Opis przedmiotu zamówienia

Dostawa i wdrożenie rozwiązań cyberbezpieczeństwa IT i OT dla Tarnowskich Wodociągów Spółka z ograniczoną odpowiedzialnością

Zamawiający:

Tarnowskie Wodociągi Sp. z o.o.,

ul. Gabriela Narutowicza 37

33-100 Tarnów.

Cyberbezpieczne Wodociągi

Przedmiotem zamówienia jest rozbudowa posiadanej infrastruktury i uruchomienie spójnego środowiska bezpieczeństwa IT i OT, obejmującego sieć, segmentację, zarządzanie politykami, kopie zapasowe, monitoring, logowanie, zarządzanie podatnościami, tożsamością i hasłami oraz obsługę incydentów. Rezultatem ma być działające i udokumentowane rozwiązanie, odebrane na podstawie testów funkcjonalnych i integracyjnych.

Główne części zamówienia

1. Pakiet 1 - Rozbudowa LAN i WLAN, zachowanie istniejącej segmentacji oraz wdrożenie kontroli dostępu NAC,
2. Pakiet 2 - Zarządzanie politykami bezpieczeństwa
3. Pakiet 3 - Lokalna infrastruktura kopii zapasowych
4. Pakiet 4 - Monitoring infrastruktury i obsługa usług IT
5. Pakiet 5 - Centralne logowanie, wykrywanie zagrożeń i obsługa incydentów
6. Pakiet 6 - Badanie podatności zarządzanie podatnościami i testów
7. Pakiet 7 - Zarządzanie tożsamością i centralny menedżer haseł
8. Pakiet 8 - Projekt wdrożenie integracje dokumentacja i utrzymanie

Pakiet 1. Rozbudowa LAN i WLAN, zachowanie istniejącej segmentacji oraz wdrożenie kontroli dostępu NAC

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja, integracja, uruchomienie, testy odbiorowe, przekazanie do eksploatacji oraz utrzymanie zintegrowanego zestawu rozwiązań technicznych służących podniesieniu poziomu cyberbezpieczeństwa środowiska IT oraz OT/ICS Zamawiającego.
Zamówienie obejmuje wdrożenie rozwiązań sprzętowych, programowych oraz usług wdrożeniowych i utrzymaniowych, których celem jest zwiększenie odporności infrastruktury teleinformatycznej i przemysłowej Zamawiającego na cyberzagrożenia, ograniczenie ryzyka utraty dostępności usług, poprawa widoczności zasobów, uporządkowanie zarządzania podatnościami, wzmocnienie segmentacji sieci, kontrola dostępu do infrastruktury oraz zapewnienie bezpiecznego dostępu administracyjnego i serwisowego do systemów krytycznych.

1.1 Zarządzane przełączniki dostępowe (2 szt)

Przedmiotem zamówienia jest dostawa, instalacja i konfiguracja 2 zarządzanych przełączników dostępowych, przeznaczonych do rozbudowy istniejącej infrastruktury Alcatel-Lucent Enterprise OmniSwitch. Nadrzędnym systemem zarządzania urządzeniami i ich profilami dostępu pozostaje posiadane przez Zamawiającego oprogramowanie OmniVista. Nie przewiduje się zastąpienia tej platformy ani wdrożenia nowego systemu NAC.

Dostarczane urządzenia muszą integrować się funkcjonalnie z istniejącym OmniVista w zakresie konfiguracji, monitoringu, profili dostępu i uwierzytelniania. Wykonawca zachowa dotychczasową segmentację sieci Zamawiającego i nie zmieni adresacji, VLAN, routingu ani reguł separacji bez wcześniejszej pisemnej akceptacji. Sam odczyt parametrów przez SNMP lub zapewnienie łączności Ethernet nie spełnia warunku integracji.

1. Integracja z posiadanym systemem zarządzania
Przełączniki muszą zostać włączone do posiadanego systemu OmniVista i umożliwiać z jego poziomu co najmniej:
a) identyfikację urządzenia, jego modelu, numeru seryjnego i wersji oprogramowania;
b) prezentację stanu urządzenia, portów i połączeń;
c) konfigurację portów, sieci VLAN i profili dostępu;
d) wykonywanie i odtwarzanie kopii konfiguracji;
e) dystrybucję aktualizacji oprogramowania;
f) obsługę alarmów i zdarzeń eksploatacyjnych.
g) możliwość stworzenia wspólnego stos Virtual Chassis
Wymagane funkcje należy uruchomić w wersji OmniVista użytkowanej przez Zamawiającego albo po jej aktualizacji uwzględnionej w cenie zamówienia, zachowującej obsługę istniejących urządzeń.

2. Współpraca z posiadanymi mechanizmami NAC
Przełączniki muszą umożliwiać wykorzystanie profili dostępu User Network Profile — UNP, zarządzanych w posiadanym środowisku OmniVista, oraz współpracę z mechanizmami Unified Policy Authentication Manager — UPAM w zakresie objętym licencją Zamawiającego.
Wymagana jest możliwość przypisywania uwierzytelnionym użytkownikom lub urządzeniom profilu obejmującego sieć VLAN, ograniczenia dostępu ACL oraz parametry ograniczenia pasma. Wykonawca zapewni zgodność sposobu definiowania i egzekwowania tych profili pomiędzy posiadanymi a dostarczanymi urządzeniami.
Wymagane są również:
a) uwierzytelnianie IEEE 802.1X;
b) uwierzytelnianie urządzeń bez obsługi 802.1X na podstawie adresu MAC, jako kontrolowany wyjątek;
c) obsługa RADIUS oraz RADIUS CoA umożliwiająca zmianę uprawnień aktywnego użytkownika lub urządzenia;
d) rejestrowanie wyniku uwierzytelnienia i zastosowanego profilu dostępu.

3. Bezpieczeństwo i odporność
Urządzenia muszą obsługiwać VLAN, ACL, MACsec IEEE 802.1AE na portach wskazanych w projekcie, LACP, mechanizmy ochrony przed pętlami, DHCP snooping oraz szyfrowane zarządzanie przez SSH i HTTPS.
Należy zapewnić redundantne połączenia z posiadaną infrastrukturą oraz dostarczyć wymagane przewody, wkładki i licencje zgodnie z wykazem połączeń.

5. Potwierdzenie zgodności i odbiór
Wykonawca przedstawi dokumentację potwierdzającą zgodność oferowanych urządzeń i wersji oprogramowania z posiadanym OmniVista oraz opisze wymagane rozszerzenia licencyjne.

Odbiór obejmie demonstrację centralnej konfiguracji VLAN, zastosowania profilu UNP, uwierzytelnienia 802.1X, zmiany uprawnień przez CoA oraz wykonania i odtworzenia kopii konfiguracji.
Urządzenia należy włączyć do posiadanego OmniVista w zakresie wykrywania, konfiguracji VLAN i profili dostępu, monitoringu portów, kopii konfiguracji i aktualizacji. Dostawa obejmuje potrzebne rozszerzenia licencji na 2 przełączniki. Ująć kompletny zestaw połączeń potrzebny dla dwóch nowych urządzeń: po dwa redundantne uplinki 10 Gb/s na urządzenie oraz połączenia stosu, jeżeli stos stanowi część projektu

1.1.2. Wymagania technicznie przełącznika zarządzanego TYP – 1 -1 szt

Lp.	Opis	Wymagania techniczne
1.	Wymagania ogólne	obudowa 1RU, do szafy rack 19 cali. Dostawa obejmuje zasilacz AC, przewód zasilający właściwy dla Polski, instrukcje oraz zestaw montażowy rack 19 cali. Wszystkie wymagane funkcje muszą być dostępne w dostarczonej wersji oprogramowania i licencjach.
2.	Parametry fizyczne i zasilanie	Możliwość montażu w szafie 19 cali; wysokość 1U. Jeden stały wewnętrzny zasilacz AC, przystosowany do sieci 230 V. Gniazdo dla drugiego, wewnętrznego modułowego zasilacza rezerwowego; możliwość dołożenia kompatybilnego zasilacza OS6560-BP. Drugi zasilacz stanowi opcję rozbudowy, bez obowiązku dostawy. Port USB do podłączenia zewnętrznej pamięci flash.
3.	Konfiguracja portów	Minimum 8 portów SFP+ 1/10 Gb/s, obsługujących kompatybilne moduły SFP 1 Gb/s i SFP+ 10 Gb/s, oraz 2 dedykowane porty QSFP+ 20 Gb/s do stackowania (VFL). Porty dostępne od frontu urządzenia. Portów QSFP+ nie należy traktować jako standardowych uplinków 40 Gb/s.
4.	Stackowanie Virtual Chassis	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: Zarządzanie stosem poprzez jeden adres IP Do min. 8 jednostek w stosie Przepustowość stackowania pojedynczego urządzenia minimum 80 Gb/s łącznie w pełnym dupleksie przez dwa porty 20 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 Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia. Stackowanie realizowane przez dedykowane porty QSFP+ 20 Gb/s. Niezbędne przewody stackujące, dobrane do docelowego połączenia urządzeń objętych dostawą, należy uwzględnić w dostawie.
5.	Wydajność przełączania	Matryca przełączająca minimum 240 Gb/s; wydajność przekazywania pakietów minimum 178,6 Mpps.
6.	Tablica adresów MAC	Obsługa min 16 000 adresów MAC
7.	Pamięć RAM	Wbudowana pamięć RAM min. 2 GB
8.	Pamięć flash	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB
9.	Sieci VLAN i QinQ	Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ) Funkcję QinQ należy dostarczyć z licencją OS6560-SW-ME, jeśli jest wymagana dla dostarczonej wersji AOS.
10.	Ramki jumbo	Obsługa ramek jumbo o wielkości min. 9 216 bajtów
11.	Rejestracja VLAN	Obsługa protokołu MVRP lub równoważny
12.	Ochrona przed pętlami	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 Wykonawca zapewni licencje wymagane do realizacji ERPv2 w dostarczonej wersji AOS.

Lp.	Opis	Wymagania techniczne
13.	Routing IPv4	Obsługa min. 256 tras dla routingu IPv4
14.	Routing IPv6	Obsługa min. 128 tras dla routingu IPv6
15.	Protokoły routingu	Obsługa protokołów routingu minimum: IPv4: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów). IPv6: minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów). Jeżeli funkcje OSPF wykraczają poza dostępny tryb Access/Stub OSPF, dostawa musi obejmować OS6560-SW-AR. Wykonawca potwierdzi obsługę co najmniej 8 interfejsów OSPF w dostarczonej konfiguracji.
16.	Wykrywanie	Obsługa protokołów LLDP i LLDP-MED
17.	Serwer DHCP	Przełącznik musi posiadać funkcjonalność DHCP Server
18.	Multicast	Obsługa ruchu multicast: IGMP Snooping v1, v2 i v3
19.	DHCP snooping	Obsługa mechanizmu DHCP snooping

1.1.3. Wymagania technicznie przełącznika zarządzanego TYP – 2 – 1 szt

Lp.	Opis	Wymagania techniczne
1.	Wymagania ogólne	Obudowa 1U, przeznaczona do montażu w szafie rack 19 cali. Dostawa obejmuje wbudowany zasilacz AC, przewód zasilający właściwy dla Polski, instrukcje oraz zestaw montażowy rack 19 cali. Wszystkie wymagane funkcje muszą być dostępne w dostarczonej wersji oprogramowania i licencjach.
2.	Parametry fizyczne i zasilanie	Jeden stały wewnętrzny zasilacz AC, przystosowany do sieci 230 V. Gniazdo dla drugiego, wewnętrznego modułowego zasilacza rezerwowego; możliwość dołożenia kompatybilnego zasilacza OS6560-BP. Drugi zasilacz stanowi opcję rozbudowy, bez obowiązku dostawy. Minimum 1 port USB do podłączenia zewnętrznej pamięci flash oraz 1 port konsolowy.
3.	Konfiguracja portów	Minimum 24 porty RJ-45 10/100/1000 Mb/s, 2 dodatkowe porty SFP 1 Gb/s oraz 4 porty SFP+ 1/10 Gb/s, obsługujące kompatybilne moduły SFP 1 Gb/s i SFP+ 10 Gb/s. Porty SFP+ 1/10 Gb/s mogą pełnić funkcję uplinków lub portów stackujących. Porty dostępne od frontu urządzenia. Model OS6560-24X4 jest wersją bez PoE.
4.	Stackowanie Virtual Chassis	Przełącznik musi umożliwiać łączenie w stosy Virtual Chassis z następującą funkcjonalnością: Zarządzanie stosem poprzez jeden adres IP. Obsługa co najmniej 8 jednostek w stosie. Przepustowość stackowania pojedynczego urządzenia minimum 40 Gb/s łącznie w pełnym dupleksie, przy wykorzystaniu dwóch połączeń 10 Gb/s. Możliwość tworzenia połączeń link aggregation zgodnie z IEEE 802.3ad/802.1AX dla portów należących do różnych jednostek stosu. Stos widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia Spanning Tree. Stackowanie realizowane przez porty SFP+ 10 Gb/s współdzielone z funkcją uplinków. Przy wykorzystaniu dwóch spośród czterech portów SFP+ 1/10 Gb/s do stackowania pozostają dwa takie porty na uplinki. Niezbędne kompatybilne przewody DAC SFP+ 10 Gb/s lub moduły optyczne wraz z okablowaniem, dobrane do docelowego połączenia urządzeń objętych dostawą, należy uwzględnić w dostawie.

