Ogłoszenie o zamówieniu
Dostawy
Dostawa i wdrożenie rozwiązań cyberbezpieczeństwa IT/OT/ICS wraz z usługami organizacyjnymi, szkoleniowymi i audytowymi

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego

Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: GMINA ABRAMÓW

1.4) Krajowy Numer Identyfikacyjny: REGON 431019900

1.5) Adres zamawiającego

1.5.1.) Ulica: ul. Szkolna 2

1.5.2.) Miejscowość: Abramów

1.5.3.) Kod pocztowy: 21-143

1.5.4.) Województwo: lubelskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL814 - Lubelski

1.5.9.) Adres poczty elektronicznej: gmina@abramow.pl

1.5.10.) Adres strony internetowej zamawiającego: https://ugabramow.bip.lubelskie.pl

1.6.) Rodzaj zamawiającego: Zamawiający publiczny - jednostka sektora finansów publicznych - jednostka samorządu terytorialnego

1.7.) Przedmiot działalności zamawiającego: Ogólne usługi publiczne

SEKCJA II – INFORMACJE PODSTAWOWE

2.1.) Ogłoszenie dotyczy:

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie

2.3.) Nazwa zamówienia albo umowy ramowej:

Dostawa i wdrożenie rozwiązań cyberbezpieczeństwa IT/OT/ICS wraz z usługami organizacyjnymi, szkoleniowymi i audytowymi

2.4.) Identyfikator postępowania: ocds-148610-8ce3ffb8-847b-4db4-8931-e08265fb35a4

2.5.) Numer ogłoszenia: 2026/BZP 00509237

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2026-10-29

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Tak

2.9.) Numer planu postępowań w BZP: 2026/BZP 00067850/10/P

2.10.) Identyfikator pozycji planu postępowań:

1.3.3 Dostawa i wdrożenie rozwiązań cyberbezpieczeństwa IT/OT/ICS wraz z usługami organizacyjnymi, szkoleniowymi i audytowymi

2.11.) O udzielenie zamówienia mogą ubiegać się wyłącznie wykonawcy, o których mowa w art. 94 ustawy: Nie

2.14.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej: Tak

2.15.) Nazwa projektu lub programu

Krajowy Plan Odbudowy i Zwiększania Odporności C3 Cyberbezpieczeństwo C3.1.1 Cyberbezpieczeństwo - CyberPL, KPOD.058.10-CW.01-001/25

2.16.) Tryb udzielenia zamówienia wraz z podstawą prawną

Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 1 ustawy

SEKCJA III – UDOSTĘPNIANIE DOKUMENTÓW ZAMÓWIENIA I KOMUNIKACJA

3.1.) Adres strony internetowej prowadzonego postępowania
https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-8ce3ffb8-847b-4db4-8931-e08265fb35a4

3.2.) Zamawiający zastrzega dostęp do dokumentów zamówienia: Nie

3.4.) Wykonawcy zobowiązani są do składania ofert, wniosków o dopuszczenie do udziału w postępowaniu, oświadczeń oraz innych dokumentów wyłącznie przy użyciu środków komunikacji elektronicznej: Tak

3.5.) Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami - adres strony internetowej: www.ezamowienia.gov.pl

