

Nr zapytania 12/2026

Opis przedmiotu zamówienia – Część II



na usługę pn.:

**Część II. - Dostawa i wdrożenie sprzętu IT oraz OT w ramach projektu pn.
„Wzmocnienie cyberodporności sieci IT i OT oraz ciągłości działania w
Zakładzie Wodociągów i Kanalizacji Sp. z o.o. Świecie poprzez wdrożenie
kluczowych środków technicznych oraz rozwój kompetencji.”,
finansowanego ze środków Unii Europejskiej w ramach Instrumentu na rzecz
Odbudowy i Zwiększania Odporności (Krajowy Plan Odbudowy – KPO)."**

Świecie, dnia: 15.07.2026 r.

Zatwierdza:
Prezes



Signed by /
Podpisano przez:
Andrzej Kozłowski
Date / Data: 2026-
07-15 14:36

Spis treści

1. Cel i charakter zamówienia	3
4. Uzasadnienie Zamawiającego	5
Dostawa Systemu ALL-IN-ONE - XDR z wbudowanymi SOAR oraz systemem do centralnego zarządzania i korelacji logów (SIEM) oraz świadczeniem usługi SOC	6
Dostawa rozwiązania typu Firewall Sieciowy	12
Dostawa Macierzy Dyskowej	19
Dostawa serwera fizycznego wraz z niezbędnymi licencjami oraz oprogramowaniem.....	21
Dostawa szafy RACK.....	25
Dostawa oprogramowania do ochrony przed ransomware – szyfrowana kopia zapasowa w chmurze.....	26
Dostawa zarządzalnych urządzeń sieciowych – przełączniki dostępowe 24p wraz z systemem NMS – 4 sztuki	30
Dostawa Access Point – 4 sztuki	36
Dostawa UPS – 2 sztuki	40
Dostawa mobilnego agregatu – 2szt wraz z wykonaniem przyłącza do agregatu – 1 szt	42
Profesjonalna usługa wdrożenia i utrzymania rozwiązań; testy oraz audyt cyberbezpieczeństwa sieci oraz wszelkie wymagania.....	48
Testy bezpieczeństwa infrastruktury IT	50
Audyt cyberbezpieczeństwa sieci IT/OT	50

Wstęp i wymagania ogólne

1. Cel i charakter zamówienia

Zgodnie z „Zasadami kwalifikowania wydatków w Przedsięwzięciach realizowanych w ramach Inwestycji C3.1.1. Krajowego Planu Odbudowy i Zwiększania Odporności”, w tym z Załącznikiem nr 1 pn. „Zamówienia udzielane w Przedsięwzięciach realizowanych w ramach Inwestycji C3.1.1.” (dalej: „Zasady udzielania zamówień C3.1.1.”), niniejszy przedmiot zamówienia został opisany w sposób jednoznaczny i wyczerpujący, za pomocą dokładnych i zrozumiałych określeń, z uwzględnieniem wszystkich wymagań i okoliczności technicznych mogących mieć wpływ na rzetelne sporządzenie oferty przez Wykonawcę. Głównym celem realizacji zamówienia jest zabezpieczenie oraz optymalizacja infrastruktury informatycznej (IT) oraz operacyjnej (OT) Zamawiającego poprzez dostarczenie, uruchomienie i zintegrowanie nowoczesnych rozwiązań sprzętowych i programowych

2. Kompleksowy zakres obowiązków Wykonawcy.

W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest do kompleksowego świadczenia usług i dostaw, obejmujących nie tylko samą dostawę sprzętu i licencji na oprogramowanie wyszczególnionych w niniejszym dokumencie, ale również pełne wdrożenie operacyjne tych rozwiązań w środowisku informatycznym (IT) oraz operacyjnym (OT) Zamawiającego.

Zakres prac powierzonych Wykonawcy obejmuje w szczególności:

- Dostawę i logistykę: Dostarczenie, rozładunek oraz wniesienie fabrycznie nowego sprzętu oraz oprogramowania do wskazanych lokalizacji Zamawiającego, z zachowaniem należytej staranności i zasad bezpieczeństwa transportu urządzeń wrażliwych.
- Wdrożenie i integrację: Przeprowadzenie fizycznej instalacji urządzeń, ich uruchomienie oraz zaawansowaną konfigurację. Wykonawca zobowiązany jest zapewnić bezkolizyjną integrację dostarczanych technologii z istniejącym środowiskiem informatycznym (IT) oraz przemysłowym (OT/ICS) Zamawiającego, minimalizując przy tym ewentualne przerwy w dostępności usług dla infrastruktury krytycznej.
- Transfer wiedzy: Przeprowadzenie specjalistycznego instruktażu oraz szkoleń dla personelu technicznego (IT oraz OT) Zamawiającego w zakresie bieżącej obsługi, administracji oraz utrzymania dostarczonych systemów.
- Zgodność z wymaganiami: Pełna realizacja wytycznych, harmonogramu oraz parametrów technicznych określonych szczegółowo w rozdziale „Wdrożenie dostarczanych rozwiązań wraz z przeszkoleniem”.

3. Odpowiedzialność za kompletność rozwiązania.

Wszelkie prace instalacyjne i wdrożeniowe muszą zostać wykonane zgodnie z najlepszymi praktykami rynkowymi, aktualnymi wytycznymi producentów sprzętu i oprogramowania, a także wymogami sztuki inżynierskiej

dla systemów informatycznych (IT) oraz operacyjnych (OT). Wykonawca zobowiązany jest uwzględnić w cenie całkowitej oferty wszystkie koszty niezbędne do prawidłowego, terminowego i kompletnego zrealizowania przedmiotu zamówienia zgodnie z jego przeznaczeniem.

I. Wymagania ogólne dotyczące dostarczanego sprzętu i oprogramowania:

Całość dostarczonego sprzętu i oprogramowania musi pochodzić z legalnego źródła, być wprowadzona do obrotu na terytorium Unii Europejskiej zgodnie z prawem i nie może być obciążona prawami osób trzecich.

Oferowane urządzenia muszą być fabrycznie nowe, nieużywane, dostarczone w oryginalnych opakowaniach.

Niedopuszczalne jest dostarczenie sprzętu naprawianego (odnawianego – tzw. refurbished), pochodzącego z demontażu lub z ekspozycji. Sprzęt musi pochodzić z bieżącej produkcji producenta i na dzień dostawy nie może być obciążony statusem zakończenia sprzedaży lub wsparcia (tzw. End of Sale / End of Life). Zamawiający traktuje powyższe jako wymagane cechy dostawy niezbędne do właściwej realizacji zamówienia.

Dostarczane licencje na oprogramowanie oraz systemy operacyjne (wyłącznie te systemy operacyjne, które są niezbędne do instalacji i utrzymania dostarczanych systemów bezpieczeństwa) muszą być nowe, niewykorzystywane uprzednio oraz nieaktywowane na innych urządzeniach (Wykonawca dostarczy dokumenty licencyjne wystawione na rzecz Zamawiającego).

Sprzęt musi być objęty gwarancją producenta świadczoną na terytorium Rzeczypospolitej Polskiej.

Gwarancja musi być realizowana bezpośrednio przez producenta urządzeń lub jego autoryzowaną placówkę serwisową (tzw. gwarancja On-Site u Zamawiającego).

Świadczenia gwarancyjne muszą być zapewnione niezależnie od sytuacji prawnej Wykonawcy, w szczególności w przypadku zaprzestania działalności lub niewypłacalności Wykonawcy.

Wykonawca oświadcza, że korzystanie przez Zamawiającego z dostarczonych produktów zgodnie z ich przeznaczeniem nie będzie naruszać praw własności intelektualnej ani majątkowych praw autorskich osób trzecich.

Cena oferty ujęta w Formularzu Oferty musi obejmować wszystkie koszty związane z kompleksową realizacją zamówienia, w tym koszty licencji, transportu, ubezpieczenia na czas transportu, wniesienia do wskazanego pomieszczenia Zamawiającego oraz instalacji i wdrożenia w środowisku IT i OT. Wykonawca zobowiązany jest do wyraźnego wyodrębnienia w ofercie kwoty netto oraz kwoty podatku VAT, ze względu na fakt, że podatek VAT w Projekcie Grantowym stanowi w całości wydatek niekwalifikowalny finansowany ze środków własnych Zamawiającego.

Dostawa zostanie zrealizowana do wskazanych lokalizacji Zamawiającego w dni robocze, w godzinach 8:00–15:00, po uprzednim uzgodnieniu terminu z Zamawiającym.

II. Zasady oceny rozwiązań równoważnych:

1. Zgodnie z Zasadami udzielania zamówień C3.1.1. opis przedmiotu zamówienia co do zasady nie powinien zawierać odniesień do znaków towarowych, patentów, pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do

uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów. W przypadku, gdy z przyczyn technicznych lub specyfiki przedmiotu zamówienia takie odniesienia znalazły się w opisie przedmiotu zamówienia, Zamawiający dopuszcza zastosowanie rozwiązań równoważnych opisywanym — odniesieniom tym każdorazowo towarzyszą wyrazy „lub równoważne”.

2. Zamawiający wskazuje kryteria stosowane w celu oceny równoważności: przez rozwiązanie równoważne Zamawiający rozumie sprzęt lub oprogramowanie o parametrach technicznych, wydajnościowych i funkcjonalnych nie gorszych (tj. takich samych lub lepszych) niż wskazane w referencyjnym opisie przedmiotu zamówienia, które w pełni umożliwią realizację celu Zamawiającego.

3. Wykonawca, który w ofercie powołuje się na rozwiązania równoważne, jest obowiązany udowodnić w swojej ofercie, że proponowane przez niego rozwiązania w równoważnym stopniu spełniają wymagania określone w Zapytaniu Ofertowym.

4. Potwierdzenie równoważności musi nastąpić poprzez złożenie wraz z ofertą odpowiednich dokumentów (np. szczegółowych kart katalogowych producenta, specyfikacji technicznych, certyfikatów lub innych dokumentów producenta), z których w sposób niebudzący wątpliwości wynika spełnienie parametrów określonych w opisie przedmiotu zamówienia.

4. Uzasadnienie Zamawiającego

Zamawiający dopuścił rozwiązania równoważne zgodnie z Zasadami udzielania zamówień C3.1.1., a wskazane wymagania mają charakter funkcjonalny i organizacyjny, wynikający z rzeczywistych potrzeb Zamawiającego oraz z konieczności zapewnienia prawidłowej realizacji zamówienia.

Wymóg dostawy sprzętu z bieżącej produkcji, nieobjętego statusem End of Sale / End of Life, jest podyktowany potrzebą zapewnienia długoterminowej dostępności wsparcia producenta, części zamiennych, aktualizacji oraz serwisu, co ma bezpośrednie znaczenie dla bezpieczeństwa eksploatacji i trwałości inwestycji finansowanej ze środków Krajowego Planu Odbudowy i Zwiększania Odporności.

Wymóg gwarancji producenta realizowanej w formule On-Site wynika z konieczności ograniczenia przestojów i zapewnienia szybkiej reakcji serwisowej, co jest szczególnie istotne przy urządzeniach wykorzystywanych do wykonywania zadań o charakterze użyteczności publicznej w zakresie zbiorowego zaopatrzenia w wodę oraz zabezpieczania infrastruktury krytycznej Zamawiającego.

