

## ZAPYTANIE CENOWE (rozeznanie rynku – oszacowanie wartości zamówienia)

### I. ZAMAWIAJĄCY

MIEJSKI ZAKŁAD GOSPODARKI KOMUNALNEJ SPÓŁKA Z OGRANICZONĄ  
ODPOWIEDZIALNOŚCIĄ

ul. Towarowa 2d

08-530 Dęblin

### II. CEL ZAPYTANIA

Niniejsze zapytanie ma na celu oszacowanie wartości zamówienia planowanego do realizacji w ramach projektu:

#### ***Podniesienie odporności cyfrowej infrastruktury wodociągowej w MZGK Sp. z o.o. w Dęblinie***

w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi.

Zapytanie nie stanowi oferty w rozumieniu Kodeksu cywilnego ani ogłoszenia o zamówieniu.

#### **Informacje ogólne o projekcie**

Miejski Zakład Gospodarki Komunalnej Sp. z o.o. z siedzibą w Dęblinie, planuje przeprowadzić działania w celu zwiększenia poziomu ochrony infrastruktury wodociągowej przed zagrożeniami cybernetycznymi. Projekt zakłada wdrożenie nowoczesnych rozwiązań z zakresu cyberbezpieczeństwa: monitoringu sieci teleinformatycznych, systemów wczesnego wykrywania incydentów oraz procedur reagowania na potencjalne ataki. Spółka planuje wdrożenie kompleksowego rozwiązania do monitorowania sieci przemysłowych i technologicznych (IDS dla OT), którego główna funkcjonalność zapewni bieżące monitorowanie sieci technologicznych pod kątem wykrywania anomalii w tym cyberzagrożeń, umożliwi inwentaryzację urządzeń sieciowych, badanie i zarządzanie podatnościami oraz monitorowanie kluczowych parametrów fizycznych procesów technologicznych.

Trwałość projektu wynosi 3 lata, w czasie których Spółka zobowiązana jest do utrzymania środków trwałych, usług nabytych w ramach projektu.

W związku z tym prosimy, aby w ofercie ująć osobno wykonanie przedmiotu zamówienia z gwarancją do końca roku oraz oddzielnie koszty utrzymania środków trwałych i usług nabytych w ramach Projektu przez 3 kolejne lata.

### III. SPOSÓB PRZYGOTOWANIA ODPOWIEDZI

Prosimy o przedstawienie:

- 1) Szacunkowej wartości netto realizacji zamówienia.
- 2) Wyszczególnienia (jeśli możliwe):
  - a) kosztów wdrożenia (jednorazowych),
  - b) kosztów utrzymania / asysty (rocznych),
  - c) krótkiego opisu proponowanego podejścia / technologii (opcjonalnie)

Dopuszcza się odpowiedź w formie np. e-mail.

### IV. OKRES UTRZYMANIA

Prosimy o uwzględnienie:

- 1) kosztów realizacji do końca roku,
- 2) kosztów utrzymania przez okres 3 lat (trwałość projektu)

### V. TERMIN PRZEKAZANIA INFORMACJI

Prosimy o przesłanie informacji do dnia: 14.05.2026 r.

### VI. SPOSÓB PRZEKAZANIA

Na adres e-mail: [przetargi@mzgk.pl](mailto:przetargi@mzgk.pl).

### VII. INFORMACJE DODATKOWE

1. Zamawiający dopuszcza rozwiązania równoważne.
2. Odpowiedzi mają charakter wyłącznie informacyjny.
3. Zapytanie nie zobowiązuje Zamawiającego do wszczęcia postępowania.

### VIII. OSOBA DO KONTAKTU

W zakresie IT: Sebastian Wilk, e-mail: [sebastian.w@mzgk.pl](mailto:sebastian.w@mzgk.pl), telefon: 502 371 163.

W zakresie OT: Marcin Kozak, e-mail: [mkozak@mzgk.pl](mailto:mkozak@mzgk.pl), telefon: 796 225 440.

## IX. OPIS PRZEDMIOTU ZAMÓWIENIA (ZAKRES ORIENTACYJNY)

### Pakiet 1, zadanie 1

- 1) Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym:
  - Polityka Bezpieczeństwa Informacji,
  - Polityka ochrony danych osobowych,
  - Polityka zarządzania systemem informatycznym,
  - Polityka zarządzania ciągłością działania,
  - Procedury zarządzania incydentami cyberbezpieczeństwa,
  - Przeprowadzenie Analizy Ryzyka Systemu Zarządzania Bezpieczeństwem Informacji,
  - Przygotowanie dokumentacji zgodnie z wymogami ustawy o KSC.
- 2) Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla STI, w tym:
  - identyfikacja procesów krytycznych oraz zasobów kluczowych (systemy IT, infrastruktura, dane, personel),
  - przeprowadzenie analizy wpływu na działalność (BIA) na potrzeby opracowania planów,
  - określenie scenariuszy awaryjnych i zakłóceń (w tym cyberincydentów),
  - zdefiniowanie strategii zapewnienia ciągłości działania oraz odtwarzania (RTO, RPO, poziomy usług),
  - opracowanie szczegółowych planów BCP i DRP (scenariusze, procedury krok po kroku),
  - opracowanie procedur reagowania, eskalacji oraz odtwarzania systemów i usług,
  - przygotowanie dokumentacji operacyjnej dla zespołów technicznych i biznesowych,
  - opracowanie scenariuszy testów planów BCP/DRP.
- 3) Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Ciągłością Działania (SZCD), w tym:
  - przeprowadzenie analizy stanu obecnego (GAP Analysis) w odniesieniu do norm i dobrych praktyk (w tym ISO 22301, NIS2),
  - identyfikacja procesów krytycznych oraz zależności organizacyjnych i technologicznych (na poziomie systemowym),
  - przeprowadzenie analizy ryzyka dla ciągłości działania,
  - opracowanie polityk, procedur oraz standardów w zakresie ciągłości działania,
  - zdefiniowanie ról, odpowiedzialności oraz struktur reagowania kryzysowego,
  - ustanowienie zasad utrzymania, przeglądu i aktualizacji planów BCP i DRP,
  - integracja SZCD z funkcjonującymi systemami zarządzania (w szczególności SZBI),
  - zaplanowanie i nadzór nad testami planów ciągłości działania (framework testów),
  - przeprowadzenie przeglądu zarządczego SZCD oraz opracowanie rekomendacji doskonalących,
  - zapewnienie mechanizmów cyklicznej aktualizacji, testowania i utrzymania SZCD.
- 4) Zakup, instalacja, konfiguracja i wdrożenie Systemu klasy GRC, w tym:
  - dostarczenie licencji lub rozwiązania (on-premise lub równoważnego) spełniającego wymagania Zamawiającego,
  - instalację i konfigurację systemu w infrastrukturze Zamawiającego,
  - konfigurację modułów systemu obejmujących co najmniej:
    - zarządzanie dokumentacją (polityki, procedury, instrukcje),

- zarządzanie ryzykiem,
- zarządzanie incydentami,
- zarządzanie ciągłością działania (BCP/DRP),
- rejestry (aktywa, ryzyka, incydenty, zgodność),
- odwzorowanie struktury organizacyjnej, ról i uprawnień użytkowników,
- konfigurację workflow (opracowanie, przegląd, zatwierdzanie, publikacja dokumentów),
- konfigurację mechanizmów powiadomień oraz eskalacji,
- zapewnienie możliwości raportowania, dashboardów oraz monitorowania poziomu zgodności,
- przeprowadzenie testów wdrożeniowych oraz uruchomienie produkcyjnego systemu,
- przygotowanie dokumentacji powdrożeniowej oraz instrukcji użytkownika i administratora,
- przeprowadzenie szkoleń dla użytkowników i administratorów systemu,
- zapewnienie wsparcia powdrożeniowego oraz asysty technicznej,
- szkolenie dla administratorów – system GRC.