Lp.	Opis	Wymagania techniczne
5.	Wydajność przełączania	Matryca przełączająca minimum 168 Gb/s; wydajność przekazywania pakietów minimum 125 Mpps.
6.	Tablica adresów MAC	Obsługa min 16 000 adresów MAC
7.	Pamięć RAM	Wbudowana pamięć RAM minimum 1 GB.
8.	Pamięć flash	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB
9.	Sieci VLAN i QinQ	Obsługa minimum 4000 sieci VLAN oraz IEEE 802.1ad QinQ (VLAN stacking). Dostawa obejmuje licencję OS6560-SW-ME udostępniającą wymagane funkcje Metro Ethernet.
10.	Ramki jumbo	Obsługa ramek jumbo o wielkości min. 9 216 bajtów
11.	Rejestracja VLAN	Obsługa protokołu MVRP lub równoważny
12.	Ochrona przed pętlami	Wsparcie dla IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multiple Spanning Tree. Obsługa osobnej instancji STP dla każdego VLAN (tryb 1x1 STP). Obsługa Ethernet Ring Protection v2 zgodnie z ITU-T G.8032/Y.1344. Dostawa obejmuje licencję OS6560-SW-ME udostępniającą wymagane funkcje Metro Ethernet.
13.	Routing IPv4	Obsługa minimum 256 tras IPv4 dla routingu statycznego i RIP.
14.	Routing IPv6	Obsługa minimum 128 tras IPv6 dla routingu statycznego i RIPng.
15.	Protokoły routingu	Obsługa routingu IPv4: statyczny, RIPv2, OSPFv2; IPv6: statyczny, RIPng, OSPFv3. Wymagana obsługa co najmniej jednego obszaru i co najmniej 8 interfejsów OSPF. Dostawa obejmuje licencję OS6560-SW-AR, zapewniającą pełną obsługę OSPFv2/OSPFv3, do 2 obszarów dowolnego typu oraz do 16 interfejsów i sąsiadów OSPF. Dopuszcza się realizację wymagań bez tej licencji wyłącznie po potwierdzeniu przez producenta obsługi wymaganego zakresu OSPF w dostarczonej wersji AOS i konfiguracji licencyjnej.
16.	Wykrywanie urządzeń	Obsługa protokołów LLDP i LLDP-MED
17.	Serwer DHCP	Przełącznik musi posiadać funkcjonalność serwera DHCPv4 i DHCPv6. Wykonawca zapewni wszystkie składniki i licencje niezbędne do uruchomienia wymaganej funkcjonalności w oferowanej konfiguracji.
18.	Multicast	Obsługa ruchu multicast: IGMP Snooping v1, v2 i v3
19.	DHCP snooping	Obsługa mechanizmu DHCP snooping

1.2 Punkty dostępowe WLAN (8 szt)

Dostawa obejmuje łącznie 8 wewnętrznych punktów dostępowych klasy, wraz z zarządzaniem i wyposażeniem montażowym. Liczba 8 dotyczy łącznej dostawy IT i OT; lokalizacje OT wymagają zatwierdzenia przez Zamawiającego

- Centralne zarządzanie w posiadanym OmniVista: konfiguracja SSID, polityk bezpieczeństwa, parametrów radiowych, aktualizacji, stanu AP i klientów. Należy dostarczyć licencje potrzebne do zarządzania 8 AP. Zarządzanie wyłącznie przez lokalny interfejs pojedynczego AP nie spełnia tego wymagania.
- Mechanizmy automatycznego doboru kanałów i mocy, wykrywania obcych AP i zarządzania grupami AP. Tryb lokalnego kontrolera w AP może być dostępny, lecz nie zastępuje wymaganej integracji z OmniVista.

- Zapewnić zasilanie 8 AP. dostarczyć 8 zgodnych injectorów PoE o standardzie i mocy wystarczających do pełnej pracy AP. Nie zakładać zasilania AP przez przełączniki bez PoE.
- Wykonać pomiar radiowy po instalacji i przekazać mapę zasięgu w uzgodnionych pomieszczeniach, identyfikację zakłóceń oraz wyniki testu roamingu i uwierzytelniania.

1.	Punkt dostępowy WiFi musi być przeznaczony do montażu wewnątrz budynków i zapewniać wsparcie dla standardów IEEE 802.11a/b/g/n/ac/ax/be
2.	Możliwość zarządzania punktem dostępowym za pomocą centralnego systemu zarządzania siecią (Network Management System) oferowanego przez producenta urządzenia. System zarządzania musi być dostępny w wariantach chmurowym oraz do instalacji lokalnej (‘on premise’).
3.	Możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego systemu zarządzania: a. musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową przy wykorzystaniu protokołu https, b. możliwość przeprowadzania wszystkich operacji konfiguracyjnych z poziomu przeglądarki, c. musi umożliwiać tworzenie klastra do 255 urządzeń, d. 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.
4.	Urządzenie musi być wyposażone w 3 niezależne moduły radiowe, które muszą wspierać pracę w pasmach 2,4 GHz, 5 GHz, 6 GHz.
5.	Punkt dostępowy musi posiadać wbudowane anteny umożliwiające pracę w trybach: • 2×2:2 @ 2,4 GHz, • 4x4:4 @ 5 GHz, • 2x2:2 @ 6 GHz, o dookólnej charakterystyce promieniowania oraz o zysku nie mniejszym niż: • 4,6 dBi dla 2,4 GHz, • 5,8 dBi dla 5 GHz, • 6,4 dBi dla 6 GHz.
6.	Punkt dostępowy musi posiadać dedykowane radio skanujące umożliwiające pracę jako analizator widma bez świadczenia usług dla klientów sieci bezprzewodowej.
7.	Punkt dostępowy musi mieć wbudowany moduł Bluetooth Low Energy będący jednocześnie bramą (Gateway) do instalacji urządzeń typu BLE.
8.	Punkt dostępowy musi mieć wbudowany moduł Zigbee będący jednocześnie bramą (Gateway) do instalacji urządzeń typu Zigbee.
9.	Punkt dostępowy musi posiadać wbudowaną antenę BLE/Zigbee o maksymalny zysku energetycznym nie mniejszym niż 4.3 dBi.
10.	Punkt dostępowy musi posiadać wbudowany moduł bezpieczeństwa TPM 2.0.
11.	Punkt dostępowy musi posiadać wbudowanego klienta Radius.
12.	Punkty dostępowy musi wspierać 802.1x, 802.11i, WPA2, WPA3, Enterprise with CNSA Option, Personal (SAE).
13.	Punkt dostępowy musi posiadać co najmniej: a. 1 port uplink RJ-45 Multigig 1/2.5/5/10 z funkcją PoE, b. 1 port uplink / downlink RJ-45 1G, c. port konsolowy, d. możliwość zasilania PoE zgodne z 802.3bt lub za pomocą dedykowanego zasilacza, e. w przypadku zasilania PoE maksymalny pobór mocy nie może przekroczyć 42 W, f. port USB 2.0 typu C, g. przycisk przywracający konfigurację fabryczną, h. slot zabezpieczający Kensingston, i. kontrolkę 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).

14.	Wsparcie dla standardów: a. IEEE 802.11a/b/g/n/ac/ax/be b. IEEE 802.11e WMM, U-APSD, c. IEEE 802.11h, 802.11i, 802.11e QoS, d. 802.1Q (VLAN Tagging), e. 802.11r Fast roaming, f. 802.11w Protected Management Frame, g. 802.11v BSS Transition Management, h. 802.11k Radio Resource Management
15.	Funkcjonaliści pasma radiowego: a. zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, b. automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe, c. stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu, d. rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma, e. wykrywanie interferencji oraz miejsc bez pokrycia sygnału, f. automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz, g. wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11a/b/g), h. możliwość ustawienia parametru, po osiągnieciu którego klient sieci bezprzewodowej zostanie rozłączony od punktu dostępowego, i. możliwość ustawienia parametru, po osiągnieciu którego klient sieci bezprzewodowej zostanie rozłączony od punktu dostępowego oferujące gorsze paramenty i podłączony do punktu dostępowego oferujące lepsze parametry radiowe, j. możliwość uruchomienia minimum 16 SSID na radio, k. możliwość dołączenia do 1200 urządzeń klienckich, l. możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane, m. pełna obsługa prawidłowego roaming'u klientów sieci bezprzewodowej – obsługa standardów 802.11r oraz 802.11v/k.
16.	Wymagane parametry pracy urządzenia, zgodność ze standardami i certyfikaty: a. temperatura otoczenia: 0-45 º C, b. wilgotność 5% - 95% nie skondensowana, c. znak CE, d. FCC, e. RoHS, REACH, WEEE, f. EMI and susceptibility (Class B), g. Bluetooth SIG, h. CB Scheme Safety, cTUVus, i. EN 60601-1-1, EN60601-1-2, j. EN 55032, k. EN 300 328, l. EN 301 893, m. EN 301 489-1, n. EN 301 489-17, o. EN 303 687, p. IEC/EN 60950 i 62368, q. UL2043 Plenum Rating, r. Wi-Fi CERTIFIED Wi-Fi 7, Passpoint R3
17.	Wraz z urządzeniem musi zostać dostarczony dedykowany przez producenta urządzenia uchwyt montażowy przeznaczony do zamocowania na ścianie/suficie.
18.	Zamawiający wymaga, aby punkt dostępowy posiadał gwarancję typu „limited lifetime", która zapewnia wymianę niesprawnego urządzenia przez producenta, po jego wcześniejszym dostarczeniu do producenta, w okresie do 5 lat od momentu ogłoszenia zakończenia sprzedaży danego modelu urządzenia.

	Dodatkowo: zamawiający wymaga, aby punkt dostępowy posiadał 3-letni rozszerzony serwis gwarancyjny na sprzęt i oprogramowanie ze wsparciem producenta oraz dostępem do najnowszych wersji oprogramowania.

1.3 Wdrożenie RADIUS, VPN oraz istniejącej kontroli dostępu NAC z zachowaniem segmentacji IT/OT

Posiadany Alcatel-Lucent Enterprise OmniVista jest nadrzędną platformą zarządzania dostępem i urządzeniami sieciowymi. Wykonawca uruchomi lub dostosuje jego funkcje NAC/UPAM, w granicach dostępnych uprawnień i uzgodnionego zakresu. Należy zachować istniejącą segmentację Zamawiającego i uniknąć nakładania sprzecznych polityk dla tych samych portów oraz SSID.

1.3.1. Zakres usługi wdrożenia RADIUS, VPN i integracji z istniejącym OmniVista

Przedmiotem zamówienia jest zaprojektowanie, dostawa, instalacja, konfiguracja, integracja, uruchomienie i udokumentowanie mechanizmów bezpieczeństwa sieciowego obejmujących:

1. centralne uwierzytelnianie użytkowników i urządzeń;
2. bezpieczny dostęp zdalny VPN;
3. segmentację sieci IT i OT;
4. konfigurację i uruchomienie mechanizmów NAC w posiadanym systemie Alcatel-Lucent Enterprise OmniVista/UPAM, bez dostawy nowej platformy NAC;
5. integrację posiadanego OmniVista/UPAM z Active Directory/LDAP, serwerem RADIUS, dostarczanymi oraz istniejącymi przełącznikami, punktami dostępowymi i urządzeniami UTM/NGFW, w zakresie zatwierdzonej architektury;

wdrożenie i testy uzgodnionych reguł uwierzytelniania, autoryzacji oraz dostępu zdalnego.

Dotychczasowy podział sieci i stref pozostaje wiążący.

Rozwiązanie powinno zostać wdrożone z uwzględnieniem podziału na strefy bezpieczeństwa, lokalizacje, typy użytkowników, typy urządzeń, role administracyjne oraz wymagania środowiska IT i OT/ICS.

1.3.2 Centralne uwierzytelnianie RADIUS

Centralne uwierzytelnianie RADIUS należy uruchomić z wykorzystaniem funkcjonalności posiadanego systemu OmniVista/UPAM, jeżeli są dostępne i aktywowane, albo w oparciu o zgodny komponent RADIUS współpracujący z tym systemem. Zakres obejmuje wdrożenie RADIUS i integrację z NAC; nie obejmuje zakupu nowej, odrębnej platformy NAC.

Należy ustanowić jeden spójny model polityk uwierzytelniania i autoryzacji dla OmniVista, RADIUS, LAN, WLAN i VPN. Wykonawca udokumentuje podział ról poszczególnych komponentów, bez dublowania polityk oraz bez zmiany istniejącej segmentacji sieci bez zatwierdzenia Zamawiającego.

Zakres wdrożenia obejmuje co najmniej:

1. integrację z Active Directory, LDAP lub rozwiązaniem równoważnym;
2. uwierzytelnianie użytkowników i urządzeń w sieci LAN, WLAN i VPN;
3. obsługę standardu 802.1X;
4. obsługę uwierzytelniania urządzeń na podstawie adresu MAC — MAB;
5. obsługę RADIUS CoA lub mechanizmu równoważnego umożliwiającego dynamiczną zmianę uprawnień;
6. przekazywanie do urządzeń sieciowych informacji o roli użytkownika, profilu dostępu oraz przypisanym VLAN;
7. prowadzenie logów prób uwierzytelnienia, decyzji dostępowych i błędów autoryzacji;
8. zapewnienie technicznej możliwości przyszłego przekazywania logów do centralnego systemu gromadzenia i analizy zdarzeń; w bieżącym zamówieniu logi NAC/RADIUS pozostają dostępne w jego własnym systemie, bez uruchamiania dodatkowego źródła SIEM.