Wymogi te nie mają na celu uprzywilejowania jakiegokolwiek wykonawcy lub producenta, lecz służą ochronie interesu Zamawiającego, zapewnieniu jakości i niezawodności dostaw oraz zachowaniu zasad uczciwej konkurencji, równego

traktowania wykonawców, przejrzystości i proporcjonalności, wynikających z Zasad udzielania zamówień C3.1.1. oraz z Umowy o powierzenie grantu zawartej z Centrum Projektów Polska Cyfrowa w ramach Przedsięwzięcia „Cyberbezpieczne Wodociągi”.

Dostawa Systemu ALL-IN-ONE - XDR z wbudowanymi SOAR oraz systemem do centralnego zarządzania i korelacji logów (SIEM) oraz świadczeniem usługi SOC

Dostawa i wdrożenie systemu klasy XDR wraz z świadczeniem usługi bezpieczeństwa polegającej na zarządzaniu bezpieczeństwem urządzeń końcowych z wykorzystaniem wdrożonego systemu klasy XDR oraz świadczenia Usługi zwaną dalej Usługą Zarządzany XDR lub Usługą.

1. Usługa Zarządzany XDR będzie świadczona przez okres 12 miesięcy licząc od daty zawarcia umowy.
2. Usługa Zarządzany XDR będzie świadczona przez Wykonawcę w czasie rzeczywistym, w trybie ciągłym 24 godziny na dobę, 7 dni w tygodniu, przez 365 dni w roku (24/7/365).
3. Wykonawca, w terminie uzgodnionym z Zamawiającym, zobowiązany jest do przeprowadzenia analizy przedwdrożeniowej oraz rozruchu Usługi Zarządzany XDR. W ramach tych działań Wykonawca zobowiązany jest do:
 - 3.1. dostosowania i uzgodnienia z Zamawiającym zasad współpracy;
 - 3.2. identyfikacji urządzeń końcowych (stacji roboczych, serwerów, urządzeń mobilnych), które zostaną objęte Usługą;
 - 3.3. opracowania reguł bezpieczeństwa, klasyfikacji incydentów oraz scenariuszy reakcji;
 - 3.4. wdrożenia systemu zapewniającego kompleksową ochronę przed zagrożeniami w standardzie Extended Detection & Response (XDR), o którym mowa w ust. 10, obejmującego ochroną:
 - a. do 40 stacji roboczych
 - b. do 20 serwerów z systemami Windows oraz Linux
 - c. do 15 urządzeń mobilnych
 - 3.5. zainstalować i skonfigurować na stacjach roboczych i serwerach dostarczane oprogramowanie XDR, w tym przenieść wszystkie polityki bezpieczeństwa z obecnie użytkowanego oprogramowania antywirusowego;
 - 3.6. przeprowadzić min. 2 dniowy instruktaż z dostarczonego systemu XDR dla personelu IT Zamawiającego.
 - 3.7. Zakończenie analizy przedwdrożeniowej i rozruchu Usługi Zarządzany XDR zostanie potwierdzone protokołem odbioru.
4. Wykonawca zobowiązany jest do zapewnienia pełnego wsparcia eksperckiego, merytorycznego i administracyjnego w zakresie realizacji przedmiotu zamówienia, zgodnie z najlepszymi praktykami i zgodnie z najnowszymi wytycznymi branżowymi i technologicznymi w tym zakresie, jak również wytycznymi z audytów przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający przez cały okres obowiązywania umowy.
5. Wykonawca zobowiązany jest do udostępnienia Zamawiającemu stałego dostępu do dedykowanego panelu klienta, w celu bezpośredniego monitorowania i weryfikowania parametrów infrastruktury teleinformatycznej objętej

Usługą Zarządzany XDR.

6. Wykonawca zobowiązany jest do instruktażu maksymalnie 2 administratorów Zamawiającego z administrowania i obsługi dostarczonego systemu XDR. Zakres instruktażu musi przygotować administratorów do pełnego wykorzystania funkcjonalności systemu XDR. Forma instruktażu zostanie ustalona podczas analizy przedwdrożeniowej.
7. Wykonawca musi monitorować oraz reagować na incydenty bezpieczeństwa na podstawie alarmów z wdrożonego systemu XDR.
8. Wykonawca zobowiązany jest do dostarczenia i wdrożenia systemu XDR wraz dokumentacją powykonawczą oraz wsparciem technicznym producenta na cały okres świadczenia Usługi Zarządzany XDR.
9. Wymagania dla systemu XDR. W ramach Usługi Wykonawca dostarczy, wdroży i będzie utrzymywał system zapewniający kompleksową ochronę przed zagrożeniami w standardzie Endpoint Detection & Response (EDR) w połączeniu z Endpoint Protection Platform (EPP), Network Detection & Response (NDR), Identity Threat Detection & Response (ITDR), Extended Detection and Response (XDR), Email Security, Domain Filtering, Web Content Filtering, SaaS & Cloud Security Posture Management (SSPM/CSPM), External Attack Surface Management (EASM), Centralized Log Management, User Behavior Analytics (UBA) oraz wbudowaną usługą 24/7 MDR i orkiestrą automatyzacji (SOAR), który:
 - 9.1. musi zapewniać centralne zarządzanie ochroną wszystkich typów urządzeń końcowych (stacje robocze, serwery) i automatyzację reakcji na incydenty;
 - 9.2. musi umożliwiać wdrożenie we wszystkich trzech modelach: cloud (SaaS), on-premise, hybrydowo;
 - 9.3. musi zapewniać centralną konsolę zarządzającą, dostępna przez przeglądarkę, wspierać autentykację wieloskładnikową (MFA) i mechanizm pojedynczego logowania (SSO) oraz granularne role i uprawnienia, jak również integrację z Active Directory;
 - 9.4. musi obsługiwać automatyczne wykrywanie i instalowanie agentów na nowych urządzeniach oraz zapewniać szybkie, bezobsługowe wdrożenie aktualizacji (bez potrzeby restartów);
 - 9.5. musi zapewniać możliwość komunikacji przez publiczne API;
 - 9.6. musi zapewniać integrację z narzędziami do monitorowania, analizowania i reagowania na zagrożenia w czasie rzeczywistym klasy SIEM;
 - 9.7. musi zapewniać możliwość zdalnego monitorowania i zarządzania Remote Monitoring and Management (RMM);
 - 9.8. musi zapewniać możliwość integracji z platformami certyfikacji bezpieczeństwa dla sprzętu, oprogramowania i urządzeń Internetu Rzeczy (IoT) Platform Security Architecture (PSA);
 - 9.9. musi natywnie oferować, bez konieczności dokupywania modułów zewnętrznych:
 - a. możliwość instalacji agenta ochrony na następujących systemach operacyjnych: Windows XP, Windows 7 i nowsze, Windows Server od 2008 R2 i nowsze, każda wiodąca dystrybucja Linux (wg. W3Techs), macOS (Intel & Apple Silicon);
 - b. kompleksową ochronę przed szeroką gamą zagrożeń, obejmującą: wirusy, ransomware, oprogramowanie szpiegujące (spyware), oprogramowanie typu rootkit, cryptominers, ataki typu fileless, exploits (w tym ataki na krytyczne komponenty OS), narzędzia hakerskie, phishing;



- c. wsparcie zaawansowanej heurystyki oraz uczenia maszynowego do analizy zachowania, a także dynamiczną analizę podejrzanych plików w czasie rzeczywistym (sandbox), umożliwiającą wykrywanie także zagrożeń typu zero-day;
- d. rozbudowane mechanizmy analizy zachowań użytkowników (User & Behavioral Analytics), wykrywania ruchu lateralnego (lateral movement), automatycznej detekcji anomalii oraz pełną widoczność ruchu procesów, plików, rejestru, systemu i sieci (detection living-off-the-land);
- e. wbudowane mechanizmy automatycznej reakcji na incydenty, w tym: izolacja stacji lub hosta, blokowanie kont użytkowników, natychmiastowe zamykanie procesów, kwarantanna plików, przywrócenie stanu systemu sprzed incydentu (rollback);
- f. możliwość blokowania urządzeń (device control) podłączanych za pomocą USB;
- g. zaawansowany threat hunting, możliwość eksportu i importu wskaźników kompromitacji IOC, integrację z syslog, SIEM oraz publiczne API dla zarządzania i automatyzacji;
- h. natywne mechanizmy deception, czyli: fałszywe pliki, pułapki na hostach i endpointach, pułapki w sieci lokalnej, honeypoty;
- i. pełną kompatybilność i koegzystencję z innym legalnie wykorzystywanym w organizacji oprogramowaniem antywirusowym lub zabezpieczającym;

9.10. musi umożliwiać wykrywanie, blokowanie i automatyczną reakcję na poniższe techniki, bazując na MITRE ATT&CK, musi umożliwiać korelację poniższych technik, ich wizualizację, automatyzację reakcji oraz pełną dokumentację incydentów z poziomu jednej konsoli:

- a. wykrywanie oraz blokowanie prób pozyskania credentiali przy nieszyfrowanych poświadczeniach (Unsecured Credentials);
- b. pełne monitorowanie procesów, wykrywanie prób enumeracji i blokowanie nieautoryzowanego dostępu do informacji o uruchomionych procesach (Process Discovery);
- c. blokowanie prób wyłączenia kluczowych usług i komponentów systemowych (Service Stop);
- d. wykrywanie i blokowanie interpretatorów komend/skryptów (np. PowerShell, WMI, Bash, CMD) i ich szkodliwego użycia (Command and Scripting Interpreter);
- e. wykrywanie prób automatycznego zbierania danych na stacjach (Automated Collection);
- f. detekcja prób automatyzowanej eksfiltracji danych (Automated Exfiltration);
- g. wykrywanie i blokowanie prób wycieku danych przez kanały Command & Control np. HTTP/S, DNS, ICMP (Exfiltration Over C2 Channel);
- h. analiza i alertowanie obfuskacji plików, kodu, informacji (Obfuscated Files or Information);
- i. detekcja prób obejścia narzędzi bezpieczeństwa (Debugger Evasion);
- j. monitoring i detekcja prób enumeracji użytkowników systemowych (System Owner/User Discovery);
- k. kontrola oraz widoczność zmian i zapytań do konfiguracji sieciowej systemów (System Network Configuration Discovery);
- l. detekcja prób zbierania informacji o systemie/hostach (System Information Discovery);
- m. identyfikacja i blokowanie niestandardowych mechanizmów uruchamiania, blokada rozwiązań typu



guardrail (Execution Guardrails);

- n. monitoring kluczy rejestru przechowujących dane uwierzytelniające (Credentials in Registry);
- o. alertowanie przy enumeracji plików i folderów (File and Directory Discovery);
- p. wykrywanie i blokowanie prób wyłączania/omijania zabezpieczeń (Impair Defenses);
- q. analiza, wykrywanie i blokowanie nadużycia legalnych (valid) kont (Valid Accounts);
- r. wykrywanie oraz blokowanie destrukcji danych (Data Destruction);
- s. detekcja i blokowanie działania ransomware oraz szyfrowania masowego plików (Data Encrypted for Impact);
- t. monitoring i zapobieganie czyszczeniu śladów/logów przez atakujących (Indicator Removal on Host);

9.11. Wymaga się, aby oferowane rozwiązanie bezpieczeństwa wykazało skuteczność potwierdzoną w niezależnych badaniach MITRE ATT&CK Evaluations (Enterprise, w scenariuszu LockBit) z roku 2024 lub nowszym, na poziomie co najmniej:

- a. 98% skuteczności w zakresie Detection Visibility (widoczność/detekcja wszystkich kroków ataku),
- b. 98% skuteczności w zakresie Protection Rate (blokowanie złośliwych kroków ataku),
- c. 98% skuteczności w zakresie Prevention (blokowanie ataków na etapie pierwszych kroków).

