Załącznik nr 1 do Zapytania ofertowego

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Sprzętowe sondy/sensory do monitorowania sieci OT
(dedykowane urządzenia do analizy protokołów przemysłowych)

---

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa sprzętowych sond/sensorów do monitorowania i ochrony sieci OT – dedykowanych urządzeń klasy przemysłowej do analizy protokołów przemysłowych – wraz z ich wdrożeniem, zgodnie z wymaganiami określonymi w niniejszym Opisie Przedmiotu Zamówienia (dalej: OPZ).

Lp.	Elementy zamówienia	Ilość
1	Sprzętowa sonda/sensor bezpieczeństwa sieci OT spełniająca wymagania rozdz. 2–4 OPZ	3 szt.
2	Wdrożenie dostarczonych urządzeń zgodnie z rozdz. 5 OPZ	1 usługa

2. Wymagania dotyczące rozwiązania

2.1. Przeznaczenie i kontekst regulacyjny

- Oferowane urządzenie stanowi kluczowy element ochrony sieci OT, przeznaczony do pracy w środowisku infrastruktury krytycznej, w szczególności w systemach sterowania procesami technologicznymi (ICS/SCADA).
- Urządzenie musi wspierać realizację obowiązków Zamawiającego wynikających z:
  - nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (UKSC),
  - dyrektywy NIS2,
  - norm IEC 62443,
- w zakresie:
  - ciągłego monitorowania sieci OT,
  - wykrywania anomalii i zagrożeń,
  - odporności na zaawansowane, ukierunkowane ataki (APT),
  - zapewnienia ciągłości i bezpieczeństwa procesów technologicznych

2.2. Charakter rozwiązania

- Zamawiający wymaga sprzętowej, zintegrowanej platformy komunikacyjnej i diagnostycznej, która w jednym urządzeniu realizuje łącznie funkcje:
  - aktywnej ochrony sieci OT,
  - analizy i korelacji ruchu przemysłowego,
  - detekcji i prewencji zagrożeń.
- Nie dopuszcza się:
  - wyłącznie pasywnych sond monitorujących,
  - rozwiązań wymagających stałego mirrorowania ruchu do zewnętrznych systemów,
  - rozwiązań, w których funkcje bezpieczeństwa realizowane są poza oferowanym urządzeniem,
  - wielofunkcyjnych urządzeń aktywnych, które w jednej fizycznej obudowie łączą realizację zadań infrastrukturalnych (routing L3, przełączanie sieciowe L2/L3, brzegowa zapora sieciowa z translacją adresów NAT lub koncentrator VPN) z funkcjami głębokiej inspekcji pakietów (IPS/IDS); wyłączenie to nie dotyczy wymaganych niniejszym OPZ funkcji filtrowania i blokowania ruchu (firewall/IPS) realizowanych przez oferowane urządzenie w trybie przezroczystym (bez adresacji MAC/IP na interfejsach monitorujących), wraz ze sprzętowym bypassem,
  - rozwiązań typu Edge Computing wyposażonych w system operacyjny oraz pamięć masową (storage), przystosowanych do pracy jako OT Security Gateway.
- Urządzenie musi być zdolne do pracy zarówno w trybie pasywnym, jak i inline, w zależności od wymagań danego segmentu OT.
  - Interfejsy monitorujące urządzenia nie mogą posiadać adresu MAC ani adresu IP, a ich włączenie w linię (np. bezpośrednio za sterownikiem PLC) nie może wymagać jakichkolwiek zmian w adresacji i konfiguracji chronionego zasobu.

2.3. Platforma sprzętowa i instalacja

- Urządzenie sprzętowe klasy przemysłowej, przystosowane do pracy ciągłej 24/7.
- Montaż na szynie DIN 35 mm (TS35) w szafie.
- Redundantne zasilanie.
- Zasoby sprzętowe umożliwiające jednoczesną realizację:
  - analizy DPI,
  - IDS/IPS,
  - analityki behawioralnej,
  - korelacji zdarzeń.

2.4. Funkcje bezpieczeństwa

- Urządzenie musi zapewniać aktywne mechanizmy bezpieczeństwa OT, w tym:
  - Detekcja i prewencja – IDS/IPS dla sieci OT
    - analiza ruchu w czasie rzeczywistym,
    - możliwość dynamicznego blokowania zagrożeń,

- niski narzut na opóźnienia – poniżej 550 µs dla ruchu mieszanego (low-latency design).

– Ochrona przed:
  - atakami DoS/DDoS,
  - nieautoryzowanym użyciem komendy zapisu w urządzeniach sterujących z wykorzystaniem protokołów przemysłowych,
  - nieautoryzowaną komunikacją między segmentami OT.

– Anomaly Detection i behavioral monitoring – detekcja anomalii komunikacyjnych w sieciach przemysłowych.

2.5. Analiza protokołów przemysłowych

- Urządzenie musi realizować głęboką analizę protokołów przemysłowych (DPI OT), co najmniej dla:
  – Modbus TCP,
  – IEC 60870-5-104,
  – PROFINET,
  – EtherNet/IP,
  – GOOSE,
  – STEP7/S7,
  – DNP3,
  – S7COMM,
  – OPC UA.
- Dla protokołów Modbus, S7COMM oraz DNP3 wymaga się, aby profile DPI realizowały inspekcję głębszą aniżeli tylko rozpoznawanie protokołu:
  – dla protokołu DNP3 wymaga się, aby w ramach profilu DPI można było zdefiniować konkretny kod wiadomości, np. 0x07 Immediate Freeze,
  – dla protokołu Modbus TCP wymaga się, aby w ramach profilu DPI można było zdefiniować konkretne funkcje i rejestry, np. 0x0F Write Multiple Coils.
- Zaawansowana analiza behawioralna i detekcja zagrożeń:
  – analiza sekwencji i relacji w ruchu sieciowym – na podstawie ustalonych wzorców behawioralnych system musi kategoryzować taką sekwencję jako podejrzaną,
  – ze względu na specyfikę środowiska OT wymaga się, aby administracja systemem umożliwiała elastyczne tworzenie listy wyjątków oraz blokad.
- Wymaga się wysoce szczegółowych logów zawierających:
  – nazwę naruszonej reguły, np. WannaCry Kill Switch Domain,
  – adres MAC i IP atakującego oraz ofiary,
  – rodzaj używanego protokołu,
  – mapowanie taktyk i technik na MITRE ATT&CK.
- System musi posiadać wbudowany mechanizm automatycznego uczenia się, który pozwala na analizę bieżącego, prawidłowego ruchu sieciowego w środowisku produkcyjnym i na tej podstawie automatycznie generuje bazowe reguły bezpieczeństwa.

  - podczas procesu budowania wzorca prawidłowego ruchu system musi weryfikować analizowane pakiety pod kątem zagrożeń; system musi pozwalać na powiązanie zadania uczącego z wybranym profilem IPS oraz trybem działania, aby od razu odfiltrować i zablokować potencjalne cyberzagrożenia z generowanej listy zaufanej,
  - wynikiem pracy zadania uczącego musi być:
    - zaproponowanie reguł dla komunikacji na poziomie MAC,
    - zaproponowanie reguł dla komunikacji na poziomie IP i protokołów L7,
    - wygenerowanie dedykowanych profili filtrowania protokołów przemysłowych (głęboka inspekcja pakietów),
  - przed ostatecznym wdrożeniem reguł do środowiska system musi udostępnić interfejs do ich przeglądu, pozwalający na:
    - weryfikację wygenerowanych reguł,
    - przegląd szczegółowych statystyk,
    - decyzyjność administratora w postaci zachowania lub odrzucenia poszczególnych reguł.
- Analiza musi obejmować:
  - rozpoznawanie poleceń i funkcji protokołów,
  - analizę zmiennych procesowych,
  - identyfikację nieautoryzowanych operacji sterujących,
  - diagnostykę komunikacji OT.

2.6. Tryby pracy i ciągłość działania

- Urządzenie musi umożliwiać dwa tryby pracy:
  - tryb pasywny – bez ingerencji w ruch procesowy,
  - tryb inline – z aktywną ochroną i blokowaniem zagrożeń.
- Dla trybu inline wymagane są mechanizmy minimalizujące ryzyko zakłócenia pracy systemów OT (fail-safe, bypass lub równoważne).

2.7. Monitoring, traceability i integracja

- Urządzenie musi zapewniać:
  - pełną traceability zdarzeń i parametrów komunikacji,
  - rejestrowanie i eksport logów bezpieczeństwa,
  - integrację z systemami klasy SIEM, SOC oraz MDR,
  - normalizację danych i możliwość mapowania zdarzeń do MITRE ATT&CK (ICS).

2.8. Zarządzanie i automatyzacja

- Zarządzanie lokalne i zdalne
  - CLI/API,
  - intuicyjny interfejs WebGUI do lokalnego zarządzania przez służby utrzymania.

- Możliwość integracji z centralną platformą zarządzania bezpieczeństwem.
- Obsługa polityk bezpieczeństwa i reguł reagowania lokalnie z poziomu WebGUI i centralnie z poziomu konsoli zarządzającej.
- Możliwość aktualizacji reguł detekcji i mechanizmów analitycznych.

2.9. Zgodność normatywna i odporność

- Oferowane urządzenie musi być przeznaczone do pracy w środowiskach OT i spełniać wymagania wynikające z nowelizacji UKSC / dyrektywy NIS2.
- Rozwiązania oparte wyłącznie na pasywnym monitoringu, bez możliwości aktywnej ochrony, nie spełniają założeń projektu.

2.10. Praca w trybie inline – egzekwowanie bezpieczeństwa

- Oferowane urządzenie musi umożliwiać pracę w trybie inline, tj. jako aktywny element toru komunikacyjnego sieci OT, z bezpośrednią możliwością blokowania ruchu sieciowego w czasie rzeczywistym, zgodnie z politykami bezpieczeństwa.
- Funkcja blokowania ruchu w trybie inline musi być realizowana bezpośrednio na oferowanym urządzeniu, bez konieczności:
  - przekazywania decyzji do zewnętrznych systemów (np. SOAR),
  - stosowania dodatkowych firewalli lub urządzeń pośredniczących,
  - rekonfiguracji topologii sieci w momencie detekcji incydentu.

