Kamil Piotr Glazer
Elektronicznie podpisany przez Kamil Piotr Glazer
Data: 2026.11.19 12:35:58 +01'00'

Załącznik nr 2 do zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Projekt pn.: „Podniesienie poziomu cyberbezpieczeństwa w PUK Olszyna”

Krajowy Plan Odbudowy i Zwiększania Odporności (KPO), Inwestycja C3.1.1. „Cyberbezpieczeństwo - CyberPL”, Konkurs Grantowy „Cyberbezpieczne Wodociągi”, nr naboru KPOD.05.10-CW.01-001/25, nr projektu KPOD.05.10-CW.01-001/25/0705

Dotyczy postępowania pn.: **„Wdrożenie systemów bezpieczeństwa IT i OT dla PUK Olszyna: projekt i nadzór, platforma i SIEM, kontrola dostępu i segmentacja, monitoring sieci OT oraz testy bezpieczeństwa”**

1. PRZEDMIOT I KONTEKST

1. Przedmiotem zamówienia są usługi wdrożenia, konfiguracji i utrzymania systemów bezpieczeństwa IT i OT Zamawiającego oraz dostawa sondy sieciowej OT, w podziale na pięć części. Oznaczenia pozycji odpowiadają kategoriom kosztów Zadania 3 „Obszar techniczny IT” i Zadania 4 „Obszar techniczny OT” projektu.
2. Systemy wdrażane są na sprzęcie dostarczanym w odrębnym postępowaniu: serwer wirtualizacji S13, serwer kopii zapasowych S14, macierz S16 (iSCSI), NAS S21, zapora sieciowa S02, 2 przełączniki S27, 3 punkty dostępowe Wi-Fi S34, 2 stacje przesiadkowe S35, 40 kluczy U2F/FIDO2 S29. Sprzęt zostanie przekazany najpóźniej do dnia 18.12.2026 r.; Zamawiający informuje wykonawców o terminach dostaw poszczególnych urządzeń.
3. Wdrażane oprogramowanie ma charakter otwarty (open source): Proxmox VE, Proxmox Backup Server, Wazuh, Suricata, OpenVAS/Greenbone, Zabbix, GLPI, FreeRADIUS oraz usługi katalogowe AD/LDAP. Dopuszcza się rozwiązania równoważne bez opłat licencyjnych dla Zamawiającego. Wykonawcy współpracują ze sobą zgodnie z projektem z Części 1 i harmonogramem uzgodnionym przez Zamawiającego.

2. LIMITY ZAKRESU PRZYJĘTE DO WYCENY

Cena ryczałtowa obejmuje prace w granicach poniższych limitów. Mniejsza liczba elementów nie zmienia wynagrodzenia; elementy ponad limity nie są objęte zamówieniem. Informacje potrzebne do wyceny i wizję lokalną Zamawiający zapewnia na zasadach z pkt 4 zapytania ofertowego; dane operacyjne przekazuje po zawarciu umowy.

Element	Zakres maksymalny	Dotyczy części
Lokalizacje	siedziba Zamawiającego w Olszynie oraz nie więcej niż 6 obiektów infrastruktury wodno-kanalizacyjnej na terenie Gminy Olszyna	2, 3, 4, 5
Konta użytkowników i stanowiska	do 40 kont użytkowników i do 40 stacji roboczych	2, 3
Serwery i urządzenia IT objęte projektem	serwery S13 i S14, macierz S16, NAS S21, zapora S02, 2 przełączniki S27, 3 punkty dostępowe S34, 2 stacje S35 oraz do 5 istniejących serwerów lub maszyn wirtualnych	2, 3, 5
Urządzenia OT	do 20 urządzeń automatyki (sterowniki PLC, panele HMI, serwer lub stacje SCADA, urządzenia komunikacyjne) i do 6 przełączników sieci OT	2, 3, 4, 5
VLAN i strefy	do 16 VLAN w sieci IT i do 6 stref w sieci OT	3, 5