Dostawca musi przedłożyć oficjalne materiały producenta lub raporty z MITRE ATT&CK Evaluations potwierdzające spełnienie powyższych progów.

9.12. musi zapewnić ochronę offline, czyli zachowanie kluczowych funkcji nawet bez stałego połączenia z serwerem zarządzającym;

9.13. Funkcjonalność opcjonalna, punktowana dodatkowo: wbudowany system deprecji w zakresie:

- a. możliwość automatycznego generowania pułapek będących imitacją endpointów i serwerów i automatyczny sygnał ostrzegawczy po wejściu lub aktywności atakującego na takim deceptive node;
- b. możliwość umieszczania plików-pułapek zachęcających do kradzieży, z funkcją monitorowania akcji i generowania alertów;
- c. system powiadomień i automatycznej reakcji po każdej nieuprawnionej próbie dostępu;
- d. tworzenie kont użytkowników-pułapek, monitorowanie prób logowania oraz wszelkich interakcji z tymi kontami;
- e. wykorzystanie deception do szybkiej identyfikacji lateral movement i prób eskalacji uprawnień przez atakującego;

9.14. musi zapewniać File Integrity Monitoring (FIM) – egzekwowanie polityk w zakresie zmiany plików/zasobów;

9.15. musi zapewniać wykrywanie skanowania sieci: detekcja aktywności skanowania na poziomie segmentu sieci oraz hosta, wykrywanie prób identyfikacji usług, portów oraz rozpoznawanie różnych technik skanowania (szybkie, wolne, rozproszone);

9.16. musi zapewniać wykrywanie zatrutowania sieci: monitoring prób zatrutowania tablic ARP, wykrywanie ataków typu



DNS spoofing, technik man-in-the-middle, identyfikacja podszywania się pod urządzenia lub serwery w sieci;

- 9.17. musi zapewniać wykrywanie tunelowania eksfiltracji: identyfikacja nietypowego, tunelowanego ruchu mającego na celu eksfiltrację (DNS tunneling, ICMP tunneling, HTTP/S tunneling), alertowanie przy transferze danych do nieautoryzowanych lokalizacji oraz detekcja długotrwałych i ukrytych połączeń;
- 9.18. musi zapewniać zarządzanie i reagowanie poprzez moduł NDR dostępny z poziomu tej samej konsoli zarządzającej;
- 9.19. musi zapewniać zaawansowane zarządzanie zasobami sprzętowymi i programowymi (asset management), risk scoring (ocena ryzyka każdego składnika);
- 9.20. musi zapewniać pełny logging oraz retencja danych zgodnie z wymogami Zamawiającego (integracja z SIEM, IOC, threat hunting);
- 9.21. musi zapewniać możliwość zaawansowanej i personalizowanej automatyzacji reakcji na incydenty (predefiniowane oraz własne playbooki);
- 9.22. musi oferować tzw. lekkiego agenta - agent na endpointy nie powinien zużywać więcej niż 250MB RAM oraz 5% CPU;
- 9.23. musi zapewniać granularne role/uprawnienia administracyjne, możliwość blokowania zmian ustawień przez użytkowników;
- 9.24. musi zapewniać, że Wszystkie metadane, telemetria, logi i dane użytkownika muszą być przechowywane wyłącznie na terytorium Unii Europejskiej – zgodnie z RODO i normami UE. M
- 9.25. musi posiadać pełną dokumentację licencyjną i wdrożeniową w języku polskim lub angielskim.
10. Wykonawca zobowiązany jest do monitorowania incydentów, zdarzeń i anomalii z dostarczonego systemu XDR.
11. Wykonawca zobowiązany jest do analizy incydentów według procedur uzgodnionych z Zamawiającym.
12. Wykonawca zobowiązany jest do obsługi incydentów zgodnie z ustalonymi z Zamawiającym scenariuszami reakcji, w tym ich kategoryzacji i priorytetyzacji.
13. Wykonawca zobowiązany jest do klasyfikacji wykrytych lub zgłoszonych incydentów według następujących kategorii:
 - 13.1. Incydenty krytyczne – powodujące poważne zakłócenia lub przerwanie ciągłości operacyjnej Zamawiającego w obszarach krytycznych;
 - 13.2. Incydenty niekrytyczne – pozostałe incydenty niezaliczane do kategorii krytycznych;
 - 13.3. False positive – błędne detekcje lub zgłoszenia, które nie wymagają reakcji zgodnie z umową, tj. nie stanowią rzeczywistego incydentu bezpieczeństwa.
14. Za podjęcie incydentu uznaje się rozpoczęcie działań przez operatora Usługi Zarządzany XDR, polegających na jego segregacji oraz analizie. Terminy reakcji i realizacji są następujące:
 - 14.1. Incydent Krytyczny: reakcja do 4 godzin,
 - 14.2. Incydent Niekrytyczny: reakcja do 8 godzin,
15. Wykonawca zobowiązany jest do obsługi zdarzeń i incydentów zgodnie z najlepszymi praktykami branżowymi z uwzględnieniem właściwego nadania priorytetów.
16. Wykonawca zobowiązany jest do przysyłania comiesięcznych raportów z wykonanych działań. Raporty będą przysyłane na adres e-mail wskazany w umowie. Wzór raportu zostanie opracowany wspólnie przez Zamawiającego

i Wykonawcę na etapie analizy przedwdrożeniowej i rozruchu Usługi Zarządzany XDR.

17. W zakresie świadczenia Usługi Zarządzany XDR Wykonawca:

- 17.1. musi monitorować i reagować na incydenty bezpieczeństwa w trybie ciągłym (24/7/365) z systemu XDR, w szczególności uwzględniać:
- a. powiadomienia o zagrożeniach ze stacji roboczych oraz serwerów, w szczególności generowanych z narzędzi ochrony, w tym z wdrożonego systemu DR;
 - b. powiadomienia o dezaktywacji narzędzi bezpieczeństwa na danym urządzeniu końcowym;
 - c. zdarzenia związane z modyfikacją mechanizmów harmonogramu w systemach operacyjnych;
 - d. zdarzenia związane z modyfikacją audytu zdarzeń i dzienników systemowych;
 - e. zdarzenia dotyczące integralności plików mogące świadczyć o zainfekowaniu oprogramowaniem złośliwym;
- 17.2. musi dokonywać wstępnej oceny zdarzeń, analizy i obsługi incydentów w zakresie posiadanych kompetencji, zgodnie z ustalonymi scenariuszami reakcji;
- 17.3. musi kontaktować się z Zamawiającym w przypadku konieczności dokonania zmian w infrastrukturze, niezbędnych do eliminacji przyczyny incydentu;
- 17.4. musi eskalować incydent zgodnie z ustalonym scenariuszem reakcji z wykorzystaniem ustalonych kanałów komunikacji;
- 17.5. musi dokumentować wykonane czynności zgodnie z przygotowanymi i zaakceptowanymi scenariuszami reakcji;
- 17.6. musi przygotowywać miesięczne raporty wykrytych zdarzeń bezpieczeństwa;
- 17.7. musi dostosowywać polityki bezpieczeństwa systemu XDR celem dostosowania ich do skuteczniejszego wykrywania zagrożeń.
- 17.8. musi zapewnić dostępność zespołu serwisowego 8/5, świadczącego usługę wsparcia przy usuwaniu awarii systemu XDR, w tym:
- a. wsparcie telefoniczne zespołu inżynierów;
 - b. pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji urządzeń;
 - c. doradztwo w zakresie konfiguracji;
 - d. zdalne wsparcie techniczne;
 - e. pomoc w zakładaniu zgłoszeń serwisowych u producenta;
 - f. przegląd konfiguracji;
 - g. zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta;
 - h. konfiguracja polityk bezpieczeństwa

Dostawa rozwiązania typu Firewall Sieciowy

Lp.	Nazwa parametru, elementu lub cechy	Wymagane parametry techniczne
	1	2
TYP		W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego urządzenia
1.	Przedmiot zamówienia	System bezpieczeństwa realizujący wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.
2.	Wymagania ogólne	- System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. - System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. - Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. - System wspiera protokoły IPv4 oraz IPv6 w zakresie: - Firewall, - Ochrony w warstwie aplikacji, - Protokołów routingu dynamicznego.
3.	Redundancja, monitoring i wykrywanie awarii	- W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. - Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych. - Monitoring stanu realizowanych połączeń VPN. - System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
4.	Interfejsy, Dysk, Zasilanie	- System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 8 portami Gigabit Ethernet RJ-45. 2 gniazdami SFP+ 10 Gbps. - System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. - System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. - System jest wyposażony w zasilanie AC.
5.	Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.



		• Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B. • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps. • Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps. • Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 4 Gbps. • Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps. • Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps.
6.	Funkcje Systemu Bezpieczeństwa	• W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: ▪ Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. ▪ Kontrola Aplikacji. ▪ Poufność transmisji danych - połączenia szyfrowane IPSec VPN. ▪ Ochrona przed malware. ▪ Ochrona przed atakami - Intrusion Prevention System. ▪ Kontrola stron WWW. ▪ Kontrola zawartości poczty – Antyspam dla protokołów SMTP. ▪ Zarządzanie pasmem (QoS, Traffic shaping). ▪ Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. ▪ Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. ▪ Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. ▪ Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
7.	Polityki, Firewall	• Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.



		• System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: ▪ Translację jeden do jeden oraz jeden do wielu. ▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP. • W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. • Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. • Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. • Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. • Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
8.	Połączenia VPN	• System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: ▪ Wsparcie dla IKE v1 oraz v2. ▪ Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). ▪ Obsługa protokołu Diffie-Hellman grup 19, 20. ▪ Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. ▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. ▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. ▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. ▪ Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. ▪ Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. ▪ Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. ▪ Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. ▪ Mechanizm „Split tunneling” dla połączeń Client-to-Site.



		• Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
9.	Routing i obsługa łączy WAN	• W zakresie routingu rozwiązanie zapewnia obsługę: ▪ Routingu statycznego. ▪ Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). ▪ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM. ▪ Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. ▪ ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. ▪ BFD (Bidirectional Forwarding Detection). ▪ Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
10.	Funkcje SD-WAN	• System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. • SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
11.	Zarządzanie pasmem	• System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. • System daje możliwość określania pasma dla poszczególnych aplikacji. • System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. • System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
12.	Ochrona przed malware	• Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). • Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. • W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. • System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.



		• System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). • Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. • Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. • Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
13.	Ochrona przed atakami	• Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • System chroni przed atakami na aplikacje pracujące na niestandardowych portach. • Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. • System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. • System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA. • Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). • Wykrywanie i blokowanie komunikacji C&C do sieci botnet. • Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
14.	Kontrola aplikacji	• Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. • Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. • Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.



		• Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. • Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). • System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
15.	Kontrola WWW	• Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. • W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. • Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. • Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. • Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). • Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. • Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. • Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. • System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
16.	Uwierzytelnianie użytkowników w ramach sesji	• System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: ▪ Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. ▪ Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. ▪ Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. • System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. • System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. • Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.



17.	Zarządzanie	• Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. • Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. • Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. • System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. • System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. • Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. • Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. • Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). • Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
18.	Logowanie	• Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. • W przypadku kiedy usługa logowania i raportowania realizowana jest w chmurze, wymagane są stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku. • W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. • Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. • Możliwość włączenia logowania per reguła w polityce firewall. • System zapewnia możliwość logowania do serwera SYSLOG. • Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
19.	Serwisy i licencje	• Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

		▪ Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy. ▪ Ochrona systemów przemysłowych SCADA na okres 12 miesięcy.
20.	Gwarancja oraz wsparcie	• System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Dostawa Macierzy Dyskowej

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
		W ofercie wymagane jest podanie modelu, symbolu oraz producenta
1.	Typ	Serwer typu NAS
2.	Obudowa	Rack, wysokość max. 1U
3.	Procesor	Klasy x86, czterordzeniowy o taktowaniu min. 2,1 GHz
4.	Szyfrowanie	Sprzętowy mechanizm szyfrowania
5.	RAM	Min. 2 GB pamięci DDR4. Możliwość rozbudowy do min. 16 GB

6.	Dyski	4 x dysk SATA HDD o pojemności min. 12TB każdy, spięte w RAID5
7.	Rozbudowa	Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap, 3.5"
8.	Porty zewnętrzne	2 porty USB 3.0
9.	Porty sieciowe	4 porty 1GbE Base-T o przepustowości min. 1 Gb/s
10.	Porty dodatkowe	1 port eSATA
11.	Chłodzenie	Wentylatory 40x40mm min. 2 szt.
12.	Obsługiwane typy macierzy RAID	Min. JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
13.	Obsługiwane protokoły sieciowe	SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP)
14.	Konto i folder współdzielony	- Min. liczba kont użytkowników lokalnych: 2 048 - Min. liczba grup lokalnych: 256 - Min. liczba folderów współdzielonych: 512 - Min. liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 500
15.	Zarządzanie pamięcią	- Min. rozmiar pojedynczego wolumenu: 108TB - Min. liczba migawek systemu: 65 500 - Min. liczba wewnętrznych wolumenów: 256
16.	Konserwacja	Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwanych szyn rack

17.	Zasilacze	Redundantne
18.	Waga	Max. 10kg
19.	Gwarancja	36 miesięcy. Uszkodzony dysk twardy pozostaje u Zamawiającego.

Dostawa serwera fizycznego wraz z niezbędnymi licencjami oraz oprogramowaniem

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
TYP 1 – 2 szt.		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
20.	Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Szyny wyposażone w organizer na kable.
21.	Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 230W. Wymagana ilość rdzeni dla procesora – 32. Minimalna częstotliwość pracy procesora 2.3GHz. Minimalna ilość kanałów procesora – 8. Wynik wydajności procesora nie powinien być niższy niż 705 punktów base w teście SPECrate 2017 Integer w teście konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org), dla ofertowanego serwera.
22.	Liczba zainstalowanych procesorów	2
23.	Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje.
24.	Pamięć operacyjna	Zainstalowane minimum 256GB pamięci RAM o częstotliwości 6400MHz. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.

25.	Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC
26.	Procesor Graficzny	Zintegrowana karta graficzna osiągająca rozdzielczość 1920x1200 przy 60 Hz.
27.	Dyski	W chwili dostawy serwer musi posiadać zainstalowane minimum 2 sztuki dysków SSD 2.5" SATA lub M.2 NVMe o pojemności przynajmniej 960 GB każdy, sterowane dedykowanym kontrolerem sprzętowym, spięte w RAID1. Ponadto serwer musi posiadać 4 sztuki dysków 2.5" HDD 10k SAS o pojemności min. 2.4TB każdy, spięte w RAID5.
28.	Kontroler dyskowy	Sprzętowy kontroler RAID obsługujący poziomy 0/1/10/5/50/6/60 wyposażony w min. 4GB pamięci cache.
29.	Zasilacze	Minimum dwa redundantne zasilacze o mocy minimum 1300W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
30.	Interfejsy sieciowe	Cztery porty 1GbE Base-T w jednej karcie niezajmującej slotu PCIe. Cztery porty 10/25GbE SFP28 w jednej karcie niezajmującej slotu PCIe. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. Komplet 4 wkładek SFP+ SR.
31.	Sloty I/O	Min. 2 sloty x16 gen.5
32.	Dodatkowe porty	Z przodu obudowy: 2x USB 3 (z czego jeden z możliwością zarządzania serwerem), zewnętrzny dedykowany port diagnostyczny. Z tyłu obudowy: 2x USB 3, 1x VGA, 1x RJ-45 do zarządzania serwerem.
33.	Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
34.	Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płycie I/O (wspomnianej w sekcji Dodatkowe Porty). Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, lokalizacja Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 Update systemowego firmware Monitoring i możliwość ograniczenia poboru prądu



	Zdalne włączanie/wyłączanie/restart Zapis video zdalnych sesji Podmontowanie lokalnych mediów z wykorzystaniem Java client Przekierowanie kosnoli szeregowej przez IPMI Zrzut ekranu w momencie zawieszenia systemu Możliwość przejęcia zdalnego ekranu Możliwość zdalnej instalacji systemu operacyjnego Alerty Syslog Przekierowanie konsoli szeregowej przez SSH Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera Możliwość mapowania obrazów ISO z lokalnego dysku operatora Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiegokolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarządzanie infrastruktura serwerówi storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń - możliwość skalowania do minimum 1000 urządzeń - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarządzania oparta o HTML 5 - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu,
--	--





		- automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń - definiowanie roli użytkowników oprogramowania - obsługa REST API oraz Windows PowerShell - obsługa SNMP, SYSLOG, Email Forwarding - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników - blokowanie możliwości podłączenia innego systemu zarządzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsługa NTP - przesyłanie alertów do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsolę albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtualizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesyłem plików diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk.
35.	Funkcje zabezpieczeń	Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płycie I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)., Zainstalowany przedni panel zamykany na klucz. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.

36.	Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
37.	Obsługa	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.
38.	Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID.
39.	Systemy operacyjne	- Windows Server 2025 Datacenter. - Dostarczona licencja musi zapewnić pełne pokrycie rdzeni procesora oferowanego serwera.
40.	Waga	maximum: 20 kg
41.	Gwarancja	36 miesięcy gwarancji producenta z reakcją NBD. W przypadku awarii dysku po wymianie dysk pozostaje u Zamawiającego.

Dostawa szafy RACK

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
	TYP	W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
	Wymiary	19" 800mm x 1200mm (Szerokość x Głębokość) Ilość miejsc instalacyjnych w szafie – min. 42U
2.	Drzwi przednie	Pojedyncze przednie drzwi umożliwiające swobodny przepływ powietrza przez całość drzwi (drzwi perforowane) min. 72% i

		posiadające zamknięcie na klucz lub inne rozwiązanie zabezpieczające przed nieautoryzowanym otwarciem.
3.	Drzwi tylne	Podwójne tylne drzwi o wymiarach umożliwiające swobodny przepływ powietrza przez całość drzwi (drzwi perforowane) min. 76%.
4.	Kolor	Czarny
5.	Nośność	Co najmniej 1500kg
6.	Gwarancja	Gwarancja min. 36 miesięcy.

Dostawa oprogramowania do ochrony przed ransomware – szyfrowana kopia zapasowa w chmurze

Informacje wstępne

1.1. Zamawiający planuje wdrożyć system kopii zapasowych Veeam Backup & Replication (VBR) (**lub równoważny**) zarządzający backupami oraz lokalne repozytorium backupu w oparciu o licencje typu rental dostarczane od obecnego dostawcy. Wykonywane są standardowe zadania backupu maszyn wirtualnych i stacji roboczych do lokalnego repozytorium zgodnie z ustanowioną polityką kopii zapasowych oraz kopie zapasowe wyniesione do obecnego dostawcy systemu kopii zapasowych. Zamawiający oczekuje od Wykonawcy przedłużenia licencji na obecne rozwiązanie wraz migracją kopii zapasowych lub dostarczenie kompletnego rozwiązania równoważnego, realizującego kopie lokalne oraz kopie wyniesione. W przypadku dostarczenia rozwiązania równoważnego, Wykonawca w ramach wdrożenia systemu zapewni również migrację lokalnych kopii zapasowych do dostarczonego systemu.

1.2. Zamawiający oczekuje dostarczenia jednego, kompletnego oprogramowania spełniającego wszystkie wymagania. Nie dopuszcza się dostarczenia dwóch odrębnych, zintegrowanych rozwiązań. Wykonawca zapewni licencje/subskrypcje ściśle dostosowane jakościowo i ilościowo do wymagań postępowania.

Wymagania dot. systemu kopii wyniesionych (off-site backup)

1.3. System musi zapewniać automatyczne wykonywanie i przechowywanie kopii zapasowych poza siedzibą Zamawiającego przez co najmniej 12 miesięcy od wdrożenia.

1.4. Komunikacja między infrastrukturą Zamawiającego a zdalnym miejscem składowania danych off-site musi odbywać się przy użyciu bezpiecznego protokołu (min. SSL/TLS lub IPSec).

1.5. System po stronie Wykonawcy nie może przyjmować ani przechowywać niezaszyfrowanych kopii zapasowych – wszystkie dane przesyłane off-site muszą być szyfrowane po stronie źródła.