2.11. Bezpieczeństwo procesu i ciągłość działania

- Praca w trybie inline musi być zaprojektowana zgodnie z zasadami bezpieczeństwa procesowego OT, w tym:
  - fail-safe / fail-open lub bypass w przypadku awarii urządzenia,
  - brak pojedynczego punktu awarii (SPOF),
  - minimalny i deterministyczny wpływ na opóźnienia transmisji – poniżej 550 µs,
  - dostarczenie minimum 1 pary portów RJ-45 działających w trybie bypass, które przepuszczą ruch nawet po pełnej utracie zasilania urządzenia.
- Zamawiający nie dopuszcza rozwiązań, w których funkcja blokowania ruchu realizowana jest:
  - wyłącznie poprzez pasywną sondę i zewnętrzny firewall,
  - poprzez systemy SOAR/MDR działające poza oferowanym urządzeniem,
  - poprzez reakcję opóźnioną (out-of-band),
  - poprzez zestaw kilku odrębnych urządzeń zamiast jednej, zintegrowanej platformy.

2.12. Jednoczesna praca aktywna i analityczna – rola urządzenia w topologii sieci OT

- Oferowane urządzenie musi być przeznaczone do pracy jako niezależna platforma analityczna monitorująca ruch sieciowy, bez ograniczeń funkcjonalnych wynikających z wyboru trybu pracy. Ze

względu na procedury ciągłości działania funkcje przełączania oraz routingu powinny być realizowane przez osobne, dedykowane urządzenie (przełącznik L2/L3) wyposażone w układy ASIC oraz TCAM.

- Analiza ruchu musi być możliwa zarówno:
  - dla ruchu przechodzącego przez urządzenie (inline),
  - jak i dla ruchu kopiowanego (SPAN/mirror/TAP) z innych elementów sieci.
- Funkcje analizy ruchu oraz egzekwowania polityk bezpieczeństwa muszą być realizowane przez jedno, spójne urządzenie sprzętowe, bez rozdzielania ich pomiędzy osobne sondy, sensory lub appliance'y.
- Zamawiający nie dopuszcza rozwiązań, w których:
  - urządzenie analityczne pełni aktywną rolę w topologii sieci, tj. pełni jednocześnie funkcję przełącznika sieciowego,
  - urządzenia wyposażone są w interfejsy rozszerzeń umożliwiające instalację modemu komórkowego oraz zewnętrznej przestrzeni dyskowej.

2.13. Uwagi dodatkowe

- Zamawiający oczekuje sprzętowej platformy OT Security, łączącej funkcje diagnostyczne i ochronne, przeznaczonej do realnej ochrony procesów technologicznych.
- Rozwiązania będące:
  - jedynie pasywną sondą,
  - platformą Edge Computing z dostosowaną nakładką na system operacyjny,
  - narzędziem IT przeniesionym do OT,
- nie będą uznane za równoważne.

1. Wymagania sprzętowe w zakresie każdej z 3 sond objętych przedmiotem zamówienia

Parametr	Wymaganie minimalne
Porty monitorujące / filtrujące	Minimum 2 × 1 Gb/s, z czego minimum 2 porty pracujące w trybie bypass. W przypadku urządzeń z większą liczbą portów wszystkie interfejsy monitorujące/filtrujące muszą mieć możliwość pracy w trybie bypass.
Port zarządzania	Dedykowany port zarządzania OOB (MGT) – 1 × RJ-45 GE

Parametr	Wymaganie minimalne
Przepustowość filtrowania ruchu	Przepustowość funkcji firewall/IPS w trybie przezroczystym: minimum 840 Mb/s (IMIX) / minimum 1,2 Gb/s (UDP, ramka 1518 B)
Jednoczesne połączenia TCP	Minimum 30 000
Opóźnienie (latency)	Poniżej 550 µs dla ruchu mieszanego
Niezawodność (MTBF)	Minimum 670 000 h (przy 25 °C)
Zasilanie	Redundantne
Montaż	Szyna DIN 35 mm (TS35)

4. Wymagania certyfikacyjne

Wymagane jest posiadanie przez oferowane urządzenie lub jego producenta następujących certyfikatów / deklaracji zgodności:

1. CE,
2. FCC Class A,
3. UL, UL 60950-1,
4. IEC 62443-4-1 – certyfikat zgodności producenta rozwiązania wydany przez niezależną jednostkę certyfikującą,
5. kompatybilność elektromagnetyczna:
   a) EMI: CISPR 32, FCC Part 15B Klasa A,
   b) EMC: EN 55032/35, VCCI Klasa B,
6. odporność na wibracje: IEC 60068-2-6.

5. Wdrożenie

1. Zakres prac wdrożeniowych: (montaż, konfiguracja trybów pracy, uruchomienie zadania uczącego, integracja z centralną konsolą i SIEM, testy akceptacyjne).
2. W terminie do 7 dni od zakończenia wdrożenia Wykonawca przekaże Zamawiającemu dokumentację powykonawczą.

6. Wymagania ogólne

Jeżeli w opisie przedmiotu zamówienia OPZ Zamawiający odnosi się do norm, europejskich Ocen technicznych, specyfikacji technicznych oraz innych systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp, to jest obowiązany wskazać, że dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy lub „równoważne".

Wymienione w jakiejkolwiek części OPZ w zakresie dostaw urządzeń wraz z oprogramowaniem: nazwy własne, marki wyrobów, materiałów, technologii nie są obligatoryjne dla wykonawców. Wykonawca ma prawo do zaoferowania innych wyrobów, materiałów, technologii pod warunkiem zapewnienia parametrów technicznych co najmniej identycznych z parametrami określonymi w dokumentacji zamówienia (dopuszcza się dostawę przedmiotu zamówienia o wyższych parametrach technicznych).

Jeżeli OPZ wskazywałby w odniesieniu do niektórych materiałów, wyrobów i technologii znaki towarowe, patenty lub pochodzenie, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, w tym w szczególności podane zostały - nazwa własna materiału, wyrobu czy technologii, numer katalogowy lub producent, należy to traktować jako rozwiązanie przykładowe, określające standardy, wygląd oraz wymagania techniczne. Wszelkie materiały, urządzenia i technologie, pochodzące od konkretnych producentów, określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać materiały, urządzenia i technologie, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia, nie mają na celu uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów. Tak zastosowane zapisy są tylko w sytuacjach, gdy zamawiający nie był w stanie opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń - w tych wypadkach należy zawsze przyjąć sformułowanie - " lub równoważny"

Zastosowane przez Wykonawcę materiały, wyroby i rozwiązania równoważne, muszą być co najmniej:

- o tej samej wytrzymałości i trwałości, o tym samym poziomie estetyki (wyroby),
- o parametrach technicznych opisanych w dokumentacji przetargowej,
- kompatybilne z istniejącą i projektowaną infrastrukturą,
- spełniać: te same funkcje, wymagania bezpieczeństwa konstrukcji, bhp i p. poż,
- posiadać stosowne dokumenty dopuszczające do stosowania w budownictwie (atesty i aprobaty techniczne).

Wykonawca musi udowodnić Zamawiającemu, że proponowany materiał, wyrób, technologia lub rozwiązanie jest równoważne, przedstawiając np. wszelkie dokumenty, obliczenia, opinie etc. potwierdzające równoważność.

Dostarczone urządzenia muszą być fabrycznie nowe, nieużywane, wolne od wad i pochodzić z autoryzowanego kanału dystrybucji producenta.

Gwarancja producenta / Wykonawcy: minimum 36 miesięcy od dnia podpisania protokołu odbioru, wraz z dostępem do aktualizacji oprogramowania i reguł detekcji w tym okresie.

Termin realizacji zamówienia: do 30 dni od podpisania Umowy.

Miejsce realizacji zamówienia: trzy lokalizacje wskazane przez Zamawiającego na terenie prowadzenia działalności.

Oprogramowanie klasy IDS (Intrusion Detection System) dedykowane sieciom OT Zintegrowany system bezpieczeństwa – Industrial Central Management dla OT

---

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa oprogramowania dedykowanego do detekcji zagrożeń i monitorowania bezpieczeństwa sieci OT (system klasy SIEM/IDS/Industrial Central Management Console), wraz z funkcjonalnością inspekcji stacji izolowanych (przenośne urządzenie skanujące USB) oraz kompletem licencji niezbędnych do jego pełnego uruchomienia i eksploatacji zgodnie z wymaganiami określonymi w niniejszym Opisie Przedmiotu Zamówienia (dalej: OPZ), przy czym:

- licencje uprawniające do korzystania ze wszystkich funkcjonalności wymaganych niniejszym OPZ muszą być bezterminowe (perpetual);
- jeżeli oferowane rozwiązanie wymaga usług o charakterze terminowym (subskrypcyjnym) – w szczególności aktualizacji oprogramowania, sygnatur, baz podatności, threat intelligence lub wsparcia producenta – Wykonawca zapewni ich świadczenie przez okres nie krótszy niż 36 miesięcy od dnia podpisania protokołu odbioru;
- po zakończeniu okresu, o którym mowa wyżej, system musi zachować pełną funkcjonalność z wykorzystaniem ostatnich prawidłowo zainstalowanych aktualizacji.

Lp.	Element zamówienia	Ilość
1	System SIEM/IDS/Industrial Central Management Console dla OT (rozdz. 2)	1 instancja
2	Przenośne urządzenie skanujące USB (rozdz. 3)	1 szt.
3	Moduł zarządzający urządzeniem skanującym (rozdz. 3)	1 instancja

2. Centralny system bezpieczeństwa OT

2.1. Architektura systemu

- Preferuje się system zintegrowany z jedną konsolą zarządzającą dla grup funkcyjnych opisanych w niniejszym OPZ.
- Dopuszcza się stosowanie wielu rozwiązań, pod warunkiem integracji umożliwiającej wizualizację danych na centralnych pulpitach bezpieczeństwa, bez konieczności uruchamiania dedykowanych konsol dla pozostałych systemów wchodzących w skład architektury.