1.3.3. Segmentacja sieci IT/OT

Wykonawca zobowiązany jest zinwentaryzować i zachować istniejący, zaakceptowany przez Zamawiającego podział na VLAN i strefy IT/OT. Poniższy katalog ma charakter referencyjny dla identyfikacji istniejących stref oraz ich wzajemnych powiązań; nie ustanawia obowiązku tworzenia nowych VLAN, zmiany adresacji ani przebudowy przyjętej segmentacji:

1. sieć użytkowników;
2. sieć serwerową;
3. sieć administracyjną;
4. sieć zarządzającą;

5. sieć urządzeń bezpieczeństwa;
6. sieć backupu;
7. sieć urządzeń technicznych i IoT;
8. sieć bezprzewodową;
9. sieć gościnną;
10. środowisko OT/ICS;
11. stacje operatorskie i komputery inżynierskie;
12. strefę DMZ;
13. strefę dostępu serwisowego;
14. strefę kwarantanny.

Zakres prac obejmuje audyt aktualnej adresacji, VLAN, tras, polityk firewall i przepływów komunikacyjnych, a następnie odwzorowanie tych ustawień na nowych urządzeniach oraz dostosowanie konfiguracji RADIUS, VPN i OmniVista. Każde odstępstwo od istniejącej segmentacji, w tym utworzenie, usunięcie, połączenie lub zmiana przeznaczenia VLAN/strefy, wymaga uprzedniej pisemnej akceptacji Zamawiającego oraz planu wdrożenia i wycofania zmiany.
Komunikacja pomiędzy strefami powinna zostać ograniczona do niezbędnych adresów, protokołów i portów, zgodnie z zasadą minimalnych uprawnień.

1.3.4. Usługa wdrożenia kontroli dostępu NAC w posiadanym Alcatel-Lucent Enterprise OmniVista
Przedmiotem zamówienia jest usługa analizy, konfiguracji, uruchomienia i integracji funkcjonalności kontroli dostępu do sieci NAC w posiadanym przez Zamawiającego oprogramowaniu Alcatel-Lucent Enterprise OmniVista, w szczególności z wykorzystaniem jego dostępnych mechanizmów zarządzania profilami UNP i uwierzytelniania UPAM. Zamawiający NIE zamawia dostawy odrębnego systemu lub platformy NAC ani licencji nowego producenta NAC.

Nadrzędnym systemem zarządzającym przełącznikami, punktami dostępowymi oraz politykami dostępu ma pozostać posiadane OmniVista. Dostarczane urządzenia muszą być włączone do istniejącego systemu; nie dopuszcza się równoległego wdrożenia konkurencyjnej konsoli NAC jako warunku realizacji podstawowych funkcji.

1.3.4.1. Analiza przedwdrożeniowa i zachowanie segmentacji

- Wykonawca ustali wersje i moduły OmniVista, dostępność i zakres UPAM/UNP, bieżące uprawnienia licencyjne, typy oraz wersje systemów przełączników i AP, funkcjonujące mechanizmy RADIUS, 802.1X, MAB i CoA.
- Wykonawca udokumentuje istniejące VLAN, strefy IT/OT, profile użytkowników i urządzeń, wyjątki technologiczne oraz reguły przydzielania dostępu. Nie zmieni ich bez pisemnej zgody Zamawiającego.
- Wykonawca określi elementy możliwe do uruchomienia przy użyciu posiadanych licencji oraz zgłosi ewentualne braki lub ograniczenia przed rozpoczęciem konfiguracji. Samo wskazanie braku licencji lub funkcji nie stanowi wykonania usługi. Nie domniemywa się dostawy nowego systemu NAC.

1.3.4.2. Konfiguracja i integracja mechanizmów NAC

- Wdrożenie i uporządkowanie polityk dostępu z wykorzystaniem istniejącej struktury OmniVista/UPAM oraz profili User Network Profile (UNP), z uwzględnieniem przyjętej segmentacji i wymaganej separacji IT/OT.
- Konfiguracja współpracy z Active Directory/LDAP i centralnym serwerem RADIUS; integracja z siecią przewodową, WLAN i VPN zgodnie z sekcjami 1.3.1–1.3.3.
- Uruchomienie uwierzytelniania IEEE 802.1X, certyfikatowego EAP-TLS (tam, gdzie wspierane), autoryzacji urządzeń niewspierających 802.1X na podstawie MAC/MAB jako kontrolowanego wyjątku oraz centralnej ewidencji wyjątków.
- Przypisanie profili dostępu, VLAN i ACL na podstawie decyzji systemu uwierzytelniania w granicach technicznych posiadanych przełączników i wersji OmniVista; zastosowanie RADIUS CoA lub wspieranego mechanizmu ponownej autoryzacji, jeżeli jest dostępny.
- Integracja nowych przełączników i ośmiu punktów dostępowych z posiadanym systemem OmniVista w zakresie konfigurowania portów/SSID, monitorowania, profili dostępowych i raportowania; zakres dodatkowych licencji urządzeniowych wynika wyłącznie z właściwych pozycji dostawy urządzeń.
- Konfiguracja odseparowanych zasad dostępu dla użytkowników, administratorów, urządzeń technicznych, gości i urządzeń OT, z zachowaniem dotychczasowych stref i wyjątków procesowych.

1.3.4.3. Testy wdrożenia i odbiór

- Odbiór obejmie wykaz urządzeń obsługiwanych w OmniVista, potwierdzenie połączenia z RADIUS/AD, pozytywną i negatywną próbę 802.1X, kontrolowany wyjątek MAB, poprawne nadanie profilu UNP/VLAN oraz odnotowanie zdarzenia autoryzacji.

- Należy przeprowadzić test dostępu gościa i urządzenia technicznego, test odmowy dostępu, test zachowania istniejącej segmentacji IT/OT oraz test cofnięcia zmiany. Test CoA/ponownej autoryzacji wykonać w zakresie możliwości potwierdzonych podczas analizy przedwdrożeniowej.
- Wykonawca przekaże dokumentację stanu przed i po wdrożeniu, macierz ról i profili, wykaz wyjątków, eksport konfiguracji, procedury zmian i awaryjnego wyłączenia egzekwowania NAC oraz protokoły testów.

Usługa nie obejmuje nabycia, dostawy ani wdrożenia nowej platformy NAC, osobnego klastra maszyn wirtualnych NAC, nowej bazy gości ani odrębnego portalu BYOD. Dodatkowe licencje posiadanego OmniVista mogą być wymagane tylko w zakresie jednoznacznie wskazanym dla dostarczanych urządzeń i wycenionym w zamówieniu. Przedmiotem odbioru jest prawidłowo uruchomiona i zintegrowana funkcjonalność posiadanego systemu.

2. Zarządzanie politykami bezpieczeństwa

Przedmiotem pakietu jest wyłącznie usługa wdrożenia i uruchomienia zarządzania cyklem życia polityk bezpieczeństwa sieci IT/OT z wykorzystaniem NATYWNYCH funkcji posiadanego klastra UTM WatchGuard: WatchGuard System Manager (w tym Policy Manager i Management Server) oraz WatchGuard Dimension jako narzędzia analizy i raportowania logów. Zmiany będą rejestrowane i akceptowane w systemie ITSM. Usługa obejmuje przegląd reguł, macierz komunikacji IT–DMZ–OT, wersjonowanie i kopie konfiguracji, proces zatwierdzania i wycofywania zmian oraz testy odbiorowe. Nie obejmuje dostawy nowej zapory, osobnej platformy NSPM, SOAR ani narzędzia zarządzającego politykami innego producenta.

2.1 Przedmiot i cel zamówienia

Przedmiotem zamówienia jest konfiguracja i uruchomienie zarządzania politykami bezpieczeństwa dla istniejącego klastra WatchGuard oraz zatwierdzonych stref i przepływów OT. Zarządzanie ma bazować na narzędziach natywnych WatchGuard System Manager/Policy Manager/Management Server, a raportowanie na WatchGuard Dimension. Wykonawca zachowa dotychczasową segmentację sieci i przygotuje proces identyfikowalnego wprowadzania, weryfikacji oraz wycofywania zmian; każda zmiana stref, VLAN lub reguł wymaga akceptacji Zamawiającego.

Zarządzanie konfiguracją realizowane będzie w WatchGuard System Manager (WSM), z wykorzystaniem Policy Manager i Management Server w trybie Fully Managed, wspieranym dla objętych usługą urządzeń i wersji Fireware. WatchGuard Dimension będzie służył do zbierania, przeglądania i analizowania logów oraz raportowania. ITSM będzie służył do rejestracji, oceny, zatwierdzania i dokumentowania zmian.

Orkiestracja w ramach usługi oznacza skoordynowaną realizację zatwierdzonych zmian przez uprawnionych administratorów w natywnych narzędziach zarządzania, według wspólnego zgłoszenia ITSM i procedury. Nie wymaga się automatycznych playbooków, konektorów API ani automatycznej zmiany konfiguracji urządzeń różnych producentów.

2.2. Weryfikacja i przygotowanie środowiska

- Wykonawca zinwentaryzuje modele urządzeń, członków klastra i tryb HA, wersje Fireware, WSM i Dimension, obecny tryb zarządzania oraz uprawnienia i limity licencyjne, w tym uprawnienia do Management Server. Wynik przedstawi w protokole weryfikacji.
- Wykonawca przygotuje projekt wdrożenia, wykaz objętych usługą stref i przepływów, plan prac i testów, okna serwisowe oraz procedurę wycofania zmian. Wskaże wymagane kanały i uprawnienia administracyjne.
- Przed zmianami Wykonawca wykona i zabezpieczy kopie konfiguracji urządzeń oraz środowiska zarządzania. Procedura odtworzenia obejmie także elementy nieobjęte samą historią XML, w szczególności wymagane certyfikaty, ustawienia zarządzanych VPN i informacje licencyjne, zgodnie z dokumentacją producenta.
- Wykonawca uruchomi lub skonfiguruje Management Server i Dimension w zasobach udostępnionych przez Zamawiającego oraz przyłączy urządzenia w zatwierdzonym trybie. Dostęp administracyjny ograniczy do imiennych kont, niezbędnych uprawnień i wydzielonej sieci zarządzania.

Usługa nie obejmuje dostawy nowych licencji ani zmiany platformy zarządzania na rozwiązanie chmurowe. Wykryte braki uprawnień lub niezgodności Wykonawca zgłosi przed uruchomieniem zmian; samo stwierdzenie braku licencji nie stanowi wykonania usługi ani podstawy do odbioru nieuruchomionych funkcji.

2.3. Macierz komunikacji i uporządkowanie polityk

Wykonawca przeprowadzi przegląd reguł oraz opracuje z Zamawiającym macierz dopuszczonej komunikacji. Dla każdego przepływu określi co najmniej strefę i adres źródłowy, strefę i adres docelowy, usługę lub protokół i porty, stronę inicjującą połączenie, uzasadnienie, właściciela, urządzenie i regułę egzekwującą dostęp oraz wymagania dotyczące logowania. Dla dostępów czasowych określi termin przeglądu lub wygaśnięcia.

Wykonawca uporządkuje nazewnictwo reguł i obiektów oraz powiąże je z macierzą. Przedstawi propozycje ograniczenia reguł nadmiernie szerokich, zbędnych i nieaktualnych. Brak zdarzeń w analizowanym okresie sam w sobie nie uzasadnia usunięcia reguły, zwłaszcza związanej z rzadką operacją technologiczną. Zmiany wymagają zatwierdzenia przez Zamawiającego, a zmiany dotyczące OT także przez właściciela procesu technologicznego.

Należy uwzględnić istniejące i docelowe mechanizmy separacji. Ochrona objęta pakietem musi dotyczyć rzeczywistych stref lub przepływów OT; ograniczenie prac do reguł dostępu sieci biurowej do Internetu nie spełnia tego wymagania.

2.4. Centralne zarządzanie konfiguracją

- Wykonawca skonfiguruje zarządzanie regułami i obiektami sieciowymi klastra z wykorzystaniem Management Server oraz sprawdzi poprawność zapisu konfiguracji i działania klastra HA po zmianie.
- Wykonawca uruchomi historię wersji konfiguracji, identyfikację autora i czasu zmiany oraz komentarz zawierający identyfikator zgłoszenia ITSM. Zapewni porównanie wersji i możliwość powrotu do zatwierdzonej konfiguracji.
- Szablony konfiguracji i harmonogramy aktualizacji należy zastosować, jeżeli wynika to z zatwierdzonego projektu i jest wspierane dla używanych wersji oraz trybu zarządzania. Dla pojedynczego klastra nie wymaga się tworzenia szablonów bez potrzeby eksploatacyjnej.
- Wykonawca opisze zasady archiwizacji historii, kopii konfiguracji i kopii środowiska zarządzania oraz uprawnienia do ich odczytu i odtworzenia.

2.5. Rejestrowanie i analiza zdarzeń

Wykonawca skonfiguruje przesyłanie do Dimension logów z klastra WatchGuard, obejmujących wybrane reguły chroniące przepływy OT, odrzucenia ruchu oraz dostępne zdarzenia administracyjne. Zakres logowania należy dobrać do potrzeb dowodowych, wydajności urządzeń i dostępnej przestrzeni. Wykonawca zapewni spójność czasu urządzeń i systemów uczestniczących w obsłudze zmian.

Wykonawca przygotuje widoki, filtry lub raporty umożliwiające wskazanie czasu zdarzenia, źródła i celu, usługi oraz reguły i decyzji zapory, w zakresie danych rejestrowanych przez Fireware. Opracuje sposób wykorzystania wyników analizy do okresowego przeglądu reguł i załączania dowodów do zgłoszenia ITSM. Retencję logów i harmonogram raportowania ustali z Zamawiającym na podstawie oszacowanego wolumenu i dostępnych zasobów, a uzgodnienia zapisze w dokumentacji.