- 1.6. Na żądanie Zamawiającego Wykonawca udostępni szczegółową lokalizację fizyczną (adres budynku, nr szafy/działu w centrum danych) urządzeń, na których przechowywane są wyniesione kopie danych.
- 1.7. Wykonawca zapewni samoobsługowy portal usługi kopii wyniesionych, umożliwiający:
 - 1.7.1. zdalne monitorowanie i zarządzanie kopiami zapasowymi z poziomu jednego, przyjaznego interfejsu WWW;
 - 1.7.2. zabezpieczenie dostępu do portalu przy użyciu SSL oraz wieloskładnikowej autentykacji (MFA – login, hasło i token);
 - 1.7.3. podgląd bieżącego i historycznego stanu zadań backupu oraz eksport raportów do pliku;
 - 1.7.4. możliwość uruchamiania, zatrzymywania, wznowiania zadań backupu oraz przeglądania ich logów (rejestrów zdarzeń);
 - 1.7.5. obsługę alarmów związanych z backupem i stanem usługi oraz eksport zdarzeń do pliku;
 - 1.7.6. funkcje raportowania i rozliczeń zasobów: przegląd wykorzystania przydzielonej przestrzeni, liczby chronionych serwerów/stacji/VM, generowanie raportów statystycznych;
 - 1.7.7. portal powinien udostępniać funkcje umożliwiające scentralizowane zarządzanie, monitorowanie oraz raportowanie usług backupu typu Backup-as-a-Service (BaaS) i Disaster Recovery-as-a-Service (DRaaS).
- 1.8. Dopuszczalne jest wykorzystanie technologii w trybie multi-tenant do realizacji kopiowania i przechowywania danych off-site (z zachowaniem izolacji klientów i szyfrowania transportu danych).
- 1.9. Wykonawca udostępni Zamawiającemu repozytorium na kopie zapasowe o pojemności 5 TB z możliwością rozbudowy do minimum 10 TB (wielkość dodatkowej rozbudowy repozytorium nie jest elementem oferty).
- 1.10. Zamawiający wymaga, aby dostarczone licencje/subskrypcje umożliwiały wykonywanie kopii zapasowych dla maszynach wirtualnych oraz stacji roboczych (komputery).
- 1.11. Sprzęt pamięci masowej musi wspierać transfer wielowątkowy danych, mieć redundancję wszystkich komponentów (brak pojedynczych punktów awarii – awaria jednego elementu nie przerywa pracy) oraz pozwalać na rozbudowę i aktualizację (firmware) w trybie online.
- 1.12. Architektura repozytorium musi gwarantować, że awaria dowolnego dysku, półki dyskowej, kontrolera, węzła czy zasilacza nie przerwie dostępu do pozostałych danych.
- 1.13. Awaryjne odtwarzanie danych z wyniesionego miejsca składowania danych musi odbywać się automatycznie za pomocą lokalnego interfejsu systemu kopii zapasowych Zamawiającego, bez udziału pracowników Wykonawcy.
- 1.14. Wykonawca zapewni wsparcie techniczne i utrzymanie rozwiązania przez cały okres realizacji przedmiotu zamówienia, tj. [12] miesięcy od wdrożenia. Na potrzeby zgłaszania zmian konfiguracji i awarii Wykonawca udostępni dedykowany kanał mailowy. Wykonawca gwarantuje:
 - 1.14.1. podjęcie zgłoszenia awarii w czasie nie dłuższym niż 4 godziny;
 - 1.14.2. usunięcie awarii w czasie nie dłuższym niż 24 godziny;
 - 1.14.3. podjęcie zgłoszenia zmiany konfiguracji w czasie nie dłuższym niż 8 godzin;
 - 1.14.4. realizację zgłoszenia zmiany konfiguracji wykonywania kopii wyniesionych w czasie nie dłuższym niż 2 dni robocze.
- 1.15. Wykonawca zobowiązany jest do zapewnienia pełnego wsparcia eksperckiego, merytorycznego i administracyjnego w zakresie realizacji przedmiotu zamówienia, zgodnie z najlepszymi praktykami i zgodnie z najnowszymi wytycznymi branżowymi i technologicznymi w tym zakresie, jak również wytycznymi z audytów przeprowadzanych przez instytucje zewnętrzne, którym podlega Zamawiający, przez cały okres obowiązywania umowy.
- 1.16. Wykonawca przygotowuje dokumentację użytkownika i administratora wdrożonego systemu.
- 1.17. Wykonawca zobowiązany jest do instruktażu 2 administratorów Zamawiającego z administrowania i obsługi dostarczonego rozwiązania.
- 1.18. Wykonawca jest odpowiedzialny za testowanie kopii zapasowych Zamawiającego pod kątem poprawności przechowywanych danych oraz konfiguracji oraz przeprowadzenie testów odtworzeniowych nie rzadziej niż dwa razy w ciągu roku.

Wymagania dot. centrum przetwarzania danych, w którym składowane będą kopie wyniesione

- 1.19. Centrum przetwarzania danych, w którym będą składowane wyniesione kopie zapasowe, musi spełniać co najmniej standard TIER III (poziom z pełną redundancją krytycznych systemów i możliwością utrzymania bez przerywania pracy centrum danych, zapewniający wysoką dostępność) lub równoważne.
- 1.20. Infrastruktura w centrum przetwarzania danych, spełnia co najmniej następujące wymagania:
 - 1.20.1. posiada aktywne elementy infrastruktury IT zapewniające pracę w modelu n+1;



- 1.20.2. musi posiadać redundantne wewnętrzne linie chłodu;
- 1.20.3. musi posiadać możliwość odłączania każdego elementu linii dystrybucji energii elektrycznej i chłodu w celu poddania czynnościom serwisowym, tak aby nie zakłócić normalnej pracy urządzeń dwuzasilaczowych;
- 1.20.4. musi posiadać wdrożoną strefową kontrolę dostępu w oparciu o karty zbliżeniowe lub rozwiązanie równoważne;
- 1.20.5. musi posiadać całodobową ochronę fizyczną z rejestracją kamer monitoringu wizyjnego na zewnątrz i wewnątrz budynku;
- 1.20.6. musi być zlokalizowane na terenie Polski w odległości nie mniejszej niż 100 km w linii prostej od siedziby Zamawiającego, gdzie znajduje się lokalne repozytorium backupu;
- 1.20.7. musi posiadać niezależne strefy pożarowe oraz system wczesnej detekcji dymu i ognia, a pomieszczenia ze sprzętem IT muszą być wyposażone w zautomatyzowaną aparaturę gaśniczą;
- 1.20.8. musi mieć zapewnione zasilanie z dwóch niezależnych linii energetycznych oraz rezerwowe zasilanie realizowane przy pomocy UPS oraz agregatu prądotwórczego;
- 1.20.9. musi posiadać zasilanie gwarantowane w układzie n+1, zapewniające nieprzerwane zasilanie;
- 1.20.10. dystrybucja energii elektrycznej odbywa się z wykorzystaniem niezależnych torów zasilania, z osobnym zabezpieczeniem nadmiarowo prądowym z gwarantowanym podtrzymaniem zasilania z wykorzystaniem UPS i agregatu prądotwórczego;
- 1.20.11. podstawowe i zapasowe łącza internetowe symetryczne każde o przepustowości nie mniejszej niż 1 Gb/s do infrastruktury, na której składowane będą wyniesione kopie zapasowe (Wykonawca nie zapewnia łącza po stronie Zamawiającego).

Warunki udziału

- 4.1. W postępowaniu może brać udział Wykonawca, który prowadzi działalność w zakresie usług informatycznych w Polsce nie krócej niż 5 lat oraz wykaże, że w okresie ostatnich 3 lat należycie wykonał co najmniej jedno zamówienie o wartości co najmniej 100 000,00 zł brutto obejmujące dostawę i wdrożenie oprogramowania do tworzenia kopii zapasowych
Zamawiający dopuszcza, aby w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek dotyczący zdolności technicznej spełniał w całości jeden Wykonawca lub Wykonawcy mogą spełniać warunek łącznie.
- 4.2. Wykonawca spełni warunek w zakresie zdolności technicznej lub zawodowej, jeżeli wykaże, że dysponuje osobami, które skieruje do realizacji przedmiotu zamówienia, a które to osoby posiadają poniższe doświadczenie, wykształcenie oraz kwalifikacje zawodowe:
 - 4.2.1. minimum dwie osoby która ciągu ostatnich 3 lat przed upływem terminu składania ofert brała udział we wdrożeniu co najmniej jednego projektu, którego przedmiotem było co najmniej wdrożenie i konfiguracja oprogramowania do tworzenia kopii zapasowych.
 - 4.2.2. minimum jedna osoba posiadająca ważny certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001 oraz ważny certyfikat Audytora Wiodącego Systemu Zarządzania Ciągłością Działania wg normy PN-EN, wydane przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338) w zakresie certyfikacji osób.

Informacje w zakresie równoważności certyfikatów:

Certyfikaty wskazane jako wymagane dla danego specjalisty mogą być zastąpione certyfikatami równoważnymi. Jako certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu wskazanego certyfikatu, co jest rozumiane jako:

- analogiczna dziedzina merytoryczna wynikająca z wiedzy, której dotyczy certyfikat (np. zarządzanie projektami, zarządzanie bazami danych, testowaniem, administracją bazami danych, programowanie, etc.),
- analogiczny stopień poziomu kompetencji (np. podstawowy, zaawansowany, ekspert),
- analogiczny poziom doświadczenia zawodowego wymagany dla otrzymania danego certyfikatu (np.: konieczność wykazania się uczestnictwem w określonej liczbie projektów w danej roli, etc.),



- uzyskanie certyfikatu potwierdzone jest egzaminem, o ile był wymagany.

Zamawiający dopuszcza, aby w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek dotyczący zdolności zawodowej spełniał w całości jeden Wykonawca lub Wykonawcy mogą spełniać warunek łącznie.

- 4.3. Zamawiający wymaga, aby Wykonawca znajdował się w dobrej sytuacji ekonomicznej umożliwiającej realizację usługi przez Wykonawcę, nie toczyło się w stosunku do niego postępowanie o ogłoszenie upadłości lub o otwarcie postępowania układowego albo zatwierdzenie układu, nie znajdował się w stanie upadłości ani nie obowiązywał go układ zatwierdzony w postępowaniu układowym, ani nie było prowadzone przeciwko niemu postępowanie egzekucyjne. Zamawiający dopuszcza, aby w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek dotyczący zdolności technicznej spełniał w całości każdy Wykonawca.
- 4.4. Zamawiający wymaga, aby Wykonawca w zakresie świadczonych usług chmurowych posiadał wdrożone i funkcjonujące systemy zarządzania zgodne z polskimi lub europejskimi standardami normalizacyjnymi, certyfikowane przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji systemów zarządzania:
- 4.4.1. PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji i zarządzania ciągłością działania w bezpieczeństwie informacji;
 - 4.4.2. PN-EN ISO 22301 dotyczące zarządzania ciągłością działania;
 - 4.4.3. PN-EN ISO/IEC 9001 dotyczące zarządzania jakością świadczenia usług;
 - 4.4.4. PN-EN ISO/IEC 14001 dotyczące zarządzania środowiskowego.

W celu potwierdzenia spełnienia wymogu Zamawiający oczekuje przedstawienia certyfikatów potwierdzających spełnienie wymogów, wydanych przez akredytowane przez PCA jednostki oceniające zgodność.

Zamawiający dopuszcza, aby w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek dotyczący zdolności technicznej spełniał w całości jeden Wykonawca lub Wykonawcy mogą spełniać warunek łącznie.

- 4.5. Zamawiający z uwagi na zapewnienie wysokiego standardu bezpieczeństwa i minimalizacji ryzyka wymaga, aby Wykonawca posiadał wdrożony system zarządzania bezpieczeństwem informacji zgodny z normą ISO 27001 nieprzerwanie przez okres nie krótszy niż 2 lat przed datą złożenia oferty. W celu potwierdzenia spełnienia wymogu Zamawiający oczekuje przedstawienia certyfikatów potwierdzających spełnienie wymogów, wydanych przez akredytowane przez PCA jednostki oceniające zgodność. Zamawiający dopuszcza, aby w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek dotyczący zdolności technicznej spełniał w całości każdy Wykonawca.
- 4.6. Zamawiający wymaga, aby Wykonawca posiadał w dniu składania oferty oraz przez cały okres świadczenia usług na rzecz Zamawiającego polisę ubezpieczenia OC z sumą gwarancyjną za szkody o wysokości minimum 500 000 zł. Zamawiający dopuszcza, aby w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek dotyczący zdolności technicznej spełniał w całości jeden Wykonawca lub Wykonawcy mogą spełniać warunek łącznie.