#### Pakiet 1, zadanie 2

- 1) Szkolenia z zakresu cyberbezpieczeństwa szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony **dla pracowników IT/OT/ICS**:
  - Szkolenia stacjonarne – 2 cykle szkoleniowe w grupach (max. 30 – 40 osób),
  - Szkolenia on-line na platformie szkoleniowej w postaci webinarów dostępnych na czas trwania projektu jako uzupełnienie szkoleń stacjonarnych – 2 zestawy szkoleń.
- 2) Szkolenia z zakresu cyberbezpieczeństwa – **szkolenia dla kadry**, istotne z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji IT/OT/ICS
  - Szkolenia stacjonarne – 1 cykl szkoleniowy w grupach (max. 20 – 30 osób),
  - Szkolenia on-line na platformie szkoleniowej w postaci webinarów dostępnych na czas trwania projektu jako uzupełnienie szkoleń stacjonarnych – 1 zestaw szkoleń.

#### Pakiet 2, zadanie 1

- 1) Audyt SZBI i SZCD przez wykwalifikowanych audytorów na zgodność z normami IT/OT/ICS, w tym:
  - przeprowadzenie audytu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
  - przeprowadzenie audytu Systemu Zarządzania Ciągłością Działania (SZCD),
  - przeprowadzenie audytów bezpieczeństwa w środowiskach IT oraz OT/ICS (w tym systemów sterowania przemysłowego),
  - identyfikację niezgodności, podatności oraz obszarów do doskonalenia,
  - opracowanie raportów z audytów zawierających ocenę zgodności, poziomu dojrzałości oraz rekomendacje działań naprawczych,
  - przedstawienie wyników audytów kadrze zarządzającej,
  - wsparcie w opracowaniu planów działań korygujących i doskonalących,
  - weryfikację wdrożenia zaleceń poaudytowych (audyt sprawdzający).
- 2) Audyt zgodności SZBI i SZCD z uoKSC przez wykwalifikowanych audytorów  
Przedmiotem zamówienia jest przeprowadzenie audytu zgodności systemów informacyjnych oraz procesów Zamawiającego z wymaganiami ustawy o Krajowym Systemie Cyberbezpieczeństwa, obejmującego w szczególności:

- analizę zgodności organizacji z wymaganiami określonymi w uoKSC (w tym w zakresie bezpieczeństwa informacji),
- przegląd polityk, procedur oraz dokumentacji (m.in. SZBI, SZCD, procedury bezpieczeństwa),
- ocenę stosowanych środków technicznych i organizacyjnych,
- analizę zarządzania dostępem, tożsamością oraz uprawnieniami użytkowników,
- ocenę mechanizmów zapewnienia ciągłości działania oraz odtwarzania po awarii,
- analizę zabezpieczeń infrastruktury IT oraz – w uzasadnionym zakresie – OT/ICS,
- ocenę sposobu zarządzania incydentami bezpieczeństwa,
- weryfikację prowadzenia rejestrów (np. aktywów, incydentów, ryzyk),
- identyfikację niezgodności oraz luk w stosunku do wymagań uoKSC,
- opracowanie raportu z audytu zawierającego:
  - ocenę poziomu zgodności,
  - wykaz niezgodności,
  - rekomendacje działań naprawczych i doskonalących,
- przedstawienie wyników audytu Zamawiającemu,
- wsparcie w opracowaniu planu działań naprawczych.

### Pakiet 3, zadanie 1

- 1) Przeprowadzenie **testów bezpieczeństwa infrastruktury sieciowej** Zamawiającego w obszarach IT, OT/ICS oraz IIoT, z wykorzystaniem narzędzi klasy vulnerability scanner (np. Tenable/Nessus lub równoważnych), obejmujących w szczególności:
  - identyfikację i inwentaryzację zasobów sieciowych podlegających testom (urządzenia, systemy, usługi),
  - przeprowadzenie skanowania podatności infrastruktury sieciowej oraz systemów informatycznych,
  - analizę konfiguracji systemów, usług oraz urządzeń sieciowych pod kątem bezpieczeństwa,
  - identyfikację podatności, błędów konfiguracyjnych oraz potencjalnych wektorów ataku,
  - klasyfikację podatności według poziomu ryzyka (np. CVSS) oraz ich wpływu na działalność Zamawiającego,
  - uwzględnienie specyfiki środowisk OT/ICS (testy nieinwazyjne, bez wpływu na ciągłość działania systemów sterowania),
  - opracowanie raportów z testów zawierających wyniki, ocenę ryzyka oraz rekomendacje działań naprawczych,
  - przedstawienie wyników testów oraz omówienie rekomendacji z Zamawiającym,
  - wsparcie w planowaniu działań remediacyjnych oraz ponowna weryfikacja po ich wdrożeniu (retest).
- 2) Przeprowadzenie **testów bezpieczeństwa stron www i platform internetowych** wykorzystywanych przez Zamawiającego w obszarach IT, OT/ICS oraz IIoT, obejmujących w szczególności:
  - identyfikację i klasyfikację aplikacji objętych testami (webowych, mobilnych, desktopowych, systemów sterowania i aplikacji przemysłowych),
  - przeprowadzenie testów bezpieczeństwa aplikacji (w tym testów typu SAST/DAST oraz testów manualnych),
  - analizę mechanizmów uwierzytelniania, autoryzacji oraz zarządzania sesją,
  - weryfikację zabezpieczeń komunikacji (np. TLS, API, integracje między systemami),
  - identyfikację podatności (m.in. OWASP Top 10, błędy logiczne, podatności w interfejsach API),
  - analizę konfiguracji aplikacji oraz środowisk uruchomieniowych,

- uwzględnienie specyfiki środowisk OT/ICS (testy kontrolowane, niezakłócające pracy systemów produkcyjnych),
- klasyfikację podatności według poziomu ryzyka (np. CVSS) oraz ich wpływu na działalność Zamawiającego,
- opracowanie raportów z testów zawierających wyniki, scenariusze ataków oraz rekomendacje działań naprawczych,
- przedstawienie wyników testów oraz omówienie rekomendacji z Zamawiającym,
- wsparcie w procesie usuwania podatności oraz ponowna weryfikacja (retest).

### 3) Testy bezpieczeństwa aplikacji IT/OT/ICS/IIoT

Przeprowadzenie testów bezpieczeństwa aplikacji wykorzystywanych przez Zamawiającego w obszarach IT, OT/ICS oraz IIoT, obejmujących w szczególności:

- identyfikację i klasyfikację aplikacji objętych testami (webowych, API, desktopowych, mobilnych oraz aplikacji systemów przemysłowych),
- przeprowadzenie testów bezpieczeństwa obejmujących:
  - testy dynamiczne (DAST),
  - testy statyczne (SAST – jeżeli dostęp do kodu),
  - testy manualne (pentesty aplikacyjne),
- analizę mechanizmów uwierzytelniania, autoryzacji oraz zarządzania sesją,
- weryfikację bezpieczeństwa interfejsów API oraz integracji między systemami,
- identyfikację podatności (m.in. OWASP Top 10, błędy logiczne, błędy autoryzacji),
- analizę konfiguracji aplikacji oraz środowisk uruchomieniowych,
- uwzględnienie specyfiki środowisk OT/ICS (testy kontrolowane, niezakłócające pracy systemów produkcyjnych),
- klasyfikację podatności według poziomu ryzyka (np. CVSS) oraz ich wpływu na działalność Zamawiającego,
- opracowanie raportów z testów zawierających:
  - opis podatności,
  - scenariusze ataku,
  - rekomendacje działań naprawczych,
- przedstawienie wyników testów oraz omówienie rekomendacji z Zamawiającym,
- wsparcie w procesie usuwania podatności oraz przeprowadzenie testów weryfikacyjnych (retest).

### 4) Usługa inwentaryzacji aktywów teleinformatycznych IT/OT/ICS/IIoT

Usługa ma na celu inwentaryzację wszystkich zasobów IT/OT/ICS/IIoT dla potrzeb stworzenia i wdrożenia polityk obowiązujących operatorów usług kluczowych.