W tym wariancie Dimension pracuje jako system logowania i analizy. Nie wymaga się Dimension Command. Historii konfiguracji i zarządzania regułami nie należy uzależniać od funkcji Dimension dostępnych wyłącznie dla urządzeń zarządzanych przez Dimension Command. Odbiór analizy logów nie zastępuje odbioru zarządzania politykami.

2.6 Proces obsługi zmian w ITSM

Wykonawca skonfiguruje formularz, statusy i uprawnienia procesu zmiany, który obejmie następujące czynności:

1. Rejestracja potrzeby zmiany, uzasadnienia, reguł i urządzeń objętych pracami oraz powiązania z macierzą komunikacji.
2. Ocena wpływu na bezpieczeństwo, dostępność i proces technologiczny oraz określenie testów i warunków wycofania.
3. Akceptacja przez upoważnioną osobę, a w zakresie OT również przez właściciela procesu technologicznego.
4. Zabezpieczenie konfiguracji wyjściowej i wykonanie zmiany w uzgodnionym oknie serwisowym.
5. Sprawdzenie dopuszczonej i zabronionej komunikacji oraz logów; zamknięcie zgłoszenia albo wycofanie zmiany i ponowna weryfikacja.

Zgłoszenie musi zawierać identyfikator, osoby wnioskującą, zatwierdzającą i wykonującą zmianę, terminy, identyfikację konfiguracji przed i po zmianie, wynik testów oraz odnośniki do dowodów. W normalnym trybie wykonawca zmiany nie zatwierdza własnych prac. Podział obowiązków zapewniają uprawnienia ITSM, uprawnienia administracyjne i procedura organizacyjna. Dla zmian awaryjnych należy ustalić sposób autoryzacji i późniejszej kontroli. Nie wymaga się realizacji obiegu akceptacji przez WSM ani automatycznej integracji API.

2.7 Spójność polityk IT i OT

Wykonawca zapewni spójność konfiguracji posiadanego klastra WatchGuard (zarządzanej natywnie przez WatchGuard System Manager/Management Server) z segmentacją, VLAN, profilami UNP i ACL realizowanymi w posiadanym Alcatel-Lucent Enterprise OmniVista. Nie tworzy się konkurencyjnego systemu NAC ani niezależnej platformy orkiestracji polityk; wspólne są macierz komunikacji, identyfikatory zmian ITSM, procedura akceptacji i testy. W przypadku odrębnej zapory OT Wykonawca uzgodni z Zamawiającym zakres jej udziału w przepływach, bez zastępowania jej natywnych narzędzi zarządzania.

2.8. Dokumentacja i warunki odbioru

Wykonawca przekaże dokumentację powykonawczą zawierającą inwentaryzację wersji i uprawnień, schemat zarządzania i stref, macierz przepływów z identyfikatorami reguł, wykaz uprawnień, konfigurację logowania i retencji, procedurę obsługi zmian, procedurę odtworzenia oraz protokoły testów. Przeprowadzi instruktaż administratorów obejmujący zmianę polityki, analizę logów i przywrócenie konfiguracji.

Odbiór obejmie co najmniej:

- Prezentację działającego zarządzania konfiguracją klastra i historii zmian w Management Server.
- Przeprowadzenie jednej bezpiecznej zmiany testowej przez pełny proces ITSM, z akceptacją właściwego właściciela OT i powiązaniem z macierzą.
- Potwierdzenie komunikacji dopuszczonej i zablokowania komunikacji niedozwolonej dla uzgodnionego scenariusza dotyczącego OT
- Wyszukanie zdarzeń z reguł WatchGuard objętych scenariuszem oraz przypisanie dowodów do zgłoszenia ITSM.
- Testy na środowisku OT wymagają zatwierdzenia zakresu, terminu i sposobu wykonania; nie mogą powodować nieuzgodnionego zakłócenia procesu technologicznego. Warunkiem odbioru są działające funkcje, pozytywne wyniki testów i przekazanie dokumentacji. Samo zainstalowanie WSM, uruchomienie Dimension lub sporządzenie procedury bez wdrożenia nie stanowi wykonania usługi.

2.9 Przemysłowa bram komunikacyjna OT

Dostawa obejmuje 1 kompletny tor sprzętowo wymuszonego przesyłania danych z OT do IT, wraz z oprogramowaniem po stronie nadawczej i odbiorczej oraz niezbędnymi licencjami. Kierunek transmisji musi wynikać z konstrukcji sprzętu i nie może być programowo odwrócony przez administratora strony IT. Tory zarządzania nie mogą tworzyć obejścia dla transmisji danych IT do OT.

- Zakres podstawowy: eksport logów i plików raportowych z kolektora OT do kolektora w DMZ/IT. Wymagana przepustowość użyteczna, rozmiar plików i liczba źródeł mają być wskazane w tabeli parametrów. Dodatkowe konektory SCADA lub historyka wymagają jawnego wyszczególnienia i wyceny.
- Dla protokołów dwukierunkowych stosować lokalne proxy lub replikację po obu stronach. Nie wymaga się przezroczystego przejścia TCP z potwierdzeniami przez fizycznie jednokierunkowy tor.
- Zapewnić buforowanie na określony czas przerwy po stronie odbiorczej, kontrolę integralności plików i raport błędów. Nie deklarować gwarantowanego potwierdzania odbioru do OT przez ten sam jednokierunkowy tor.
- Przekazać opis architektury sprzętowej producenta i wykonać test negatywny próby komunikacji IT do OT, test przesłania logów i plików, odtworzenia po przerwie oraz alarmowania o awarii.
- Dostawa, konfiguracja i uruchomienie jednokierunkowej przemysłowej bramy komunikacyjnej LTE/Ethernet” – ilość 1 szt

Obszar / parametr	Minimalne wymaganie Zamawiającego
Typ urządzenia	Przemysłowa brama komunikacyjna LTE/Ethernet do zastosowań telemetrycznych i automatyki przemysłowej.
Transmisja komórkowa	Wbudowany modem obsługujący transmisję pakietową w sieciach 2G/3G/LTE oraz obsługę SMS.
Standard LTE	LTE Cat. 1 lub technologia równoważna, zapewniająca stabilną transmisję danych w sieciach operatorów komórkowych w Polsce/UE.
Port Ethernet	Co najmniej 1 x RJ-45 Ethernet 10Base-T/100Base-TX, auto MDI/MDI-X lub równoważne.
Porty szeregowe	Co najmniej 2 porty szeregowe, w tym RS-485 oraz RS-232 lub RS-232/RS-485; minimum jeden port izolowany lub równoważny poziom ochrony komunikacji.
Wejścia/wyjścia binarne	Co najmniej 4 wejścia binarne oraz co najmniej 2 wyjścia binarne lub kanały konfigurowalne jako wyjścia binarne.
Protokoły przemysłowe	Obsługa Modbus RTU i Modbus TCP.

Protokoły sieciowe	Obsługa UDP, IPv4, NAT, przekierowania portów oraz DHCP klient/serwer lub funkcji równoważnych.
SNMP i monitoring	Obsługa SNMP v2c/v3, SNMP Trap lub równoważnego mechanizmu monitorowania i wysyłania zdarzeń.
VPN	Obsługa OpenVPN lub rozwiązania równoważnego zapewniającego szyfrowaną transmisję zdalną.
Dostęp administracyjny	Obsługa SSH lub równoważnego szyfrowanego dostępu administracyjnego.
Kontrola dostępu	Możliwość ograniczenia dostępu administracyjnego do autoryzowanych adresów IP i/lub numerów telefonów oraz obsługa ról/uprawnień użytkowników.
Centralne uwierzytelnianie	Obsługa RADIUS, 802.1x lub mechanizmu równoważnego.
Zapora / filtrowanie	Obsługa zapory sieciowej, filtrowania ruchu lub mechanizmu równoważnego.
WebGUI	Wbudowany interfejs WebGUI lub równoważny interfejs zarządzania przez przeglądarkę do konfiguracji, diagnostyki i podglądu danych.
Konwerter protokołów	Możliwość transmisji danych z urządzeń podłączonych do portu szeregowego i portu Ethernet oraz konwersji/proxy komunikacji między interfejsami.
Funkcja lokalnego Mastera	Cykliczne odpytywanie i analiza danych z urządzeń zewnętrznych oraz wyzwalanie zdarzeń na podstawie wartości, stanów wejść/wyjść lub warunków logicznych.
Rejestrator danych	Lokalny zapis danych na karcie microSD lub równoważnym nośniku; obsługa co najmniej 128 GB, preferowana obsługa do 256 GB.
Rozdzielczość rejestracji	Rejestracja danych z rozdzielczością nie gorszą niż 1 s; preferowana 0,1 s.
Logika lokalna / PLC	Możliwość lokalnego przetwarzania danych i realizacji prostych funkcji logicznych/sterujących w oparciu o wejścia, wyjścia, flagi, rejestry, liczniki lub zegary.
Alarmowanie SMS	Konfigurowalne wiadomości SMS wyzwalane alarmami, zmianą stanu wejścia/wyjścia lub warunkami logicznymi; obsługa wartości dynamicznych, nazw symbolicznych lub makr, jeżeli dostępne.
Zdalna konfiguracja	Możliwość zdalnej konfiguracji i programowania przez sieć komórkową oraz Ethernet.
Aktualizacja firmware	Możliwość zdalnej aktualizacji firmware/FOTA lub równoważnej bezpiecznej aktualizacji oprogramowania wewnętrznego.
Autodiagnostyka i Watchdog	Wbudowana autodiagnostyka, mechanizm Watchdog oraz sygnalizacja stanu pracy.
Synchronizacja czasu	Obsługa SNTP lub równoważnego mechanizmu synchronizacji czasu.
Integracja z systemami monitoringu	Możliwość integracji z systemami klasy SCADA, automatyki lub monitoringu infrastruktury, np. przez Modbus, SNMP, OPC/driver komunikacyjny lub mechanizmy równoważne.
Montaż	Montaż na szynie DIN 35 mm.

Zasilanie	Zasilanie DC, zakres nie gorszy niż 12/24 V DC; preferowany szeroki zakres, np. 10,8-53 V DC lub równoważny.
Redundancja zasilania	Redundantne wejścia zasilające lub rozwiązanie równoważne zwiększające odporność na awarie.
Warunki środowiskowe	Temperatura pracy co najmniej od -20°C do +60°C; preferowany zakres od -30°C do +65°C; wilgotność do 95% bez kondensacji.
Obudowa i złącza	Obudowa przemysłowa, stopień ochrony co najmniej IP20 dla montażu w szafie, złączki śrubowe lub równoważne.
Port serwisowy	Port USB-C lub równoważny port lokalnej konfiguracji/programowania.
Karta SIM / redundancja transmisji	Obsługa karty SIM; dopuszcza się rozwiązanie Dual-SIM/MIM jako funkcję preferowaną dla podniesienia niezawodności transmisji.
Dokumenty certyfikaty	Karta katalogowa oferowanego urządzenia, dokumentacja techniczna lub instrukcja użytkownika, informacja o mechanizmach bezpieczeństwa, informacja o gwarancji i dostępności aktualizacji firmware.
Gwarancja i wsparcie	Minimum 36 miesięcy gwarancji od dnia podpisania protokołu odbioru końcowego. W okresie gwarancji Wykonawca zapewni usuwanie wad, wsparcie w odtworzeniu konfiguracji po awarii, dostęp do aktualizacji firmware oraz naprawę albo wymianę urządzenia w przypadku awarii objętej gwarancją.

Pakiet 3. Lokalna infrastruktura kopii zapasowych

3.1 Serwer backupu

Dostawa jednego niezależnego serwera fizycznego do lokalnego wykonywania, przechowywania, weryfikacji i odtwarzania kopii zapasowych. Nie przewiduje się backupu do chmury publicznej ani usługi zewnętrznego repozytorium online.

Należy zintegrować Backup Server z oferowaną infrastrukturą wirtualizacyjną, macierzą oraz jednym fizycznym NAS stanowiącym wydzielone repozytorium kopii IT i OT. Dostęp do repozytorium musi odbywać się przez kontrolowane połączenia w dedykowanej strefie backupu; sieć użytkowników nie może mieć bezpośredniego dostępu. Nie dopuszcza się przesyłania ani składowania kopii w publicznej lub prywatnej chmurze dostawcy.

- Uruchomić backup Server lokalnie, z konfiguracją magazynów danych, kopii maszyn wirtualnych i kontenerów, zadań tworzenia kopii, retencji, deduplikacji, szyfrowania i automatycznej weryfikacji. Zasoby nienatywnie obsługiwane np. wybrane dane hostów fizycznych, należy zabezpieczyć za pomocą wspieranego mechanizmu zgodnego z uzgodnioną architekturą. Nie dopuszcza się zewnętrznej chmurowej usługi backupu ani niezależnego abonamentu na przestrzeń online.
- Zapewnić lokalne kopie maszyn wirtualnych, kontenerów, wskazanych danych i konfiguracji, harmonogramy, retencję, szyfrowanie, deduplikację , kontrolę integralności oraz procedury przywrócenia pojedynczego pliku i całej maszyny wirtualnej. Podać rzeczywistą lokalizację wszystkich repozytoriów, pojemność netto, plan retencji i zasady odtwarzania danych IT oraz OT.
- Przed wyceną Wykonawca zweryfikuje liczbę chronionych maszyn, rodzaje źródeł, wolumen danych, zmienność i okres retencji oraz wymagania RTO/RPO. Zgodność wszystkich źródeł danych oraz sposób backupu systemów niewspieranych natywnie muszą zostać potwierdzone. Nie przewiduje się osobnego, opłacanego zewnętrznie repozytorium w chmurze.