Dostawa zarządzalnych urządzeń sieciowych – przełączniki dostępowe 24p wraz z systemem NMS – 4 sztuki

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
TYP		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
42.	Wymagania ogólne	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack.
43.	Wymagane parametry fizyczne	Wymagane parametry fizyczne • możliwość montażu w szafie 19" • jeden wewnętrzny zasilacz 230V AC. Z możliwością dołożenia dodatkowego zasilacza o tych samych parametrach. (nie dopuszcza się rozwiązań zewnętrznych zasilaczy). Dołożenie dodatkowe redundantnego zasilacza nie jest wymagane w ramach tego zadania. • zasilacz powinien zapewnić budżet mocy PoE minimum 530 W • port USB umożliwiający podłączenie zewnętrznej pamięci flash
44.	Wymagana konfiguracja portów	Przełącznik musi posiadać minimum: • 24 portów Ethernet 100/1000 RJ-45 ze wsparciem dla standardu 802.3at • 4 porty typu SFP+ (1G/10G) do wykorzystania jako porty typu uplink / stacking • Dodatkowe 2 porty 1GE SFP+ z możliwością licencyjnego podniesienia przepustowości portu do 10G. W ramach zadania dostarczenie tej licencji nie jest wymagane. • Wszystkie powyższe porty muszą być dostępne od frontu urządzenia. Wraz z przełącznikiem należy dostarczyć odpowiednią ilość kompatybilnych modułów SFP/SFP+/DAC pozwalających zestawzić uzgodnione na etapie wdrożenia połączenia.
45.	Przełącznik	Przełącznik musi umożliwiać łączenie w stopy z zachowaniem następującej funkcjonalności: • Zarządzanie stosem poprzez jeden adres IP

		• Do min. 8 jednostek w stosie • Magistrala statkująca o wydajności 40 Gb/s • Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie • Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree • Przełącznik musi wspierać tzw. in-service software upgrade (ISSU) czyli aktualizację przełączników w stosie bez przerywania pracy całego stosu przełączników
46.	Matryca przełączająca	• Matryca przełączająca o wydajności min. 168 Gbps, wydajność przełączania przynajmniej 125 Mpps.
47.		• Obsługa min 16 000 adresów MAC
48.		• Wbudowana pamięć RAM min. 1 GB
49.		• Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB
50.		• Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
51.		• Obsługa ramek jumbo o wielkości min. 9 216 bajtów
52.		• Obsługa protokołu MVRP lub równoważny
53.		Wsparcie dla protokołów: • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 16 instancji protokołu MSTP lub zastosowanie osobnej instancji STP dla każdego VLANu. • Ethernet Ring Protection version 2
54.		• Obsługa min. 256 tras dla routingu IPv4
55.		• Obsługa min. 128 tras dla routingu IPv6

56.		Obsługa protokołów routingu minimum: - IPv4: statyczny, RIPv2 - IPv6: minimum: statyczny, RIPng
57.		Obsługa protokołów LLDP i LLDP-MED
58.		Przełącznik musi posiadać funkcjonalność DHCP Server
59.		Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3.
60.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: - min. 4 poziomy dostępu administracyjnego poprzez konsolę - autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL - możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www - zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6 - możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP - obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard - możliwość synchronizacji czasu zgodnie z NTP - Możliwość uwierzytelnienia użytkowników przez wbudowany w przełącznik CaptivePortal – nie dopuszcza się rozwiązań z uwierzytelnieniem na zewnętrznym Captive Portal.
61.	Wymagane opcje zarządzania	- możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN, - plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC), - urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych, - dedykowany port konsoli zgodny ze standardem RS-232, - Obsługa skryptów BASH oraz Python

		Możliwość zarządzania przełącznikiem przez Rest API – konieczność obsługi wszystkich funkcji przełącznika.
62.		Wraz z urządzeniami muszą zostać dostarczone: - pełna dokumentacja w języku polskim lub angielskim, - dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana.
63.		Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
64.		Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.
65.		Przełącznik powinien być objęty co najmniej ograniczoną dożywotnią gwarancją producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła przełącznik spełniający minimalne parametry techniczne wskazane w niniejszym dokumencie Dodatkowo: zamawiający wymaga, aby przełącznik posiadał 1-roczny serwis gwarancyjny na sprzęt. Wymiana uszkodzonego elementu w trybie 9x5xNBD, wraz z dostępem do najnowszych wersji oprogramowania.

System NMS – System do zarządzania siecią

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
-----	-------------------------------------	---

	1	2
TYP		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
1.	Wymagania ogólne	• System musi zapewnić możliwość zarządzania siecią przewodową (LAN) i bezprzewodową (WLAN) pochodzącą od tego samego producenta co NMS. • System musi pochodzić od tego samego producenta co dostarczane przełączniki LAN. • System musi zapewnić możliwość zarządzania urządzeniami sieciowymi (przełączniki LAN i access-pointy WLAN – jeśli dotyczy) zgodnie z ilościami dostarczonymi w ramach zadania, oraz mieć możliwość dalszej rozbudowy za pomocą licencji typu pojemnościowego. Minimalna pojemność systemu nie może być mniejsza niż: ○ 1000 przełączników sieciowych ○ 3000 punktów dostępowych • System musi być dostępny w formie maszyny wirtualnej możliwej do uruchomienia na platformach VMWare ESXi, Microsoft Hyper-V i Linux-KVM • System musi mieć możliwość rozszerzenia funkcjonalności za pomocą licencji, tak aby był w stanie wspierać mechanizmy wysokiej dostępności (praca w trybie High Availability). Jej dostarczenie w ramach tego zadania nie jest wymagane. • System musi posiadać zintegrowany moduł kontroli dostępu (Network Access Control) z różnymi możliwościami uwierzytelniania, takimi jak 802.1x, MAC i uwierzytelnianie oparte na certyfikatach. • System powinien posiadać wbudowany serwer RADIUS i funkcje Captive Portal • System musi obsługiwać zewnętrzne serwery RADIUS i LDAP z możliwością przypisywania ról oraz możliwość integracji z usługami Active Directory. • System musi obsługiwać ujednoliconą konfigurację zasad bezpieczeństwa dla uwierzytelniania urządzeń i użytkowników. • System powinien posiadać wbudowaną lokalną bazę danych zapewniającą obsługę dla urządzeń firmowych / należących do organizacji, kont użytkowników dla pracowników oraz gości. • Obsługa system musi być możliwa poprzez interfejs graficzny z wykorzystaniem przeglądarki WWW oraz skalowanie interfejsu umożliwiające wykorzystanie przeglądarek w urządzeniach mobilnych. • System musi zapewnić ujednolicony widok topologii sieci zarówno dla punktów dostępowych jak i przełączników, widok sąsiednich elementów sieci oraz ich połączeń i trybu w jakim obecnie pracują. • System musi wspierać geolokalizację zapewniając odwzorowanie topologii sieci bazując na koordynatach GPS lub podanym adresie fizycznym. • System musi zapewnić lokalizowanie użytkowników w infrastrukturze sieciowej tj. miejsce podłączenia switch/port oraz informacje nt.

		usługi L2 tj.: VLAN, usługa SPB, VxLAN, GRE Tunel. Weryfikowanie lokalizacji po adresie, nazwie sieciowej użytkownika, IP oraz MAC. • System powinien umożliwiać konfigurację przełączników sieciowych za pomocą predefiniowanych w systemie szablonów konfiguracji. • System musi posiadać narzędzia do automatycznego wykrywania urządzeń sieciowych instalowanych w sieci wraz z ich automatyczną konfiguracją tj. autoprovisioning. Nie dopuszcza się systemów NMS które wymagają fizycznego dostępu administratorów do przekazania przełącznikowi konfiguracji inicjalnej. • System musi posiadać możliwość granularnego definiowania poziomu dostępu dla administratorów, w tym możliwość tworzenia własnych ról z elastycznym wyborem uprawnień dla odczytu i/lub zapisu dla poszczególnych elementów systemu zarządzania oraz możliwość uwierzytelniania administratorów w oparciu o zewnętrzną bazę. • System musi obsługiwać uwierzytelnianie dwuskładnikowe dla dostępu administratora. • System musi zapewnić monitorowanie wydajności sieci i wskaźników KPI w czasie rzeczywistym za pomocą konfigurowalnego pulpitu z wizualnymi widżetami. • System powinien zapewniać możliwość tworzenia kopii zapasowych i przywracania konfiguracji urządzeń sieciowych. • System powinien obsługiwać zautomatyzowaną aktualizację oprogramowania sprzętowego urządzeń sieciowych w całej sieci. • Obsługa monitoringu przez SNMP v2/v3 • System musi zapewnić wsparcie dla konfiguracji: ○ sFlow ○ protokołu mDNS ○ multicast (m.in. PIM) w całej sieci ○ interfejsów VLAN w sieci przewodowej i bezprzewodowej ○ polityk QoS ○ pakietów SIP ○ VXLAN • System umożliwia konfigurację urządzeń poprzez terminal CLI bezpośrednio ze strony internetowej systemu zarządzania • System musi zapewniać wsparcie dla REST API, umożliwiające integrację z urządzeniami innych producentów. • System musi zapewnić obsługę priorytetyzacji ruchu dla dostępu gościnnego. • System musi zapewnić możliwość uwierzytelniania użytkowników typu BYOD oraz typu Gość w ilości min. 10 dla każdego typu, za pomocą wbudowanego captive portal, bez konieczności stosowania jakichkolwiek dodatkowych urządzeń/oprogramowania. • System musi zapewniać obsługę dostępu gościnnego poprzez ○ Samodzielną rejestrację klientów w oparciu o adres email, numer telefonu (wiadomość SMS)
--	--	---



		○ Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link) ○ Logowanie w oparciu o konta w mediach społecznościowych (min. Facebook, Google).
2.		• Zamawiający wymaga, aby system zarządzania posiadał minimum 1-roczny serwis tj. dostęp do najnowszych wersji oprogramowania, obsługę zgłoszeń serwisowych, pomoc w konfiguracji oraz analizie błędów.

Dostawa Access Point – 4 sztuki

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
TYP		W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
1.	Wymagania ogólne	Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków.

		Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na ścianie lub suficie.
2.	Parametry podstawowe	1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie: a. 5GHz - 802.11a/n/ac/ax b. 2.4GHz - 802.11b/g/n/ax 2. Możliwość zdalnego zarządzania punktem dostępowym. 3. Możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej, w szczególności z kontrolerami opisanymi w tym postępowaniu. 4. Możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: i. Musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową przy wykorzystaniu protokołu https, ii. Możliwość przeprowadzania wszystkich operacji konfiguracyjnych z poziomu przeglądarki, iii. Przełączenia punktu dostępowego do pracy z centralnym kontrolerem tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania. iv. Tworzenie klastra do 255 urządzeń 5. Punkt dostępowy musi posiadać wbudowane anteny do pracy w trybach 2x2:2 @ 2.4 GHz, 2x2:2 @ 5 GHz o zysku nie mniejszym niż 3dBi 6. Specyfikację radia 802.11a/n/ac/ax: a. Obsługiwana technologia OFDM oraz OFDMA, b. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM. c. Moc transmisji konfigurowalna przez administratora – możliwość konfiguracji zakresu ustawianej mocy

	d. Od 6,5 Mbps do 400 Mbps dla 802.11n e. Od 6,5 Mbps do 850 Mbps dla 802.11ac f. Od 3,6 Mbps do 573 Mbps dla 802.11ax (2,4GHz) g. Od 3,6 Mbps do 1200 Mbps dla 802.11ax (5GHz) h. Obsługa HT – kanały 20/40MHz dla 802.11n i. Obsługa VHT – kanały 20/40/80 dla 802.11ac j. Obsługa HE – kanały 20/40/80/ dla 802.11ax k. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz l. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac m. Wsparcie dla: n. STBC (Space-time block coding) o. LDPC (Low-density parity check) p. Technologia TxBF
	7. Specyfikacja radia 802.11b/g/n/ax: a. Technologia direct sequence spread spectrum (DSSS – tylko dla 802.11b), OFDM (tylko dla 802.11a/g/n/ac), OFDMA (tylko dla 802.11ax) b. Typy modulacji – CCK, BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM c. Moc transmisji konfigurowalna przez administratora
	8. Punkt dostępowy musi posiadać co najmniej a. 2 interfejsy 10/100/1000 Base-T • z funkcją POE

		• zgodny ze standardem 802.3az Energy Efficient Ethernet EEE b. zasilanie PoE 48V DC zgodne z 802.3af lub z zasilacza c. port USB d. przycisk przywracający konfigurację fabryczną e. Kontrolka LED do określania statusu systemu i interfejsów radiowych w tym możliwość fizycznej lokalizacji Punktu dostępowego poprzez ustawienie specjalnego trybu pracy kontroli LED (miganie lub zmiana kolorów). 9. Parametry pracy urządzenia: a. Temperatura otoczenia: 0-45 ° C b. Wilgotność 5% - 95% nie skondensowana c. Znak CE d. EN 60601-1-1, EN60601-1-2
3.	Parametry radiowe	1. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów. 2. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe 3. Monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu. 4. Rozkład ruchu pomiędzy różnymi punktami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma 5. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału 6. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz

		7. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11a/b/g). 8. Możliwość ustawienia parametru, po osiągnięciu którego klient sieci bezprzewodowej zostanie rozłączony od punktu dostępowego. 9. Możliwość ustawienia parametru, po osiągnięciu którego klient sieci bezprzewodowej zostanie rozłączony od punktu dostępowego oferujące gorsze parametry i podłączony do punktu dostępowego oferujące lepsze parametry radiowe. 10. Możliwość uruchomienia min 8 szt. SSID per radio (16 SSID na punkt dostępowy) 11. Możliwość zdefiniowania per SSID lub per Punkt Dostępowy transmisji ramek 802.11 z Guard Interval na poziomie 800ns – możliwość wyłączenia tzw. Short GI – w SSID działających w standardach 802.11n/ac 12. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane. 13. Pełna obsługa prawidłowego roamingu klientów sieci bezprzewodowej – obsługa standardów 802.11r oraz 802.11v/k
4.	Gwarancja	Zamawiający wymaga, aby urządzenie posiadało 1 roczny serwis gwarancyjny na sprzęt. Wymiana uszkodzonego elementu w trybie 9x5xNBD, wraz z dostępem do najnowszych wersji oprogramowania.

Dostawa UPS – 2 sztuki

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań
1	Moc pozorna	6 kVA
2	Moc rzeczywista	6 kW
3	Wyjściowy współczynnik mocy	1
4	Topologia (klasyfikacja IEC 62040-3)	Podwójna konwersja on-line
5	Typ obudowy	Uniwersalna tower/rack
6	Sprawność UPS'a	Minimum 96.4% przy pełnym obciążeniu w trybie online
7	Liczba, typ gniazd wyjściowych	Listwa zaciskowa + 6xC13 oraz co najmniej 6 uniwersalnych gniazd, pozwalających na podłączenie zarówno wtyku C14, jak i C20



7	Liczba, typ gniazd wyjściowych na bypassie serwisowym	Listwa zaciskowa + 2xC13 oraz co najmniej 3 uniwersalne gniazda, pozwalających na podłączenie zarówno wtyku C14, jak i C20
8	Typ gniazda wejściowego	Listwa zaciskowa (1ph)
9	Wymagany czas podtrzymania dla obciążenia mocą 5kW	16 minut
10	Dodatkowe baterie	Możliwość wydłużenia czasu podtrzymania do 170 minut przy obc. mocą 6 kW poprzez dołożenie dodatkowych modułów baterii zewnętrznych.
11	Napięcie znamionowe wejściowe	230 V (domyślnie) / 200/208/220/240 V
12	Tolerancja napięcia prostownika	176-276 V przy 100% obciążeniu, 100-276 V przy obciążeniu poniżej 40%
13	Częstotliwość znamionowa	50/60 Hz autodetekcja
14	Tolerancja częstotliwości	40 – 70 Hz
15	Kształt napięcia	Sinusoidalny
16	Napięcie znamionowe wyjściowe	230 V (domyślnie) / 200/208/220/240 V
17	Zakres zmian napięcia wyjściowego	+/-1% napięcia nominalnego
18	Częstotliwość wyjściowa	50/60 Hz
19	Całkowite odkształcenia napięcia THDu	< 1% dla obciążenia liniowego, < 5% dla obciążenia nieliniowego
20	THDi na wejściu	< 3% dla obciążenia liniowego, < 5% dla obciążenia nieliniowego
21	Przeciążalność falownika	do 125% przez 10 min., do 150% przez 30 s
22	Zdolność zwarciorowa falownika	90 A przez 5 okresów
23	Baterie wymieniane przez użytkownika "na gorąco"	Tak
24	Ochrona przed głębokim rozładowaniem	Tak
25	Okresowy automatyczny test baterii	Tak
26	Zimny start	Tak
27	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
28	Czas ładowania	Max. 3 godziny do poziomu 90%
29	Interfejs komunikacyjny	• USB
		• RS232 DB-9
		• miniport wyłącznik awaryjny RPO
		• miniport wyłącznik ON/OFF
		• 2 wyjścia bezpotencjałowe
		• slot na karte komunikacyjną SNMP



30	Panel sterowania z wyświetlaczem LCD	Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS'a) ze wskazaniami pomiarów napięcia i częstotliwości na wejściu oraz wyjściu, poziomu obciążenia (VA, W, %), poziomu naładowania baterii (%), pozostałego czasu podtrzymania (minuty), z możliwością sterowania poszczególnymi segmentami odbiorów.
		Poziomy rząd przycisków sterowania
		Poziomy rząd wskaźników stanu: trybu online (zielony), trybu bateryjnego (pomarańczowy), trybu bypass (pomarańczowy), usterki (czerwony)
31	Przyciski sterujące i wskaźniki diodowe LED	sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie)
		przycisk Escape (anulowanie)
		przyciski funkcyjne (przewijanie w górę i w dół)
		przycisk Enter (potwierdzający)
32	Wypożyczenie	UPS 6 kVA, instrukcja "szybki start", instrukcja bezpieczeństwa oraz zewnętrzny bypass serwisowy
		2 przewody IEC 10 A o długości min. 1,2 m
		kabel USB
		karta SNMP
		podstawki do montażu pionowego (wieża)
		zestaw szyn montażowych do szafy 19"
33	Karta SNMP	obsługiwane protokoły: IPv4/v6, TLS, SNMPv1/v3, DHCP, SSH, LDAP
		prędkość gigabit'owa (half-duplex, full-duplex)
		różne poziomy nadawania dostępu do konta administratora lub użytkownika
34	Zgodność z normami dot. cyberbezpieczeństwa	UL 2900-1 / IEC62443-4-2
36	Maksymalna wysokość wraz z dodatkowym modulem bateryjnym	6U
37	Poziom hałasu w odl. 1m	< 38 dB w trybie normalnym i obciążeniu poniżej 60%, < 49 dB w trybie bateryjnym
38	Zgodność z normami UE	Deklaracja zgodności producenta
39	Dodatkowe certyfikaty	ISO9001 producenta urządzenia, Energy Star, zgodność z EU CoC 2021 Elite
40	Gwarancja producenta	36 miesięcy na elektronikę, 24 miesiące na baterie - gwarancja będzie realizowana w miejscu pracy urządzenia (on-site)

Dostawa mobilnego agregatu – 2szt wraz z wykonaniem przyłącza do agregatu – 1 szt

Agregat prądotwórczy mobilny (na przyczepie) 20 kW / 25 kVA – awaryjne źródło zasilania

Dostawa fabrycznie nowego, mobilnego zespołu prądotwórczego posadowionego na przyczepie transportowej, spełniającego minimalne parametry techniczne określone w poniższej tabeli. Podane wartości stanowią wymagania minimalne – dopuszcza się urządzenia o parametrach nie gorszych niż wskazane.

W ramach dostawy należy zaprojektować oraz wykonać przyłącze do agregatu w siedzibie Zamawiającego.

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
	1	2
TYP		W ofercie należy podać producenta, model / typ oraz kraj pochodzenia oferowanego agregatu prądotwórczego oraz przyczepy transportowej.
1	Przeznaczenie i wykonanie	Agregat prądotwórczy przeznaczony do pracy jako awaryjne (rezerwowe) źródło zasilania elektrycznego. Wykonanie mobilne – zespół prądotwórczy posadowiony na przyczepie transportowej dopuszczonej do ruchu drogowego, dostarczony jako gotowy do jazdy zestaw. Agregat w obudowie dźwiękochłonnej (wyciszonej), przystosowany do pracy na zewnątrz. Agregat dostarczony w pełni przygotowany do pracy, wraz z kompletem płynów eksploatacyjnych (bez paliwa).
2	Moc znamionowa i maksymalna	Moc stała (ciągła): nie mniej niż 16 kW / 20 kVA. Moc maksymalna (chwilowa): nie mniej niż 18 kW / 22,5 kVA. Współczynnik mocy $\cos\phi = 0,8$.

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
3	Napięcie i częstotliwość	Napięcie znamionowe 400 / 230 V, układ trójfazowy 4-przewodowy. Częstotliwość znamionowa 50 Hz. Elektroniczna stabilizacja napięcia; tolerancja napięcia nie gorsza niż $\pm 3\%$.
4	Silnik	Silnik wysokoprężny, 4-cylindrowy, wolnossący, chłodzony cieczą. Prędkość obrotowa: 1500 obr/min. Rozruch elektryczny. Układ podgrzewania kolektora (dolotu powietrza). Paliwo zgodne z normą EN 590.
5	Prądnica	Prądnica bezszczotkowa, samowzbudna, synchroniczna. Elektroniczna stabilizacja napięcia (AVR); tolerancja nie gorsza niż $\pm 3\%$. Stopień ochrony: nie niższy niż IP21. Współczynnik mocy $\cos\phi = 0,8$.
6	Panel odbioru mocy	Panel (listwa) odbioru mocy z wyłącznikiem, wyposażony co najmniej w: a) 2 $\times$ gniazdo 230V, b) 1 $\times$ gniazdo 400V.