## Pakiet 3, zadanie 2

### 1) Dostawa, konfiguracja oraz uruchomienie **urządzeń klasy UTM** (Unified Threat Management) stanowiących zabezpieczenie łącz sieciowych w lokalizacji głównej i lokalizacjach dodatkowych Zamawiającego, obejmujące w szczególności:

- dostawę **2 urządzeń** klasy UTM pracujących w trybie HA jako zabezpieczenie łącza głównego wraz z niezbędnymi licencjami i subskrypcjami bezpieczeństwa (np. pakiet Unified Threat Protection lub równoważny) z zapewnieniem funkcjonalności co najmniej równoważnych do urządzeń klasy FortiGate-60F, w tym:
  - a) zaporę sieciową (Firewall) nowej generacji (NGFW),
  - b) system zapobiegania włamaniom (IPS),
  - c) ochrona przed złośliwym oprogramowaniem (antywirus, sandboxing lub równoważne),
  - d) filtrowanie treści WWW (URL filtering, DNS filtering),
  - e) kontrola aplikacji (Application Control),



- f) ochrona antyspamowa,
  - g) obsługa bezpiecznych połączeń VPN (site-to-site oraz zdalny dostęp),
  - h) zapewnienie centralnego zarządzania oraz monitorowania zdarzeń bezpieczeństwa,
  - i) konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
  - j) integrację z istniejącą infrastrukturą sieciową oraz systemami bezpieczeństwa,
  - k) wdrożenie mechanizmów aktualizacji sygnatur oraz baz zagrożeń,
  - l) uruchomienie i testy poprawności działania w środowisku produkcyjnym,
  - m) przygotowanie dokumentacji powdrożeniowej (schematy, konfiguracja, polityki),
  - n) zapewnienie wsparcia technicznego producenta (np. klasy FortiCare Premium lub równoważnego) przez okres minimum 12 miesięcy.
- dostawę **3 urządzeń** klasy FortiGate-30G jako zabezpieczenie łącza zdalnego pracującego w trybie site-to-site z łączem głównym:
    - a) zaporę sieciową (Firewall) nowej generacji (NGFW),
    - b) system zapobiegania włamaniom (IPS),
    - c) obsługa bezpiecznych połączeń VPN (site-to-site oraz zdalny dostęp),
    - d) zapewnienie centralnego zarządzania oraz monitorowania zdarzeń bezpieczeństwa,
    - e) konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
    - f) integrację z istniejącą infrastrukturą sieciową oraz systemami bezpieczeństwa,
    - g) wdrożenie mechanizmów aktualizacji sygnatur oraz baz zagrożeń,
    - h) uruchomienie i testy poprawności działania w środowisku produkcyjnym,
    - i) przygotowanie dokumentacji powdrożeniowej (schematy, konfiguracja, polityki),
  - zapewnienie wsparcia technicznego producenta (np. klasy FortiCare Premium lub równoważnego) przez okres minimum 12 miesięcy,
  - przeszkolenie administratorów z zakresu obsługi i zarządzania systemem.
2. Dostawa **3 przełączników sieciowych**, zarządzalnych (L2/L3)
- a) minimalne parametry techniczne:
    - min. 24 porty 10/100/1000BASE-T,
    - min. 4 porty uplink SFP/SFP+ (1/2.5G lub równoważne),
    - obsługa VLAN (IEEE 802.1Q),
    - obsługa uwierzytelniania portowego 802.1X (integracja z NAC/RADIUS),
    - obsługa szyfrowania ruchu na poziomie warstwy 2 (MACsec – IEEE 802.1AE),
  - b) zapewnienie funkcjonalności bezpieczeństwa i zarządzania:
    - segmentacja sieci (VLAN),
    - kontrola dostępu do portów (ACL),
    - ochrona przed atakami warstwy 2 (np. DHCP snooping, ARP inspection, BPDU guard lub równoważne),
    - QoS (priorytetyzacja ruchu),
  - c) integrację z systemem NAC oraz istniejącą infrastrukturą sieciową Zamawiającego,
  - d) możliwość centralnego zarządzania i monitorowania (CLI/GUI/SNMP lub równoważne),
  - e) konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
  - f) przygotowanie dokumentacji powdrożeniowej (schematy sieci, konfiguracja VLAN, polityki dostępu),
  - g) przeprowadzenie testów poprawności działania (w tym 802.1X, VLAN, segmentacja),
  - h) przeszkolenie administratorów w zakresie zarządzania przełącznikami,
  - i) zapewnienie wsparcia technicznego producenta przez okres minimum 12 miesięcy.
- 3) Dostawa, instalacja oraz konfiguracja **15 zarządzalnych przełączników sieciowych** (switchy) przeznaczonych do lokalizacji o ograniczonej liczbie urządzeń, zapewniających bezpieczną komunikację oraz kontrolę dostępu do sieci, obejmujących w szczególności:

- dostawę przełączników zarządzalnych o parametrach co najmniej:
    - **min. 5 portów** 10/100/1000BASE-T,
  - zapewnienie funkcjonalności bezpieczeństwa:
    - obsługa VLAN (IEEE 802.1Q),
    - obsługa uwierzytelniania portowego 802.1X (integracja z NAC/RADIUS),
    - obsługa szyfrowania ruchu MACsec (IEEE 802.1AE) lub równoważnego mechanizmu zabezpieczenia komunikacji,
  - zapewnienie podstawowych mechanizmów zarządzania i ochrony:
    - kontrola dostępu do portów (ACL),
    - ochrona warstwy 2 (np. DHCP snooping, ARP inspection lub równoważne),
    - możliwość zarządzania poprzez interfejs WWW/CLI/SNMP,
    - integrację z systemem NAC oraz istniejącą infrastrukturą sieciową Zamawiającego,
    - konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
  - przygotowanie dokumentacji powdrożeniowej (schematy połączeń, konfiguracja VLAN i polityk dostępu),
  - przeprowadzenie testów poprawności działania (w tym 802.1X i segmentacja VLAN),
  - przeszkolenie administratorów w zakresie zarządzania urządzeniami,
  - zapewnienie wsparcia technicznego producenta przez okres minimum 12 miesięcy.
- 4) Dostawa, instalacja oraz konfiguracja **8 Przemysłowych przełączników PoE Switch** (switchy) przeznaczonych do lokalizacji o ograniczonej liczbie urządzeń, zapewniających bezpieczną komunikację oraz kontrolę dostępu do sieci, obejmujących w szczególności:
- dostawę przełączników zarządzalnych o parametrach co najmniej:
    - a) min. 4 portów 10/100/1000BASE-T,
    - b) zapewnienie funkcjonalności bezpieczeństwa:
      - obsługa VLAN (IEEE 802.1Q),
      - obsługa uwierzytelniania portowego 802.1X (integracja z NAC/RADIUS),
      - obsługa szyfrowania ruchu MACsec (IEEE 802.1AE) lub równoważnego mechanizmu zabezpieczenia komunikacji,
    - c) zapewnienie podstawowych mechanizmów zarządzania i ochrony:
      - kontrola dostępu do portów (ACL),
      - ochrona warstwy 2 (np. DHCP snooping, ARP inspection lub równoważne),
    - d) możliwość zarządzania poprzez interfejs WWW/CLI/SNMP,
    - e) integrację z systemem NAC oraz istniejącą infrastrukturą sieciową Zamawiającego,
    - f) możliwość montażu na szynie DIN lub montaż ścienny,
    - g) Wilgotność: 5%~90%,
    - h) Temperatura pracy: -40+85 °C,
  - konfigurację urządzeń zgodnie z polityką bezpieczeństwa Zamawiającego,
  - przygotowanie dokumentacji powdrożeniowej (schematy połączeń, konfiguracja VLAN i polityk dostępu),
  - przeprowadzenie testów poprawności działania (w tym 802.1X i segmentacja VLAN),
  - przeszkolenie administratorów w zakresie zarządzania urządzeniami,
  - zapewnienie wsparcia technicznego producenta przez okres minimum 12 miesięcy.
- 5) **Zaprojektowanie, wdrożenie oraz uruchomienie segmentacji sieci** Zamawiającego w obszarach IT, OT/ICS oraz IIoT, w celu zwiększenia poziomu bezpieczeństwa, ograniczenia rozprzestrzeniania się incydentów oraz zapewnienia zgodności z wymaganiami regulacyjnymi (m.in. NIS2), obejmujące w szczególności:
- przeprowadzenie analizy stanu obecnego infrastruktury sieciowej (IT/OT/ICS/IIoT),