W ramach analizy przedwdrożeniowej Wykonawca wspólnie z Zamawiającym wskaże maszyny wirtualne i usługi krytyczne wymagające awaryjnego uruchomienia na serwerze backupu oraz potwierdzi, że zasoby CPU, RAM, pamięci masowej i interfejsów sieciowych serwera backupu są wystarczające do ich czasowego uruchomienia. Minimalne parametry techniczne wskazane w tabeli stanowią wartości graniczne; jeżeli analiza wykaże konieczność zastosowania większych zasobów dla spełnienia tego wymagania, Wykonawca uwzględni odpowiednią konfigurację w cenie oferty.

Wykonawca przygotuje i wdroży procedurę awaryjnego odtworzenia oraz uruchomienia wskazanych usług krytycznych na serwerze backupu, obejmującą co najmniej kolejność odtwarzania, zależności usług, konfigurację sieciową, sposób podłączenia repozytoriów oraz warunki powrotu na host podstawowy.
Dla każdej wskazanej usługi krytycznej Wykonawca określi w dokumentacji DR maksymalny czas odtworzenia (RTO), podlegający zatwierdzeniu przez Zamawiającego przed odbiorem rozwiązania.
Przed odbiorem końcowym Wykonawca przeprowadzi udokumentowany test awaryjny obejmujący co najmniej symulację niedostępności hosta podstawowego, odtworzenie i uruchomienie na serwerze backupu co najmniej jednej wskazanej maszyny wirtualnej lub reprezentatywnego zestawu usług krytycznych oraz pomiar rzeczywistego czasu odtworzenia. Wynik testu zostanie ujęty w protokole odbiorowym

Element konfiguracji	**Wymagania minimalne**
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia) Możliwość instalacji czujnika otwarcia obudowy współpracującego z BIOS/UEFI. Serwer z możliwością instalacji zdejmowanego panelu przedniego wraz z zamkiem chroniącym przed nieuprawionym dostępem do dysków.
Procesor	Zainstalowany min. jeden procesory min 16-rdzeniowy, x86 - 64 bity, pracujący z częstotliwością bazową min. 2.0 GHz i osiągający w testach SPECrate2017_int_base wynik nie gorszy niż 265 punktów dla testu oferowanego modelu serwera z 2 procesorami. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org Płyta główna wspierająca zastosowanie dwóch procesorów do 64 rdzeni, mocy do min. 350W
Liczba procesorów	Min. 1 procesor, możliwość zainstalowania łącznie 2 procesorów
Pamięć operacyjna	Min. 128GB RDIMM DDR5 o taktowaniu dopasowanym do zastosowanego procesora, w modułach pamięci o pojemności min. 32 GB każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB.
Sloty rozszerzeń	Min. 6 aktywnych gniazd PCI-Express generacji 5, gniazda pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi, w tym min. 1 slot x16 (szybkość slotu – bus width). Serwer z możliwością rozbudowy do 8 gniazd PCI-Express generacji 5, gniazda pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi, w tym min. 4 sloty x16 (szybkość slotu – bus width).
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania min. 8 dysków SFF typu Hot Swap, SAS/SATA/SSD. Serwer z możliwością rozbudowy do obsługi min. 16 dysków SFF typu Hot Swap, SAS/SATA/SSD/ NVMe. Zainstalowane min. 2 szt. dysków 1,92TB SATA SSD MU typu Hot-swap Zainstalowane min. 4 szt. dysków 2.4TB 10k SAS typu Hot Swap.
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę min. 8 napędów dyskowych SSD/SATA/SAS/NVMe. Kontroler nie zajmujący gniazd opisanych w sekcji „Sloty rozszerzeń". Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie. Możliwość rozbudowy o kontroler z min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, min. 32 portowy obsługujący

	poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę min. 24 napędów dyskowych SSD/SATA/SAS/NVMe.
Interfejsy sieciowe	Zainstalowane min. 2 karty 2 portowe 10GB BASE-T, 1 karty po 4 porty 1gb base-t
Karta graficzna	Zintegrowana karta graficzna
Porty	4 x USB 3.2 (w tym 2 porty wewnętrzne) 1x VGA Możliwość rozbudowy/rekonfiguracji o: 1x cyfrowy port video (Display Port lub HDMI), bez użycia przejściówek z portu VGA lub USB 1x port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W klasy Titanium.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Diagnostyka	Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze.
Bezpieczeństwo	Serwer wyposażony w moduł TPM 2.0
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • uwierzytelnianie oprogramowania sprzętowego PCIe z protokołem bezpieczeństwa i modelem danych (SPDM) zapewnia integralność komponentu • obsługa zdalnego serwera logowania (remote syslog)

	• wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power capping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2022, 2025 Ubuntu 20.04 LTS, 22.04 LTS Red Hat Enterprise Linux (RHEL) 8.6, 9.0 SUSE Linux Enterprise Server (SLES) 15 SP4 VMware ESXi 7.0 U3, 8.0, 8.0 U1/U2
System Operacyjny	• Zainstalowany system operacyjny Windows Serwer Standard w wersji najnowszej 2025 Dodatkowe licencje umożliwiające uruchomienie 2 maszyn wirtualnych na serwerze fizycznym z 1 procesorem (min. 16 rdzeni), w środowisku systemu serwerowego klasy enterprise
Wsparcie techniczne	Minimum **3-letnia gwarancja producenta** w miejscu instalacji. Czas reakcji NBD (w kolejnym dniu roboczym), w przypadku wystąpienia awarii dysków, uszkodzone dyski pozostają u Zamaiajacego.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

3.2 Dostawa Macierzy – 1 szt

L.p.	Cecha	Wymagania minimalne
1.	Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”.
2.	Przestrzeń dyskowa	Macierz musi posiadać minimum 7,68 TB przestrzeni RAW zbudowanej w oparciu o minimum 4 dysków SSD w technologii SAS oraz minimum 14,4TB przestrzeni RAW w oparciu o dyski HDD 2,4TB SAS o prędkości min. 10 tyś obrotów/ min dla każdego dysku.
3.	Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 240 dysków twardych.
4.	Obsługa dysków	Macierz musi obsługiwać dyski SSD, SAS i NL SAS. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. Komunikacja z dyskami 12Gb SAS.
5.	Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). Macierz musi umożliwiać utworzenie pojedynczej grupy RAID zabezpieczonej podwójną parzystością stworzonej ze 128 dysków.
6.	Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci iSCSI 10Gb. Kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC i LAN.
7.	Pamięć cache	Każdy kontroler macierzowy musi być wyposażony w minimum 12GB pamięci Cache, 24 GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
8.	Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.
9.	Interfejsy do hostów	Macierz musi posiadać, co najmniej 8 portów 10Gb. 2 porty per kontroler muszą być obsadzone minimum 4 wkładkami SFP SW 10Gb/s.
10.	Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
11.	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Możliwość tworzenia wolumenów logicznych o pojemności maksymalnej co najmniej 140TB. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.
12.	Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

13.	Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 500 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
14.	Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
15.	Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
16.	Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
17.	Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
18.	Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
19.	Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.

20.	Gwarancja	Minimum **3-letnia gwarancja producenta** na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2-godzinnym czasem reakcji (standardowe dni robocze). Przybycie na miejsce w następnym dniu roboczym. Uszkodzone dyski pozostają własnością Zamawiającego. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.

3.3 Serwer NAS (IT i OT) 1 szt — wspólne, separowane repozytorium kopii zapasowych

Celem dostawy jednej sieciowej pamięci NAS jest zapewnienie lokalnego, bezpiecznego repozytorium kopii maszyn wirtualnych, konfiguracji i danych wskazanych zasobów IT/OT, z zachowaniem ścisłej separacji logicznej, sieciowej i uprawnień oraz bez przekazywania kopii do usług chmurowych.

- Należy dostarczyć kompletene rozwiązanie wyposażone komplet dysków klasy NAS do pracy ciągłej, zgodnych z listą producenta, zapewniających dla jednego urządzenia co najmniej 12 TB przestrzeni netto po RAID6;
- Skonfigurować odrębne logiczne repozytoria, udziały/dataset i konta techniczne IT oraz OT, z separacją ACL, uprawnień administracyjnych, uprawnień zapisu i odczytu, rejestrowaniem dostępu oraz niezależną polityką retencji. Zastosować wyodrębnione interfejsy lub VLAN, reguły zapór i dostęp wyłącznie z zatwierdzonych hostów backupu; urządzenie NAS nie może routować ruchu pomiędzy IT a OT ani tworzyć obejścia istniejących mechanizmów separacji. Administracja NAS tylko z zatwierdzonej strefy zarządzania, z szyfrowanym dostępem i aktualizacjami. Serwer NAS nie może powodować logicznego połączenia sieci IT i OT. Wykonawca przedstawi schemat połączeń, matrycę dopuszczonych przepływów, konfigurację izolacji oraz testy wykazujące brak nieautoryzowanego dostępu między repozytoriami. Odtwarzanie lokalnych danych OT nie może zależeć od publicznej chmury ani od niedostępnych usług IT.

Opis wymagania	Wymagania minimalne
Procesor	Procesor 64-bitowy ARM, minimum 4-rdzeniowy, taktowanie minimum 1,7 GHz; AnnapurnaLabs Alpine AL324 ARM Cortex-A57.
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Zainstalowane minimum 4 GB DDR4 UDIMM. Model bazowy ma 4 GB i jedno gniazdo pamięci; wymagane zastąpienie modułu fabrycznego modułem minimum 8 GB zgodnym z wymaganiami producenta. Obsługiwana rozbudowa do 16 GB.
Pamięć Flash	Minimum 512 MB, z ochroną podwójnego uruchamiania systemu operacyjnego.
Liczba zatok na dyski twarde	Minimum 8 zatok SATA 6 Gb/s dla dysków 3,5 cala; obsługa wymiany dysków podczas pracy (hot-swap).
Obsługiwane dyski twarde	Obsługa dysków HDD SATA 3,5 cala oraz HDD i SSD SATA 2,5 cala. Zainstalowanie dyski min 4x 12TB zgodne z lista kompatybilności ofertowanego serwera NAS
Złącza M.2	Niewymagane w konfiguracji dostawy. Model nie ma wbudowanych gniazd M.2; rozbudowa możliwa przez kompatybilną kartę PCIe.
Pojemność dysków twardych	Zainstalowane minimum 4 dyski HDD SATA 3,5 cala, każdy o pojemności minimum 12 TB, przeznaczone do pracy ciągłej w NAS i znajdujące się na liście zgodności producenta dla oferowanego modelu. Łączna pojemność surowa minimum 48 TB, przed uwzględnieniem RAID, formatowania i rezerwy na migawki.
Możliwość podłączenia modułu rozszerzającego	Możliwość rozbudowy przez kompatybilne jednostki rozszerzające zgodnie z listą zgodności producenta. Jednostki rozszerzające i wymagane do nich karty nie są wymagane w konfiguracji dostawy.
Porty LAN 2,5 GbE	Minimum 2
Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2 Gen 1	Minimum 4 porty USB 3.2 Gen 1 (5 Gb/s).
Porty LAN 10 GbE	Minimum 2 porty 10GbE SFP+.
Gniazdo PCIe	Minimum 1 gniazdo PCIe Gen 2 x2.
Przyciski	Reset, Zasilanie

Opis wymagania	Wymagania minimalne
Typ obudowy	Do montażu w szafie rack 19 cali, wysokość 2U.
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5–95% RH, bez kondensacji.
Zasilanie	Zasilacz 250 W, napięcie wejściowe 100–240 V AC. Moc znamionowa zasilacza nie oznacza stałego poboru mocy urządzenia.
Specyfikacja oprogramowania	
Agregacja łączy	Tak

3.4 Wirtualizacja z środowiskiem backup'u oraz funkcjami deduplikacji

Dostawa i wdrożenie systemu wirtualizacji w środowisku Zamawiającego wraz ze wsparciem technicznym o parametrach minimalnych jak niżej lub oprogramowanie równoważne. Dostarczyć platformę kontenerową w postaci maszyn wirtualnych Linux z silnikiem kontenerów i zarządzaniem deklaratywnym, np. klasę Docker Engine z Compose lub Podman, a dla komponentów wymagających Kubernetes odpowiednio wspieraną platformę

Licencja - Należy zapewnić subskrypcję producenta oprogramowania dla wszystkich zainstalowanych lub wykorzystywanych w nich gniazd procesorowych przez okres minimum 36 miesięcy.
1. Rozwiązanie musi zapewnić możliwość natywnej obsługi wielu instancji maszyn wirtualnych i kontenerów na każdym serwerze fizycznym. 2. Klaster fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji powinien skalować się bez nałożonych limitów licencyjnych. 3. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej z funkcjonalnością przekazywania informacji TRIM/DISCARD do zasobów przechowywania danych oraz definiowanymi limitami prędkości odczytów i zapisów na utworzonym dysku, w wartościach MB/s oraz IOP/s wykonywanych na wybranym zasobie. 4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych na danym serwerze z możliwością sumarycznego przydzielenia puli pamięci operacyjnej RAM większej niż dostępna w działającym serwerze, nie mniej niż 192GB 5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć skonfigurowanie od 1 do co najmniej 12 wirtualnych kart sieciowych. 6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania przekierowania używanych portów USB do maszyn wirtualnych w trybie „hot plug", zarówno za pomocą nr portu jak i numerów identyfikacyjnych 'Producent/Urządzenie'. 7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania przekierowania używanych fizycznych urządzeń zainstalowanych w gniazdach PCI/PCIe serwera wraz z przekierowaniem akceleratorów GPU. 8. Rozwiązanie wirtualizacyjne musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 9. Rozwiązanie wirtualizacyjne powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 10. Rozwiązanie wirtualizacyjne musi wspierać m.in. następujące systemy operacyjne: Windows XP/7/8/10/11, Windows Server 2012/2016/2019/2022, Systemy z rodziny Linux (kernel 2.4 – 6.0) 11. System wirtualizacji musi wspierać konfigurację w trybie graficznym rozwiązań zarówno dla obiektowego przechowywania danych jak i technik 'erasure coding' z użyciem osobnych urządzeń typu SSD do hybrydowych operacji z udziałem metadanych, w celu uzyskania redundancji bezpieczeństwa operacji na danych, ich przechowywania i maksymalnej wydajności. 12. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania manualnych i zautomatyzowanych kopii pełnych oraz migawkowych (tzw. snapshot) instancji maszyn wirtualnych na potrzeby tworzenia kopii zapasowych bez przerywania pracy systemów. Wbudowana w interfejs graficzny konfiguracja zautomatyzowanych kopii maszyn wirtualnych oraz kontenerów powinna umożliwiać wyłączenie z procesu archiwizacji wybranych dysków wirtualnych w maszynach, dowolne harmonogramowanie zadań,

wybór kompresji (m.in. ZSTD), poziomy ilościowe i jakościowe retencji oraz dodanie komentarzy. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania manualnych i zautomatyzowanych kopii pełnych oraz migawkowych (tzw. snapshot) instancji maszyn wirtualnych na potrzeby tworzenia kopii zapasowych bez przerywania pracy systemów. Wbudowana w interfejs graficzny konfiguracja zautomatyzowanych kopii maszyn wirtualnych oraz kontenerów powinna umożliwiać wyłączenie z procesu archiwizacji wybranych dysków wirtualnych w maszynach, dowolne harmonogramowanie zadań, wybór kompresji (m.in. ZSTD), poziomy ilościowe i jakościowe retencji oraz dodanie komentarzy.