3.6.) Wymagania techniczne i organizacyjne dotyczące korespondencji elektronicznej: 11. Komunikacja w postępowaniu, z wyłączeniem składania ofert, odbywa się drogą elektroniczną za pośrednictwem formularzy do komunikacji dostępnych w zakładce „Formularze" („Formularze do komunikacji"). Za pośrednictwem „Formularzy do komunikacji" odbywa się w szczególności przekazywanie wezwań i zawiadomień, zadawanie pytań i udzielanie odpowiedzi. Formularze do komunikacji umożliwiają również dołączenie załącznika do przesyłanej wiadomości (przycisk „dodaj załącznik"). W przypadku załączników, które są zgodnie z ustawą Pzp lub rozporządzeniem Prezesa Rady Ministrów w sprawie wymagań dla dokumentów elektronicznych opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, mogą być opatrzone, zgodnie z wyborem wykonawcy/wykonawcy wspólnie ubiegającego się o udzielenie zamówienia/podmiotu udostępniającego zasoby, podpisem zewnętrznym lub wewnętrznym. W zależności od rodzaju podpisu i jego typu (zewnętrzny, wewnętrzny) dodaje się do przesyłanej wiadomości uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny).
12. Możliwość korzystania w postępowaniu z „Formularzy do komunikacji" w pełnym zakresie wymaga posiadania konta „Wykonawcy" na Platformie e-Zamówienia oraz zalogowania się na Platformie e-Zamówienia. Do korzystania z „Formularzy do komunikacji" służących do zadawania pytań dotyczących treści dokumentów zamówienia wystarczające jest posiadanie tzw. konta uproszczonego na Platformie
e-Zamówienia.
13. Wszystkie wysłane i odebrane w postępowaniu przez wykonawcę wiadomości widoczne są po zalogowaniu w podglądzie postępowania w zakładce „Komunikacja".
14. Maksymalny rozmiar plików przesyłanych za pośrednictwem „Formularzy do komunikacji" wynosi 150 MB (wielkość ta dotyczy plików przesyłanych jako załączniki do jednego formularza).
15. Minimalne wymagania techniczne dotyczące sprzętu używanego w celu korzystania z usług Platformy e-Zamówienia oraz informacje dotyczące specyfikacji połączenia określa Regulamin Platformy e-Zamówienia, w szczególności:
1) W celu prawidłowego korzystania z usług Platformy e-Zamówienia wymagany jest:
a) Komputer PC:
˜ parametry minimum: Intel Core2 Duo, 2 GB RAM, HDD,
˜ zainstalowany jeden z poniższych systemów operacyjnych:
MS Windows 7 lub nowszy
OSX/Mac OS 10.10,.
Ubuntu 14.04
˜ Zainstalowana jedna z poniższych przeglądarek:
Chrome 66.0 lub nowsza
Firefox 59.0 lub nowszy
Safari 11.1 lub nowsza
Edge 14.0 i nowsze
albo
b) 1.2 Tablet/Telefon:
Parametry minimum: 4 rdzenie procesora, 2GB RAM, Android 6.0 Marshmallow, iOS 10.3, Przeglądarka Chrome 61 lub nowa.
2) Dla skorzystania z pełnej funkcjonalności może być konieczne włączenie w przeglądarce obsługi protokołu bezpiecznej transmisji danych SSL, obsługi Java Script, oraz cookies;
3) Specyfikacja połączenia, formatu przesyłanych danych oraz kodowania i oznaczania czasu odbioru danych:
a) specyfikacja połączenia – formularze udostępnione są za pomocą protokołu TLS 1.2,
b) 1.2 format danych oraz kodowanie: formularze dostępne są w formacie HTML z kodowaniem UTF-8,
c) oznaczenia czasu odbioru danych: wszelkie operacje opierają się o czas serwera i dane zapisywane są z dokładnością co do sekundy.
16. W przypadku problemów technicznych i awarii związanych z funkcjonowaniem Platformy e-Zamówienia użytkownicy mogą skorzystać ze wsparcia technicznego dostępnego pod numerem telefonu (22) 458 77 99 lub drogą elektroniczną poprzez formularz udostępniony na stronie internetowej https://ezamowienia.gov.pl w zakładce „Zgłoś problem".
17. W szczególnie uzasadnionych przypadkach uniemożliwiających komunikację wykonawcy i Zamawiającego za pośrednictwem Platformy e-Zamówienia, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres e-mail: gmina@abramow.pl (nie dotyczy składania ofert).

3.8.) Zamawiający wymaga sporządzenia i przedstawienia ofert przy użyciu narzędzi elektronicznego modelowania danych budowlanych lub innych podobnych narzędzi, które nie są ogólnie dostępne: Nie

3.12.) Oferta - katalog elektroniczny: Nie dotyczy

3.14.) Języki, w jakich mogą być sporządzane dokumenty składane w postępowaniu:

polski

3.15.) RODO (obowiązek informacyjny): 1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o danych) (Dz. U. UE L119 z dnia 4 maja 2016 r., str. 1; zwanym dalej „RODO") informujemy, że:
1) administratorem Pani/Pana danych osobowych jest Gmina Abramów
2) administrator wyznaczył inspektora ochrony danych, z którym można się kontaktować pod adresem e-mail: inspektor@cbi24.pl
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego, prowadzonym w trybie podstawowym bez negocjacji
4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 74 ustawy Pzp.
5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy. Dane będą następnie przechowywane w celach archiwalnych, przez okres, który wyznaczony zostanie przede wszystkim na podstawie rozporządzenia Prezesa Rady Ministrów w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, chyba że przepisy szczególne stanowią inaczej, a w przypadku zamówień dofinansowanych ze środków zewnętrznych – przez okres trwałości projektu;
6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisanych ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego.
7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Informacje ogólne odnoszące się do przedmiotu zamówienia.

