu szacowania)

**Dodatkowa usługa wsparcia w celu bardziej zaawansowanego wykorzystania posiadanego rozwiązania SIEM (Wazuh) w GDOŚ na okres 12 miesięcy wraz ze szkoleniem z obsługi rozwiązania SIEM**

### I. WPROWADZENIE

1. Przedmiotem zamówienia jest usługa obejmująca aktualizację eksploatowanego przez Zamawiającego systemu klasy SIEM/XDR Wazuh, wdrożenie monitorowania bezpieczeństwa serwerów, konfigurację powiadomień e-mail, wielopoziomowej retencji danych i importu logów przekazywanych przez zewnętrzną usługę SOC, przeprowadzenie szkolenia administratorów oraz świadczenie usługi wsparcia technicznego w formie puli roboczogodzin przez okres 12 miesięcy.
2. Celem zamówienia jest wykorzystanie Systemu jako technicznego środka zarządzania ryzykiem w zakresie: ciągłego nadzoru nad podatnościami, oceny utwardzenia konfiguracji serwerów, monitorowania integralności plików, wczesnego alarmowania o zdarzeniach krytycznych (wsparcie obowiązków zgłaszania incydentów wynikających z ustawy o krajowym systemie cyberbezpieczeństwa) oraz zapewnienia rozliczalności i przechowywania dzienników zdarzeń przez okres wymagany przepisami (Krajowe Ramy Interoperacyjności).
3. Zamówienie jest finansowane w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności (dalej: „KPO”), Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd, w zakresie wydatków kwalifikowalnych poniesionych do dnia 31 grudnia 2026 r., a w pozostałym zakresie – ze środków budżetowych Zamawiającego.
4. Zamawiający: Skarb Państwa – Generalna Dyrekcja Ochrony Środowiska, Al. Jerozolimskie 136, 02-305 Warszawa, NIP 7010151052, REGON 141628410.
5. Użyte w OPZ określenia oznaczają:
  - 1) **System** – system Wazuh (oprogramowanie open source) eksploatowany przez Zamawiającego, obejmujący komponenty Wazuh Manager, Wazuh Indexer i Wazuh Dashboard;
  - 2) **Agent** – agent Wazuh instalowany na monitorowanym serwerze;
  - 3) **Paczka SOC** – udostępniany raz w miesiącu przez wykonawcę usługi SOC świadczonej na rzecz Zamawiającego plik z dziennikami zdarzeń (JSON / JSON Lines, skompresowany) wraz z sumą kontrolną SHA-256;
  - 4) **Repozytorium archiwalne** – zasób pamięci masowej lub kopii zapasowych Zamawiającego przeznaczony do przechowywania migawek (snapshotów) i archiwów dzienników;
  - 5) **Etap I, Etap II, Etap III** – odpowiednio: wdrożenie (rozdz. III), szkolenie (rozdz. IV) i usługa wsparcia (rozdz. V);
  - 6) **rbh** – roboczogodzina, tj. 60 minut pracy jednego specjalisty Wykonawcy;

- 7) **dzień roboczy** – dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy; godziny robocze: 8:00–16:00.

## II. STAN OBECNY I ZAKRES ZAMÓWIENIA

1. Stan obecny: Zamawiający posiada zainstalowany i działający w środowisku wirtualnym System (Wazuh Manager, Wazuh Indexer / OpenSearch, Wazuh Dashboard). System wymaga aktualizacji do bieżącej wersji, optymalizacji i dostosowania konfiguracji. Jeżeli na części serwerów są zainstalowane Agenty, Wykonawca je zaktualizuje i włączy do konfiguracji docelowej.
2. Zakres monitorowania: do 50 serwerów Zamawiającego (maszyny wirtualne), w tym kontrolery domeny Active Directory, serwery bazodanowe, serwery aplikacyjne i usługowe Windows Server oraz serwery z systemami Linux. Wykaz serwerów zostanie przekazany Wykonawcy po zawarciu umowy.
3. Zamówienie nie obejmuje: monitorowania stacji roboczych, integracji z konsolą ESET PROTECT i zaporami sieciowymi Stormshield, usługi SOC w trybie 24/7, obsługi incydentów w imieniu Zamawiającego, dostawy licencji komercyjnych ani sprzętu. Usługa SOC jest świadczona na rzecz Zamawiającego na podstawie odrębnej umowy; niniejsze zamówienie ma charakter uzupełniający (własny nadzór Zamawiającego nad serwerami i archiwum dzienników) i nie powiela czynności wykonawcy SOC.
4. Zamawiający zapewni: dostęp zdalny przez VPN wskazany przez Zamawiającego, konta z uprawnieniami niezbędnymi do realizacji prac, zasoby maszyn wirtualnych i Repozytorium archiwalne według zapotrzebowania określonego w Koncepcji wdrożenia, konfigurację po stronie usługi Microsoft 365 niezbędną do wysyłki powiadomień (np. konektor lub konto usługowe) oraz przykładową Paczkę SOC.