- identyfikację zasobów, systemów oraz przepływów komunikacyjnych (mapowanie ruchu),
- klasyfikację systemów i stref bezpieczeństwa (np. model Purdue lub równoważny),
- opracowanie architektury segmentacji sieci (strefy, podsieci, VLAN, strefy bezpieczeństwa),
- zaprojektowanie zasad komunikacji między segmentami (reguły firewall, ACL, mikrosegmentacja),
- wdrożenie segmentacji logicznej (VLAN, routing, ACL) oraz – w uzasadnionych przypadkach – fizycznej separacji sieci,
- integrację segmentacji z systemami bezpieczeństwa (UTM, NAC, systemy monitorowania),
- konfigurację mechanizmów kontroli dostępu do sieci (802.1X, NAC, przypisywanie do VLAN),
- wdrożenie zasad ograniczania ruchu między strefami IT i OT (kontrola komunikacji, dostęp uprzywilejowany),
- przeprowadzenie testów poprawności działania segmentacji oraz odporności na nieautoryzowany dostęp,
- opracowanie dokumentacji powdrożeniowej (architektura, schematy, polityki komunikacji),
- przeszkolenie administratorów w zakresie zarządzania segmentacją,
- opracowanie wytycznych utrzymania i dalszego rozwoju segmentacji,
- zapewnienie wsparcia technicznego producenta przez okres minimum 12 miesięcy.

### Pakiet 3, zadanie 3

- 1) Dostawa, instalacja oraz konfiguracja **2 macierzy dyskowych typu NAS** (Network Attached Storage), jako części klastra HA, przeznaczonych do realizacji kopii zapasowych danych Zamawiającego, obejmujących w szczególności:
  - dostawę urządzenia klasy NAS w obudowie rack wraz z niezbędnymi komponentami (np. dyski, karty sieciowe, szyny montażowe) o łącznej pojemności użytkowej min. 30 TB,
  - zapewnienie rozwiązania co najmniej równoważnego do:
    - a) 2 x urządzenie,
    - b) 2 x zestaw montażowy rack (szyny),
    - c) dyski klasy enterprise,
    - d) 2 x karta sieciowa 10 GbE (np. 2-portowa lub równoważna),
  - instalację i konfigurację macierzy w infrastrukturze Zamawiającego,
  - konfigurację macierzy dyskowych (RAID, wolumeny, przestrzeń backupowa),
  - zapewnienie wysokiej dostępności i odporności na awarie (np. RAID, replikacja, snapshoty),
  - konfigurację usług sieciowych (SMB/NFS/iSCSI) oraz integrację z infrastrukturą IT Zamawiającego,
  - integrację z systemami backupu (np. oprogramowanie do kopii zapasowych, systemy wirtualizacji),
  - zapewnienie mechanizmów ochrony danych (snapshoty, wersjonowanie, ochrona przed ransomware),
  - konfigurację monitoringu, alertów oraz raportowania stanu systemu,
  - przygotowanie dokumentacji powdrożeniowej (konfiguracja, schematy, polityki backupu),
  - przeprowadzenie testów odtwarzania danych (restore),
  - przeszkolenie administratorów z zakresu obsługi i zarządzania systemem,
  - zapewnienie wsparcia technicznego producenta przez okres minimum 12 miesięcy.
- 2) Dostawa, instalacja oraz konfiguracja **1 serwera fizycznego przeznaczonego do uruchomienia** systemów bezpieczeństwa oraz usług wysokiej dostępności (HA), obejmującego w szczególności:
  - dostawę 1 serwera klasy enterprise (rack 1U/2U) o parametrach:

- procesor klasy serwerowej min. 1 x Intel Xeon Gold (np. 5318Y lub równoważny, min. 24 rdzenie),
- pamięć RAM min. 256 GB (np. 8 x 32 GB DDR4 lub równoważne),
- dyski SSD NVMe klasy enterprise o łącznej pojemności min. 3–4 TB (np. 1.92 TB x 2 lub równoważne),
- kontroler dyskowy RAID/NVMe (sprzętowy lub równoważny),
- karta sieciowa min. 2 x 10 Gb SFP+,
- zapewnienie redundancji komponentów:
  - zasilacze redundantne (hot-plug),
  - możliwość pracy w klastrze wysokiej dostępności (HA),
- instalację i konfigurację serwera w środowisku Zamawiającego,
- przygotowanie środowiska pod wdrożenie systemów bezpieczeństwa (np. GRC, NAC, sandbox, systemy monitoringu),
- konfigurację wirtualizacji (jeżeli dotyczy) oraz przygotowanie zasobów dla usług HA,
- integrację z istniejącą infrastrukturą sieciową i storage,
- konfigurację monitoringu sprzętu (np. iLO lub równoważne),
- przygotowanie dokumentacji powdrożeniowej (konfiguracja, schematy, zasoby),
- przeprowadzenie testów poprawności działania oraz scenariuszy HA (jeżeli wdrażane),
- przeszkolenie administratorów,
- zapewnienie wsparcia technicznego producenta przez okres minimum 12 miesięcy.

3) Rozbudowa istniejącego serwera Dell PowerEdge R760xs o przestrzeń dyskową SSD obejmująca w szczególności:

- dostawę i montaż dysków SSD klasy enterprise o łącznej pojemności min. 4 TB (pojemność użytkowa zależna od konfiguracji RAID),
- zapewnienie kompatybilności dostarczonych komponentów z posiadanym serwerem (interfejs SAS/SATA/NVMe, kontroler RAID, kieszenie dyskowe),
- konfigurację macierzy dyskowej (np. RAID1/RAID10 – zgodnie z wymaganiami Zamawiającego),
- integrację nowych dysków z istniejącą infrastrukturą serwera (kontroler RAID, system operacyjny, wirtualizacja),
- aktualizację firmware, BIOS oraz kontrolera RAID (jeżeli wymagane),
- przeprowadzenie testów poprawności działania oraz wydajności,
- przygotowanie dokumentacji powdrożeniowej (konfiguracja, schematy, parametry),
- dostawę i montaż pamięci RAM klasy serwerowej o łącznej pojemności min. 128 GB,
- zapewnienie kompatybilności modułów RAM z posiadanym serwerem (typ, taktowanie, architektura, lista kompatybilności producenta),
- zastosowanie pamięci typu ECC Registered (RDIMM) lub równoważnej, przeznaczonej do pracy w środowiskach serwerowych,
- dostosowanie konfiguracji pamięci do architektury serwera (np. optymalne rozmieszczenie modułów w kanałach pamięci),
- integrację nowej pamięci z istniejącą konfiguracją sprzętową,
- aktualizację firmware/BIOS (jeżeli wymagane),
- przeprowadzenie testów poprawności działania oraz stabilności systemu,
- przygotowanie dokumentacji powdrożeniowej (konfiguracja, rozmieszczenie modułów).