4.1.1.) Przed wszczęciem postępowania przeprowadzono konsultacje rynkowe: Nie

4.1.2.) Numer referencyjny: ZP.271.19.2026

4.1.3.) Rodzaj zamówienia: Dostawy

4.1.4.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Nie

4.1.8.) Możliwe jest składanie ofert częściowych: Nie

4.1.13.) Zamawiający uwzględnia aspekty społeczne, środowiskowe lub etykiety w opisie przedmiotu zamówienia: Nie

4.2. Informacje szczegółowe odnoszące się do przedmiotu zamówienia:

4.2.2.) Krótki opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja, uruchomienie, integracja, dokumentacja i odbiór rozwiązań cyberbezpieczeństwa oraz wykonanie usług organizacyjnych i szkoleniowych wskazanych w Załączniku nr 2 – OPZ. Dodatkowo w zakres wchodzą U20, U25 oraz rozwiązania wskazane w macierzy OPZ. U42 – przygotowanie projektu grantowego – nie stanowi przedmiotu niniejszej dostawy; koszty pośrednie również są poza nią.
Zakres obejmuje w szczególności:
• opracowanie i wdrożenie SZBI i SZCD, przeglądy SZBI, BCP/DRP oraz niezależną ocenę zgodności i audyt SZBI/SZCD/KRI/uoKSC;
• szkolenia z zakresu cyberbezpieczeństwa, w tym szkolenia specjalistyczne i testy socjotechniczne;
• wdrożenie antywirusa, XDR, ITDR, NDR, monitorowania infrastruktury, WAF, zabezpieczeń poczty, certyfikatów TLS/SSL;
• dostawę łącznie 4 urządzeń UTM: 1 szt. dla sieci IT oraz 3 szt. dla OT (1 UTM główny OT i 2 UTM SUW);
• dostawę NAS, macierzy dyskowej, serwera fizycznego, szafy RACK, 2 zarządzalnych switchy, 2 punktów dostępowych WiFi oraz UPS;
• konfigurację, hardening, segmentację i integrację rozwiązań IT/OT/ICS;
• wykonanie inwentaryzacji aktywów oraz dokumentacji powykonawczej i testów odbiorowych.
Szczegółowy opis, minimalne parametry, zasady równoważności oraz warunki odbioru określa OPZ

4.2.6.) Główny kod CPV: 48730000-4 - Pakiety oprogramowania zabezpieczającego

4.2.7.) Dodatkowy kod CPV:

32420000-3 - Urządzenia sieciowe

48820000-2 - Serwery

72263000-6 - Usługi wdrażania oprogramowania

72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

80533100-0 - Usługi szkolenia komputerowego

4.2.8.) Zamówienie obejmuje opcje: Nie

4.2.10.) Okres realizacji zamówienia albo umowy ramowej: do 2026-12-21

4.2.11.) Zamawiający przewiduje wznowienia: Nie

4.2.13.) Zamawiający przewiduje udzielenie dotychczasowemu wykonawcy zamówień na podobne usługi lub roboty budowlane: Nie

4.3.) Kryteria oceny ofert

4.3.1.) Sposób oceny ofert: 18. Kryteria oceny ofert
Kryterium Waga
Cena brutto (C) 60 pkt
Okres gwarancji producenta na serwer fizyczny (G) 20 pkt
Okres wsparcia producenta/subskrypcji dla urządzeń UTM/NGFW (U) 20 pkt
18.1. Cena – 60 pkt
C = (najniższa cena brutto / cena brutto badanej oferty) × 60 pkt.
18.2. Gwarancja producenta na serwer – 20 pkt
Oferowany okres gwarancji Punkty
24–35 miesięcy 0 pkt
36–47 miesięcy 8 pkt
48–59 miesięcy 14 pkt
60 miesięcy i więcej 20 pkt
Punkty w kryterium G przyznaje się za zadeklarowany w formularzu ofertowym okres gwarancji producenta na serwer fizyczny, wyrażony w pełnych miesiącach, zgodnie z poniższą tabelą. Minimalny wymagany okres gwarancji wynosi 24 miesiące. Za okres 60 miesięcy lub dłuższy przyznaje się maksymalnie 20 pkt; okresy pośrednie ocenia się według wskazanych przedziałów.
W razie niewskazania okresu gwarancji Zamawiający przyjmuje okres minimalny 24 miesięcy i przyznaje 0 pkt. Zadeklarowanie okresu krótszego niż wymagane 24 miesiące oznacza niespełnienie wymagań minimalnych i podlega ocenie zgodnie z Pzp.
18.3. Wsparcie producenta/subskrypcja UTM/NGFW – 20 pkt
Oferowany okres pełnego wsparcia Punkty
36–47 miesięcy 0 pkt
48–59 miesięcy 10 pkt
60 miesięcy i więcej 20 pkt
Punkty w kryterium U przyznaje się za zadeklarowany w formularzu ofertowym okres pełnego wsparcia producenta/subskrypcji dla wszystkich czterech urządzeń UTM/NGFW objętych zamówieniem (1 urządzenie IT/główny OT oraz 3 urządzenia lokalne OT), wyrażony w pełnych miesiącach. Minimalny wymagany okres wynosi 36 miesięcy. Punktacja zgodnie z tabelą poniżej; za 60 miesięcy lub więcej przyznaje się maksymalnie 20 pkt. Jeżeli oferowane okresy różnią się między urządzeniami, do oceny przyjmuje się najkrótszy z nich. Niewskazanie okresu oznacza przyjęcie 36 miesięcy i 0 pkt, a zadeklarowanie okresu krótszego niż 36 miesięcy oznacza niespełnienie wymagań minimalnych i podlega ocenie zgodnie z Pzp.
Punktacja łączna: P = C + G + U (maksymalnie 100 pkt). Za najkorzystniejszą zostanie uznana oferta z najwyższą łączną liczbą punktów. Kryteria G i U są oceniane na podstawie liczby pełnych miesięcy wpisanej w formularzu ofertowym, z uwzględnieniem powyższych przedziałów.