## III. ETAP I – AKTUALIZACJA SYSTEMU I WDROŻENIE MONITOROWANIA

1. Termin: 30 dni od dnia zawarcia umowy, nie później niż do dnia 15 grudnia 2026 r.
2. **Analiza i Koncepcja wdrożenia.** W terminie 7 dni od dnia zawarcia umowy Wykonawca przekaże do akceptacji Koncepcję wdrożenia zawierającą co najmniej: wyniki weryfikacji stanu obecnego (konfiguracja menedżera, zasoby i podział dysków, stan indeksów i shardów, certyfikaty TLS), docelową wersję i plan aktualizacji z planem wycofania zmian, zapotrzebowanie na zasoby i pojemność Repozytorium archiwalnego dla okresu retencji, grupy Agentów i zakres modułów, progi i matrycę odbiorców powiadomień, sposób integracji z Microsoft 365, plan testów i harmonogram.
3. **Kopia zapasowa i aktualizacja Systemu:**
  - 1) przed rozpoczęciem prac – pełna kopia zapasowa konfiguracji menedżera, kluczy Agentów i istniejących indeksów, umożliwiającą wycofanie zmian bez utraty danych;
  - 2) aktualizacja komponentów Wazuh Manager, Wazuh Indexer i Wazuh Dashboard do najnowszej stabilnej wersji wspieranej przez producenta, z zachowaniem danych historycznych; przerwa w gromadzeniu zdarzeń wyłącznie w oknie uzgodnionym z Zamawiającym;
  - 3) zabezpieczenie komunikacji między komponentami i z Agentami protokołem TLS 1.2 lub 1.3 z poprawnymi certyfikatami;
  - 4) uwierzytelnianie do Wazuh Dashboard kontami domenowymi (LDAPS / Active Directory) z przypisaniem ról (RBAC) oraz włączenie dziennika audytu działań administracyjnych.

**4. Agenty na serwerach:**

- 1) instalacja lub aktualizacja Agentów na wszystkich serwerach z wykazu, w trybie nienadzorowanym i zautomatyzowanym (np. PowerShell/WinRM dla Windows Server, Ansible/Bash dla Linux lub narzędzia równoważne), z rejestracją chronioną hasłem lub tokenem;
- 2) grupy Agentów co najmniej: kontrolery domeny, serwery bazodanowe, serwery aplikacyjne/usługowe Windows, serwery Linux; konfiguracja zarządzana centralnie dla grup (agent.conf), bez ręcznych zmian na serwerach;
- 3) ograniczenie obciążenia serwerów (limity zdarzeń na sekundę, bufor, harmonogram i priorytet skanów) według Koncepcji; brak istotnego wpływu na wydajność serwerów potwierdza się w testach akceptacyjnych.

**5. Moduły i reguły detekcji:**

- 1) zbieranie dzienników: Windows (Security, System, Application, PowerShell – zdarzenie 4104), Linux (auditd, auth.log, sudo); Sysmon na serwerach wskazanych w Koncepcji;
- 2) kontrolery domeny: reguły dla zdarzeń tożsamości, w tym zmian członkostwa w grupach uprzywilejowanych, tworzenia i modyfikacji kont, blokad kont, anomalii uwierzytelniania Kerberos/NTLM, ataków typu brute-force i password spraying;
- 3) wykrywanie podatności oprogramowania serwerów (CVE);
- 4) cykliczna ocena konfiguracji (SCA) według wytycznych CIS dla używanych wersji Windows Server i Linux;
- 5) monitorowanie integralności plików (FIM) w czasie rzeczywistym dla plików systemowych, certyfikatów, plików wykonywalnych i kluczowych gałęzi rejestru Windows, z wykluczeniami dla dynamicznych plików baz danych i dzienników;
- 6) wykrywanie rootkitów i anomalii, klasyfikacja zdarzeń według MITRE ATT&CK; mechanizmy Active Response wyłącznie po akceptacji Zamawiającego i testach;
- 7) strojenie reguł przez 10 dni roboczych po uruchomieniu monitorowania w celu ograniczenia alertów fałszywie dodatnich.