4) Dostawa, wdrożenie oraz **uruchomienie oprogramowania do wykonywania i zarządzania kopiami zapasowymi** danych (backup), obejmującego w szczególności:

- a) dostawę licencji oprogramowania do wykonywania kopii zapasowych dla serwerów oraz stacji roboczych,
  - b) instalację i konfigurację systemu backupu w infrastrukturze Zamawiającego,
  - c) zapewnienie funkcjonalności wykonywania kopii zapasowych:
    - pełnych, przyrostowych i różnicowych,
    - z mechanizmami deduplikacji i kompresji danych,
    - obsługę środowisk fizycznych i wirtualnych (w tym systemów serwerowych i stacji roboczych),
    - możliwość wykonywania kopii zapasowych systemów plików, baz danych oraz maszyn wirtualnych,
    - integrację z macierzami NAS oraz istniejącą infrastrukturą IT Zamawiającego,
    - możliwość harmonogramowania zadań backupu oraz zarządzania politykami retencji danych,
    - zapewnienie mechanizmów ochrony przed ransomware (np. immutable backup, wersjonowanie, separacja kopii),
    - szyfrowanie danych w trakcie transmisji i przechowywania,
    - możliwość centralnego zarządzania kopiami zapasowymi (konsola zarządzająca),
    - monitorowanie procesu backupu oraz generowanie raportów i alertów,
    - możliwość odtwarzania danych na poziomie:
      - plików,
      - systemów,
      - maszyn wirtualnych,
  - d) przeprowadzenie testów odtwarzania danych (restore),
  - e) przygotowanie dokumentacji powdrożeniowej (polityki backupu, procedury odtwarzania),
  - f) przeszkolenie administratorów w zakresie obsługi systemu,
  - g) zapewnienie wsparcia technicznego oraz aktualizacji przez okres minimum 12 miesięcy.
- 5) Dostawa, instalacja oraz konfiguracja **systemu archiwizacji danych opartego o bibliotekę taśmową** (streamer), przeznaczonego do długoterminowego przechowywania kopii zapasowych, obejmującego w szczególności:
- a) dostawę biblioteki taśmowej (autoloadera) wraz z napędem LTO-8 SAS lub równoważnym, o parametrach co najmniej:
    - min. 8 slotów na nośniki taśmowe,
    - obsługa pojemności do min. 120 TB (po kompresji lub równoważnej),
  - b) dostawę odpowiedniej liczby nośników (kaset) taśmowych umożliwiających realizację polityki backupu Zamawiającego,
  - c) instalację i konfigurację urządzenia w infrastrukturze Zamawiającego,
  - d) integrację z oprogramowaniem do wykonywania kopii zapasowych,
  - e) konfigurację polityk archiwizacji danych (retencja, rotacja nośników, harmonogramy),
  - f) zapewnienie mechanizmów szyfrowania danych zapisywanych na nośnikach,
  - g) konfigurację zarządzania nośnikami (oznaczenia, ewidencja, rotacja, przechowywanie off-site),
  - h) przeprowadzenie testów zapisu i odczytu danych (backup/restore),
  - i) przygotowanie dokumentacji powdrożeniowej (konfiguracja, procedury obsługi, polityki archiwizacji),
  - j) przeszkolenie administratorów w zakresie obsługi i zarządzania biblioteką taśmową,
  - k) zapewnienie wsparcia technicznego producenta przez okres minimum 12 miesięcy.

- 6) Dostawa, wdrożenie oraz uruchomienie **systemu wirtualizacyjnego** przeznaczonego do hostowania systemów z zakresu cyberbezpieczeństwa, obejmującego w szczególności:
- dostawę licencji oraz wdrożenie platformy wirtualizacyjnej (np. VMware, Proxmox, Hyper-V lub rozwiązanie równoważne) na 2 serwerach fizycznych,
  - instalację i konfigurację środowiska wirtualizacyjnego na dostarczonej infrastrukturze serwerowej,
  - utworzenie i konfigurację maszyn wirtualnych dla systemów bezpieczeństwa (np. SIEM, NAC, GRC, sandbox, system backupu),
  - zapewnienie mechanizmów wysokiej dostępności (HA) oraz automatycznego restartu usług (w przypadku dostępności infrastruktury wieloserwerowej),
  - konfigurację zarządzania zasobami (CPU, RAM, storage) oraz izolacji środowisk,
  - integrację z systemami storage (NAS, backup) oraz siecią (VLAN, segmentacja),
  - zapewnienie mechanizmów snapshotów, backupu maszyn wirtualnych oraz ich odtwarzania,
  - konfigurację sieci wirtualnych (vSwitch, VLAN tagging, segmentacja ruchu),
  - integrację z systemami bezpieczeństwa i zarządzania (np. AD, SIEM),
  - przygotowanie dokumentacji powdrożeniowej (architektura, konfiguracja, przydział zasobów),
  - przeprowadzenie testów poprawności działania środowiska (w tym testów odtwarzania i HA – jeżeli dotyczy),
  - przeszkolenie administratorów w zakresie zarządzania środowiskiem,
  - zapewnienie wsparcia technicznego i aktualizacji przez okres minimum 12 miesięcy.
- 7) Dostawa licencji, instalacja oraz konfiguracja **systemu operacyjnego serwerowego** wraz z wdrożeniem usług katalogowych i sieciowych, obejmujących w szczególności:
- dostawę **2 licencji** systemu operacyjnego klasy Microsoft Windows Server (np. Windows Server 2025 Standard 16 Core lub równoważnego),
  - dostawę **50 licencji CAL**,
  - instalację i konfigurację systemu operacyjnego na wskazanej infrastrukturze serwerowej,
  - wdrożenie usług katalogowych (Active Directory Domain Services – AD DS),
  - wdrożenie usług DNS (Domain Name System),
  - wdrożenie usług DHCP (Dynamic Host Configuration Protocol),
  - konfigurację struktury domenowej (OU, grupy, polityki GPO),
  - integrację z systemami bezpieczeństwa i zarządzania (m.in. NAC, SIEM, systemy backupu),
  - konfigurację uwierzytelniania i autoryzacji użytkowników oraz urządzeń w sieci,
  - wdrożenie mechanizmów bezpieczeństwa (polityki hasel, kontrola dostępu, audyt logowania),
  - przygotowanie dokumentacji powdrożeniowej (architektura AD, konfiguracja usług),
  - przeprowadzenie testów poprawności działania usług (logowanie, przydział adresów DHCP, rozwiązywanie nazw DNS),
  - przeszkolenie administratorów,
  - zapewnienie wsparcia technicznego oraz aktualizacji przez okres minimum 12 miesięcy.

#### Pakiet 3, zadanie 4

- 1) Dostawa, wdrożenie i uruchomienie **systemu kontroli dostępu** do sieci klasy NAC (Network Access Control) dla **150 endpoint devices**, obejmującego w szczególności:
- dostawę licencji oraz wdrożenie oprogramowania klasy NAC,
  - instalację i konfigurację rozwiązania w środowisku Zamawiającego (np. wirtualizacja / VM),
  - identyfikację i kontrolę urządzeń podłączanych do sieci (profilowanie urządzeń, klasyfikacja, polityki dostępu),

- egzekwowanie polityk dostępu do sieci (802.1X, uwierzytelnianie użytkowników i urządzeń, segmentacja),
  - integrację z usługami katalogowymi (np. Active Directory) oraz infrastrukturą sieciową (przełączniki, punkty dostępowe, firewalle),
  - monitorowanie urządzeń końcowych oraz wykrywanie nieautoryzowanych lub niezgodnych urządzeń,
  - możliwość kwarantanny urządzeń niespełniających wymagań bezpieczeństwa,
  - rejestrowanie zdarzeń i generowanie raportów na potrzeby audytów i zgodności (np. NIS2),
  - konfigurację ról i polityk dostępu zgodnie z polityką bezpieczeństwa Zamawiającego,
  - przygotowanie dokumentacji powdrożeniowej i przeszkolenie administratorów,
  - zapewnienie wsparcia technicznego i aktualizacji przez okres minimum 12 miesięcy,
  - przeszkolenie administratorów z zakresu obsługi i zarządzania systemem.
- 2) Dostawa, wdrożenie oraz uruchomienie **systemu klasy SIEM** (Security Information and Event Management) służącego do centralnego zbierania, korelacji i analizy zdarzeń bezpieczeństwa, obejmującego w szczególności:
- dostawę licencji systemu **SIEM dla min. 100 zasobów** (assets),
  - instalację i konfigurację systemu w infrastrukturze Zamawiającego (on-premise lub równoważne),
  - integrację z systemami i urządzeniami Zamawiającego, w szczególności:
    - a) urządzeniami sieciowymi (UTM, przełączniki),
    - b) systemami NAC,
    - c) systemami serwerowymi i stacjami roboczymi,
    - d) systemami OT/ICS (jeżeli dostępne logi),
    - e) centralizację logów oraz ich bezpieczne przechowywanie,
    - f) konfigurację reguł korelacyjnych i scenariuszy detekcji incydentów bezpieczeństwa,
    - g) monitorowanie zdarzeń w czasie rzeczywistym oraz generowanie alertów,
    - h) zapewnienie dashboardów, raportów oraz wizualizacji zdarzeń bezpieczeństwa,
    - i) możliwość spełnienia wymagań raportowych wynikających z przepisów (m.in. NIS2, KSC),
    - j) konfigurację retencji logów zgodnie z wymaganiami Zamawiającego,
    - k) integrację z innymi systemami bezpieczeństwa (np. NAC, UTM, sandbox, system backupu),
  - przygotowanie dokumentacji powdrożeniowej oraz scenariuszy użycia (use-case),
  - przeprowadzenie szkoleń dla administratorów i użytkowników,
  - zapewnienie wsparcia technicznego oraz aktualizacji przez okres minimum 12 miesięcy.
- 3) Dostawa, wdrożenie oraz uruchomienie **rozwiązania typu Sandbox** służącego do analizy bezpieczeństwa plików oraz aplikacji, obejmującego w szczególności:
- dostawę licencji oraz wdrożenie rozwiązania typu sandbox (on-premise lub równoważnego),
  - instalację i konfigurację systemu w infrastrukturze Zamawiającego (w tym w środowisku wirtualnym),
  - analizę podejrzanych plików i aplikacji w odizolowanym środowisku (sandbox),
  - wykrywanie złośliwego oprogramowania, w tym zagrożeń typu zero-day oraz APT,
  - analizę behawioralną (zachowanie plików/aplikacji podczas uruchomienia),
  - możliwość integracji z istniejącą infrastrukturą bezpieczeństwa (np. UTM, poczta, systemy EDR/XDR, SIEM),
  - automatyzację przekazywania próbek do analizy (np. z systemów pocztowych, bram bezpieczeństwa, UTM),