3. WYMAGANIA WSPÓLNE

1) Wykonawca opracowuje dokumentację powykonawczą każdej wdrożonej pozycji (konfiguracja, adresacja, konta techniczne, procedury administracyjne i odtworzeniowe) w języku polskim i przekazuje dane dostępowe odrębnym, zabezpieczonym kanałem.
2) Prace w sieci OT i zmiany wpływające na działanie instalacji technologicznych wykonuje się wyłącznie po uzgodnieniu z Zamawiającym, w obecności jego pracownika, w uzgodnionych oknach serwisowych, po wykonaniu kopii konfiguracji i z planem wycofania zmian; każda zmiana jest wpisywana do rejestru zmian przekazywanego Zamawiającemu. Wykonawca nie zmienia programów sterowników. W sieci OT stosuje się metody pasywne; aktywne skanowanie urządzeń OT dopuszcza się wyłącznie za zgodą Zamawiającego, w oknie serwisowym. Dostęp zdalny wyłącznie przez bastion lub rozwiązanie wskazane przez Zamawiającego.
3) Wykonawca stosuje zasady SZBI Zamawiającego, zachowuje poufność informacji o infrastrukturze, korzysta z kont imiennych i dostępu zdalnego wyłącznie przez rozwiązania wskazane przez Zamawiającego.
4) Konfiguracja zgodna z projektem z Części 1; rozbieżności z projektem Wykonawca zgłasza Zamawiającemu i wykonawcy Części 1 przed ich wprowadzeniem.
5) Odbiór każdej pozycji następuje protokołem po przekazaniu dokumentacji i wykonaniu testów potwierdzających działanie; dopuszcza się odbiory częściowe zakończonych pozycji. Zamawiający przeprowadza odbiór w terminie do 2 dni roboczych od zgłoszenia, a odbiór końcowy najpóźniej 23.12.2026 r.; czas odbioru nie wlicza się do terminu wykonania. Wdrożenia objęte testami bezpieczeństwa (Część 5) zgłasza się do odbioru w terminie 3 dni roboczych od przekazania sprzętu, nie później niż do dnia 21.12.2026 r.
6) Prace niewymagające sprzętu dostarczanego w odrębnym postępowaniu Wykonawca rozpoczyna niezwłocznie po zawarciu umowy. Przed dostawą sprzętu Wykonawca przygotowuje konfiguracje, obrazy i maszyny wirtualne tak, aby wdrożenie na dostarczonym sprzęcie zakończyć w terminie 3 dni roboczych od jego przekazania.

4. CZĘŚĆ 1 - PROJEKT ROZWIĄZANIA I NADZÓR NAD WDROŻENIEM

Kody CPV: 71241000-9 Studium wykonalności, usługi doradcze, analizy; 72224000-1 Usługi doradcze w zakresie zarządzania projektem.

4.1. U18 (Zadanie 3) - Zaprojektowanie architektury systemów bezpieczeństwa IT/OT

a) analiza stanu infrastruktury IT i OT oraz wymagań SZBI Zamawiającego, z wykorzystaniem wyników audytu wstępnego,
b) projekt architektury bezpieczeństwa: rozmieszczenie maszyn wirtualnych na platformie Proxmox VE, integracja SIEM, IDS, skanera podatności, monitoringu i kopii zapasowych (model 3-2-1), plan adresacji, VLAN i stref, zasady segmentacji IT/OT, kontrola dostępu 802.1X, VPN i MFA,
c) harmonogram wdrożeń uzgodniony z wykonawcami pozostałych części i Zamawiającym,
d) dokumentacja projektowa przekazana Zamawiającemu i wykonawcom pozostałych części w ciągu 5 dni od zawarcia umowy, z aktualizacją po uwagach Zamawiającego.

4.2. U19 (Zadanie 3) - Nadzór nad realizacją wdrożeń i odbiory techniczne

a) nadzór nad realizacją wdrożeń w Częściach 2-4 pod kątem zgodności z projektem, w tym udział w kluczowych etapach i odbiorach,
b) weryfikacja dokumentacji powykonawczej i protokołów testów przekazywanych przez wykonawców,
c) udział w odbiorach technicznych i rekomendacja ich przyjęcia lub odmowy,
d) raport końcowy z nadzoru.

5. CZĘŚĆ 2 - PLATFORMA WIRTUALIZACJI, SIEM, SKANER PODATNOŚCI, MONITORING I INWENTARYZACJA

Kody CPV: 72222300-0 Usługi w zakresie technologii informatycznych; 72253200-5 Usługi w zakresie wsparcia systemu; 72267000-4 Usługi w zakresie konserwacji i naprawy oprogramowania.

5.1. U09 (Zadanie 3) - Wdrożenie platformy Proxmox VE i systemu kopii zapasowych Proxmox Backup Server

a) instalacja i konfiguracja Proxmox VE na serwerze S13 (pamięć lokalna, podłączenie macierzy S16 przez iSCSI, sieci i VLAN zgodnie z projektem),

b) konfiguracja Proxmox Backup Server na serwerze S14: zadania kopii maszyn wirtualnych, retencja, weryfikacja, szyfrowanie kopii,

c) uruchomienie drugiej kopii na NAS S21 (synchronizacja lub replikacja) z migawkami chronionymi przed usunięciem,

d) test odtworzenia co najmniej jednej maszyny wirtualnej z obu miejsc przechowywania kopii, z protokołem.