**6. Powiadomienia e-mail i raporty:**

- 1) integracja wysyłki powiadomień z pocztą Zamawiającego w usłudze Microsoft 365 (Exchange Online), metodą wspieraną przez Microsoft i zabezpieczoną szyfrowaniem TLS (np. przekaźnik SMTP z konektorem lub lokalny przekaźnik pocztowy na serwerze menedżera), uzgodnioną w Koncepcji;
- 2) powiadomienia w czasie rzeczywistym dla zdarzeń o poziomie istotności nie niższym niż próg ustalony w Koncepcji (domyślnie 10);
- 3) powiadomienia dedykowane, niezależnie od poziomu, co najmniej dla: dodania konta do grupy uprzywilejowanej w AD, serii nieudanych logowań (brute-force / password spraying), nieautoryzowanej zmiany pliku krytycznego wykrytej przez FIM, wykrycia podatności krytycznej (CVSS  $\geq 9,0$ );
- 4) limit liczby wiadomości w jednostce czasu, zapobiegający zalaniu skrzynek przy zdarzeniach masowych;
- 5) kierowanie powiadomień do różnych grup odbiorców zależnie od kategorii zdarzenia, według matrycy uzgodnionej z Zamawiającym;

- 6) cykliczne raporty (co najmniej tygodniowy i miesięczny, PDF lub CSV) wysyłane automatycznie – zestawienie najczęstszych alertów, stan podatności, wyniki SCA – oraz monitory progowe (np. skok liczby zdarzeń lub błędów uwierzytelniania), z użyciem mechanizmów dostępnych w zaktualizowanej wersji Systemu lub równoważnych;
- 7) co najmniej 5 pulpitów (stan Agentów, podatności, SCA, alerty wg MITRE ATT&CK, zdarzenia tożsamości z kontrolerów domen).

#### 7. Import Paczek SOC:

- 1) model działania: administrator Zamawiającego raz w miesiącu pobiera Paczkę SOC z zasobów wykonawcy usługi SOC i umieszcza ją we wskazanym katalogu na serwerze Zamawiającego;
- 2) Wykonawca opracuje i wdroży narzędzie importu (np. Logstash, Filebeat lub równoważne), które po wskazaniu pliku automatycznie: weryfikuje sumę SHA-256, rozpakowuje dane w katalogu roboczym, parsuje zdarzenia i zapisuje je w Wazuh Indexer oraz raportuje wynik importu;
- 3) zachowanie oryginalnego czasu zdarzenia – mapowanie znacznika czasu z pliku na pole @timestamp; niedopuszczalne jest zastąpienie go czasem importu;
- 4) zapis do odrębnego indeksu miesięcznego (np. soc-archive-RRRR.MM), poza strumieniem alertów czasu rzeczywistego;
- 5) wzorzec indeksu i pulpit w Wazuh Dashboard umożliwiające przeszukiwanie danych z SOC i ich zestawianie z danymi z serwerów;
- 6) archiwizacja oryginalnej Paczki SOC w Repozytorium archiwalnym wraz z sumą kontrolną; format danych zostanie potwierdzony na podstawie przykładowej Paczki SOC przekazanej przez Zamawiającego.

#### 8. Retencja wielopoziomowa:

- 1) warstwa bieżąca (do 30 dni): indeksy aktywne na szybkich zasobach dyskowych;
- 2) warstwa pośrednia (do 6 miesięcy): indeksy tylko do odczytu, zoptymalizowane (scalenie segmentów), dostępne online w Wazuh Dashboard;
- 3) warstwa archiwalna (łącznie co najmniej 24 miesiące): migawki indeksów w Repozytorium archiwalnym, usuwanie indeksu z Wazuh Indexer wyłącznie po potwierdzeniu poprawnego wykonania migawki; kompresja surowych dzienników (archives) z sumami SHA-256;
- 4) automatyzacja przejść między warstwami (polityki Index State Management lub równoważne) i harmonogram migawek;
- 5) procedura odtworzenia archiwalnego indeksu miesięcznego do stanu przeszukiwalnego w Wazuh Dashboard – przetestowana, z czasem odtworzenia poniżej 2 godzin.