13. System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji powyżej 4 000 portów.
14. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii fizycznej karty sieciowej. Wspierane powinny być technologie redundancji i balansowania LACP (802.3ad) do warstwy 3+4 włącznie.
15. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
16. Oprogramowanie wirtualizacyjne powinno być licencjonowane w oparciu o licencję GNU Affero GPL, v3. W innym przypadku polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego, bez względu na ilość dostępnych zasobów sprzętowych tj. ilość gniazd/rdzeni CPU, pamięci RAM, wszelkich kontrolerów i zasobów magazynów danych. Wsparcie techniczne dla błędów oprogramowania musi być świadczone bezpośrednio przez producenta oprogramowania. Sposób licencjonowania lub subskrypcji musi umożliwiać rozszerzenie wsparcia o dodatkowe usługi zdalnego łączenia się inżyniera producenta oprogramowania do zgłoszonego serwera.
17. Oprogramowanie do wirtualizacji musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora.
18. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi, również w trybie działającej maszyny, która jest klonowana.
19. Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
20. Rozwiązanie wirtualizacyjne musi posiadać wbudowany interfejs programistyczny (API) zapewniający integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
21. Rozwiązanie wirtualizacyjne musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna dostarczana jest w postaci gotowej, wstępnie skonfigurowanej. Dostęp do konsoli powinien być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5 i zabezpieczony certyfikatem SSL
22. Rozwiązanie wirtualizacyjne musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne.
23. Rozwiązanie wirtualizacyjne musi mieć zaimplementowany firewall, natywnie konfigurowalny w web GUI, z rozróżnieniem dla każdego serwera w klastrze.
24. Rozwiązanie wirtualizacyjne musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
25. Rozwiązanie wirtualizacyjne musi mieć możliwość migracji maszyn wirtualnych w czasie ich pracy oraz w trybie wyłączonym pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać konfigurację min. 8 procesów przenoszenia jednocześnie.
26. Rozwiązanie wirtualizacyjne musi zapewniać funkcjonalność z poziomu konsoli graficznej przypisywania dla konkretnej maszyny wirtualnej wybranych rdzeni konkretnego procesora lub grupy rdzeni procesorów w serwerze.
27. System zapewnia odpowiednią redundancję dla uruchomionych usług w oparciu o mechanizm wysokiej dostępności (HA), aby w przypadku awarii lub niedostępności co najmniej 2 serwerów fizycznych w klastrze, wybrane przez administratora i uruchomione w nim wirtualne maszyny oraz kontenery zostały uruchomione na innych serwerach w tym samym klastrze. Rozwiązanie musi posiadać co najmniej dwie, dedykowane, dodatkowo redundantne sieci wzajemnej komunikacji między serwerami w klastrze, niezależnie dla warstwy synchronizacji pracy (hypervisorów) klastra oraz niezależnie dla warstwy współdzielonej w klastrze przestrzeni danych, gwarantujące właściwe działanie mechanizmów wysokiej dostępności dla usług na wypadek izolacji sieciowej serwerów fizycznych, awarii samych serwerów lub poszczególnych komponentów krytycznych w nich zawartych.

28. Należy dostarczyć licencję dla oferowanego środowiska wirtualnego z wsparciem technicznym na min. 36 miesięcy. Wsparcie producenta oprogramowania umożliwiające dostępu do poprawek i uaktualnień w wersji dla środowisk produkcyjnych. Dla tego samego okresu, wsparcie serwisowe musi być świadczone przez dostawcę rozwiązania, ze zgłoszeniami w trybie dni roboczych i czasem reakcji do 1 dnia roboczego.
29. Wdrożenie wymaga przedstawienia końcowej dokumentacji opisującej infrastrukturę, jej konfigurację i wszelkie dane dostępowe do wszystkich elementów systemu.
30. Warstwa pamięci masowej

Serwer musi wykorzystywać mechanizm Software Defined Storage (SDS) oparty o system plików działący z zaoferowanym rozwiązaniem wirtualizacji , zapewniający programową realizację funkcji pamięci masowej bez konieczności stosowania dedykowanych macierzy dyskowych. Rozwiązanie powinno umożliwiać tworzenie odpornych na awarie pul dyskowych, realizację mechanizmów RAID programowego, wykonywanie migawek (snapshotów), klonowania danych, kompresji oraz deduplikacji blokowej, zwiększając efektywność wykorzystania przestrzeni dyskowej. Zastosowanie SDS ma zapewniać integralność danych poprzez sumy kontrolne, automatyczne wykrywanie i naprawę błędów oraz wysoką dostępność i skalowalność zasobów pamięci masowej.

Minimalne wymagania techniczne dla lokalnego systemu kopii zapasowych)

Wymagane minimalne parametry techniczne
System wspiera kopie zapasowe maszyn wirtualnych, kontenerów i danych z fizycznych hostów
Rozwiązanie instalowane i uruchamiane wyłącznie lokalnie (on-premises) w środowisku Zamawiającego, Kopie zapasowe i metadane nie mogą być przesyłane ani przechowywane w publicznej ani prywatnej chmurze zewnętrznego dostawcy. Nie wymaga się ani nie dopuszcza połączenia VPN do chmurowego magazynu backupów.
System zapewnia dostęp do lokalnego repozytorium o przestrzeni roboczej nie mniejszej niż 2 TB, z możliwością wykorzystania wspólnego fizycznego NAS (1 szt.) jako dodatkowego wydzielonego zasobu archiwizacji/kopii, z separacją IT/OT. Należy przedstawić plan przestrzeni, retencji i ochrony repozytorium; nie przewiduje się zakupu abonamentu na zewnętrzną przestrzeń online.
Możliwość przywracania pojedynczych plików lub katalogów, kopii zapasowych kontenerów i maszyn wirtualnych
Obsługa inkrementacyjnych kopii zapasowych
Obsługa deduplikacji przechowywanych kopii zapasowych, również pochodzących z różnych źródeł
Integracja z dostarczonym systemem wirtualizacyjnym umożliwiająca tworzenie kopii zapasowych bez wyłączania maszyn wirtualnych.
Funkcjonalność terminarza wyzwalającego w sposób automatyczny wykonywanie kopii zapasowych
Możliwość wywołania realizacji kopii zapasowej manualnie z poziomu klienta
Funkcjonalność umożliwiająca zautomatyzowane zarządzanie retencji kopii zapasowych w zakresie: zachowaj X kopii, zachowaj kopie z X godzin, zachowaj kopie z X tygodni, zachowaj kopię z X miesięcy.
System umożliwia szyfrowanie danych po stronie klienta w trybie AES-256 dla metody Galois/Counter Mode (GCM). Ponadto dostęp do zaszyfrowanych danych działa wyłącznie na podstawie pary kluczy RSA - system umożliwia z konsoli graficznej zapisać/drukować klucz szyfrujący.
System posiada wewnętrzny mechanizm autentykacji i praw dostępu dla użytkowników oraz posiada możliwość połączenia przez OpenID Connect w celu realizacji SSO

System posiada wbudowany mechanizm sprawdzania spójności backupów oparty między innymi na sumach kontrolnych SHA-256. Rozwiązanie umożliwia automatyzację okresowego sprawdzania spójności odczytu kopii zapasowych.
Rozwiązanie wspiera tryb serwisowy w którym uwidacznia aktywne operacje wraz z interfejsem do przywracania kopii, tworzenie i zarządzanie miejscami przechowywania, wgląd w statystyki wydajności i aktywne zadania, zintegrowaną dokumentację, wykonywanie aktualizacji i zarządzanie przepustowością sieci w celu uniknięcia wysycenia łącz.
System umożliwia okresowe kopiowanie lub synchronizację danych pomiędzy lokalnymi magazynami , jeśli w zatwierdzonej architekturze istnieją co najmniej dwa magazyny. Synchronizacja nie może wykorzystywać publicznej chmury ani stwarzać obejścia segmentacji IT/OT. Nie wymaga się drugiej fizycznej jednostki NAS.
System wspiera bezpieczeństwo logowania przy pomocy technologii “Two Factor Authentication (2FA)” przez GUI oraz “Time-based One Time Passwords (TOTP)”.
System umożliwia obsługę przez konsolę web archiwizacji długoterminowej LTO-5 i nowszych.
Dla oferowanego systemu wymagane jest 36 miesięczne wsparcie producenta oprogramowania w zakresie dostępu do poprawek i uaktualnień. Dla tego samego okresu, wsparcie serwisowe musi być świadczone przez dostawcę rozwiązania, ze zgłoszeniami w trybie dni roboczych i czasem reakcji do 1 dnia roboczego.
Wdrożenie zakończyć dokumentacją lokalnej architektury , konfiguracji backupu, separacji repozytoriów IT/OT, polityk retencji, procedur odtworzenia oraz zarządzania kluczami i dostępami. Poświadczenia administracyjne przekazać wyłącznie bezpiecznym kanałem, bez zapisywania jawnych haseł w dokumentacji. Przeprowadzić minimum 12-godzinny instruktaż stanowiskowy dla administratorów.

4. Pakiet Monitoring i zarządzanie usługami IT/OT

Dostarczyć i wdrożyć 1 centralny system monitoringu. Zakres projektowy: do 150 monitorowanych hostów, w tym dostarczane urządzenia oraz wskazane serwery, urządzenia sieciowe, macierz, NAS i usługi.

- Monitorować dostępność, obciążenie CPU i RAM, dyski i wolumeny, status RAID, interfejsy, błędy portów, zasilanie, temperatury oraz działanie wskazanych usług DNS, LDAP, HTTPS i backupu w granicach dostępnych interfejsów.
- Korzystać z SNMPv3, agentów szyfrowanych, API lub innych udokumentowanych mechanizmów. Dla OT preferować lokalny kolektor i zatwierdzone odpytywanie; aktywnych testów nie wykonywać bez oceny wpływu.
- Skonfigurować szablony, mapę zależności, progi, okna serwisowe, ograniczenie powielanych alarmów, eskalacje, powiadomienia i raport dostępności. Brak danych z kolektora ma wywoływać odrębny alarm.
- Projektowa retencja: historia szczegółowa 90 dni, agregaty 12 miesięcy. Wykonawca przedstawi kalkulację miejsca według liczby elementów i częstotliwości odczytu.
- Integracja z ITSM: utworzenie zgłoszenia, aktualizacja stanu i informacja o powrocie usługi. Dla izolowanej strefy OT wysyłka wyników wymaga lokalnego eksportera przez diodę; standardowe połączenie Zabbix proxy nie może być bez sprawdzenia uznane za zgodne z torem jednokierunkowym.

4.1 Pakiet inwentaryzacji, CMDB, ITSM, monitoringu i zarządzania zmianą

Dostarczyć system klasy ITSM wraz z modułami niezbędnymi do wymaganego zakresu: zgłoszenia, incydenty, problemy, zmiany, baza wiedzy, ewidencja zasobów i relacje CMDB.. System monitorowania infrastruktury odpowiada za dostępność, wydajność, pojemność, stan urządzeń i usług oraz SLA. Centralne gromadzenie i korelacja logów bezpieczeństwa, logi EDR/XDR i UTM oraz funkcje SIEM/SOAR są realizowane w Pakiecie 4 przez system centralnego logowania.

Przedmiotem zamówienia jest rozbudowa posiadanego przez Zamawiającego systemu do zarządzania infrastrukturą IT – eAuditor Standard o dodatkowe funkcjonalności oraz dostarczenie systemu eHelpDesk.

Zakres rzeczowy zamówienia

W ramach realizacji zamówienia Wykonawca zobowiązany jest do:

1) Rozszerzenia systemu eAuditor o funkcjonalności opcjonalne:

a) zdalna instalacja
b) zarządzanie poprawkami i aktualizacjami
c) webRTC.

2) Dostarczenie systemu eHelpDesk dla 1 serwisanta z SLA do 12.06.2028 r.

Zamawiający dopuszcza rozwiązania równoważne.