5.2. U09 (Zadanie 3) - Wdrożenie systemu SIEM Wazuh z sondą IDS Suricata i utrzymanie do końca okresu realizacji

a) instalacja systemu Wazuh na platformie Proxmox VE, agenty na serwerach, maszynach wirtualnych i stacjach S35 oraz na stacjach roboczych w granicach limitu,

b) integracja logów z katalogu AD/LDAP, serwerów, zapory S02, przełączników, punktów dostępowych, macierzy i NAS oraz z sondy IDS Suricata uruchomionej na portach lustrzanych przełączników,

c) konfiguracja reguł korelacji, powiadomień, retencji logów i pulpitów,

d) utrzymanie od uruchomienia do dnia zakończenia umowy: analiza alertów, strojenie reguł, aktualizacje, raport końcowy z obsługi,

e) przekazanie instrukcji administratora i przeszkolenie administratorów Zamawiającego (do 4 godzin).

5.3. U09 (Zadanie 3) - Wsparcie w obsłudze incydentów bezpieczeństwa w okresie utrzymania systemu SIEM

a) w okresie utrzymania systemu SIEM, od jego uruchomienia do dnia zakończenia umowy: analiza logów i alertów, wstępna ocena i klasyfikacja zdarzeń bezpieczeństwa,

b) wsparcie Zamawiającego w obsłudze incydentu, w tym w ograniczaniu jego skutków i zabezpieczeniu śladów, zgodnie z procedurą zarządzania incydentami SZBI Zamawiającego, zdalnie lub na miejscu,

c) rekomendacje działań naprawczych po każdym obsłużonym incydencie oraz zestawienie obsłużonych zdarzeń w raporcie końcowym; łączny wymiar wsparcia do 40 godzin w okresie świadczenia usługi.

5.4. U09 (Zadanie 3) - Wdrożenie skanera podatności OpenVAS/Greenbone

a) instalacja OpenVAS/Greenbone na platformie Proxmox VE,

b) konfiguracja zakresów skanowania, harmonogramów i raportów, integracja wyników z systemem SIEM,

c) wykonanie pierwszego pełnego skanu i przekazanie raportu.

5.5. U09 (Zadanie 3) - Wdrożenie systemu monitoringu Zabbix (IT)

a) instalacja Zabbix na platformie Proxmox VE i monitorowanie serwerów, urządzeń sieciowych, macierzy, NAS i usług,

b) konfiguracja progów, powiadomień i integracji alertów z systemem SIEM.

5.6. U09 (Zadanie 4) - Integracja systemu Zabbix z infrastrukturą OT

a) monitorowanie dostępności urządzeń sieci OT i parametrów środowiskowych dostępnych przez SNMP lub równoważne mechanizmy, bez ingerencji w programy sterowników,

b) przekazywanie alertów do systemu SIEM.

5.7. U09 (Zadanie 3) - Wdrożenie systemu GLPI (CMDB)

a) instalacja GLPI na platformie Proxmox VE, konfiguracja kategorii aktywów, właścicieli, lokalizacji i podstawowego procesu zarządzania zmianą,

b) automatyczne zbieranie danych o stacjach i serwerach (agent) w granicach limitu.

5.8. U33 (Zadanie 3) - Inwentaryzacja aktywów IT

a) inwentaryzacja sprzętu, oprogramowania i licencji IT w granicach limitu, z wprowadzeniem do GLPI,

b) rejestr aktywów zgodny z wymaganiami SZBI Zamawiającego.

5.9. U33 (Zadanie 4) - Inwentaryzacja aktywów OT

a) inwentaryzacja urządzeń OT (typ, model, wersja oprogramowania, lokalizacja, połączenia) w granicach limitu, z wprowadzeniem do GLPI,

b) dokumentacja schematów połączeń sieci OT.

6. CZĘŚĆ 3 - TOŻSAMOŚĆ I KONTROLA DOSTĘPU, SEGMENTACJA SIECI, BASTION OT I HARDENING

Kody CPV: 72222300-0 Usługi w zakresie technologii informatycznych; 72700000-7 Usługi w zakresie sieci komputerowych; 72611000-6 Usługi w zakresie wsparcia technicznego.