9. **Testy akceptacyjne** z udziałem Zamawiającego, co najmniej: aktualizacja bez utraty danych historycznych; status aktywny i poprawne zasilanie danymi (FIM, SCA, podatności) wszystkich Agentów z podziałem na grupy; kontrolowane zdarzenia testowe (np. zmiana pliku FIM, seria nieudanych logowań, dodanie konta testowego do grupy uprzywilejowanej) i odbiór powiadomień e-mail; import przykładowej Paczki SOC z weryfikacją SHA-256 i zachowaniem czasu zdarzeń; wykonanie i odtworzenie migawki testowej; brak istotnego wpływu Agentów na wydajność serwerów.

10. **Dokumentacja powykonawcza** w języku polskim (format edytowalny i PDF): raport z weryfikacji i aktualizacji; architektura, macierz komunikacji sieciowej i konfiguracja Systemu; macierz grup Agentów z wykazem serwerów i zakresem modułów; konfiguracja powiadomień (integracja z Microsoft 365, progi, matryca odbiorców); procedura importu Paczek SOC; instrukcja retencji, migawek i odtwarzania; procedury eksploatacyjne (dodanie i usunięcie Agentu, aktualizacja, kopia zapasowa). Skrypty, reguły, dekodery i konfiguracje przekazuje się w postaci plików.
11. Odbiór Etapu I następuje protokołem odbioru po pozytywnych testach akceptacyjnych i przekazaniu dokumentacji powykonawczej.

#### IV. ETAP II – SZKOLENIE ADMINISTRATORÓW

1. Jedno szkolenie dla do 7 administratorów Zamawiającego, 2 dni po 8 godzin zegarowych (łącznie 16 godzin, z przerwami), w trybie zdalnym (online), nie później niż do dnia 15 grudnia 2026 r. Szkolenie odbywa się po odbiorze Etapu I albo po zakończeniu testów akceptacyjnych, w terminie uzgodnionym z co najmniej 7-dniowym wyprzedzeniem.
2. Warunki szkolenia online:
  - 1) prowadzenie na żywo przez trenera (niedopuszczalne odtwarzanie nagrań);
  - 2) platforma Microsoft Teams Zamawiającego albo platforma Wykonawcy zaakceptowana przez Zamawiającego, zapewniająca dwukierunkowy dźwięk i obraz, udostępnianie ekranu, czat i interakcję z trenerem;
  - 3) ćwiczenia praktyczne na środowisku Systemu Zamawiającego (dostęp przez VPN Zamawiającego) albo na środowisku laboratoryjnym Wykonawcy odzwierciedlającym konfigurację z Etapu I;
  - 4) nagranie sesji do wyłącznie wewnętrznego użytku Zamawiającego jako bazy wiedzy, po uzyskaniu zgody trenera i uczestników; nagrania przekazywane w formacie MP4.
3. Program obejmuje co najmniej:
  - a) dzień I: architektura zaktualizowanego Systemu; zarządzanie grupami Agentów i konfiguracją centralną; FIM (zmiany plików i rejestru, wyjątki); SCA i interpretacja wyników CIS; wykrywanie podatności i obsługa podatności krytycznych; zdarzenia tożsamości z kontrolerów domeny;
  - b) dzień II: wyszukiwanie i analiza w Wazuh Dashboard, budowa pulpitów; konfiguracja powiadomień e-mail i raportów (progi, odbiorcy, diagnostyka wysyłki); procedura importu Paczki SOC; zarządzanie retencją i odtwarzanie indeksu z migawki (warsztat); tworzenie reguł własnych i ograniczanie fałszywych alarmów.
4. Wykonawca przekaże do akceptacji, najpóźniej 5 dni roboczych przed szkoleniem, program i materiały w języku polskim (PDF) wraz z wykorzystywanymi skryptami, a po szkoleniu – imienne certyfikaty (elektroniczne) oraz listę obecności (raport logowania z platformy potwierdzony przez trenera i Zamawiającego). Materiały, certyfikaty i lista obecności oznaczone zgodnie z zasadami oznakowania KPO.
5. Szkolenie prowadzi trener z praktycznym doświadczeniem we wdrażaniu systemu Wazuh (rozdz. VIII).