4.3.2.) Sposób określania wagi kryteriów oceny ofert: Punktowo

4.3.3.) Stosowane kryteria oceny ofert: Kryterium ceny oraz kryteria jakościowe

Kryterium 1

4.3.5.) Nazwa kryterium: Cena

4.3.6.) Waga: 60

Kryterium 2

4.3.4.) Rodzaj kryterium:
serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: okres gwarancji

4.3.6.) Waga: 20

Kryterium 3

4.3.4.) Rodzaj kryterium:
serwis posprzedażny, pomoc techniczna, warunki dostawy takich jak termin, sposób lub czas dostawy, oraz okresu realizacji.

4.3.5.) Nazwa kryterium: okres pełnego wsparcia

4.3.6.) Waga: 20

4.3.10.) Zamawiający określa aspekty społeczne, środowiskowe lub innowacyjne, żąda etykiet lub stosuje rachunek kosztów cyklu życia w odniesieniu do kryterium oceny ofert: Nie

SEKCJA V - KWALIFIKACJA WYKONAWCÓW

5.1.) Zamawiający przewiduje fakultatywne podstawy wykluczenia: Tak

5.2.) Fakultatywne podstawy wykluczenia:

Art. 109 ust. 1 pkt 4

Art. 109 ust. 1 pkt 5

Art. 109 ust. 1 pkt 7

Art. 109 ust. 1 pkt 8

Art. 109 ust. 1 pkt 10

5.3.) Warunki udziału w postępowaniu: Tak

5.4.) Nazwa i opis warunków udziału w postępowaniu.
6.3. Zdolność techniczna lub zawodowa – doświadczenie Wykonawcy
Wykonawca spełni warunek, jeżeli wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał co najmniej 2 zamówienia dotyczące infrastruktury teleinformatycznej lub cyberbezpieczeństwa.
Łącznie w ramach wykazanych zamówień Wykonawca musi potwierdzić:
• co najmniej jedno zamówienie o charakterze wdrożeniowym obejmujące co najmniej 4 z następujących obszarów: NGFW/UTM, switching/routing/VLAN, serwery/wirtualizacja, storage/NAS, backup/DR, AD/IAM/MFA/PKI, SIEM, endpoint security, hardening;
• co najmniej jedno zamówienie usługowe obejmujące co najmniej 2 z następujących obszarów: SZBI/SZCD/BCP/DRP, zarządzanie podatnościami lub hardening, MIDS/MDR/SOC/CTI/Incident Response, szkolenia z cyberbezpieczeństwa i testy socjotechniczne.
Jedno zamówienie może potwierdzać oba wymagania, jeżeli jego rzeczywisty zakres obejmował wszystkie wymagane elementy. Nie wymaga się, aby każda referencja obejmowała całość technologii występujących w przedmiotowym zamówieniu.
6.4. Wymagania ogólne dotyczące zespołu
• Wykonawca wykaże, że dysponuje lub będzie dysponował zespołem osób posiadających kwalifikacje, wiedzę i doświadczenie niezbędne do należytej realizacji zamówienia.
• Zamawiający nie określa minimalnej łącznej liczby osób w zespole. Jedna osoba może pełnić nie więcej niż 3 funkcje wskazane w pkt 6.5, pod warunkiem spełnienia wszystkich wymagań dla każdej funkcji oraz zapewnienia realnej możliwości wykonywania tych funkcji w harmonogramie zamówienia.
• Samo posiadanie certyfikatu, zaświadczenia lub ukończenie szkolenia nie jest wystarczające, jeżeli dla danej funkcji wymagane jest również doświadczenie praktyczne.
• Ten sam projekt może służyć do wykazania doświadczenia jednej osoby dla więcej niż jednej funkcji, jeżeli Wykonawca jednoznacznie wskaże czynności wykonywane osobiście przez tę osobę.
• Osoby wskazane dla potwierdzenia warunków udziału muszą faktycznie uczestniczyć w realizacji zamówienia w zakresie odpowiadającym wykazywanej funkcji.
• Dopuszcza się doświadczenie zdobyte na rzecz podmiotów publicznych i prywatnych, jeżeli zakres wykonanych prac odpowiada wymaganiom danej funkcji.
6.5. Minimalne wymagania dla funkcji w zespole
6.5.1. Kierownik Techniczny / Architekt Cyberbezpieczeństwa
Wykonawca zapewni co najmniej jedną osobę pełniącą tę funkcję, która spełnia łącznie następujące wymagania:
• co najmniej 5 lat doświadczenia zawodowego w IT, w tym co najmniej 3 lata w cyberbezpieczeństwie, projektowaniu infrastruktury lub architekturze systemów teleinformatycznych;
• udział w co najmniej 2 zakończonych projektach obejmujących budowę, modernizację, migrację lub zabezpieczenie infrastruktury teleinformatycznej;
• w co najmniej jednym z tych projektów udział w integracji co najmniej 3 obszarów spośród: LAN/WAN/WLAN, NGFW/UTM, Active Directory/IAM, MFA/PKI, SIEM, wirtualizacja, backup/DR, storage/NAS, endpoint security, hardening;
• w co najmniej jednym projekcie pełnienie funkcji kierownika technicznego, architekta, głównego inżyniera albo osoby odpowiedzialnej za integrację techniczną;