2.2. Parametry systemu SIEM/IDS/Central Console OT

Parametr	Opis / wartość parametru	Ilość
Liczba zarządzanych urządzeń	Liczba urządzeń/węzłów (np. sond OT, urządzeń brzegowych) objętych licencją i zarządzanych z poziomu systemu	Minimum 50
Liczba użytkowników	Liczba licencjonowanych kont użytkowników (administratorów/operatorów) oraz jednoczesnych logowań	Minimum 2
Okres objęty licencją	Licencja bezterminowa (perpetual)	n/d
Dostęp dla użytkownika	Przez przeglądarkę internetową	n/d
Projektowanie widoczności danych	Poprzez interfejs GUI	n/d

Parametr	Opis / wartość parametru	Ilość
Liczba instancji	Liczba wymaganych instalacji przez Zamawiającego	1
Miejsce instalacji	Lokalna oraz chmurowa – do wyboru Zamawiającego	n/d

2.3. Opis ogólny

- Wymagany system powinien stanowić centralny panel wizualizacji stanu bezpieczeństwa OT i aktywności systemu cyberbezpieczeństwa. Musi umożliwiać operatorowi SOC (Security Operations Center) lub administratorowi IT/OT szybki wgląd w sytuację bezpieczeństwa, liczbę zdarzeń, alarmów oraz aktywność urządzeń w sieci.
- Zamawiający oczekuje zintegrowanego systemu klasy SIEM/IDS/Industrial Central Management Console dla środowisk przemysłowych, łączącego funkcje bezpieczeństwa, inwentaryzacji i zarządzania politykami w jednym środowisku. System musi być zaprojektowany specjalnie dla infrastruktury OT/ICS Zamawiającego i oferować pasywne monitorowanie, automatyczną analizę, raportowanie ryzyka i korelację zdarzeń bez domyślnej ingerencji w proces produkcyjny.

2.4. Wymagane minimalne funkcjonalności

- **Scentralizowane zarządzanie bezpieczeństwem OT** – umożliwienie centralnego wdrażania i egzekwowania polityk bezpieczeństwa dla rozproszonych urządzeń brzegowych z poziomu jednej, intuicyjnej konsoli.
- **Pełna widoczność i kontrola zasobów** – automatyczne wykrywanie i identyfikacja aktywów sieci ICS, relacji między nimi oraz wykrywanie nieautoryzowanych urządzeń w sieci (tzw. Shadow OT).
- **Skalowalność i ciągłość działania** – architektura systemu musi pozwalać na obsługę od kilkudziesięciu do 500 urządzeń w wielu lokalizacjach jednocześnie, posiadając mechanizmy fail-safe zapewniające ciągłość operacyjną.
- **Zarządzanie politykami bezpieczeństwa** – wsparcie dla ścieżki dualnej, tj. jednoczesnego centralnego i zdecentralizowanego zarządzania regułami bezpieczeństwa:
  - możliwość uruchomienia mechanizmu automatycznego uczenia na urządzeniach brzegowych, tj. sondach OT, celem zaktualizowania polityk bezpieczeństwa z poziomu systemu centralnego.
- **Integracja i interoperacyjność** – wsparcie dla integracji z systemami zewnętrznymi klasy SIEM, SOC oraz XDR za pomocą otwartego interfejsu API.

2.5. Architektura i wymagania techniczne (wersja Virtual Appliance)

- System musi umożliwiać wdrożenie zarówno w chmurze obliczeniowej (AWS, Azure, Google Cloud), jak i w środowisku lokalnym jako instancja wirtualna (Virtual Appliance). Wymagana jest pełna możliwość pracy i aktualizacji systemu w środowisku odizolowanym, tj. bez dostępu do Internetu.
- Wspierane środowiska wirtualizacji (hypervisory) – system w wersji on-premises musi być w pełni kompatybilny z co najmniej jednym z poniższych środowisk:
  - VMware ESX 6.0 lub nowszy / VMware Workstation 14 lub nowszy,
  - KVM 2.x lub nowszy,
  - Hyper-V 10.x lub nowszy,
  - Nutanix AHV 20220304.34 / 6.5.2 LTS lub nowszy.
- Skalowalność zasobów sprzętowych – w zależności od liczby zarządzanych węzłów (node count) system musi bezproblemowo działać przy zachowaniu minimalnych parametrów przypisanych zasobów; dla **do 50 węzłów/urządzeń: min. 4 rdzenie CPU, 16 GB RAM, dysk 480 GB.**

2.6. Analityka, raportowanie i kontrola dostępu

- **Analityka i dashboard** – dostęp do spersonalizowanego panelu monitorowania incydentów oraz analizy aktywności w czasie rzeczywistym.
- **Raportowanie i powiadomienia** – możliwość generowania raportów na żądanie oraz według harmonogramu, wraz z wysyłaniem natychmiastowych alertów e-mail do administratorów po wykryciu incydentu.
- **Audytowalność** – pełne logowanie zdarzeń systemowych, zmian w politykach, filtrów protokołów oraz wykrytych zasobów.
- **Kontrola dostępu (RBAC)** – obsługa wielu kont administratorów z precyzyjnie definiowanymi poziomami uprawnień i ról.

3. Funkcjonalność inspekcji stacji izolowanych

3.1. Zakres funkcjonalności

Centralny system bezpieczeństwa OT musi zostać uzupełniony o funkcjonalność umożliwiającą kontrolę stacji roboczych, które:

- pracują w sieciach odizolowanych,
- nie posiadają dostępu do Internetu,
- nie mogą komunikować się bezpośrednio z centralnym systemem bezpieczeństwa,
- nie umożliwiają instalacji tradycyjnego oprogramowania antywirusowego lub oprogramowania agentowego.

Funkcjonalność ta musi być realizowana przy wykorzystaniu przenośnego urządzenia skanującego w postaci nośnika USB, współpracującego z konsolą zarządzającą dostarczanego systemu bezpieczeństwa.

Dopuszcza się zastosowanie dedykowanego modułu zarządzającego urządzeniem skanującym, pod warunkiem jego integracji z centralnym systemem bezpieczeństwa OT w zakresie prezentowania wyników skanowania, wykrytych zagrożeń, podatności, danych inwentaryzacyjnych oraz stanu urządzenia.

Dane pochodzące z urządzenia skanującego powinny być możliwe do prezentowania na centralnych pulpitach bezpieczeństwa bez konieczności każdorazowego uruchamiania dodatkowej konsoli administracyjnej.

Parametr	**Opis / wartość parametru**	**Ilość**
Przenośne urządzenie skanujące	Urządzenie w postaci nośnika USB, wyposażone we wbudowane oprogramowanie służące do skanowania, inwentaryzacji i analizy podatności stacji roboczych w środowisku OT	1 szt.
Moduł zarządzający	Funkcjonalność centralnego systemu lub zintegrowany komponent umożliwiający zarządzanie urządzeniem, politykami, aktualizacjami i wynikami skanowania	1 instancja
Sposób wdrożenia	W ramach centralnego systemu bezpieczeństwa lub jako maszyna wirtualna zintegrowana z tym systemem	n/d
Miejsce instalacji	Środowisko lokalne Zamawiającego z możliwością pracy bez dostępu do Internetu	n/d
Dostęp administracyjny	Przez przeglądarkę internetową z wykorzystaniem szyfrowanego połączenia HTTPS	n/d
Okres licencji	Licencja bezterminowa na korzystanie z dostarczonego urządzenia i funkcjonalności zarządzającej	n/d

Parametr	Opis / wartość parametru	Ilość
Okres wsparcia i aktualizacji	Minimum 36 miesięcy od dnia podpisania protokołu odbioru	n/d

3.2. Przenośne urządzenie skanujące

Urządzenie musi:

- mieć formę przenośnego nośnika USB,
- zawierać wbudowane, niezależne oprogramowanie skanujące,
- umożliwiać uruchomienie skanowania bez instalowania oprogramowania na kontrolowanej stacji roboczej,
- umożliwiać pracę na stacjach pozbawionych dostępu do Internetu,
- umożliwiać wykonanie skanowania bez stałej komunikacji z centralnym systemem bezpieczeństwa,
- zapisywać wyniki skanowania oraz umożliwiać ich późniejsze przekazanie do centralnego systemu,
- umożliwiać wielokrotne wykorzystanie na różnych stacjach roboczych,
- stosować polityki skanowania określone centralnie przez administratora.

Oprogramowanie skanujące musi działać co najmniej w następujących środowiskach:

- Microsoft Windows XP oraz nowsze wersje systemu Microsoft Windows,
- systemy operacyjne Linux.

Wykonawca zobowiązany jest przedstawić listę wspieranych systemów operacyjnych i architektur sprzętowych.

3.3. Funkcje wykrywania zagrożeń i inwentaryzacji

Urządzenie skanujące musi posiadać silnik wykrywania złośliwego oprogramowania wykorzystujący co najmniej aktualizowane sygnatury zagrożeń.

System musi umożliwiać:

- skanowanie plików i wskazanych lokalizacji systemowych,
- skanowanie plików znajdujących się w archiwach,
- wykrywanie złośliwego oprogramowania,
- wykrywanie potencjalnie niepożądanych aplikacji,

- rejestrowanie nazwy wykrytego zagrożenia,
- rejestrowanie lokalizacji wykrytego pliku,
- rejestrowanie daty i godziny wykrycia,
- rejestrowanie działania podjętego wobec wykrytego zagrożenia.

Urządzenie musi zbierać co najmniej następujące informacje inwentaryzacyjne:

- nazwę i identyfikator skanowanego urządzenia,
- informacje o sprzęcie,
- informacje o procesorze, pamięci operacyjnej i przestrzeni dyskowej,
- informacje o systemie operacyjnym i jego wersji,
- informacje o zainstalowanych poprawkach systemowych,
- listę zainstalowanych aplikacji i ich wersji,
- informacje o wykrytych podatnościach systemu operacyjnego i aplikacji,
- datę i godzinę wykonania inspekcji,
- wersję wykorzystanego silnika skanującego, sygnatur oraz bazy podatności.

3.4. Synchronizacja z centralnym systemem bezpieczeństwa

System musi umożliwiać synchronizację urządzenia skanującego za pośrednictwem autoryzowanej stacji roboczej posiadającej komunikację z centralnym systemem bezpieczeństwa lub jego modułem zarządzającym.

Synchronizacja musi umożliwiać co najmniej:

- pobieranie polityk skanowania,
- pobieranie konfiguracji urządzenia,
- pobieranie aktualizacji oprogramowania,
- pobieranie aktualizacji silników skanujących,
- pobieranie sygnatur antywirusowych,
- pobieranie aktualizacji bazy podatności,
- przekazywanie wyników przeprowadzonych skanowań,
- przekazywanie danych inwentaryzacyjnych,
- przekazywanie informacji o wykrytych zagrożeniach i podatnościach,
- przekazywanie dzienników aktywności urządzenia.

Synchronizacja nie może wymagać zapewnienia skanowanej stacji roboczej dostępu do Internetu ani bezpośredniego dostępu do centralnego systemu bezpieczeństwa.

3.5. Centralne zarządzanie urządzeniem skanującym

Zarządzanie urządzeniem skanującym musi odbywać się z poziomu centralnego systemu bezpieczeństwa OT lub komponentu ściśle z nim zintegrowanego.