6.1. U09 (Zadanie 3) - Wdrożenie katalogu AD/LDAP z integracją 802.1X, VPN i kluczy U2F

a) wdrożenie katalogu AD/LDAP na platformie Proxmox VE (usługi katalogowe w oprogramowaniu otwartym lub licencjonowanym przez Zamawiającego), konta, grupy, polityki haseł i blokad,

b) integracja z FreeRADIUS, VPN zapory S02 oraz uwierzytelnianiem kluczami U2F/FIDO2 dla kont uprzywilejowanych,

c) rejestracja 40 kluczy S29 dla użytkowników wskazanych przez Zamawiającego.

6.2. U09 (Zadanie 3) - Wdrożenie FreeRADIUS i uwierzytelniania 802.1X dla LAN i Wi-Fi (IT)

a) wdrożenie FreeRADIUS na platformie Proxmox VE z integracją AD/LDAP,

b) uwierzytelnianie 802.1X na przełącznikach S27 (z MAB dla urządzeń bez 802.1X) i w sieci Wi-Fi S34 (WPA3-Enterprise), przypisanie VLAN, przełączenie portów w tryb wymuszający.

6.3. U09 (Zadanie 4) - FreeRADIUS i 802.1X dla VLAN-ów OT

a) konfiguracja uwierzytelniania 802.1X lub MAB dla VLAN-ów OT na przełącznikach sieci OT obsługujących tę funkcję, w uzgodnieniu z Zamawiającym, bez przerw w pracy instalacji.

6.4. U41 (Zadanie 3) - Projekt i wdrożenie segmentacji sieci IT (VLAN, ACL, 802.1X, polityki zapory)

a) projekt wykonawczy i wdrożenie VLAN, list ACL i stref zapory S02 zgodnie z projektem z Części 1,

b) konfiguracja zapory S02: polityki ruchu, IPS, filtrowanie, VPN z MFA, wysyłanie logów do SIEM, przełączenie ruchu produkcyjnego na zaporę w uzgodnionym oknie serwisowym,

c) testy poprawności segmentacji i dokumentacja powykonawcza.

6.5. U41 (Zadanie 4) - Projekt i wdrożenie segmentacji granicy IT/OT

a) projekt i wdrożenie segmentacji granicy IT/OT: strefy, listy dozwolonej komunikacji między konkretnymi urządzeniami, reguły ACL i zapory,

b) wdrożenie w uzgodnionych oknach serwisowych, z planem wycofania zmian, bez przerw w procesach technologicznych.

6.6. U41 (Zadanie 4) - Wdrożenie bastionu serwisowego OT na stacji S35 z nagrywaniem sesji

a) konfiguracja stacji S35 jako bastionu serwisowego OT: dostęp zdalny dla serwisantów przez VPN z MFA, kontrola uprawnień, nagrywanie sesji z przekazywaniem logów do SIEM,

b) procedura udzielania i odbierania dostępu serwisowego.

6.7. U39 (Zadanie 3) - Hardening i konfiguracja bezpieczeństwa 12 systemów i urządzeń IT

a) hardening 12 systemów i urządzeń: serwery S13 i S14, macierz S16, NAS S21, 2 przełączniki S27, 2 stacje S35, zapora S02, katalog AD/LDAP, host Proxmox VE (11 elementów wymienionych we wniosku) oraz jeden wdrażany system bezpieczeństwa (maszyna wirtualna) wskazany przez Zamawiającego w harmonogramie,

b) zakres: zabezpieczenie usług administracyjnych, polityki haseł i MFA, zasady grup, ograniczenie powierzchni ataku, szyfrowanie i retencja logów, kontrola integralności, weryfikacja konfiguracji według CIS Benchmarks lub równoważnych,

c) raport z konfiguracji przed i po hardeningu.

6.8. U39 (Zadanie 4) - Hardening infrastruktury OT

a) hardening infrastruktury OT w granicach limitu: białe listy protokołów, zarządzanie kontami serwisowymi, zmiana haseł domyślnych, wyłączenie zbędnych usług i wzmocnienie konfiguracji urządzeń sterujących, tam gdzie jest to technicznie możliwe bez wpływu na proces,

b) każda zmiana uzgadniana z Zamawiającym i jego serwisem automatyki, z planem wycofania.

7. CZĘŚĆ 4 - MONITORING BEZPIECZEŃSTWA SIECI OT: SONDA, INTEGRACJA Z SIEM I USŁUGA MIDS

Kody CPV: 32424000-1 Infrastruktura sieciowa; 72222300-0 Usługi w zakresie technologii informatycznych; 79711000-1 Usługi monitorowania alarmów.