• doświadczenie w przygotowaniu lub odbiorze dokumentacji technicznej, np. planu wdrożenia, migracji, testów, dokumentacji powdrożeniowej lub planu odtworzeniowego;
• co najmniej jeden certyfikat potwierdzający kompetencje w zakresie cyberbezpieczeństwa, inżynierii bezpieczeństwa lub zarządzania bezpieczeństwem na poziomie co najmniej średniozaawansowanym, np. CySA+, CASP+, CISSP, CISM lub równoważny.
6.5.2. Ekspert ds. Systemu Zarządzania Bezpieczeństwem Informacji – SZBI
Wykonawca zapewni co najmniej jedną osobę pełniącą tę funkcję, która spełnia łącznie następujące wymagania:
• co najmniej 3 lata doświadczenia w zakresie bezpieczeństwa informacji, audytu lub SZBI;
• udział w co najmniej 2 projektach obejmujących opracowanie, wdrożenie lub aktualizację SZBI;
• w co najmniej jednym projekcie odpowiedzialność za opracowanie lub koordynację istotnej części dokumentacji SZBI;
• praktyczne doświadczenie obejmujące co najmniej 4 z obszarów: analiza ryzyka, polityki bezpieczeństwa, zarządzanie dostępem, zarządzanie incydentami, zarządzanie podatnościami lub zmianą, ciągłość działania, ocena zabezpieczeń, zarządzanie dostawcami;
• certyfikat ISO/IEC 27001 Lead Auditor, ISO/IEC 27001 Lead Implementer lub równoważny;
• w odniesieniu do OT/ICS nie wymaga się doświadczenia w programowaniu PLC; wystarczająca jest wiedza pozwalająca uwzględnić zależności IT–OT w SZBI i analizie ryzyka.
6.5.3. Ekspert ds. Ciągłości Działania / BCM / DR
Wykonawca zapewni co najmniej jedną osobę pełniącą tę funkcję, która spełnia łącznie następujące wymagania:
• co najmniej 3 lata doświadczenia w zakresie ciągłości działania, Disaster Recovery, bezpieczeństwa informacji lub zarządzania ryzykiem;
• udział w co najmniej 1 projekcie obejmującym co najmniej 3 z elementów: BIA, BCP, DRP, RTO/RPO, procedury awaryjne, procedury odtworzeniowe;
• udział w co najmniej jednym rzeczywistym albo kontrolowanym teście ciągłości działania lub odtworzenia;
• certyfikat albo ukończone specjalistyczne szkolenie dotyczące ISO 22301, BCM lub rozwiązania równoważnego;
• doświadczenie lub wiedza pozwalająca uwzględnić zależności IT–OT w BIA, BCP i DRP.
6.5.4. Senior Inżynier Sieci i Bezpieczeństwa Sieciowego / NGFW
Wykonawca zapewni co najmniej jedną osobę pełniącą tę funkcję, która spełnia łącznie następujące wymagania:
• co najmniej 4 lata doświadczenia w sieciach komputerowych, w tym co najmniej 2 lata w bezpieczeństwie sieciowym;
• udział w co najmniej 2 produkcyjnych wdrożeniach infrastruktury sieciowej;
• udział w co najmniej jednym wdrożeniu obejmującym NGFW/UTM oraz co najmniej 3 z elementów: VLAN, routing, ACL, VPN, IPS/Threat Prevention, URL Filtering, Application Control, LDAP/AD, RADIUS/MFA, integracja z SIEM;
• praktyczne doświadczenie w segmentacji sieci, politykach firewall i zabezpieczeniach warstwy L2;
• co najmniej jedna techniczna kwalifikacja z zakresu sieci komputerowych albo cyberbezpieczeństwa sieciowego.