System musi umożliwiać:

- centralną konfigurację urządzenia,
- zarządzanie politykami skanowania,
- zarządzanie aktualizacjami,
- odbieranie i przechowywanie wyników skanowań,
- analizę wykrytych zagrożeń i podatności,
- przeglądanie danych inwentaryzacyjnych,
- raportowanie stanu bezpieczeństwa skanowanych zasobów,
- audyt działań administracyjnych,
- grupowanie urządzeń i zasobów,
- stosowanie polityk dla grup lub pojedynczych urządzeń,
- blokowanie możliwości lokalnej zmiany polityki skanowania,
- rejestrowanie zmian konfiguracji i polityk bezpieczeństwa.

System musi pozwalać na definiowanie co najmniej następujących rodzajów skanowania:

- pełnego skanowania wszystkich dostępnych folderów lokalnych,
- szybkiego skanowania domyślnych i krytycznych lokalizacji systemowych,
- skanowania wskazanych przez administratora ścieżek,
- skanowania plików znajdujących się w archiwach.

Administrator musi mieć możliwość określenia sposobu postępowania po wykryciu zagrożenia, w tym:

- żądania potwierdzenia działania,
- wyłącznie zarejestrowania zdarzenia,
- wykonania działania zalecanego przez producenta,
- zablokowania dostępu do wykrytego obiektu,
- przeniesienia obiektu do kwarantanny.

3.6. Analiza podatności i zmian w zasobach

Centralny system bezpieczeństwa lub zintegrowany z nim moduł musi automatycznie analizować dane zebrane podczas inspekcji stacji roboczych.

System musi:

- identyfikować znane podatności systemu operacyjnego i zainstalowanych aplikacji,
- przypisywać podatnościom identyfikatory CVE,
- prezentować ocenę podatności zgodnie ze standardem CVSS 3.0 lub nowszym,
- klasyfikować podatności co najmniej jako krytyczne, wysokie, średnie i niskie,
- wskazywać zasoby, na których wykryto podatność,
- umożliwiać filtrowanie podatności według poziomu ryzyka, zasobu, aplikacji i identyfikatora CVE.

Dla wykrytych podatności system powinien przedstawiać zalecenia naprawcze, obejmujące w szczególności:

- wskazanie wymaganej poprawki systemowej,
- wskazanie aktualizacji dostępnej w Microsoft Update Catalog,
- wskazanie wymaganej lub zalecanej wersji oprogramowania,
- wskazanie sposobu ograniczenia ryzyka.

System musi umożliwiać:

- ustanowienie wybranego wyniku skanowania jako skanu bazowego,
- porównanie kolejnych wyników ze skanem bazowym,
- identyfikowanie nowych i usuniętych podatności,
- identyfikowanie zmian sprzętowych,
- identyfikowanie zmian systemu operacyjnego,
- identyfikowanie nowych, usuniętych lub zaktualizowanych aplikacji,
- prezentowanie historii skanowania danego zasobu.

3.7. Raportowanie i logowanie

Dane pochodzące z urządzenia skanującego muszą być uwzględniane w mechanizmach raportowania i wizualizacji centralnego systemu bezpieczeństwa OT.

System musi zbierać i przechowywać:

- dzienniki przeprowadzonych skanowań,
- informacje o wykrytych zagrożeniach,
- informacje o podjętych działaniach,
- dane inwentaryzacyjne,
- informacje o wykrytych podatnościach,
- dzienniki synchronizacji,
- dzienniki aktualizacji,
- dzienniki zdarzeń systemowych,
- dzienniki audytowe działań administracyjnych.

System musi umożliwiać:

- generowanie raportów na żądanie,
- generowanie raportów dla pojedynczego zasobu lub grupy zasobów,
- wybór zakresu danych uwzględnianych w raporcie,
- filtrowanie danych według daty, urządzenia, zagrożenia, podatności i poziomu ryzyka,
- eksport raportów co najmniej do formatów PDF i CSV.

3.8. Aktualizacje

Centralny system bezpieczeństwa lub jego zintegrowany komponent musi umożliwiać zarządzanie aktualizacjami:

- oprogramowania urządzenia skanującego,
- oprogramowania modułu zarządzającego,
- oprogramowania sprzętowego urządzenia, jeżeli ma zastosowanie,
- silników skanujących,
- sygnatur antywirusowych,
- baz wzorców zagrożeń,
- bazy podatności producenta.

System musi umożliwiać:

- automatyczne pobieranie aktualizacji w środowisku posiadającym dostęp do Internetu,
- pobieranie aktualizacji za pośrednictwem serwera proxy,
- ręczne pobieranie i instalowanie pakietów aktualizacyjnych,
- przenoszenie pakietów aktualizacyjnych do środowiska odizolowanego,
- aktualizację urządzenia skanującego bez zapewnienia mu bezpośredniego dostępu do Internetu,
- prezentowanie wersji zainstalowanych aktualizacji,
- prezentowanie daty ostatniej prawidłowej aktualizacji.

Rozwiązanie musi zachowywać funkcjonalność w środowisku odizolowanym, z wykorzystaniem ostatnich prawidłowo zainstalowanych aktualizacji.

3.9. Bezpieczeństwo i administracja

Zarządzanie funkcjonalnością inspekcji stacji izolowanych musi wykorzystywać mechanizmy kontroli dostępu opartej na rolach (RBAC). Wymagane są co najmniej następujące poziomy uprawnień:

- Administrator – posiadający pełny dostęp do systemu,
- Administrator Lokalny – posiadający możliwość zarządzania przypisaną grupą urządzeń,
- Użytkownik – posiadający dostęp wyłącznie do odczytu danych dotyczących przypisanych zasobów.

System musi umożliwiać:

- tworzenie wielu kont administratorów i użytkowników,
- przypisywanie ról,
- ograniczanie dostępu do wybranych grup urządzeń lub zasobów,
- rejestrowanie logowań i operacji użytkowników,
- blokowanie lub dezaktywowanie kont.

Dostęp do komponentu zarządzającego musi odbywać się z wykorzystaniem szyfrowanego protokołu HTTPS. System musi umożliwiać:

- wygenerowanie własnego certyfikatu SSL,
- zastąpienie certyfikatu systemowego certyfikatem korporacyjnym Zamawiającego,
- import certyfikatów co najmniej w formacie PEM.

3.10. Integracja i sposób wdrożenia

Funkcjonalność zarządzania urządzeniem skanującym może być:

- bezpośrednim elementem centralnego systemu bezpieczeństwa OT,
- modułem dostarczonym w ramach tego systemu,
- odrębnym komponentem technicznym, pod warunkiem pełnej integracji z centralnym systemem bezpieczeństwa.

W przypadku zastosowania odrębnego komponentu musi on zostać dostarczony w postaci maszyny wirtualnej w formacie OVA, gotowej do importu do środowiska wirtualizacyjnego Zamawiającego.

Integracja musi umożliwiać przekazywanie co najmniej:

- informacji o wykonanych skanowaniach,
- informacji o wykrytych zagrożeniach,
- informacji o wykrytych podatnościach,
- danych inwentaryzacyjnych,
- informacji o poziomie ryzyka zasobów,
- zdarzeń systemowych i alarmów.

Integracja może być realizowana przy wykorzystaniu udokumentowanego interfejsu API, protokołu syslog, konektora producenta lub innego udokumentowanego mechanizmu integracyjnego.

System musi posiadać możliwość integracji z rozwiązaniem klasy XDR dostawcy sond bezpieczeństwa OT lub rozwiązaniem równoważnym.

4. Licencje

Licencja na korzystanie z dostarczonej funkcjonalności, urządzenia skanującego oraz komponentu zarządzającego musi być bezterminowa.

Usługi o charakterze terminowym (aktualizacje oprogramowania, silników skanujących, sygnatur i bazy podatności oraz wsparcie producenta) muszą być zapewnione przez okres nie krótszy niż 36 miesięcy od dnia podpisania protokołu odbioru, zgodnie z rozdz. 1 OPZ.

Po zakończeniu okresu wsparcia system musi umożliwiać dalsze korzystanie z urządzenia i zgromadzonych danych oraz wykonywanie skanowań z wykorzystaniem ostatnich dostępnych aktualizacji.

5. Certyfikacja producenta

Producent dostarczanego centralnego systemu bezpieczeństwa lub producent komponentu odpowiedzialnego za funkcjonalność inspekcji stacji izolowanych musi posiadać ważny certyfikat zgodności procesu bezpiecznego rozwoju produktu z normą IEC 62443-4-1. Certyfikat musi być wydany przez niezależną jednostkę certyfikującą.

Na żądanie Zamawiającego Wykonawca zobowiązany będzie przedstawić:

- kopię certyfikatu,
- informację o jednostce, która wydała certyfikat,
- zakres certyfikacji,
- okres ważności certyfikatu,
- dokument lub odnośnik umożliwiający zweryfikowanie ważności certyfikatu.

6. Wymagania ogólne

Jeżeli w opisie przedmiotu zamówienia OPZ Zamawiający odnosi się do norm, europejskich Ocen technicznych, specyfikacji technicznych oraz innych systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp, to jest obowiązany wskazać, że dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy lub „równoważne".

Wymienione w jakiejkolwiek części OPZ w zakresie dostaw urządzeń wraz z oprogramowaniem: nazwy własne, marki wyrobów, materiałów, technologii nie są obligatoryjne dla wykonawców. Wykonawca ma prawo do zaoferowania innych wyrobów, materiałów, technologii pod warunkiem zapewnienia parametrów technicznych co najmniej identycznych z parametrami określonymi w dokumentacji zamówienia (dopuszcza się dostawę przedmiotu zamówienia o wyższych parametrach technicznych).

Jeżeli OPZ wskazywałby w odniesieniu do niektórych materiałów, wyrobów i technologii znaki towarowe, patenty lub pochodzenie, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, w tym w szczególności podane zostały - nazwa własna materiału,

wyrobu czy technologii, numer katalogowy lub producent, należy to traktować jako rozwiązanie przykładowe, określające standardy, wygląd oraz wymagania techniczne. Wszelkie materiały, urządzenia i technologie, pochodzące od konkretnych producentów, określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać materiały, urządzenia i technologie, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia, nie mają na celu uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów. Tak zastosowane zapisy są tylko w sytuacjach, gdy zamawiający nie był w stanie opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń - w tych wypadkach należy zawsze przyjąć sformułowanie - " lub równoważny"

Zastosowane przez Wykonawcę materiały, wyroby i rozwiązania równoważne, muszą być co najmniej:

- o tej samej wytrzymałości i trwałości, o tym samym poziomie estetyki (wyroby),
- o parametrach technicznych opisanych w dokumentacji przetargowej,
- kompatybilne z istniejącą i projektowaną infrastrukturą,
- spełniać: te same funkcje, wymagania bezpieczeństwa konstrukcji, bhp i p. poż,
- posiadać stosowne dokumenty dopuszczające do stosowania w budownictwie (atesty i aprobaty techniczne).