SYSTEM DO ZARZĄDZANIA INFRASTRUKTURĄ IT

1. Architektura / budowa

1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 100 Klientów jednocześnie.
1.2.
1.3. Architektura / budowa:
1.3.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
1.3.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
1.3.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
1.3.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
1.3.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
1.4. Konfiguracja Architektury:
1.4.1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
1.4.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

2. Wymagania systemowe

2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Edge, FireFox, Chrome, Opera).
2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2019/2022/2025, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2
2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2022/2025, Windows 7/8/8.1/10/11.
2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2022/2025, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9.
2.5. Baza danych musi działać na silniku Microsoft SQL Server 2022/2025 w wersji bezpłatnej Microsoft SQL Server Express Edition.
2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

3. Interfejsy

3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
3.2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
3.3. System zapewnia integrację z modelem LLM.

4. Funkcjonalności systemu zarządzania infrastrukturą IT

4.1. Funkcjonalność Klienta
4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.
4.2. Funkcjonalność konsoli administracyjnej.
4.2.1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.

4.2.2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.

4.2.3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.

4.3. Funkcjonalność panelu pracownika

4.3.1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.

4.4. Zarządzanie licencjami

4.4.1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.

4.5. Wzorce aplikacji i pakietów

4.5.1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.

4.6. Inwentaryzacja sprzętu komputerowego i urządzeń.

4.6.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.

4.7. Inwentaryzacja urządzeń sieciowych.

4.7.1. System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.

4.8. Inwentaryzacja sprzętu.

4.8.1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.

4.9. Ochrona danych (DLP)

4.9.1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.

4.10. Zdalna administracja komputerami

4.10.1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.

4.11. System musi umożliwiać zdalne w technologii WEBRTC.

4.11.1. System musi zapewniać zdalne zarządzanie komputerami przy użyciu technologii WEBRTC, umożliwiając jednoczesne połączenia z wieloma urządzeniami. Powinien oferować funkcje takie jak przejęcie kontroli nad pulpitami, zarządzanie plikami, uruchamianie i zarządzanie aplikacjami oraz instalowanie oprogramowania i aktualizacji. System powinien umożliwiać konfigurację połączeń WEBRTC, w tym instalację i konfigurację odpowiednich serwerów i portów. Dodatkowo, system

powinien obsługiwać różne tryby przejęcia sesji, włączając opcje z lub bez zgody użytkownika, a także umożliwiać nagrywanie i zarządzanie sesjami połączeń, w tym wykonywanie zrzutów ekranu i nagrywanie sesji. System powinien również wspierać różnorodne konfiguracje wyświetlania i jakości sesji, a także umożliwiać uruchomienie do 12 sesji na jednym ekranie.

4.12. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.

4.13. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.

4.14. Zdalna instalacja

4.14.1. System musi umożliwiać zdalną instalację pakietów MSI i plików .exe, korzystając z Windows Management Instrumentation (WMI) oraz usługi Klient bez dodatkowych poświadczeń, wykorzystując lokalne i sieciowe repozytoria. Powinien obsługiwać tworzenie repozytorium instalatorów z możliwością dodawania aplikacji, zarządzania wersjami oraz kategoryzacji. System musi również umożliwiać tworzenie grup instalacyjnych, definiowanie schematów instalacyjnych i automatyzację procesu instalacji na nowych urządzeniach. Powinien zawierać kiosk aplikacji umożliwiający użytkownikom samodzielną instalację aplikacji oraz rejestrować i raportować wszystkie procesy instalacji, umożliwiając również ich przerwanie.

4.15. Zarządzanie Poprawkami i Aktualizacjami

4.15.1. System musi zapewniać ciągłe monitorowanie i identyfikację brakujących aktualizacji systemowych i komponentów infrastruktury IT, oferując funkcje rozpoznawania niezainstalowanych poprawek, ich pobierania, oraz klasyfikacji. Musi umożliwiać aktualizacje bez zakłócania pracy użytkowników, zarówno zbiorowo jak i indywidualnie, z opcją szybkiego przywrócenia poprzedniego stanu systemu poprzez odinstalowanie niechcianych poprawek. System powinien również umożliwiać pomijanie niechcianych poprawek i dostarczać szczegółowe raporty dotyczące stanu aktualizacji oraz urządzeń, które mogą wymagać restartu.

4.16. Zdalne Zarządzanie Zaporą (Firewall)

4.16.1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.

4.17. Automatyzacja

4.17.1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.

4.18. Zarządzanie magazynem IT

4.18.1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.

4.19. Repozytorium

4.19.1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.

4.20. Kody kreskowe

4.20.1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.

4.21. Wysyłanie wiadomości

4.21.1. System musi umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.

4.22. System musi posiadać możliwość eksportu / importu treści.

4.23. Monitorowanie drukarek sieciowych i wydruków

4.23.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.

4.24. Monitorowanie stron www

4.24.1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.

4.25. Monitorowanie serwerów WWW

4.25.1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.

4.26. Monitorowanie dziennika zdarzeń

4.26.1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.

4.27. System musi umożliwiać monitorowanie komunikatów Syslog.

4.28. Monitorowanie pracy komputerów

4.28.1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.

4.29. Monitorowanie uprawnień ACL

4.29.1. System musi umożliwić skanowanie i monitorowanie uprawnień ACL, oferując szczegółowe raporty, automatyczną aktualizacją danych i filtrami do zarządzania informacjami.

4.30. Monitorowanie sensorów

4.30.1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.

4.31. Repozytorium CMDB

4.31.1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.

4.32. Worktime manager

4.32.1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika.

4.33. Raportowanie i eksport danych

4.33.1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.

4.34. System musi zapewnić interfejs API.

4.34.1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.

4.35. Powiadomienia

4.35.1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.

4.36. Bezpieczeństwo

4.36.1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

5. Wsparcie i pomoc
   5.1.1. Pomoc techniczna
      5.1.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
      5.1.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.
      5.1.1.3. Czas trwania usługi SLA min 12 mcy

Systemu do Zarządzania Zgłoszeniami – eHelpDesk Professional

1) Licencjonowanie

Zamawiający wymaga, aby oferowana licencja na Oprogramowanie miała charakter licencji bezterminowej (na czas nieokreślony) dla 1 serwisanta.

2) Wsparcie techniczne

Wykonawca zapewni wsparcie techniczne do 12.06.2028.

3) Wdrożenie

Wykonawca zobowiązany jest do przeprowadzenia zdalnego wdrożenia Oprogramowania na serwerze lub maszynie wirtualnej wskazanej przez Zamawiającego oraz na wybranym stanowisku roboczych wskazanych przez Zamawiającego.

4) Szkolenia

Wykonawca zapewni zdalne szkolenie z zakresu obsługi Oprogramowania dla użytkowników wskazanych przez Zamawiającego, w łącznym wymiarze minimum 8 godzin, w tym:

- szkolenia wdrożeniowe – 4 godzin,
- szkolenia powdrożeniowe realizowane w okresie obowiązywania wsparcia technicznego – 4 godzin.

Lp.	Wymagania ogólne
1.	Architektura
1.1	Konsola administracyjna – w postaci w pełni funkcjonalnej aplikacji internetowej (webowej) pozwalająca na realizację pełnego zarządzania aplikacją oraz wyposażona w mechanizmy do edycji/modyfikacji/usuwania i analizy danych, zawierająca wbudowane mechanizmy raportowania.
1.2	System musi zawierać moduły: 1.2.1. Zarządzanie Incydentem. 1.2.2. Zarządzanie Problemem. 1.2.3. Zarządzanie Zmianą. 1.2.4. Zarządzanie umowami SLA. 1.2.5. Portal Pomocy Technicznej. 1.2.6. Baza wiedzy. 1.2.7. Raportowanie 1.2.8. Platforma zgłoszeń Sygnalistów. 1.2.9. Panel pracownika.
1.3	System musi aktualizować konsolę administracyjną, bazę danych, słowniki, raporty i inne komponenty w sposób w pełni automatyczny za pośrednictwem bezpiecznego połączenia z serwerami aktualizacji producenta systemu w czasie nie dłuższym niż 24h od wydania przez producenta nowej wersji. W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnej poprzez pobranie ze strony producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.
1.4	System musi umożliwiać logowanie do konsoli w sieciach lokalnych i rozległych.
1.5	System musi umożliwiać bezproblemową i stabilną obsługę co najmniej 3000 jednocześnie zalogowanym administratorom/ użytkownikom.
1.7	System musi umożliwiać instalację w środowisku Windows oraz Linux.

1.10	System musi być zgodny z ITIL v4.
1.11	System musi zapewniać integrację z systemem zarządzania zasobami IT.
1.12	System musi zapewnić zgodność z OWASP Application Security Verification Standard (ASVS), wersja 4.0.3 na poziomie 2, wykluczając punkty wymagające analizy kodu źródłowego.
2.	Wymagania systemowe
2.1	System operacyjny: Ubuntu (20.04 LTS, 22.04 LTS, 24.04 TLS), Debian (11, 12), Red Hat Enterprise Linux (RHEL 8, RHEL 9), CentOS Stream (8, 9), Windows Serwer (2016, 2019, 2022)
2.2	Minimalne wymagania sprzętowe: Procesor: 4-rdzeniowy procesor 2.0 GHz lub szybszy (x86_64), RAM: 8 GB, Dysk twardy: 20 GB dostępnej przestrzeni na dysku (zależnie od bazy danych i ilości danych), Karta sieciowa: Przepustowość 1 Gbps Rekomendowane wymagania: Procesor: 8-rdzeniowy procesor 2.5 GHz lub szybszy (x86_64), RAM: 16 GB lub więcej (dla środowisk produkcyjnych), Dysk twardy: SSD 100 GB, Karta sieciowa: Przepustowość 1 Gbps lub więcej
2.3	Wymagania dotyczące oprogramowania: - Java Development Kit (JDK): Wersja: JDK 8 (Java 8), Rekomendowane: OpenJDK - Apache Tomcat: Wersja: 10.x, Porty: 80, 443 lub inny wskazany przez klienta. - PostgreSQL: Wersja: 16.x, Porty: Port 5432 (domyślny port PostgreSQL) lub inny zgodnie z konfiguracją.
2.4	Przeglądarka musi spełniać następujące wymagania, aby zapewnić poprawne działanie aplikacji, bezpieczeństwo oraz pełną kompatybilność z technologiami webowymi. Przeglądarka powinna wspierać następujące standardy: - HTML5 - JavaScript ES6 i nowsze - DOM Level 3 - Obsługa certyfikatów SSL/TLS - Wsparcie dla TLS 1.2 i 1.3 - Obsługa cookies - Wsparcie local storage/sessian storage Zalecane przeglądarki: - Google Chrome - Mozilla Firefox - Microsoft Edge - Safari
3.	Interfejs
3.1	System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
3.2	Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej np.) – podczas importu zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.
3.3	System musi umożliwiać import danych z zewnętrznego pliku CSV, Excel, Microsoft SQL, MySQL, PostgreSQL, Oracle.
3.4	System musi posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu danych. Import musi umożliwiać pobieranie danych z dowolnego źródła danych o dowolnej strukturze danych z wykorzystaniem sterownika ODBC (np. z pliku tekstowego, pliku xls, pliku xml) w sposób jednorazowy lub zgodnie ze zdefiniowanym harmonogramem. Import aktualizuje dane już wcześniej zaimportowane.
	Funkcjonalności
4.	Zakres funkcjonalny
4.1	Moduł Zarządzanie Incydentem musi obsługiwać: 4.1.1. Różne typy zgłoszeń. 4.1.2. Dokładną rejestrację i klasyfikację incydentów. 4.1.3. Diagnostykę i rozwiązywanie zgłoszeń z wykorzystaniem modułu zarządzania wiedzą. 4.1.4. Szczegółowe raporty trendów w incydentach. 4.1.5. Ewidencję czasu pracy serwisanta.