6.5.5. Inżynier SIEM / Monitoringu Bezpieczeństwa / Linux
Wykonawca zapewni co najmniej jedną osobę pełniącą tę funkcję, która spełnia łącznie następujące wymagania:
• co najmniej 3 lata doświadczenia w pracy z systemami Linux, systemami bezpieczeństwa lub rozwiązaniami centralnego logowania;
• co najmniej 2 lata doświadczenia w pracy z systemami SIEM;
• udział w co najmniej jednym produkcyjnym wdrożeniu albo istotnej modernizacji systemu SIEM;
• osobiste wykonanie co najmniej 4 czynności spośród: instalacja agentów, integracja źródeł logów, konfiguracja kolektorów, konfiguracja reguł i alertów, konfiguracja dashboardów, FIM, vulnerability detection, SCA/CIS, Active Response, tuning false positives;
• doświadczenie w środowisku obejmującym systemy Windows i Linux. Na etapie warunku udziału nie wymaga się certyfikatu konkretnego producenta SIEM.
6.5.6. Inżynier Wirtualizacji, Backupu, Storage i NAS
Wykonawca zapewni co najmniej jedną osobę pełniącą tę funkcję, która spełnia łącznie następujące wymagania:
• co najmniej 4 lata doświadczenia w zakresie infrastruktury serwerowej, wirtualizacji, backupu lub pamięci masowej;
• udział w co najmniej 2 projektach infrastrukturalnych;
• łączne doświadczenie w co najmniej 3 z obszarów: wirtualizacja, storage/NAS, backup maszyn wirtualnych, replikacja, HA/redundancja, testowe odtworzenie danych lub systemu;
• udział w co najmniej jednym udokumentowanym teście odtworzenia danych, maszyny wirtualnej lub systemu.
6.5.7. Inżynier Microsoft / AD / IAM / PKI / MFA
Wykonawca zapewni co najmniej jedną osobę pełniącą tę funkcję, która spełnia łącznie następujące wymagania:
• co najmniej 4 lata doświadczenia w pracy z Windows Server i Active Directory;
• udział w co najmniej jednym produkcyjnym wdrożeniu albo istotnej modernizacji Active Directory;
• praktyczne doświadczenie w co najmniej 4 z obszarów: AD DS, GPO, DNS, DHCP, LAPS, BitLocker, WSUS, Defender, Credential Guard, WDAC/AppLocker, AD CS/PKI, NPS/RADIUS, PAW, MFA;
• formalne techniczne potwierdzenie kompetencji w zakresie Windows Server, Active Directory, GPO, PKI albo bezpieczeństwa rozwiązań Microsoft lub kwalifikacja równoważna.
6.5.8. Specjalista ds. Bezpieczeństwa OT/ICS
Wykonawca zapewni co najmniej jedną osobę pełniącą tę funkcję, która spełnia łącznie następujące wymagania:
• co najmniej 3 lata doświadczenia w cyberbezpieczeństwie, sieciach przemysłowych, automatyce lub infrastrukturze OT/ICS;
• udział w co najmniej jednym projekcie dotyczącym środowiska OT/ICS, infrastruktury przemysłowej albo infrastruktury krytycznej lub komunalnej;
• doświadczenie w co najmniej 3 z obszarów: segmentacja IT–OT, strefy bezpieczeństwa, firewall/UTM dla OT, bezpieczny

dostęp zdalny, IDS/NDR/MIDS dla OT, inwentaryzacja aktywów OT, hardening urządzeń i systemów OT, kopie zapasowe lub ciągłość działania OT;
• znajomość zasad minimalizacji wpływu działań bezpieczeństwa na dostępność procesów technologicznych.