Wykonawca musi udowodnić Zamawiającemu, że proponowany materiał, wyrób, technologia lub rozwiązanie jest równoważne, przedstawiając np. wszelkie dokumenty, obliczenia, opinie etc. potwierdzające równoważność.

Dostarczone oprogramowanie i licencje muszą pochodzić z autoryzowanego kanału dystrybucji producenta i być przeznaczone dla Zamawiającego jako licencjobiorcy.

Przenośne urządzenie skanujące musi być fabrycznie nowe i nieużywane. Gwarancja na urządzenie: minimum 24 miesięcy od dnia podpisania protokołu odbioru.

Termin realizacji zamówienia: do 30 dni od podpisania Umowy.

Miejsce realizacji zamówienia: Siedziba Zamawiającego.

Rozwiązanie klasy SIEM/XDR dla środowisk IT i OT
wraz z wdrożeniem, szkoleniem i asystą techniczną

---

1. Przedmiot i cel zamówienia

Przedmiotem zamówienia jest dostawa, instalacja i wdrożenie platformy klasy SIEM/XDR w dwóch odrębnych środowiskach – IT oraz OT – wraz z przeszkoleniem personelu Zamawiającego, wsparciem technicznym oraz asystą techniczną, zgodnie z wymaganiami określonymi w niniejszym Opisie Przedmiotu Zamówienia (dalej: OPZ).

Wdrożenie platformy SIEM w dwóch odrębnych środowiskach IT oraz OT ma na celu zwiększenie poziomu cyberbezpieczeństwa organizacji poprzez centralizację monitorowania zdarzeń, analizę logów, wykrywanie zagrożeń oraz identyfikację potencjalnych nieprawidłowości w infrastrukturze informatycznej i przemysłowej. Rozdzielenie platformy na niezależne instancje pozwoli dostosować konfigurację, reguły detekcji i polityki bezpieczeństwa do specyfiki każdego środowiska, z uwzględnieniem odmiennych wymagań w zakresie dostępności, ciągłości działania i kontroli dostępu.

W środowisku IT rozwiązanie wesprze ochronę serwerów, stacji roboczych i usług informatycznych, natomiast w środowisku OT umożliwi monitorowanie zdarzeń bezpieczeństwa w systemach wspierających procesy technologiczne, przy zachowaniu szczególnej ostrożności, aby nie zakłócać ich działania. Wdrożenie rozwiązania SIEM zwiększy widoczność zagrożeń, usprawni wykrywanie i analizę incydentów oraz zapewni lepszą kontrolę nad stanem bezpieczeństwa obu obszarów, przy jednoczesnym zachowaniu ich organizacyjnej i technicznej separacji.

2. Wymagania dotyczące rozwiązania SIEM/XDR

2.1. Zamawiający wymaga, aby system operacyjny hostujący centralną część wdrażanego rozwiązania SIEM/XDR był oparty na licencji Open Source.

2.2. Platforma SIEM/XDR zostanie wdrożona na dwóch serwerach fizycznych udostępnionych przez Zamawiającego, w dwóch osobnych środowiskach (IT i OT).

2.3. Rozwiązanie musi mieć możliwość instalacji i poprawnej pracy na serwerze o następujących parametrach: procesor (CPU) 8 rdzeni, pamięć RAM 32 GB oraz dysk twardy (HDD) 1 TB.

2.4. Architektura rozwiązania SIEM/XDR powinna bazować na komponentach licencjonowanych w modelu Open Source, której strukturę można podzielić na cztery zasadnicze części: usługę indeksowania danych, usługę analizowania danych, usługę wizualizacji danych (GUI do codziennej pracy) oraz usługę agenta monitorującego serwery i stacje robocze w sieci Zamawiającego.

2.5. Usługa indeksowania danych powinna wspierać osadzenie jej na serwerze z systemem Linux w najnowszej dostępnej stabilnej wersji LTS i zapewnić stabilną pracę przy przydzielonych parametrach: 8 GB pamięci RAM i 4 rdzenie.

2.6. Usługa analizowania danych powinna wspierać osadzenie jej na serwerze z systemem Linux w najnowszej dostępnej stabilnej wersji LTS i zapewnić stabilną pracę przy przydzielonych parametrach 8 GB pamięci RAM i 2 rdzenie.

2.7. Usługa wizualizacji danych powinna wspierać osadzenie jej na serwerze z systemem Linux w najnowszej dostępnej stabilnej wersji LTS i zapewnić stabilną pracę przy przydzielonych parametrach: 8 GB pamięci RAM i 2 rdzenie.

2.8. Usługi, o których mowa w pkt 2.5–2.7, muszą zapewnić stabilną pracę przy jednoczesnym uruchomieniu na jednym serwerze fizycznym w każdym ze środowisk (IT i OT), w ramach zasobów określonych w pkt 2.3 (łącznie 8 rdzeni CPU i 24 GB RAM przydzielonych usługom centralnym, z zachowaniem pozostałych zasobów na potrzeby systemu operacyjnego i buforowania). Dopuszcza się instalację komponentów bezpośrednio w systemie operacyjnym, w kontenerach lub w maszynach wirtualnych.

2.9. Zamawiający wymaga, aby usługa agenta monitorującego była kompatybilna w jego środowisku z następującymi systemami:

- Windows 10 i nowszy,
- Windows Server 2022 i nowszy,
- Linux Fedora 22 i nowszy,
- Ubuntu 20.04 LTS i nowszy,
- Debian 11 Bullseye i nowszy,
- Rocky Linux 8 i nowszy.

2.10. Tworzenie użytkowników w systemie SIEM/XDR powinno odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie, przez definiowanie kont w samym rozwiązaniu.

2.11. Rozwiązanie powinno oferować możliwość analizy napływających logów zgodnie z metodyką MITRE ATT&CK w kontekście wykrywania i opisywania możliwych ataków i naruszeń.

2.12. Rozwiązanie powinno oferować możliwość oceny poziomu bezpieczeństwa i poprawności konfiguracji urządzeń zgodnie z metrykami CIS Controls.

2.13. Rozwiązanie powinno oferować możliwość wykrywania konfiguracji sprzętowej urządzeń objętych monitoringiem w zakresie co najmniej: architektury, procesora, pamięci RAM oraz numeru seryjnego urządzenia.

2.14. Rozwiązanie powinno oferować możliwość wykrywania zainstalowanych aplikacji na urządzeniach objętych monitoringiem.

2.15. Rozwiązanie powinno oferować możliwość wykrywania i oceny podatności zgodnie z metodyką CVE (MITRE) dla systemów operacyjnych i wykrytych aplikacji.

2.16. Rozwiązanie powinno pozwalać na generowanie raportów i eksport danych z każdego dostępnego w nim widoku.

2.17. Rozwiązanie powinno pozwalać na zdefiniowanie akcji alarmowych, które mogą być wysyłane co najmniej na adres e-mail lub do wybranego komunikatora np. MS Teams.

2.18. Rozwiązanie powinno zapewniać wsparcie dla realizacji wymagań regulacyjnych w zakresie RODO, PCI DSS, HIPAA oraz NIST.

3. Zakres wdrożenia

W ramach wdrożenia proponowanego rozwiązania Wykonawca wykona następujące czynności, obejmujące zarówno konfigurację rozwiązania, jak i szkolenie z codziennego wykorzystania systemu SIEM/XDR:

3.1. Instalacja systemu operacyjnego będącego bazą systemu na wskazanych przez Zamawiającego serwerach.

3.2. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracją parametrów podstawowej pracy, w tym polityk dostępu dla pracowników zespołu IT Zamawiającego.

3.3. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów polityk bezpieczeństwa Zamawiającego.

3.4. Konfiguracja mechanizmów powiadamiania zespołu IT o zagrożeniach w oparciu o komunikację e-mail.

3.5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi monitorowania urządzeń typu serwery i stacje robocze. Zamawiający informuje, że w jego środowisku znajdują się:

- 8 × serwer Windows,
- 2 × serwer Linux,
- 75 × stacja robocza Windows 10 i 11.

3.6. Zdefiniowanie mechanizmów oceny konfiguracji stacji roboczych i serwerów objętych pracą agenta oraz usług osadzonych na serwerach z metrykami CIS Controls.

3.7. Zdefiniowanie mechanizmów wykrywania podatności w zakresie systemów operacyjnych oraz aplikacji dla urządzeń z zaimplementowanym agentem, zgodnie ze standardem CVE (MITRE).

3.8. Zdefiniowanie mechanizmów wykrywania działania szkodliwego oprogramowania, w tym malware i ransomware. Mechanizm ten powinien działać w oparciu o metodyki oceny konfiguracji bezpieczeństwa monitorowanego urządzenia (SCA), „rootchecks" oraz monitoring integralności plików (FIM).

3.9. Zdefiniowanie mechanizmów analizy logów w oparciu o metodykę MITRE ATT&CK dla danych napływających od urządzeń z zaimplementowanym agentem. Mechanizm powinien gwarantować opisywanie logów w kontekście taktyk i technik ataków wraz z ich klasyfikacją dla napływających danych.

3.10. Przeprowadzenie szkolenia w siedzibie Zamawiającego w dni powszednie od poniedziałku do piątku, w godzinach pracy Zamawiającego. Przed planowanym szkoleniem Wykonawca przedstawi Zamawiającemu do akceptacji harmonogram szkolenia z zarządzania i administracji wdrażanego rozwiązania, w wymiarze nie mniejszym niż 1 dzień roboczy.

4. Gwarancja, wsparcie i asysta techniczna

4.1. Zamawiający wymaga, aby Wykonawca zapewnił wsparcie techniczne rozwiązania świadczone w trybie 8/5, polegające na obsłudze otrzymywanych zgłoszeń dotyczących awarii lub problemów z systemem za pomocą dedykowanego panelu lub drogą mailową, przez okres 36 miesięcy od dnia odbioru wdrożenia.

4.2. Zamawiający wymaga, aby Wykonawca w okresie do 12 miesięcy od wdrożenia rozwiązania świadczył asystę techniczną w łącznym wymiarze 20 godzin zegarowych w zakresie weryfikacji poprawnego funkcjonowania zarówno systemu, jak i jego komponentów, tworzenia raportów bezpieczeństwa dotyczących zarejestrowanych incydentów i wykrytych podatności oraz zgodności ze stworzonymi politykami.