- generowanie raportów z analizy (technicznych i zarządczych),
  - możliwość definiowania polityk analizy oraz progów alarmowych,
  - archiwizację wyników analiz oraz możliwość ich dalszego wykorzystania (np. w procesach reagowania na incydenty),
  - przygotowanie dokumentacji powdrożeniowej oraz przeprowadzenie szkoleń dla administratorów,
  - zapewnienie wsparcia technicznego i aktualizacji przez okres minimum 12 miesięcy,
  - przeszkolenie administratorów z zakresu obsługi i zarządzania systemem.
- 4) Dostawa, wdrożenie oraz uruchomienie **systemu klasy PAM/PIM** (Privileged Access Management / Privileged Identity Management) **dla min. 5 administratorów** służącego do zarządzania, kontroli oraz monitorowania dostępu uprzywilejowanego do systemów Zamawiającego, obejmującego w szczególności:
- instalację i konfigurację systemu w infrastrukturze Zamawiającego (on-premise lub równoważne),
  - identyfikację i inwentaryzację kont uprzywilejowanych (administratorzy, konta serwisowe, konta techniczne),
  - centralne zarządzanie dostępem uprzywilejowanym (nadawanie, odbieranie, czasowy dostęp – just-in-time),
  - bezpieczne przechowywanie danych uwierzytelniających (vault haseł),
  - rotację i automatyczną zmianę haseł dla kont uprzywilejowanych,
  - rejestrowanie oraz monitorowanie sesji uprzywilejowanych (w tym nagrywanie sesji),
  - kontrolę i zatwierdzanie dostępu (workflow, zasada „4 oczu”),
  - integrację z systemami katalogowymi (np. Active Directory) oraz systemami bezpieczeństwa (SIEM),
  - integrację z systemami IT/OT/ICS (w tym dostęp do urządzeń sieciowych, serwerów, systemów przemysłowych),
  - generowanie raportów oraz audytów dostępu uprzywilejowanego,
  - konfigurację polityk bezpieczeństwa dla kont uprzywilejowanych,
  - przygotowanie dokumentacji powdrożeniowej oraz procedur zarządzania dostępem,
  - przeprowadzenie szkoleń z obsługi,
  - zapewnienie wsparcia technicznego oraz aktualizacji przez okres minimum 12 miesięcy.
- 5) Dostawa i montaż szafy instalacyjnej rack 19” (min. 32U) w ilości 2 sztuki
- a) wyposażenie szafy instalacyjnej rack przeznaczonej do montażu urządzeń i systemów z zakresu cyberbezpieczeństwa, obejmujące w szczególności:
- wysokość min. 32U oraz wymiarach umożliwiających montaż urządzeń serwerowych (np. min. 600–800 mm szerokości i 800–1000 mm głębokości lub równoważne),
  - zapewnienie konstrukcji o odpowiedniej nośności dostosowanej do instalacji urządzeń IT/OT,
  - drzwi przednie (przeszkłone lub perforowane) oraz tylne (perforowane), zapewniające odpowiednią wentylację,
  - zapewnienie możliwości organizacji okablowania (organizery pionowe i poziome, przepusty kablowe),
  - listwy zasilające PDU lub możliwość ich montażu,
- b) zapewnienie możliwości montażu systemów chłodzenia (wentylatory, integracja z klimatyzacją pomieszczenia),
- c) zapewnienie zabezpieczenia dostępu (zamki, kontrola fizyczna dostępu),

- d) instalację i ustawienie szafy w lokalizacji wskazanej przez Zamawiającego.
- 6) Dostawa i montaż szafy instalacyjnej rack 19" (min. 9U) w ilości 3 sztuki o parametrach:
- wisząca lub stojąca o wymiarach umożliwiających montaż urządzeń sieciowych i zabezpieczeń (np. min. 450–600 mm głębokości lub równoważne),
  - zapewnienie konstrukcji o odpowiedniej nośności dostosowanej do instalacji urządzeń (np. UTM, switch, urządzenia OT),
  - wyposażenie w drzwi przednie (przeszkłone lub perforowane) zapewniające wentylację oraz zabezpieczenie dostępu,
  - zapewnienie możliwości organizacji okablowania (przepusty kablowe, podstawowe organizery),
  - możliwość montażu listwy zasilającej PDU,
  - zapewnienie możliwości montażu wentylatorów (jeżeli wymagane).

### Pakiet 3, zadanie 5

- 1) Dostawa, wdrożenie oraz uruchomienie **systemu wykrywania włamań IDS – Intrusion Detection System) dedykowanego środowiskom OT/ICS (w tym SCADA)**, obejmującego w szczególności:
- dostawę licencji systemu IDS dedykowanego sieciom przemysłowym,
  - instalację i konfigurację systemu w infrastrukturze Zamawiającego (on-premise lub równoważne),
  - monitorowanie ruchu sieciowego w środowiskach OT/ICS (SCADA, sterowniki PLC, IIoT),
  - wykrywanie anomalii oraz znanych wzorców ataków na systemy przemysłowe,
  - analizę protokołów przemysłowych (np. Modbus, DNP3, IEC 60870-5-104 lub równoważne),
  - zapewnienie pracy w trybie pasywnym (bez ingerencji w ciągłość działania systemów produkcyjnych),
  - identyfikację urządzeń i mapowanie komunikacji w sieci OT,
  - generowanie alertów bezpieczeństwa oraz klasyfikację zdarzeń,
  - integrację z systemem SIEM (przekazywanie logów i zdarzeń),
  - możliwość tworzenia reguł detekcji dostosowanych do środowiska Zamawiającego,
  - zapewnienie dashboardów, raportów oraz wizualizacji ruchu i incydentów,
  - przygotowanie dokumentacji powdrożeniowej (architektura, konfiguracja, scenariusze detekcji),
  - przeprowadzenie szkoleń dla administratorów i operatorów,
  - zapewnienie wsparcia technicznego oraz aktualizacji przez okres minimum 12 miesięcy.
- 2) Dostawa, instalacja oraz konfiguracja sprzętowa **1 zestawu** składającego się z **3 sond/sensorów** przeznaczonych do monitorowania ruchu w sieciach OT/ICS, obejmujących w szczególności analizę protokołów przemysłowych oraz wykrywanie zagrożeń cyberbezpieczeństwa, obejmujące w szczególności:
- dostawę dedykowanych urządzeń (sensorów) do pasywnego monitorowania ruchu sieciowego w środowiskach OT/ICS,
  - instalację i konfigurację sensorów w kluczowych punktach sieci (np. SPAN/TAP),
  - zapewnienie analizy protokołów przemysłowych (np. Modbus, DNP3, IEC 60870-5-104 lub równoważne),
  - identyfikację urządzeń OT/ICS (PLC, RTU, HMI, IIoT) oraz mapowanie komunikacji,
  - wykrywanie anomalii, nieautoryzowanych połączeń oraz potencjalnych incydentów bezpieczeństwa,