7.1. OT3 (Zadanie 4) - Sonda sieciowa OT do pasywnej analizy ruchu przemysłowego

a) dostawa, montaż i uruchomienie sondy sieciowej OT do pasywnej analizy ruchu przemysłowego (co najmniej Modbus TCP oraz inne protokoły przemysłowe stosowane w sieci Zamawiającego, w tym IEC 60870-5-104 i DNP3, jeżeli występują; informację o stosowanych protokołach Zamawiający udostępnia na zasadach z pkt 4 zapytania ofertowego), z identyfikacją urządzeń, mapą komunikacji i wykrywaniem anomalii; dostawa i uruchomienie w terminie do 10 dni od zawarcia umowy,

b) sonda pracuje wyłącznie pasywnie (port lustrzany lub tap), bez wpływu na ruch; licencje i subskrypcje na okres co najmniej do 31.12.2026 r.; gwarancja na sprzęt min. 24 miesiące,

c) Wykonawca wskaże okres obowiązywania licencji i subskrypcji oraz funkcje urządzenia, których działanie zależy od ich aktywności; dokumentacja musi jednoznacznie określać funkcjonalności pozostające dostępne po wygaśnięciu subskrypcji oraz zasady i koszty jej ewentualnego odnowienia.

7.2. U09 (Zadanie 4) - Integracja sondy OT z systemem SIEM Wazuh

a) integracja sondy OT z systemem SIEM Wazuh: przekazywanie alarmów i zdarzeń, reguły korelacji IT/OT, powiadomienia.

7.3. U36 (Zadanie 4) - Usługa MIDS dla sieci OT do końca okresu realizacji

a) usługa MIDS obejmuje całodobowy monitoring zdarzeń bezpieczeństwa infrastruktury OT (24 godziny na dobę, 7 dni w tygodniu) przez zespół SOC, analizę alarmów, identyfikację potencjalnych incydentów oraz ich eskalację do wskazanych przedstawicieli Zamawiającego; monitoring jest świadczony od dnia uruchomienia i odbioru sondy OT do zakończenia okresu świadczenia usługi określonego w umowie,

b) aktualizacja reguł detekcji w okresie świadczenia usługi oraz rekomendacje działań naprawczych dla każdego eskalowanego incydentu,

c) raport bezpieczeństwa za okres świadczenia usługi, przekazany przy odbiorze końcowym, wraz z zestawieniem zgłoszonych alarmów i eskalacji.

8. CZĘŚĆ 5 - TESTY BEZPIECZEŃSTWA INFRASTRUKTURY SIECIOWEJ IT I OT

Kody CPV: 72810000-1 Usługi audytu komputerowego; 79212000-3 Usługi audytu.

8.1. U02 (Zadanie 3) - Testy bezpieczeństwa infrastruktury sieciowej IT

a) testy bezpieczeństwa sieci IT po zakończeniu wdrożeń: skanowanie, testy penetracyjne z sieci wewnętrznej i z Internetu, weryfikacja konfiguracji zapory, przełączników, Wi-Fi i 802.1X oraz segmentacji, w tym przegląd konfiguracji urządzeń sieciowych względem zaleceń producentów i uznanych wytycznych konfiguracyjnych,

b) raport z wynikami, oceną ryzyka i rekomendacjami oraz retest poprawek przekazanych do 3 dni przed terminem końcowym.

8.2. U02 (Zadanie 3) - Testy bezpieczeństwa serwisów internetowych Zamawiającego według OWASP Top 10

a) testy bezpieczeństwa serwisów internetowych Zamawiającego udostępnianych w Internecie (strona internetowa i inne serwisy wskazane przez Zamawiającego, nie więcej niż 2), prowadzone przez testera według OWASP Top 10, w zakresie funkcji udostępnianych przez serwis: uwierzytelnianie i autoryzacja, zarządzanie sesją, walidacja danych wejściowych, logika działania aplikacji i konfiguracja serwera,

b) testy wykonywane bez wpływu na dostępność serwisów, po zawarciu umowy, w terminie uzgodnionym z Zamawiającym i podmiotem utrzymującym serwis,

c) raport techniczny z wynikami, oceną ryzyka i rekomendacjami działań korygujących oraz ponowny test poprawek przekazanych do 3 dni przed terminem końcowym.

8.3. U02 (Zadanie 4) - Testy bezpieczeństwa systemów OT

a) testy bezpieczeństwa systemów OT metodami nieinwazyjnymi lub w uzgodnionych oknach serwisowych: analiza protokołów i ruchu przemysłowego, weryfikacja segmentacji IT/OT i dostępu serwisowego,

b) raport podatności z rekomendacjami.