5.5.) Zamawiający wymaga złożenia oświadczenia, o którym mowa w art.125 ust. 1 ustawy: Tak

5.9.) Zamawiający przewiduje uzupełnienie przedmiotowych środków dowodowych: Nie

SEKCJA VI - WARUNKI ZAMÓWIENIA

6.1.) Zamawiający wymaga albo dopuszcza oferty wariantowe: Nie

6.3.) Zamawiający przewiduje aukcję elektroniczną: Nie

6.4.) Zamawiający wymaga wadium: Nie

6.5.) Zamawiający wymaga zabezpieczenia należytego wykonania umowy: Tak

6.6.) Wymagania dotyczące składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia:
1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku wszyscy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Do oferty należy dołączyć stosowne pełnomocnictwo, podpisane przez osoby upoważnione do składania oświadczeń woli w imieniu każdego ze wspólników. Pełnomocnictwo musi być złożone w oryginale w takiej samej formie, jak składana oferta (tj. w formie elektronicznej (opatrzone kwalifikowanym podpisem elektronicznym) lub postaci elektronicznej opatrzone podpisem zaufanym lub podpisem osobistym). Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie z art. 97 § 2 ustawy z dnia 14 lutego 1991 r. - Prawo o notariacie, które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym mocodawcy.
2. W odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z wykonawców, którzy wykonają dostawy lub usługi, do realizacji których te zdolności są wymagane. W takim przypadku Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do oferty oświadczenie, z którego wynika, które dostawy lub usługi wykonają poszczególni wykonawcy (wzór stanowi załącznik nr 11 do SWZ).
3. Oświadczenia i dokumenty dotyczące podstaw wykluczenia wskazanych w dziale 7 SWZ składa każdy z Wykonawców wspólnie ubiegających się o zamówienie, zgodnie z zasadami i na etapach określonych w dziale 8 SWZ. Oświadczenia potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

6.7.) Zamawiający przewiduje unieważnienie postępowania, jeśli środki publiczne, które zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia nie zostały przyznane: Tak

SEKCJA VII - PROJEKTOWANE POSTANOWIENIA UMOWY

7.1.) Zamawiający przewiduje udzielenia zaliczek: Nie

7.3.) Zamawiający przewiduje zmiany umowy: Tak

7.4.) Rodzaj i zakres zmian umowy oraz warunki ich wprowadzenia:
1. Dopuszcza się zmianę Umowy w zakresie i na warunkach określonych poniżej, zgodnie z art. 455 ust. 1 pkt 1 Pzp, o ile zmiana nie modyfikuje ogólnego charakteru Umowy. Pozostałe zmiany mogą nastąpić wyłącznie w granicach innych przesłanek art. 455 Pzp, po ich udokumentowaniu.
2. W razie udokumentowanego zakończenia produkcji, wycofania ze sprzedaży lub trwałej niedostępności oferowanego modelu dopuszcza się zastąpienie go modelem o parametrach, funkcjonalności, gwarancji i interoperacyjności nie gorszych od wymaganych i oferowanych, bez zwiększenia wynagrodzenia i bez zmiany zakresu funkcjonalnego; Wykonawca przedstawia dokumenty porównawcze do pisemnej akceptacji Zamawiającego.
3. Zmiana wersji oprogramowania, modelu licencjonowania lub sposobu świadczenia usługi chmurowej jest dopuszczalna, jeżeli jest obiektywnie uzasadniona zmianą oferty producenta albo rozwiązaniem problemu technicznego, zapewnia co najmniej niezmienione funkcje, bezpieczeństwo, okres licencji i dostępność danych, nie zwiększa kosztów Zamawiającego i zostanie wykazana analizą porównawczą.
4. Termin lub harmonogram może zostać zmieniony wyłącznie w zakresie i o czas bezpośrednio wynikający z udokumentowanej przeszkody niezależnej od Wykonawcy (siła wyższa, decyzja właściwego organu, zmiana wiążących warunków finansowania), pod warunkiem niezwłocznego zawiadomienia Zamawiającego i wykazania wpływu na ścieżkę krytyczną. Sama trudność z pozyskaniem sprzętu nie uprawnia automatycznie do zmiany. Zmiana nie może naruszać terminu kwalifikowalności wydatków ani warunków projektu.
5. Zmiana przepisów prawa lub obowiązkowych wymagań cyberbezpieczeństwa dopuszcza niezbędną zmianę sposobu realizacji, o ile zakres ogranicza się do dostosowania do nowych wymogów, nie obniża bezpieczeństwa ani nie zmienia ogólnego charakteru Umowy. Skutki finansowe wymagają odrębnej podstawy prawnej wynikającej z art. 455 Pzp.
6. Zmiana personelu kluczowego jest dopuszczalna po wykazaniu, że osoba zastępująca spełnia warunki nie niższe od