4.3. Zamawiający wymaga, aby ww. usługi były świadczone od poniedziałku do piątku w godzinach 8:00–16:00.

4.4. Zamawiający akceptuje, że każda interwencja wymagać będzie zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji (system zgłoszeń elektronicznych lub komunikacja mailowa) zostanie wyznaczony przez Wykonawcę.

5. Wymagania ogólne

- Wszelkie wskazane w niniejszym OPZ normy, standardy, certyfikaty, oceny techniczne i systemy referencji technicznych należy rozumieć jako opatrzone wyrazami „lub równoważne" (art. 101 ust. 4 ustawy Prawo zamówień publicznych). Ewentualne wskazanie znaku towarowego, patentu lub pochodzenia ma charakter przykładowy i należy je rozumieć jako opatrzone wyrazami „lub równoważny" (art. 99 ust. 5 ustawy Pzp).
- Wykonawca, który powołuje się na rozwiązania równoważne, jest obowiązany wykazać, że oferowane rozwiązanie spełnia wszystkie wymagania określone w niniejszym OPZ.
- Wykonawca wraz z ofertą złoży przedmiotowe środki dowodowe potwierdzające spełnienie wymagań OPZ, w szczególności: (np. karty katalogowe, dokumentację producenta, kopie certyfikatów).
- Po zakończeniu wdrożenia Wykonawca przekaże Zamawiającemu dokumentację powykonawczą obejmującą co najmniej: architekturę wdrożenia, konfigurację komponentów, wdrożone polityki i reguły oraz procedury administracyjne.
- Termin realizacji zamówienia: do 30 dni od dnia podpisania Umowy.
- Miejsce realizacji zamówienia: siedziba Zamawiającego.

Usługa montażu i konfiguracji

Montaż fizyczny 8 serwerów i 4 urządzeń NAS w dwóch szafach rack oraz wdrożenie Proxmox VE (HA) i Proxmox Backup Server

---

1. Przedmiot zamówienia

Przedmiotem zamówienia jest usługa montażu fizycznego, instalacji i konfiguracji infrastruktury serwerowej i pamięci masowej w dwóch szafach rack zlokalizowanych w siedzibie Zamawiającego, obejmująca w szczególności:

- montaż fizyczny 8 serwerów (po 4 w każdej szafie) oraz 4 urządzeń NAS (po 2 w każdej szafie), wraz z podłączeniem zasilania i okablowaniem;
- instalację i konfigurację w każdej szafie dwuwęzłowego klastra wirtualizacji Proxmox VE (lub równoważnego) pracującego w trybie wysokiej dostępności (HA), przeznaczonego do uruchomienia rozwiązania bezpieczeństwa Zamawiającego;
- instalację i konfigurację w każdej szafie dwóch instancji Proxmox Backup Server (lub równoważnego) pracujących w układzie redundantnym (HA w rozumieniu rozdz. 5 OPZ);
- konfigurację urządzeń NAS jako pamięci masowej dla Proxmox Backup Server oraz dla kopii zapasowych wybranych maszyn fizycznych;
- zabezpieczenie (hardening) wdrożonych systemów, testy odbiorowe, dokumentację powykonawczą, szkolenie oraz wsparcie powdrożeniowe.

Zestawienie urządzeń objętych usługą:

Lp.	Urządzenie / rola	Szafa A	Szafa B	Razem
1	Serwer – węzeł klastra Proxmox VE (HA) dla rozwiązania bezpieczeństwa	2 szt.	2 szt.	4 szt.
2	Serwer – Proxmox Backup Server (instancja podstawowa i zapasowa)	2 szt.	2 szt.	4 szt.
3	Urządzenie NAS – pamięć masowa kopii zapasowych	2 szt.	2 szt.	4 szt.
	Razem urządzeń do montażu	**6 szt.**	**6 szt.**	**12 szt.**

Sprzęt, o którym mowa wyżej, zapewnia Zamawiający. Przedmiotem zamówienia nie jest dostawa serwerów, urządzeń NAS, dysków ani przełączników sieciowych. Subskrypcje wsparcia producenta oprogramowania Proxmox (repozytorium enterprise) zapewnia: Wykonawca.

2. Stan istniejący i założenia

- Miejsce realizacji: siedziba Zamawiającego.
- Szafy rack: 2 szafy 19", wysokość 42 U, wyposażone w listwy zasilające PDU w dwóch niezależnych torach zasilania (A/B) zasilanych z UPS.
- Każda szafa stanowi odrębne, niezależne środowisko (IT i OT). Rozwiązania wdrażane w poszczególnych szafach nie mogą być ze sobą łączone (wspólny klaster, wspólny datastore, synchronizacja kopii zapasowych) bez pisemnej zgody Zamawiającego.
- Zamawiający zapewnia: przełączniki sieciowe wraz z wolnymi portami, plan adresacji IP i sieci VLAN, dostęp do pomieszczeń w uzgodnionych terminach oraz osoby kontaktowe po stronie IT.
- Wykonawca ma możliwość odbycia wizji lokalnej przed złożeniem oferty, po wcześniejszym uzgodnieniu terminu z Zamawiającym oraz po podpisaniu umowy o zachowaniu poufności (NDA).

3. Montaż fizyczny i konfiguracja sprzętowa

3.1. Prace przygotowawcze

- Weryfikacja kompletności i stanu technicznego dostarczonych urządzeń, potwierdzona protokołem.
- Opracowanie i przedstawienie do akceptacji Zamawiającego planu rozmieszczenia urządzeń w szafach (elewacja szaf), z uwzględnieniem masy urządzeń, kierunku przepływu powietrza i dostępności serwisowej.
- Sporządzenie bilansu mocy i obciążenia torów zasilania A/B każdej szafy oraz poinformowanie Zamawiającego o ewentualnym ryzyku przekroczenia dopuszczalnego obciążenia PDU/UPS przed rozpoczęciem montażu.

3.2. Montaż urządzeń

- Montaż serwerów i urządzeń NAS w szafach z wykorzystaniem szyn/prowadnic zgodnych z zaleceniami producenta urządzeń, wraz z ramionami do prowadzenia kabli, o ile są dostępne w zestawie.
- Montaż w sposób niepowodujący utraty gwarancji producenta sprzętu, z zachowaniem wymagań producenta dotyczących chłodzenia i uziemienia.

3.3. Zasilanie

- Podłączenie każdego urządzenia wyposażonego w zasilacze redundantne do dwóch różnych torów zasilania (PDU A i PDU B).
- Weryfikacja poprawności działania redundancji zasilania (praca urządzenia przy odłączeniu jednego toru).

3.4. Okablowanie

- Wykonanie połączeń sieciowych pomiędzy urządzeniami a przełącznikami Zamawiającego zgodnie z zatwierdzonym planem połączeń.
- Prowadzenie okablowania w sposób uporządkowany, z wykorzystaniem organizerów, z zachowaniem minimalnych promieni gięcia oraz separacji przewodów zasilających i transmisyjnych, zgodnie z normą PN-EN 50174-2 lub równoważną.
- Trwałe oznaczenie obu końców każdego przewodu (zasilającego i sieciowego) zgodnie z przyjętym u Zamawiającego standardem lub normą ANSI/TIA-606 lub równoważną.
- Wykonawca zapewnia materiały instalacyjne, w szczególności: patchcordy miedziane kat. 6A i/lub światłowodowe, opaski typu rzep, etykiety, śruby i nakrętki koszyczkowe. Moduły SFP/SFP+, jeśli okażą się niezbędne zapewnia: Wykonawca.
- Konfiguracja kart zdalnego zarządzania (BMC, np. iDRAC/iLO/IPMI lub równoważne) w sieci zarządzającej wskazanej przez Zamawiającego, zmiana domyślnych danych logowania, włączenie powiadomień o awariach.
- Po zakończeniu prac – usunięcie i utylizacja opakowań oraz uporządkowanie miejsca prac.

4. Klaster Proxmox VE w trybie HA (w każdej szafie)

4.1. Instalacja

- Instalacja na 2 serwerach w każdej szafie najnowszej stabilnej wersji Proxmox VE (nie starszej niż 9.x) lub oprogramowania równoważnego, na dyskach systemowych w konfiguracji mirror.
- Konfiguracja repozytoriów aktualizacji (repozytorium enterprise – w przypadku zapewnienia subskrypcji), synchronizacji czasu (NTP), DNS oraz powiadomień e-mail (SMTP Zamawiającego).

4.2. Klaster i kworum

- Utworzenie w każdej szafie odrębnego klastra dwuwęzłowego.
- Zapewnienie trzeciego głosu kworum poprzez zewnętrzny arbiter (Corosync QDevice / corosync-qnetd lub równoważny), uruchomiony poza węzłami klastra – na hoście wskazanym przez Zamawiającego lub zaproponowanym przez Wykonawcę i zaakceptowanym przez Zamawiającego (np. na jednym z serwerów Proxmox Backup Server w danej szafie). Nie dopuszcza się konfiguracji HA bez zewnętrznego arbitra ani rozwiązań polegających na ręcznym obniżaniu wymaganej liczby głosów (expected votes).

4.3. Sieć

- Konfiguracja odrębnych sieci logicznych (VLAN) i – w miarę dostępności interfejsów – fizycznych dla: zarządzania, komunikacji klastra (Corosync), replikacji i migracji maszyn, ruchu do serwerów kopii zapasowych oraz ruchu maszyn wirtualnych.
- Komunikacja klastra (Corosync) musi wykorzystywać dedykowany interfejs fizyczny (min. 1 Gb/s) oraz drugie, zapasowe łącze w innej sieci fizycznej.
- Agregacja interfejsów (LACP 802.3ad lub active-backup) dla ruchu maszyn wirtualnych i replikacji – zgodnie z możliwościami przełączników Zamawiającego.

4.4. Pamięć masowa i replikacja

- Konfiguracja lokalnej pamięci masowej ZFS na każdym węźle oraz replikacji maszyn objętych HA pomiędzy węzłami (storage replication) z interwałem nie dłuższym niż 5 min.
- Zamawiający przyjmuje do wiadomości, że w przypadku awarii węzła maszyny są uruchamiane na drugim węźle ze stanem dysków z ostatniej replikacji (RPO równe interwałowi replikacji).
- Dopuszcza się zaproponowanie przez Wykonawcę innego rozwiązania pamięci dla HA o co najmniej równoważnym poziomie ochrony, po akceptacji Zamawiającego, przy czym urządzenia NAS przeznaczone są wyłącznie do przechowywania kopii zapasowych.