#### V. ETAP III – USŁUGA WSPARCIA (PUŁA ROBOCZOGODZIN)

1. Puła do 60 rbh do wykorzystania przez 12 miesięcy od dnia odbioru Etapu I bez uwag. Zamawiający nie jest zobowiązany do wykorzystania puli w całości ani w części;

wynagrodzenie przysługuje wyłącznie za rbh faktycznie wykorzystane, a Wykonawcy nie przysługują roszczenia z tytułu niewykorzystania puli.

2. Pula może być wykorzystana w szczególności na: rozszerzenie monitorowania na kolejne serwery, nowe reguły, dekodery, pulpity i raporty, strojenie detekcji, aktualizacje Systemu i Agentów, dostosowanie importu Paczek SOC do zmian formatu, diagnozę problemów niebędących wadą objętą gwarancją oraz konsultacje dotyczące analizy alertów.
3. Zasady zgłaszania potrzeb i poziom usług (SLA):
  - 1) **Zgłoszenie** – przekazują osoby wskazane przez Zamawiającego, przez uzgodniony kanał (adres e-mail lub system zgłoszeń Wykonawcy), w dni robocze w godz. 8:00–16:00; zgłoszenie przekazane po godz. 16:00 lub w dniu wolnym uważa się za przekazane o godz. 8:00 następnego dnia roboczego. Zgłoszenie zawiera: opis potrzeby lub problemu, oczekiwany rezultat, wskazanie, czy dotyczy awarii;
  - 2) **Reakcja – do 4 godzin roboczych** od zgłoszenia: potwierdzenie przyjęcia z nadaniem numeru, wstępna diagnoza oraz propozycja zakresu prac, terminu wykonania i szacowanej liczby rbh. W przypadku awarii (System nie zbiera, nie przetwarza lub nie udostępnia zdarzeń) Wykonawca w tym czasie rozpoczyna prace naprawcze, a zakres i liczbę rbh przedstawia niezwłocznie;
  - 3) **Przyjęcie do realizacji** – Zamawiający akceptuje propozycję wiadomością e-mail, zgłasza uwagi albo rezygnuje ze zgłoszenia. Czas przyjęcia, diagnozy i wyceny zgłoszenia nie podlega rozliczeniu w rbh, a zgłoszenie niezaaceptowane nie jest rozliczane;
  - 4) **Realizacja – do 2 dni roboczych** od przyjęcia zgłoszenia do realizacji. Dłuższy termin jest dopuszczalny wyłącznie dla zadań rozwojowych, których pracochłonność obiektywnie to uzasadnia, jeżeli Wykonawca wskaże go w propozycji (pkt 2) i Zamawiający go zaakceptuje;
  - 5) **Zamknięcie** – Wykonawca informuje o wykonaniu, opisuje wykonane czynności i faktyczną liczbę rbh; Zamawiający potwierdza wykonanie albo zgłasza zastrzeżenia w ciągu 2 dni roboczych. Przekroczenie zaakceptowanej liczby rbh wymaga uprzedniej zgody Zamawiającego;
  - 6) **Rejestr i rozliczenie** – każde zgłoszenie jest rejestrowane (numer, data i godzina zgłoszenia, reakcji, przyjęcia do realizacji i zakończenia, opis, wykonane czynności, liczba rbh). Rozliczenie następuje miesięcznie, w jednostkach 0,5 rbh, wyłącznie za zgłoszenia zamknięte w danym miesiącu, na podstawie protokołu realizacji zgłoszeń zatwierdzonego przez Zamawiającego; protokół stanowi podstawę wystawienia faktury.
4. Wykonawca prowadzi rejestr w sposób umożliwiający Zamawiającemu weryfikację dotrzymania czasów reakcji i realizacji; przekroczenia wykazuje w protokole realizacji zgłoszeń.

## VI. GWARANCJA

1. Wykonawca udziela 12-miesięcznej gwarancji, liczonej od dnia odbioru Etapu I, na prawidłowe działanie wykonanej konfiguracji Systemu, skryptów instalacyjnych, narzędzia importu Paczek SOC, mechanizmów retencji i powiadomień.
2. Usuwanie wad objętych gwarancją jest nieodpłatne i nie pomniejsza puli rbh. Do zgłaszania wad stosuje się zasady i czasy reakcji oraz realizacji określone w rozdz. V ust. 3, z tym że czas usuwania wady nie jest rozliczany w rbh.