postawionych pierwotnie, w tym wymagania związane z kryteriami oceny ofert, jeśli dotyczy; wymaga uprzedniej pisemnej akceptacji Zamawiającego.
7. W razie ustawowej zmiany stawki VAT zmienia się kwota podatku i wynagrodzenie brutto dla części świadczenia objętej nową stawką, przy zachowaniu wynagrodzenia netto, chyba że bezwzględnie obowiązujące przepisy wymagają innego rozliczenia. Każda zmiana wymaga przedłożenia uzasadnienia i dokumentów potwierdzających przesłanki oraz aneksu w formie wymaganej dla Umowy; żadna ze zmian nie może prowadzić do obejścia przepisów Pzp.

7.5.) Zamawiający uwzględnił aspekty społeczne, środowiskowe, innowacyjne lub etykiety związane z realizacją zamówienia: Nie

SEKCJA VIII – PROCEDURA

8.1.) Termin składania ofert: 2026-11-06 10:00

8.2.) Miejsce składania ofert: Miejscem składania ofert jest Platforma e-zamowienia, dostępna pod adresem https://ezamowienia.gov.pl. Wykonawca składa ofertę za pośrednictwem zakładki "Oferty/wnioski".

8.3.) Termin otwarcia ofert: 2026-11-06 10:15

8.4.) Termin związania ofertą: 30 dni

SEKCJA IX – POZOSTAŁE INFORMACJE

Ciąg dalszy RODO
8) posiada Pani/Pan:
a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących (w przypadku, gdy skorzystanie z tego prawa wymagałoby po stronie administratora niewspółmiernie dużego wysiłku może zostać Pani/Pan zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu albo sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia);
b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników);
c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia publicznego lub konkursu oraz przypadków, o których mowa w art. 18 ust. 2 RODO (prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
9) nie przysługuje Pani/Panu:
a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO;
10) przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa
Ciąg dalszy udziału w postępowaniu:
6.5.9. Specjalista ds. SOC / MDR / CTI / Incident Response
Wykonawca zapewni co najmniej jedną osobę pełniącą tę funkcję, która spełnia łącznie następujące wymagania:
• co najmniej 3 lata doświadczenia w obszarze SOC, incident response, threat detection, MDR, MIDS lub CTI;
• udział w co najmniej jednej usłudze lub projekcie operacyjnym dotyczącym SOC/MDR/MIDS/CTI albo obsługi incydentów;
• doświadczenie w co najmniej 4 z obszarów: triage alertów, analiza incydentów, threat hunting, IOC/TTP, MITRE ATT&CK, SIEM, EDR/XDR/NDR, CTI, containment/remediation, raporty poincydentowe;
• doświadczenie w pracy z danymi telemetrycznymi pochodzącymi z więcej niż jednej klasy systemu bezpieczeństwa.
6.5.10. Trener / Specjalista ds. Cyberhigieny i Socjotechniki
Wykonawca zapewni co najmniej jedną osobę pełniącą tę funkcję, która spełnia łącznie następujące wymagania:
• co najmniej 2 lata doświadczenia w szkoleniach lub działaniach edukacyjnych z zakresu cyberbezpieczeństwa;
• w okresie ostatnich 3 lat przeprowadzenie co najmniej 3 szkoleń z zakresu cyberbezpieczeństwa lub cyberhigieny;
• w okresie ostatnich 3 lat przeprowadzenie co najmniej 2 kampanii phishingowych albo innych kontrolowanych testów socjotechnicznych;
• co najmniej jeden certyfikat z zakresu cyberbezpieczeństwa, np. Security+, CySA+, CEH, PenTest+, BTL1, ECIH lub równoważny, albo udokumentowane doświadczenie obejmujące co najmniej 5 przeprowadzonych szkoleń i 3 kampanie socjotechniczne.