4.5. Wysoka dostępność (HA)

- Konfiguracja menedżera HA dla maszyn wirtualnych (rozwiązania bezpieczeństwa, wraz z regułami rozmieszczenia (preferowany węzeł) oraz polityką zachowania przy planowanym wyłączeniu węzła).

- Konfiguracja mechanizmu watchdog do samoizolacji węzła (fencing) – sprzętowego (np. przez BMC/IPMI), jeżeli jest dostępny, w przeciwnym razie programowego.
- Weryfikacja, że zasoby (CPU, RAM, pamięć masowa) każdego węzła są wystarczające do uruchomienia wszystkich maszyn objętych HA na jednym węźle (zasada N+1) i przekazanie Zamawiającemu wyniku weryfikacji.

4.6. Przygotowanie pod rozwiązanie bezpieczeństwa

- Przygotowanie środowiska pod rozwiązanie bezpieczeństwa Zamawiającego: (liczba i parametry maszyn wirtualnych, sieci/mostów, w tym ewentualnych interfejsów do odbioru ruchu kopiowanego SPAN/TAP).
- Instalacja i konfiguracja samego rozwiązania bezpieczeństwa w maszynach wirtualnych nie wchodzi w zakres zamówienia i objęte jest odrębnym postępowaniem.

5. Proxmox Backup Server w układzie redundantnym (w każdej szafie)

5.1. Definicja trybu HA

Zamawiający informuje, że Proxmox Backup Server nie posiada natywnego mechanizmu klastra wysokiej dostępności. Przez „tryb HA" w rozumieniu niniejszego OPZ Zamawiający rozumie układ dwóch niezależnych instancji (podstawowej i zapasowej), w którym:

- każda instancja przechowuje dane na odrębnym urządzeniu NAS,
- instancja zapasowa posiada aktualną kopię kopii zapasowych dzięki cyklicznej synchronizacji,
- w przypadku awarii instancji podstawowej możliwe jest odtwarzanie danych oraz wykonywanie nowych kopii zapasowych z wykorzystaniem instancji zapasowej, zgodnie z udokumentowaną i przetestowaną procedurą przełączenia.

5.2. Instalacja i przypisanie pamięci

- Instalacja na 2 serwerach w każdej szafie najnowszej stabilnej wersji Proxmox Backup Server (nie starszej niż 4.x) lub oprogramowania równoważnego, na lokalnych dyskach systemowych w konfiguracji mirror.
- Przypisanie pamięci: instancja podstawowa – datastore na NAS nr 1 danej szafy, instancja zapasowa – datastore na NAS nr 2 danej szafy.

5.3. Synchronizacja instancji

- Konfiguracja zadań synchronizacji (sync jobs) w kierunku pull – instancja zapasowa pobiera dane z instancji podstawowej – z harmonogramem nie rzadszym niż 1 dzień po zakończeniu okna kopii zapasowych.
- Opcja usuwania na instancji zapasowej kopii usuniętych na instancji podstawowej (remove vanished) musi być wyłączona, chyba że Zamawiający postanowi inaczej.

- Wykorzystanie dedykowanych kont/tokenów API o minimalnych wymaganych uprawnieniach dla każdego zadania synchronizacji.

5.4. Integracja z klastrem Proxmox VE

- Dodanie obu instancji jako magazynów kopii zapasowych w klastrze Proxmox VE danej szafy; zadania kopii zapasowych kierowane do instancji podstawowej.
- Opracowanie i przetestowanie procedury przełączenia zadań kopii zapasowych i odtwarzania na instancję zapasową.

5.5. Polityki kopii zapasowych

- Harmonogramy kopii zapasowych maszyn wirtualnych: 1 dzień.
- Polityka retencji (prune): 7 dziennych, 4 tygodniowe, 12 miesięcznych, 3 roczne.
- Cykliczne zadania odzyskiwania przestrzeni (garbage collection) oraz weryfikacji integralności kopii (verify).
- Szyfrowanie kopii zapasowych po stronie klienta; klucze szyfrujące (wraz z kopią w postaci papierowej lub kluczem głównym) Wykonawca przekaże Zamawiającemu w sposób bezpieczny, z protokołem.
- Powiadomienia e-mail o niepowodzeniu zadań kopii zapasowych, synchronizacji i weryfikacji.

6. Urządzenia NAS jako pamięć masowa

6.1. Konfiguracja urządzeń NAS

- Konfiguracja macierzy dyskowych w poziomie RAUD 5 z dyskiem zapasowym (hot spare), o ile pozwala na to liczba dysków.
- Wyłączenie zbędnych usług i funkcji (m.in. usług chmurowych i zdalnego dostępu producenta, UPnP, domyślnych kont administracyjnych), włączenie uwierzytelniania dwuskładnikowego, NTP, powiadomień e-mail i przekazywania logów (syslog).
- Włączenie migawek (snapshotów) wolumenów z kopiami zapasowymi z harmonogramem i retencją – w tym migawek niemodyfikowalnych (immutable), jeżeli urządzenie NAS to umożliwia.

6.2. Udostępnienie pamięci dla Proxmox Backup Server

- Utworzenie dla każdej instancji Proxmox Backup Server dedykowanego wolumenu udostępnionego w protokole iSCSI (preferowany; system plików ext4, XFS lub ZFS po stronie serwera) lub NFS (z dostępem ograniczonym do adresu IP danego serwera).
- Połączenie realizowane w dedykowanej sieci/VLAN kopii zapasowych. Zalecana przepustowość łącza: min. 10 Gb/s. W przypadku łączy o niższej przepustowości Wykonawca poinformuje Zamawiającego o wpływie na wydajność kopii zapasowych, odtwarzania i weryfikacji.

6.3. Kopie zapasowe wybranych maszyn fizycznych

- Zakres: maszyny fizyczne wskazane przez Zamawiającego (nazwa, system operacyjny, zakres danych, harmonogram).
- Maszyny z systemem Linux – kopie zapasowe wykonywane z wykorzystaniem klienta Proxmox Backup (proxmox-backup-client) lub równoważnego do instancji Proxmox Backup Server, z szyfrowaniem i automatycznym harmonogramem.
- Maszyny z systemem Windows i innymi systemami nieobsługiwanymi przez klienta Proxmox Backup – kopie zapasowe wykonywane na dedykowany udział sieciowy NAS (SMB 3 z szyfrowaniem/podpisywaniem), z wykorzystaniem natywnego narzędzia systemu operacyjnego, oprogramowania producenta NAS lub narzędzia wskazanego przez Zamawiającego, z wersjonowaniem i migawkami.
- Dostęp do udziałów z kopiami zapasowymi – z wykorzystaniem odrębnych kont dla każdej maszyny lub grupy maszyn, z minimalnymi uprawnieniami.
- Replikacja udziałów z kopiami maszyn fizycznych pomiędzy NAS nr 1 i NAS nr 2 w ramach danej szafy: (wymagana / niewymagana), o ile urządzenia NAS to umożliwiają.

7. Zabezpieczenie i monitoring systemów

- Zmiana wszystkich domyślnych haseł; utworzenie imiennych kont administracyjnych z rolami (RBAC) zgodnie z listą przekazaną przez Zamawiającego.
- Uwierzytelnianie dwuskładnikowe (TOTP/WebAuthn lub równoważne) dla interfejsów administracyjnych Proxmox VE, Proxmox Backup Server i NAS.
- Dostęp SSH wyłącznie z wykorzystaniem kluczy, bez logowania hasłem dla konta root; dostęp do interfejsów zarządzających ograniczony do sieci zarządzającej.
- Konfiguracja zapory sieciowej wbudowanej w Proxmox VE na poziomie centrum danych i hostów; ograniczenie dostępu do usług wyłącznie z wymaganych sieci.
- Instalacja aktualnych poprawek bezpieczeństwa na dzień odbioru.
- Przekazywanie logów systemowych i zdarzeń bezpieczeństwa do systemu SIEM Zamawiającego (syslog lub agent).
- Przekazanie Zamawiającemu wszystkich danych dostępowych w sposób bezpieczny (np. do menedżera haseł Zamawiającego), z protokołem.

8. Testy odbiorowe

Wykonawca przedstawi do akceptacji scenariusz testów, przeprowadzi testy w obecności przedstawiciela Zamawiającego i sporządzi protokół. Minimalny zakres testów (dla każdej szafy):

Lp.	Test	Kryterium akceptacji
1	Awaria węzła Proxmox VE (odłączenie zasilania)	Maszyny objęte HA uruchomione automatycznie na drugim węźle w czasie nie dłuższym niż 2 min
2	Awaria podstawowego łącza Corosync	Klaster zachowuje kworum, brak restartu węzłów
3	Niedostępność arbitra kworum (QDevice)	Klaster działa dalej z kworum, maszyny bez przerwy w pracy
4	Migracja maszyny wirtualnej na żywo (live migration)	Migracja bez przerwy w pracy maszyny
5	Kopia zapasowa i pełne odtworzenie maszyny wirtualnej	Maszyna odtworzona i uruchomiona poprawnie
6	Odtworzenie pojedynczego pliku z kopii maszyny wirtualnej	Plik odtworzony poprawnie
7	Synchronizacja i przełączenie instancji Proxmox Backup Server	Przy wyłączonej instancji podstawowej odtworzenie maszyny z instancji zapasowej oraz wykonanie nowej kopii zapasowej
8	Weryfikacja integralności kopii (verify)	Zakończona bez błędów

Lp.	Test	Kryterium akceptacji
9	Kopia zapasowa i odtworzenie danych maszyny fizycznej (Linux oraz Windows)	Wskazane dane odtworzone poprawnie
10	Odłączenie jednego toru zasilania (A lub B)	Wszystkie urządzenia pracują bez przerwy
11	Powiadomienia o awariach i niepowodzeniu zadań	Powiadomienia dostarczone na wskazane adresy e-mail

Wykryte nieprawidłowości Wykonawca usunie na własny koszt, a testy, których dotyczyły, zostaną powtórzone.