## **VII. WYMAGANIA OGÓLNE**

1. Prace wykonywane są z zachowaniem ciągłości działania infrastruktury Zamawiającego; czynności mogące spowodować przerwę Wykonawca uzgadnia z wyprzedzeniem co najmniej 2 dni roboczych.
2. Wykonawca stosuje się do polityk bezpieczeństwa Zamawiającego, korzysta wyłącznie z przydzielonych kont imiennych, nie kopiuje danych z Systemu poza infrastrukturę Zamawiającego, a dokumentację przekazuje w zaszyfrowanych archiwach (AES-256), z hasłem przekazany innym kanałem.
3. Członkowie zespołu Wykonawcy składają oświadczenie o zachowaniu poufności przez okres obowiązywania umowy oraz 5 lat po jej wygaśnięciu.
4. Dane przetwarzane w Systemie (dzienniki zdarzeń, w tym z kontrolerów domeny i Paczek SOC) zawierają dane osobowe; Wykonawca zawrze z Zamawiającym umowę powierzenia przetwarzania danych osobowych (art. 28 RODO).
5. Wykonawca nie dostarcza oprogramowania wymagającego zakupu licencji przez Zamawiającego; dopuszcza się wyłącznie komponenty open source albo narzędzia, których licencja wieczysta przechodzi na Zamawiającego w ramach wynagrodzenia.
6. Oznakowanie KPO: wszystkie dokumenty wytworzone w ramach zamówienia (Koncepcja, dokumentacja, materiały szkoleniowe, certyfikaty, raporty, protokoły) Wykonawca oznacza zgodnie z Księgą Identyfikacji Wizualnej KPO oraz Strategią promocji i informacji KPO (<https://www.kpo.gov.pl/strony/o-kpo/dla-instytucji/dokumenty/strategia-promocji-i-informacji-kpo/>).
7. Klauzula ICT: Wykonawca oferuje wyłącznie produkty, usługi i procesy ICT, które na dzień składania ofert nie są objęte rekomendacją, o której mowa w art. 33 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa, ani decyzją o uznaniu dostawcy za dostawcę wysokiego ryzyka (art. 67b ust. 15 tej ustawy); dotyczy to także narzędzi zdalnego dostępu i systemu zgłoszeń Wykonawcy.
8. Zasada DNSH: przedmiot zamówienia nie wyrządza znaczącej szkody celom środowiskowym; dokumenty przekazywane są wyłącznie w formie elektronicznej, a szkolenie realizowane jest zdalnie.
9. Zakaz podwójnego finansowania: zakres zamówienia nie pokrywa się z usługami realizowanymi na podstawie innych umów Zamawiającego (w tym umowy na usługę SOC); Wykonawca opisuje czynności w protokołach w sposób umożliwiający ich jednoznaczne przypisanie do niniejszego zamówienia.
10. Komunikacja, dokumentacja i szkolenie – w języku polskim.

## **VIII. PLANOWANE WARUNKI UDZIAŁU I KRYTERIA OCENY OFERT**

Informacja ma charakter orientacyjny i służy oszacowaniu kosztów; ostateczne warunki i kryteria zostaną określone w zapytaniu ofertowym.

1. Warunek udziału – personel: co najmniej 1 inżynier, który w okresie ostatnich 3 lat uczestniczył w co najmniej 1 wdrożeniu systemu Wazuh, oraz trener, który przeprowadził co najmniej 1 szkolenie z systemu Wazuh (dopuszcza się wskazanie jednej osoby w obu rolach).
2. Planowane kryteria oceny ofert:

| <b>Kryterium</b>        | <b>Opis</b>                                                                                                                                                                                                                             | <b>Waga</b> |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| Cena łączna             | cena brutto za Etap I, Etap II oraz 60 rbh Etapu III; $P_c = (C_{min} / C_{bad}) \times 60$                                                                                                                                             | 60 pkt      |
| Cena 1 rbh              | cena brutto za 1 rbh w Etapie III; $P_r = (R_{min} / R_{bad}) \times 10$                                                                                                                                                                | 10 pkt      |
| Doświadczenie inżyniera | udział inżyniera skierowanego do realizacji zamówienia w więcej niż 3 wdrożeniach systemu Wazuh w jednostkach zatrudniających powyżej 100 użytkowników, w okresie ostatnich 3 lat: więcej niż 3 wdrożenia – 30 pkt; 3 lub mniej – 0 pkt | 30 pkt      |