- zapewnienie pracy w trybie pasywnym (bez wpływu na ciągłość działania systemów przemysłowych),
- integrację z systemem IDS/OT oraz systemem SIEM (przekazywanie danych i zdarzeń),
- możliwość centralnego zarządzania sensorami oraz agregacji danych,
- zapewnienie dashboardów i raportów dotyczących ruchu sieciowego i zdarzeń bezpieczeństwa,
- konfigurację polityk monitorowania i progów alarmowych,
- przygotowanie dokumentacji powdrożeniowej (lokalizacja sensorów, schematy, konfiguracja),
- przeprowadzenie testów poprawności działania,
- przeszkolenie administratorów,
- zapewnienie wsparcia technicznego producenta przez okres minimum 12 miesięcy.

### Pakiet 3, zadanie 6

- 1) Dostawa, instalacja oraz konfiguracja **2 zasilaczy** awaryjnych UPS przeznaczonych do zabezpieczenia infrastruktury IT/OT Zamawiającego przed skutkami przerw w zasilaniu, obejmujących w szczególności:
  - dostawę zasilaczy UPS typu online (podwójna konwersja) o mocy znamionowej min. **2,2 kVA** lub równoważnej,
  - zapewnienie możliwości rozbudowy oraz konfiguracji parametrów pracy urządzenia,
  - zapewnienie podtrzymania zasilania dla urządzeń krytycznych (serwery, urządzenia sieciowe, systemy OT/ICS),
  - wyposażenie w interfejsy komunikacyjne (np. USB, SNMP lub równoważne) umożliwiające monitoring i zarządzanie,
  - możliwość integracji z systemami monitorowania (np. SIEM, systemy zarządzania infrastrukturą),
  - konfigurację parametrów pracy (czasy podtrzymania, automatyczne zamykanie systemów),
  - zapewnienie ochrony przed przepięciami, spadkami napięcia oraz zakłóceniami,
  - instalację i uruchomienie urządzeń w infrastrukturze Zamawiającego,
  - przeprowadzenie testów poprawności działania (w tym testów zaniku zasilania),
  - przygotowanie dokumentacji powdrożeniowej (parametry, schematy podłączeń),
  - przeszkolenie administratorów,
  - zapewnienie wsparcia technicznego producenta przez okres minimum 12 miesięcy.
- 2) Dostawa, instalacja oraz konfiguracja **3 zasilaczy** awaryjnych UPS przeznaczonych do zabezpieczenia urządzeń w lokalizacjach o mniejszym zapotrzebowaniu mocy, obejmujących w szczególności:
  - dostawę zasilaczy UPS typu online (podwójna konwersja) o mocy znamionowej min. **1 kVA** lub równoważnej,
  - zapewnienie podtrzymania zasilania dla urządzeń sieciowych i systemów lokalnych (np. przetworniki, urządzenia OT/ICS, systemy komunikacyjne),
  - wyposażenie w interfejsy komunikacyjne (np. USB, SNMP lub równoważne) umożliwiające monitoring i zarządzanie,
  - możliwość integracji z systemami monitorowania oraz zarządzania infrastrukturą,
  - konfigurację parametrów pracy (czasy podtrzymania, automatyczne zamykanie systemów – jeżeli dotyczy),
  - zapewnienie ochrony przed przepięciami, spadkami napięcia oraz zakłóceniami,

- instalację i uruchomienie urządzeń w infrastrukturze Zamawiającego,
- przeprowadzenie testów poprawności działania (w tym testów zaniku zasilania),
- przygotowanie dokumentacji powdrożeniowej (parametry, schematy podłączeń),
- przeszkolenie administratorów,
- zapewnienie wsparcia technicznego producenta przez okres minimum 12 miesięcy.

3) Dostawa i wdrożenie agregatu prądotwórczego obejmującego w szczególności:

- dostawę agregatu prądotwórczego o mocy znamionowej min. 60 kVA (moc ciągła) lub równoważnej,
- zapewnienie automatycznego uruchamiania (autostart) w przypadku zaniku zasilania,
- dostawę i konfigurację układu SZR (samoczynne załączanie rezerwy),
- zapewnienie stabilnych parametrów napięcia i częstotliwości odpowiednich dla urządzeń IT/OT,
- zapewnienie pracy ciągłej przez określony czas (np. min. 8 godzin przy nominalnym obciążeniu lub równoważne),
- wyposażenie w system monitoringu, diagnostyki oraz sygnalizacji alarmów,
- instalację agregatu (wewnętrzną lub zewnętrzną) wraz z wykonaniem niezbędnych przyłączy elektrycznych,
- integrację z istniejącą infrastrukturą zasilania oraz systemami UPS,
- zapewnienie zabezpieczeń (przeciążeniowych, zwarciovych, awaryjnego wyłączenia),
- przeprowadzenie testów funkcjonalnych (w tym testów zaniku zasilania i przetęczenia SZR),
- przygotowanie dokumentacji powdrożeniowej (schematy, parametry, instrukcje eksploatacji),
- przeszkolenie personelu w zakresie obsługi i eksploatacji,
- zapewnienie wsparcia serwisowego oraz przeglądów technicznych przez okres minimum 12 miesięcy.

4) Dostawa i wdrożenie agregatu prądotwórczego obejmującego w szczególności:

- dostawę agregatu prądotwórczego o mocy znamionowej min. 80 kVA (moc ciągła) lub równoważnej,
- zapewnienie automatycznego uruchamiania (autostart) w przypadku zaniku zasilania,
- dostawę i konfigurację podwójnego układu SZR (samoczynne załączanie rezerwy),
- zapewnienie stabilnych parametrów napięcia i częstotliwości odpowiednich dla urządzeń IT/OT,
- zapewnienie pracy ciągłej przez określony czas (np. min. 8 godzin przy nominalnym obciążeniu lub równoważne),
- wyposażenie w system monitoringu, diagnostyki oraz sygnalizacji alarmów,
- instalację agregatu (wewnętrzną lub zewnętrzną) wraz z wykonaniem niezbędnych przyłączy elektrycznych,
- integrację z istniejącą infrastrukturą zasilania oraz systemami UPS,
- zapewnienie zabezpieczeń (przeciążeniowych, zwarciovych, awaryjnego wyłączenia),
- przeprowadzenie testów funkcjonalnych (w tym testów zaniku zasilania i przetęczenia SZR),
- przygotowanie dokumentacji powdrożeniowej (schematy, parametry, instrukcje eksploatacji),
- przeszkolenie personelu w zakresie obsługi i eksploatacji,
- zapewnienie wsparcia serwisowego oraz przeglądów technicznych przez okres minimum 12 miesięcy.