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
		Każde gniazdo zabezpieczone; wyłącznik / zabezpieczenie nadprądowe dobrane do prądu znamionowego agregatu. W komplecie wtyczki do oferowanych gniazd.
7	Zbiornik paliwa	Zintegrowany zbiornik paliwa zapewniający pracę ciągłą agregatu. Kontrola poziomu paliwa (odczyt w sterowniku).
8	Poziom hałasu	Obudowa dźwiękochłonna zapewniająca obniżony poziom hałasu, umożliwiającą pracę w sąsiedztwie zabudowy.
9	Automatyka i sterowanie (SZR)	Mikroprocesorowy sterownik agregatu z wyświetlaczem (komputer pokładowy), umożliwiający kontrolę co najmniej: obrotów silnika, temperatury silnika / cieczy, czasu pracy, poziomu paliwa, pobieranej mocy oraz napięcia. Zintegrowany moduł SZR / ATS (samoczynne załączanie rezerwy): automatyczny start agregatu przy zaniku zasilania sieciowego, automatyczne przejęcie zasilania, a po powrocie sieci – przełączenie na sieć, schłodzenie i wyłączenie agregatu. Zabezpieczenia generatora (nad-/podnapięciowe, częstotliwościowe, przeciążeniowe). Automatyczny prostownik – podtrzymanie i ładowanie akumulatora rozruchowego.

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
		Układ podgrzewania bloku silnika (grzałka) utrzymujący gotowość rozruchową.
10	Wypożyczenie podstawowe	Agregat wyposażony co najmniej w: a) obudowę dźwiękochłonną z czerpniami i wyrzutniami powietrza, b) komplet wibroizolatorów, c) tłumik odprowadzający spaliny, d) akumulator rozruchowy wraz z instalacją, e) komplet płynów eksploatacyjnych (bez paliwa).
11	Przyczepa transportowa	Przyczepa specjalna z osią hamowaną, dopuszczona do ruchu drogowego. Dopuszczalna masa całkowita (DMC): nie mniejsza niż 1200 kg, zapewniająca zapas ładowności względem masy zestawu (agregat wraz z osprzętem i paliwem) nie mniejszy niż 20%. Osie oraz zaczep (hak) produkcji Al-Ko (Niemcy) lub równoważne. Konstrukcja ramy ażurowa, ocynkowana. Koła w rozmiarze 185 R14C. Homologacja / dokumenty umożliwiające rejestrację i dopuszczenie do ruchu drogowego.

Lp.	Nazwa parametru, elementu lub cechy	Wymagane minimalne parametry techniczne
12	Wymiary i masa agregatu	Wymiary agregatu (dł. × szer. × wys.): ok. 190 × 95 × 110 cm. Masa netto agregatu: ok. 770 kg.
13	Dokumentacja i zgodność	Wraz z urządzeniem należy dostarczyć: a) dokumentację techniczno-ruchową (DTR) / instrukcję obsługi w języku polskim, b) deklarację zgodności CE, c) dokumenty przyczepy umożliwiające jej rejestrację / dopuszczenie do ruchu drogowego.
14	Warunki dostawy	Urządzenie fabrycznie nowe, kompletne, gotowe do uruchomienia. Urządzenie pochodzące z autoryzowanego kanału dystrybucji na teren Unii Europejskiej.
15	Gwarancja i serwis	Gwarancja: nie krócej niż 24 miesiące. Przeglądy okresowe oraz serwisowanie agregatu w okresie gwarancji realizuje Zamawiający we własnym zakresie i na własny koszt, zgodnie z wymaganiami producenta; ich wykonanie stanowi warunek utrzymania gwarancji. Serwis gwarancyjny realizowany na terenie Polski; zapewniony dostęp do części zamiennych i serwisu pogwarancyjnego.

Wszędzie tam, gdzie parametry określono poprzez odniesienie do konkretnych wartości, norm, marek lub oznaczeń, Zamawiający dopuszcza rozwiązania równoważne o parametrach nie gorszych niż wskazane. Wykazanie równoważności spoczywa na Wykonawcy.

Profesjonalna usługa wdrożenia i utrzymania rozwiązań; testy oraz audyt cyberbezpieczeństwa sieci oraz wszelkie wymagania

Wymagania dot. montażu sprzętu, instalacji i konfiguracji sprzętu oraz oprogramowania.

Wszystkie dostarczone urządzenia zostaną podłączone i skonfigurowane zgodnie z aktualną wiedzą techniczną i zaleceniami producenta oraz przez osobę odpowiednio wykwalifikowaną. Prace wdrożeniowe będą obejmowały instalację i konfigurację urządzeń oraz oprogramowania.

Minimalny zakres :

- fizyczny montaż urządzeń w miejscu wskazanym przez Zamawiającego
- podłączenie urządzeń do istniejącej instalacji prądowej
- podłączenie urządzeń do sieci LAN Zamawiającego
- instalacja i konfiguracja serwerów
- instalacja i konfiguracja przełączników LAN
- instalacja i konfiguracja UTM
- instalacja i konfiguracja systemu kopii zapasowych
- konfiguracja polityk wykonywania kopii zapasowych
- wykonanie weryfikacji prawidłowego działania dostarczonych urządzeń oraz oprogramowania
- **segmentacja sieci** – wykonana zgodnie z dobrymi praktykami
- wdrożenie oprogramowania ALL-IN-One – i świadczenie usługi SOC
- wdrożenie rozwiązania typu IDS

Szczegółowy zakres:

1. Usługi w zakresie Serwerów z oprogramowaniem,

- Instalacja urządzeń w szafie RACK w miejscu wyznaczonym przez Zamawiającego,
- Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego,
- Okablowanie sieciowe urządzeń,
- Uruchomienie i weryfikacja poprawności działania urządzeń,
- Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,
- Konfiguracja adresacji IP interfejsów zarządzania,
- Konfiguracja protokołu synchronizacji czasu NTP,

- Konfiguracja protokołu rozwiązywania nazw DNS,
- Instalacja systemu wirtualizacji, w oparciu o najlepsze praktyki producenta w zakresie konfiguracji oraz bezpieczeństwa,
- Konfiguracja sieci zarządzania wirtualizatora w tym IPv4, NTP, DNS,
- Konfiguracja klastra wysokiej dostępności
- Konfiguracja wirtualnych sieci – VLAN,
- Wdrożenie wirtualnej maszyny z systemem operacyjnym Microsoft Windows Server 2025,
- Integracja Lokalnego centrum certyfikacji z domeną Microsoft Active Directory,
- Przygotowanie polityk bezpieczeństwa na UTM Zamawiającego, w celu zabezpieczenia serwerów produkcyjnych.

2. Usługi w zakresie Przełącznik LAN typu ACCESS

- Instalacja urządzeń w szafie RACK w miejscu wyznaczonym przez Zamawiającego,
- Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego,
- Okablowanie sieciowe urządzeń,
- Uruchomienie i weryfikacja poprawności działania urządzeń,
- Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,
- Konfiguracja nadmiarowej konstrukcji stosu,
- Konfiguracja adresacji IP interfejsów zarządzania,
- Konfiguracja protokołu synchronizacji czasu NTP,
- Konfiguracja protokołu rozwiązywania nazw DNS,
- Konfiguracja wirtualnych sieci VLAN,

3. Uruchomienie rozwiązania All-In-One

- Wdrożenie oprogramowania na środowisku Zamawiającego
- Włączenie ochrony wszystkich endpointów
- Weryfikacja alertów, a także polityk
- Konfiguracja integracji z wdrażanymi rozwiązaniami
- Po pozytywnym wdrożeniu przedstawienie wszelkich procedur związanych ze świadczeniem usługi SOC i linii kontaktu

Dostarczenie wszelkich komponentów potrzebnych do zamontowania dostarczonych urządzeń oraz do połączenia urządzeń do infrastruktury pasywnej (np. przewody krosowe).

Wykonawca po zainstalowaniu wszystkich dostarczonych urządzeń opracuje dokumentację techniczną powykonawczą zawierającą opis montażu, instalacji i konfiguracji zainstalowanych komponentów.

Testy bezpieczeństwa infrastruktury IT

1. Celem testów bezpieczeństwa jest:
 - a. Identyfikacja podatności i błędów konfiguracyjnych w elementach infrastruktury IT.
 - b. Ograniczenie ryzyka naruszeń poprzez rekomendacje działań naprawczych.
 - c. Dostarczenie wyników możliwych do wdrożenia i audytowania.
2. Zakres testów obejmuje:
 - a. Testy zewnętrzne – skany podatności urządzeń oraz usług osiągalnych z publicznej sieci Internet.
 - b. Testy wewnętrzne – skany podatności urządzeń oraz usług dostępnych w sieci wewnętrznej LAN. Testami należy objąć urządzenia oraz usługi IT, w tym: routery, przełączniki, zapory sieciowe, VPN, stacje klienckie, serwery usług katalogowych oraz usług sieciowych, Windows/Linux.
3. Testy zostaną przeprowadzone zgodnie z wybranymi elementami standardów i metodyk, takich jak:
 - a. OWASP Testing Guide
 - b. OSSTMM
 - c. PTES
 - d. NIST SP 800-115

Zakres prac obejmuje identyfikację podatności i błędów konfiguracyjnych bez aktywnej eksploatacji, testów typu DoS/DDoS oraz bez wykonywania testów iniekcyjnych, a więc bez działań mogących wpływać na integralność, poufność lub dostępność danych i systemów – działania te podlegają wyłączeniu względem ww. standardów i metodyk.

4. Raport z testów powinien zawierać co najmniej:
 - a. Opis środowiska testowego
 - b. Wykryte słabości i podatności
 - c. Poziomy ryzyka (np. CVSS)
 - d. Rekomendacje naprawcze dla podatności średnich, wysokich i krytycznych
5. Warunki techniczne i organizacyjne:
 - a. Zamawiający udostępni Wykonawcy niezbędne informacje, w tym: adresy IP, pliki konfiguracyjne i dokumentację, wymagane do przeprowadzenia testów.
 - b. Testy powinny zostać wykonywane w sposób kontrolowany, po uprzednim ustaleniu z Zamawiającym zakresu oraz ram czasowych.

Audyt cyberbezpieczeństwa sieci IT/OT

1. Celem audytu jest techniczna ocena bezpieczeństwa sieci IT/OT w celu oceny poziomu zabezpieczeń, identyfikacji nieprawidłowości konfiguracyjnych, luk bezpieczeństwa oraz ryzyk związanych z komunikacją pomiędzy strefami sieciowymi, a także dostępem zdalnym i administracyjnym.
2. Audyt powinien obejmować weryfikację konfiguracji i aktualności urządzeń związanych z bezpieczeństwem sieci. Zakres audytu obejmuje:
 - a. Przegląd architektury sieci IT/OT
 - b. Audyt segmentacji sieci IT/OT

- c. Audyt konfiguracji urządzeń sieciowych
 - d. Przegląd reguł firewall/UTM
 - e. Przegląd tuneli VPN oraz dostępu zdalnego VPN
 - f. Przegląd kont administracyjnych wraz z weryfikacją zmiany domyślnych poświadczeń oraz stosowaną polityką haseł
 - g. Wykrycie oraz audyt aplikacji i usług udostępnionych do publicznej sieci Internet
 - h. Weryfikacja poufności danych przesyłanych w sieci
3. Minimalny zakres informacji w raporcie obejmuje:
- a. Opis audytowanego środowiska
 - b. Rekomendacje działań korygujących lub naprawczych
 - c. Rekomendacje w zakresie infrastruktury sieciowej: jej architektury, konfiguracji, stosowanych zabezpieczeń, adekwatności do wymaganego / oczekiwanego poziomu bezpieczeństwa

Wymagania dotyczące zdolności technicznej i organizacyjnej znajdują się w zapytaniu ofertowym w punkcie 5.3.2.

Część II.