9. Dokumentacja powykonawcza

Wykonawca przekaże Zamawiającemu dokumentację powykonawczą w języku polskim, w formie elektronicznej (format edytowalny oraz PDF), obejmującą co najmniej:

- elewacje szaf, zestawienie połączeń (zasilających i sieciowych) oraz schemat fizyczny i logiczny sieci,
- adresację IP, sieci VLAN, nazwy hostów i zestawienie usług,
- opis konfiguracji klastrów Proxmox VE, HA, arbitra kworum, replikacji, Proxmox Backup Server, NAS oraz kopii zapasowych maszyn fizycznych;
- procedury eksploatacyjne: odtwarzanie maszyn wirtualnych, plików i danych maszyn fizycznych, przełączenie na zapasową instancję Proxmox Backup Server, aktualizacja klastra bez przerwy w pracy usług, kontrolowane wyłączenie i uruchomienie środowiska (kolejność), postępowanie w razie awarii węzła, NAS lub dysku;
- protokoły testów odbiorowych.

10. Szkolenie

- Szkolenie dla wskazanej liczby administratorów Zamawiającego, w siedzibie Zamawiającego, w wymiarze nie mniejszym niż 4 godziny, na wdrożonym środowisku.

- Zakres: administracja klastrem i HA, zarządzanie maszynami wirtualnymi, kopie zapasowe i odtwarzanie, synchronizacja i przełączenie Proxmox Backup Server, obsługa NAS, aktualizacje, monitoring i diagnostyka.

11. Gwarancja i wsparcie powdrożeniowe

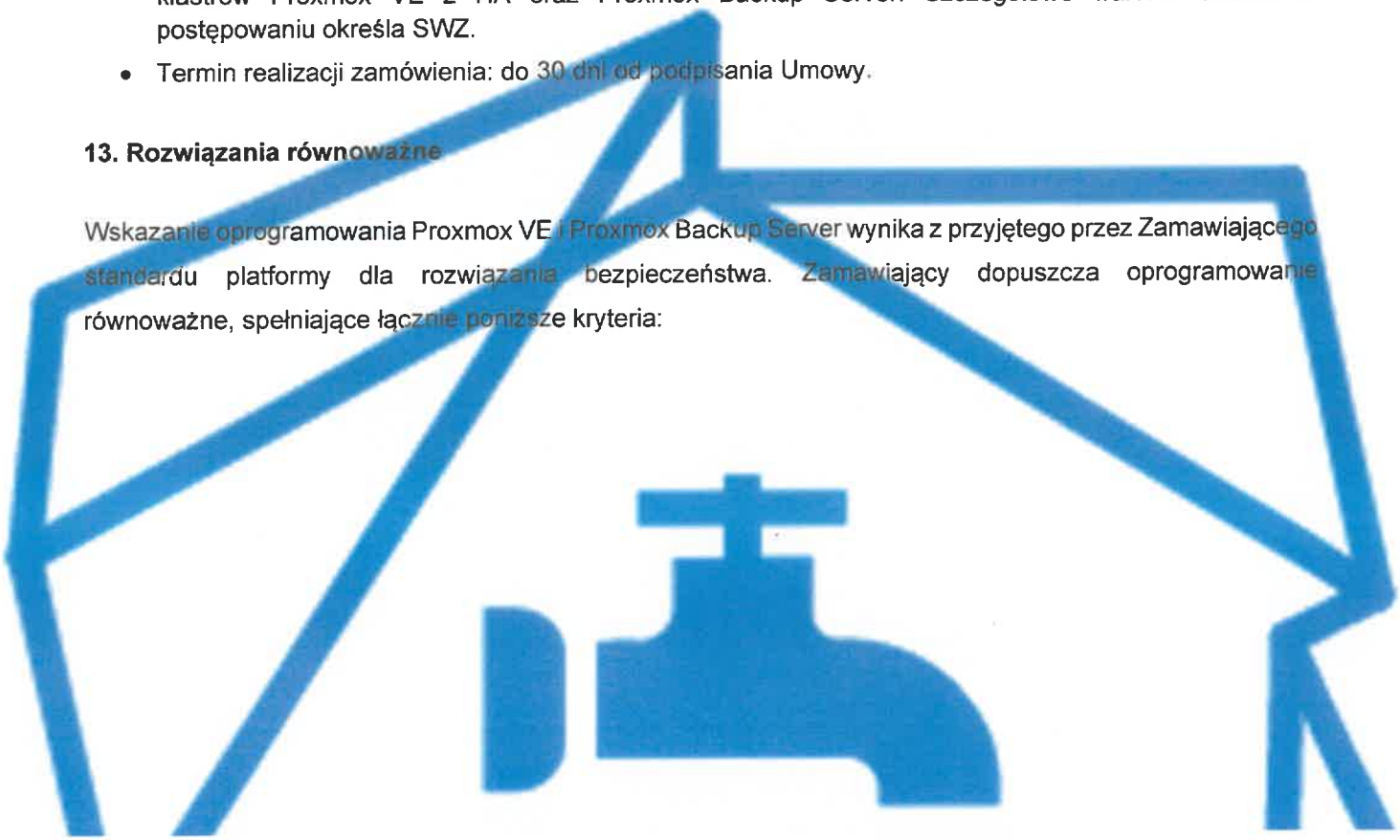
- Gwarancja na wykonane prace montażowe i konfiguracyjne: 24 miesięcy od dnia podpisania protokołu odbioru końcowego.
- Wsparcie techniczne w trybie 8/5 (dni robocze, 8:00–16:00) przez okres 36 miesięcy od odbioru, z czasem reakcji nie dłuższym niż 8 godzin roboczych; zgłoszenia przyjmowane drogą elektroniczną.

12. Organizacja prac

- Wykonawca przedstawi harmonogram prac w terminie 2 dni od dnia zawarcia umowy. Prace mogące wpływać na działanie istniejących systemów Zamawiającego będą prowadzone wyłącznie w uzgodnionych oknach serwisowych.
- Wykonawca przekaże listę osób realizujących prace w siedzibie Zamawiającego. Osoby te są zobowiązane do przestrzegania wewnętrznych regulaminów Zamawiającego, w tym zasad bezpieczeństwa fizycznego i informacji, oraz do zachowania poufności.
- Wykonawca ponosi odpowiedzialność za uszkodzenia sprzętu i infrastruktury Zamawiającego powstałe w wyniku realizacji prac.
- Prace konfiguracyjne prowadzone będą przez osobę posiadającą doświadczenie we wdrażaniu klastrów Proxmox VE z HA oraz Proxmox Backup Server. Szczegółowe warunki udziału w postępowaniu określa SWZ.
- Termin realizacji zamówienia: do 30 dni od podpisania Umowy.

13. Rozwiązania równoważne

Wskazanie oprogramowania Proxmox VE i Proxmox Backup Server wynika z przyjętego przez Zamawiającego standardu platformy dla rozwiązania bezpieczeństwa. Zamawiający dopuszcza oprogramowanie równoważne, spełniające łącznie poniższe kryteria:



Obszar	Kryteria równoważności
Platforma wirtualizacji (równoważna Proxmox VE)	Licencja niewymagająca opłat za korzystanie z pełnej funkcjonalności; hiperwizor obsługujący maszyny wirtualne i kontenery; wbudowany klaster z automatycznym ponownym uruchamianiem maszyn po awarii węzła w konfiguracji 2 węzły + zewnętrzny arbiter; replikacja maszyn pomiędzy węzłami bez pamięci współdzielonej; migracja na żywo; zarządzanie przez przeglądarkę, API i CLI; wbudowana zapora sieciowa; RBAC i uwierzytelnianie dwuskładnikowe; kompatybilność z rozwiązaniem bezpieczeństwa Zamawiającego.
System kopii zapasowych (równoważny Proxmox Backup Server)	Licencja niewymagająca opłat za korzystanie z pełnej funkcjonalności; kopie przyrostowe z deduplikacją; szyfrowanie po stronie klienta; weryfikacja integralności kopii; synchronizacja kopii pomiędzy instancjami; kopie maszyn wirtualnych z oferowanej platformy wirtualizacji oraz kopie hostów fizycznych z systemem Linux; odtwarzanie pojedynczych plików; polityki retencji; pełna integracja z platformą wirtualizacji.

Jeżeli w opisie przedmiotu zamówienia OPZ Zamawiający odnosi się do norm, europejskich Ocen technicznych, specyfikacji technicznych oraz innych systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp, to jest obowiązany wskazać, że dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu towarzyszą wyrazy lub „równoważne".

Wymienione w jakiejkolwiek części OPZ w zakresie dostaw urządzeń wraz z oprogramowaniem: nazwy własne, marki wyrobów, materiałów, technologii nie są obligatoryjne dla wykonawców. Wykonawca ma prawo do zaoferowania innych wyrobów, materiałów, technologii pod warunkiem zapewnienia parametrów technicznych co najmniej identycznych z parametrami określonymi w dokumentacji zamówienia (dopuszcza się dostawę przedmiotu zamówienia o wyższych parametrach technicznych).

Jeżeli OPZ wskazywałby w odniesieniu do niektórych materiałów, wyrobów i technologii znaki towarowe, patenty lub pochodzenie, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, w tym w szczególności podane zostały - nazwa własna materiału, wyrobu czy technologii, numer katalogowy lub producent, należy to traktować jako rozwiązanie przykładowe, określające standardy, wygląd oraz wymagania techniczne. Wszelkie materiały, urządzenia i technologie pochodzące od konkretnych producentów, określają minimalne parametry jakościowe i cechy użytkowe, jakim muszą odpowiadać materiały, urządzenia i technologie, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia, nie mają na celu uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów. Tak zastosowane zapisy są tylko w sytuacjach, gdy zamawiający nie był w stanie opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń - w tych wypadkach należy zawsze przyjąć sformułowanie " lub równoważny"

Zastosowane przez Wykonawcę materiały, wyroby i rozwiązania równoważne, muszą być co najmniej:

- o tej samej wytrzymałości i trwałości, o tym samym poziomie estetyki (wyroby),
- o parametrach technicznych opisanych w dokumentacji przetargowej,
- kompatybilne z istniejącą i projektowaną infrastrukturą,
- spełniać: te same funkcje, wymagania bezpieczeństwa konstrukcji, bhp i p. poż,
- posiadać stosowne dokumenty dopuszczające do stosowania w budownictwie (atesty i aprobaty techniczne).

Wykonawca musi udowodnić Zamawiającemu, że proponowany materiał, wyrób, technologia lub rozwiązanie jest równoważne, przedstawiając np. wszelkie dokumenty, obliczenia, opinie etc. potwierdzające równoważność.

Gminne Przedsiębiorstwo Komunalne
„EKO-BABICE"
spółka z ograniczoną odpowiedzialnością
05-082 Stare Babice, ul. Kutrzeby 36
tel./fax 22 752-90-08, 22 752-92-53
NIP 1231[illegible]152 Regon 016026808
BDO 000055262

Prezes Zarządu
Marcin Łasiński