## Formularz cenowy

| Lp.                        | Nazwa  | Cena netto | Ilość | Wartość netto | Wartość netto rocznej asysty | Wartość netto 3-letniej asysty |
|----------------------------|--|------------|-------|---------------|------------------------------|--------------------------------|
| <b>Pakiet 1, zadanie 1</b> |  |            |       |               |                              |                                |
| 1                          | Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) |            | 1     |               |                              |                                |
| 2                          | Opracowanie planów ciągłości działania (BCP) i odtwarzania po awarii (DRP) dla STI – BCP DRP         |            | 1     |               |                              |                                |
| 3                          | Opracowanie, wdrożenie, przegląd, aktualizacja Systemu Zarządzania Ciągłością Działania STI (SZCD)   |            | 1     |               |                              |                                |
| 4                          | System klasy GRC   |            | 1     |               |                              |                                |
| 5                          | Wdrożenie Systemu GRC  |            | 1     |               |                              |                                |
| 6                          | Szkolenie dla administratorów – system GRC   |            | 1     |               |                              |                                |
| <b>Pakiet 1, zadanie 2</b> |  |            |       |               |                              |                                |
| 1                          | Szkolenie z zakresu cyberbezpieczeństwa dla pracowników – stacjonarne                                |            | 2     |               |                              |                                |
| 2                          | Szkolenie z zakresu cyberbezpieczeństwa dla pracowników – platforma szkoleniowa                      |            | 2     |               |                              |                                |
| 3                          | Szkolenie z zakresu cyberbezpieczeństwa dla kadry kierowniczej – stacjonarne                         |            | 1     |               |                              |                                |
| 4                          | Szkolenie z zakresu cyberbezpieczeństwa dla kadry kierowniczej – platforma szkoleniowa               |            | 1     |               |                              |                                |
| <b>Pakiet 2, zadanie 1</b> |  |            |       |               |                              |                                |
| 1                          | Audyt SZBI i SZCD przez wykwalifikowanych audytorów na zgodność z normami IT/OT/ICS                  |            | 1     |               |                              |                                |
| 2                          | Audyt zgodności SZBI i SZCD z uoKSC przez wykwalifikowanych audytorów                                |            | 1     |               |                              |                                |
| <b>Pakiet 3, zadanie 1</b> |  |            |       |               |                              |                                |
| 1                          | Testy bezpieczeństwa Infrastruktury Sieciowej  |            |       |               |                              |                                |
| 2                          | Testy bezpieczeństwa stron www i platform internetowych  |            |       |               |                              |                                |
| 3                          | Testy bezpieczeństwa systemów informatycznych  |            |       |               |                              |                                |
| 4                          | Inwentaryzacja aktywów teleinformatycznych   |            |       |               |                              |                                |
| <b>Pakiet 3, zadanie 2</b> |  |            |       |               |                              |                                |
| 1                          | UTM lokalizacja główna   |            | 2     |               |                              |                                |
| 2                          | UTM lokalizacja dodatkowa  |            | 2     |               |                              |                                |
| 3                          | Szkolenia specjalistyczne dla administratorów UTM  |            | 1     |               |                              |                                |
| 4                          | Przełącznik 24 port 10/100/1000BASE-T 4x1/2.5G   |            | 3     |               |                              |                                |
| 5                          | Przełącznik 5 port 10/100/1000BASE-T   |            | 15    |               |                              |                                |
| 6                          | Przemysłowy przełącznik PoE Switch 4*10/100/1000Base-T RJ45  |            | 8     |               |                              |                                |
| 7                          | Zaprojektowanie, wdrożenie oraz uruchomienie segmentacji sieci                                       |            | 1     |               |                              |                                |
| 8                          | Szkolenia specjalistyczne dla administratorów segmentacja sieci                                      |            | 1     |               |                              |                                |



|                            |   |  |    |  |  |
|----------------------------|---|--|----|--|--|
| <b>Pakiet 3, zadanie 3</b> |   |  |    |  |  |
| 1                          | NAS RackStation o pojemności 30 TB na potrzeby kopii zapasowych w klastrze HA   |  | 2  |  |  |
| 2                          | Instalacja, konfiguracja i wdrożenie rozwiązania NAS  |  | 1  |  |  |
| 3                          | Szkolenia specjalistyczne dla administratorów NAS   |  | 1  |  |  |
| 4                          | Zakup serwera do instalacji zakupionych systemów systemów wspierających zarządzanie cyberbezpieczeństwem w klastrze HA                |  | 1  |  |  |
| 5                          | Rozbudowa starego serwera 4TB SSD - Rozbudowa starego serwera R760XS 4TB SSD  |  | 1  |  |  |
| 6                          | Pamięć RAM do serwerów- Rozbudowa starego serwera R760XS 32GB   |  | 4  |  |  |
| 7                          | Oprogramowanie zarządzania kopiami zapasowymi na serwerach i stacjach roboczych   |  | 1  |  |  |
| 8                          | Instalacja, konfiguracja i wdrożenie rozwiązania kopii zapasowych   |  | 1  |  |  |
| 9                          | Szkolenia specjalistyczne dla administratorów rozwiązania kopii zapasowych  |  | 1  |  |  |
| 10                         | Biblioteka taśmowa - AutoLoader LTO-8 SAS 8 Slots up to 120TB   |  | 1  |  |  |
| 11                         | System wirtualizacji  |  | 1  |  |  |
| 12                         | Usługa wdrożenia i utrzymania rozwiązań wirtualizacji   |  | 1  |  |  |
| 13                         | Szkolenia specjalistyczne z zakresu wirtualizacji   |  | 1  |  |  |
| 14                         | Microsoft Windows Server 2025 Standard (16 Core) Serwer AD/DNS/DHCP   |  | 2  |  |  |
| 15                         | Windows Server 2025 - 1 User CAL  |  | 50 |  |  |
| 16                         | Instalacja systemu Windows Server 2025 Standard, AD, DNS, DHCP, konfiguracja i integracja z nowymi istniejącymi systemami w jednostce |  | 1  |  |  |
| 17                         | Szkolenia specjalistyczne dla administratorów AD, DNS, DHCP   |  | 1  |  |  |
| <b>Pakiet 3, zadanie 4</b> |   |  |    |  |  |
| 1                          | Oprogramowanie NAC (Network Access Control)   |  | 1  |  |  |
| 2                          | Instalacja, konfiguracja i wdrożenie rozwiązań NAC  |  | 1  |  |  |
| 3                          | Szkolenie specjalistyczne dla administratorów NAC   |  | 1  |  |  |
| 4                          | Zintegrowane rozwiązanie SIEM/SOAR  |  | 1  |  |  |
| 5                          | Wdrożenie SIEM/SOAR   |  | 1  |  |  |
| 6                          | Szkolenia specjalistyczne dla administratorów monitoring IT SIEM/SOAR   |  | 1  |  |  |
| 7                          | Oprogramowanie typu sandbox do badania bezpieczeństwa aplikacji oraz plików   |  | 1  |  |  |
| 8                          | Instalacja, konfiguracja i wdrożenie rozwiązania sandbox  |  | 1  |  |  |
| 9                          | Szkolenie specjalistyczne dla administratorów sandbox   |  | 1  |  |  |
| 10                         | Oprogramowanie PAM- Privileged Access Management/ PIM - Privileged Identity Management  |  | 1  |  |  |
| 11                         | Wdrożenia rozwiązań zarządzania uprawnieniami użytkownikami uprzywilejowanymi – PAM   |  | 1  |  |  |
| 12                         | Dostawa i montaż szafy instalacyjnej rack 19" (min. 32U)  |  | 2  |  |  |
| 13                         | Dostawa i montaż szafy instalacyjnej rack 19" (min. 9U)   |  | 3  |  |  |
| <b>Pakiet 3, zadanie 5</b> |   |  |    |  |  |
| 1                          | Oprogramowanie / licencje IDS (Intrusion Detection System) dedykowany sieciom OT  |  | 1  |  |  |

|                            |   |  |   |  |  |  |
|----------------------------|---|--|---|--|--|--|
| 2                          | Sprzętowe sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych) |  | 3 |  |  |  |
| 3                          | Profesjonalna usługa wdrożenia i/lub utrzymania rozwiązań monitoring OT                                       |  | 1 |  |  |  |
| 4                          | CyberOchrona Twojej sieci OT - Praktyczne Szkolenie   |  | 1 |  |  |  |
| <b>Pakiet 3, zadanie 6</b> |   |  |   |  |  |  |
| 1                          | APC SRTL2200RMXLI-NC APC SMART-UPS SRT LI-ION 2200VA RM 230V  |  | 2 |  |  |  |
| 2                          | APC Easy UPS SRV RM 1000VA 230V - do szaf (zasilanie switchy)   |  | 3 |  |  |  |
| 3                          | Agregat prądotwórczy 60 KVA   |  | 1 |  |  |  |
| 4                          | Agregat prądotwórczy 80 KVA   |  | 1 |  |  |  |