	4.1.6. Zatwierdzanie rozwiązania incydentu przez użytkownika. 4.1.7. Pełną historię zgłoszenia. 4.1.8. Możliwość ustawienia automatycznej odpowiedzi na zgłoszenia użytkowników za pomocą sztucznej inteligencji. 4.1.9. Moduł Zarządzanie Problemem musi obsługiwać: 4.1.10. Rejestracja nowego problemu lub powiązanie wielu incydentów w jeden problem. 4.1.11. Diagnostyka powiązanych problemów i poszukiwanie głównej przyczyny incydentów. 4.1.12. Tworzenie rozwiązań tymczasowych i docelowych. 4.1.13. Szczegółowe raporty trendów – działania prewencyjne. 4.1.14. Analizy, rozwiązania i zadania dodatkowe.
4.2.	Moduł Zarządzanie Problemem musi obsługiwać: 4.1.1. Rejestracja nowego problemu lub powiązanie wielu incydentów w jeden problem. 4.1.2. Diagnostyka powiązanych problemów i poszukiwanie głównej przyczyny incydentów. 4.1.3. Tworzenie rozwiązań tymczasowych i docelowych. 4.1.4. Szczegółowe raporty trendów – działania prewencyjne. 4.1.5. Analizy, rozwiązania i zadania dodatkowe.
4.3.	Moduł Zarządzanie Zmianą musi obsługiwać: 4.3.1. Planowanie zmiany i harmonogramu projektów w webowym interfejsie GUI. 4.3.2. Możliwości ustawiania schematów zatwierdzeń zmiany. 4.3.3. Możliwości przypisania wielu osób do schematu zatwierdzeń zmiany. 4.3.4. Obsługa wielu zmian i projektów w oparciu o wspólny schemat kalendarza, umożliwiający kontrolę przebiegu zmiany. 4.3.5. Możliwości modyfikacji z poziomu GUI elementów projektu i formularza zmiany. 4.3.6. Automatyczne powiadomienia oraz system zatwierdzeń, wysyłane do właściwych osób. 4.3.7. Możliwość ograniczenia widoku zmian i planowania ze względu na uprawnienia osób. 4.3.8. Możliwości powiązania zmian z systemem ticketowym oraz zasobami systemu ticketowego. 4.3.9. Możliwości śledzenia przebiegu zmiany przez supervisora. 4.3.10. Możliwość zatwierdzenia przez osobę bez dostępu do systemu, o ile została uwzględniona w schemacie zatwierdzeń.
4.4.	Moduł Zarządzanie Umowami SLA w zakresie oprogramowania musi obsługiwać: 4.4.1. Definiowanie reguł SLA ze względu na użytkownika, jednostkę organizacyjną przedsiębiorstwa, kategorię czy priorytet. 4.4.2. Automatyczną aktualizację zgłoszeń, aby zapewnić zgodny z SLA czas rozwiązania. 4.4.3. Czuwanie nad zakończeniem rozwiązania problemu w zdefiniowanym uprzednio przedziale czasu i w razie potrzeby zastosowanie mechanizmu eskalacji (do 4 poziomów). 4.4.4. Pomiar jakości SLA – raportowanie. 4.4.5. Powiadomienia serwisantów o zbliżającym się końcu czasu przeznaczonego na rozwiązanie zgłoszenia.
4.5.	Moduł Portal Pomocy Technicznej musi obsługiwać: 4.5.1. Przyjazny interfejs i łatwość tworzenia zgłoszeń. 4.5.2. Szablony standardowych zgłoszeń. 4.5.3. Możliwość sprawdzania statusu zgłoszeń w realizacji. 4.5.4. Wbudowana baza wiedzy. 4.5.5. Dostęp do zgłoszeń historycznych.
4.6.	Moduł Baza Wiedzy musi obsługiwać: 4.6.1. Dostęp do tworzonej przez dział IT bazy 24h/7d. 4.6.2. Indeksowanie przy użyciu słów – kluczy. 4.6.3. Rozdzielenie bazy wiedzy pomiędzy serwisantów (IT) i użytkowników końcowych z dostępem tylko do prostych rozwiązań (z którymi mogą sobie sami poradzić). 4.6.4. Grupowanie rozwiązań wg tematów. 4.6.5. Dostęp do "najbardziej popularnych" i "ostatnio dodanych" rozwiązań.
4.7.	Moduł Raportowanie musi obsługiwać: 4.7.1. Obsługa raportów w standardzie Stimulsoft lub zgodnym. 4.7.2. Raporty parametryczne z parametrami statycznymi i dynamicznymi. 4.7.3. Predefiniowane raporty obejmujące całokształt funkcjonalności zgodne z ITIL v. 4. 4.7.4. CMDB
4.8.	Moduł Platforma Zgłoszeń Sygnalistów musi obsługiwać:

	4.8.1. Webową i powszechnie dostępną, niewymagającą logowania platformę dostępu dla sygnalistów. 4.8.2. Platformę publikacji dokumentów firmowych. 4.8.3. Szyfrowaną dwukierunkową komunikację pomiędzy sygnalistą a osobą obsługującą na każdym etapie zgłoszenia, bez pobierania jakichkolwiek danych od sygnalisty, w tym bez pobierania adresu mailowego. 4.8.4. Możliwość załączania plików do formularza zgłoszenia. 4.8.5. Modyfikowalny formularz zgłoszenia, dostosowywany z poziomu GUI systemu przez administratora nieposiadającego fachowej wiedzy informatycznej. 4.8.6. Możliwość ustawienia interaktywnych formularzy zgłoszeń dla poszczególnych kategorii zgłoszeń. 4.8.7. Możliwość ustawienia minimalnych wymagań formularza zgłoszenia. 4.8.8. Zabezpieczenia captcha dla komunikacji z sygnalistą. 4.8.9. Możliwość dodania klauzuli RODO. 4.8.10. Interaktywny widok zgłoszeń sygnalistów. 4.8.11. Oddzielny od systemu ticketowego system uprawnień i obsługi administracyjnej. 4.8.12. Zabezpieczone powiadomienia o próbach ingerencji w uprawnienia użytkowników systemu. 4.8.13. Możliwość integracji z systemami obsługi wniosków.
4.9.	Moduł Panel Pracownika musi: 4.9.1. Być niezależną aplikacją webową. 4.9.2. Być uruchamiany na komputerach pracowników. 4.9.3. Udostępniać wybrane dane z konsoli administracyjnej oraz pozwalać na interakcję z pracownikiem w wybranych obszarach. 4.9.4. Udostępniać zakładkę „Zgłoszenia”, która umożliwi z jego poziomu wypełnienia formularza dotyczącego zgłaszanego problemu. 4.9.5. Udostępniać zakładkę „Moje zgłoszenia”, która umożliwi z jego poziomu mieć dostęp do ewidencji wysłanych zgłoszeń w tym informacji o przydzielonej grupie wsparcia, serwisancie, statusie, a także mieć możliwość prowadzenia korespondencji. 4.9.6. Udostępniać zakładkę „Baza wiedzy”, która umożliwi z jego poziomu mieć dostęp do artykułów wprowadzonych przez serwisantów do bazy wiedzy z możliwością filtrowania ich po frazach.
4.10.	Powiadomienia/Pop up’y. 4.10.1. Moduł musi umożliwiać ustawienie Powiadomienia/Pop up’y – lista opracowanych w systemie powiadomień. 4.10.2. Po zdefiniowaniu warunków jego wyświetlania administrator musi mieć możliwość określenia, gdzie dane powiadomienie będzie wyświetlane (e-mail, przeglądarka itp.) oraz jego treść. 4.10.3. Moduł musi posiadać podział powiadomień/pop up’ów na: 4.10.3.1. zgłoszenia – powiadomienia dotyczące zgłoszeń: przydzielenie serwisanta do zgłoszenia, zmieniono status zgłoszenia, korespondencja- zawartość wysłanego e-maila, odpowiedź na zgłoszenie wysłane e-mailem, przydzielenie grupy wsparcia do zgłoszenia, 4.10.3.2. zarządzanie zmianą – powiadomienia dotyczące zarządzania zmianą (CM), 4.10.3.3. nieobecności – powiadomienia dotyczące nieobecności: nadanie zastępstwa, odebranie następstwa, zmieniono datę zastępstwa, 4.10.3.4. użytkownicy – powiadomienia dotyczące zmian w obrębie użytkowników. Zmiany: loginów, jednostek organizacyjnych, działów, stanowisk, przełożonych.
4.11.	Komunikaty 4.11.1. Widok musi zawierać listę zdefiniowanych komunikatów, które administrator może wybrać do wyświetlenia na ekranie startowym. Widok musi umożliwiać na wprowadzenie: Lp, Nazwa, Włączony, Widoczne dla, Treść.
4.12.	Kopia bezpieczeństwa. 4.12.1. Widok musi umożliwiać na ustawienie okresowych kopii bezpieczeństwa baz danych. 4.12.2. Moduł musi mieć możliwość ustawienia kopii dla katalogów dla kopii ręcznej oraz automatycznej wraz z możliwością wskazania częstotliwości wykonywania kopii, startu, następnej, ostatniego wyniku, statusu oraz konserwacji po typach: 4.12.1.1. shrink: częstotliwość, start, następny, ostatni wyniku, status, 4.12.1.2. reindex: częstotliwość, start, następny, ostatni wyniku, status,
4.13.	Import danych.

	4.13.1. Moduł musi obsługiwać Import danych – zdefiniowane w systemie ustawienia do importów. 4.13.2. Administrator po ich określeniu musi być w stanie z widoku uruchomić import. 4.13.3. Moduł musi umożliwiać na import danych ze wskazanych typów źródeł danych: 4.13.3.1. CSV, 4.13.3.2. Excel, 4.13.3.3. FIL, 4.13.3.4. Microsoft SQL Server, 4.13.3.5. MySQL, 4.13.3.6. PostgreSQL, 4.13.3.7. Oracle 4.13.4. Moduł musi mieć możliwość na wprowadzenie dozwolonej ścieżki importu. 4.13.5. Moduł musi pozwalać na określenie harmonogramu importu ze wskazaniem na jego częstotliwość i datę rozpoczęcia. 4.13.6. Moduł musi wysyłać powiadomienia o błędach, które wystąpiły podczas importu. 4.13.7. Moduł musi zezwalać na określenie klucza, po którym nastąpi dopasowywanie rekordów źródłowych z rekordami docelowymi. 4.13.8. Moduł musi zezwalać na określenie wartości dla pola „aktualizuj, gdy”: 4.13.8.1. zawsze (dane w kolumnie będą zawsze dopisywane), 4.13.8.2. docelowa pusta (dane w kolumnie będą nadpisywane tylko wtedy, gdy w kolumnie docelowej nie ma wartości), 4.13.8.3. źródłowa niepusta (dane w kolumnie będą nadpisywane, gdy w kolumnie źródłowej są dane). 4.13.9. Moduł musi zezwalać na aktualizację zaimportowanych danych poprzez wskazanie czy dane mają zostać zaktualizowane, gdy wpisy już istnieją, czy ma zostać utworzony nowy wpis z danymi.
4.10	Narzędzia serwisowe. 4.10.1. Widok musi umożliwiać konfigurację następujących kolumn w zakresie: 4.10.1.1. szczegółowych logów: włączone, wyłącz o godzinie, 4.10.1.2. prace serwisowe: włączone, komunikat na ekranie logowania, komunikat dla aktualnie zalogowanych, czas do wylogowania (hh:mm:ss),
4.11	Otwarte sesje. 4.11.1. Widok musi zawierać informacje o otwartych sesjach logowania do systemu. Widok musi zawierać następujące informacje: 4.11.1.1. wprowadź nazwę do odnalezienia, 4.11.1.2. created, 4.11.1.3. login, 4.11.1.4. IP, 4.11.1.5. SID.
4.13	Punkty serwisantów. 4.13.1. Widok musi zawierać podział punktów na: miesięczne, kwartalne, roczne. 4.13.2. Na widoku muszą znajdować się dane takie jak: 4.13.1.1. login, 4.13.1.2. rok, 4.13.1.3. miesiąc, 4.13.1.4. pracochłonność(hh:mm), 4.13.1.5. punkty, 4.13.1.6. imię, 4.13.1.7. nazwisko.
4.14	Użytkownicy. 4.14.1. System musi posiadać zestawienie Użytkowników - widok zawierający wszystkich użytkowników systemu, którymi mogą być osoby logujące się do systemu, pracownicy obszarów, wykonawcy oraz serwisanci. 4.14.2. Moduł musi umożliwiać na przypisanie przez administratora odpowiedniej grupy uprawnień użytkownikowi. 4.14.3. Moduł musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.

4.14.4. Import obiektów z MS Active Directory musi być odporny na zmianę nazw obiektów (nazwy użytkownika, struktury organizacyjnej itp.) – podczas importu zmienione dane muszą zostać odpowiednio zaktualizowane wg klucza UUID.
4.14.5. Moduł musi umożliwiać import danych z zewnętrznego pliku CSV, Excel, Microsoft SQL, MySQL, PostgreSQL, Oracle.
4.14.6. Widok listy użytkowników musi być podzielony na widoki: wszystko, pracownicy obszarów, pracownicy wykonawców, pracownicy grup wsparcia.
4.14.7. Widok listy użytkowników musi prezentować informacje zawierające:
4.14.7.1. automatyczny serwisant,
4.14.7.2. biuro,
4.14.7.3. dział,
4.14.7.4. e-mail,
4.14.7.5. EmployeeID,
4.14.7.6. grupy wsparcia,
4.14.7.7. ID użytkownika
4.14.7.8. ilość zapytań AI (bieżący miesiąc),
4.14.7.9. ilość zapytań AI (ost. 30 dni),
4.14.7.10. ilość zapytań AI (ost. 90 dni),
4.14.7.11. imię,
4.14.7.12. jednostka organizacyjna,
4.14.7.13. login,
4.14.7.14. logowanie dwuetapowe z kodem na maila,
4.14.7.15. logowanie dwuetapowe z kodem authenticatora,
4.14.7.16. nazwa cert,
4.14.7.17. nazwisko,
4.14.7.18. nr tel.,
4.14.7.19. obszary,
4.14.7.20. opis,
4.14.7.21. ostatnie wylogowanie,
4.14.7.22. ostatnie zalogowanie: host,
4.14.7.23. ostatnie zalogowanie: przeglądarka,
4.14.7.24. ostatnie zalogowanie,
4.14.7.25. przełożony (login),
4.14.7.26. przypisany do grup,
4.14.7.27. przypisany do grup (ilość),
4.14.7.28. rodzaje obszarów,
4.14.7.29. średnia ocena (bieżący miesiąc),
4.14.7.30. średnia ocena (ost. 30 dni),
4.14.7.31. średnia ocena (ost. 90 dni),
4.14.7.32. stanowisko,
4.14.7.33. status obecności,
4.14.7.34. szablony zatwierdzeń,
4.14.7.35. szablony zgłoszeń,
4.14.7.36. typ licencji,
4.14.7.37. typy obszarów,
4.14.7.38. użyty szablon zgłoszeń,
4.14.7.39. włączony,
4.14.7.40. wykonawca,
4.14.7.41. wymagany certyfikat,
4.14.7.42. wymuś zmianę hasła,
4.14.7.43. zatrudnienie do,
4.14.7.44. zatrudnienie od,
4.14.7.45. przeszkolony,
4.14.7.46. przeszkolony: data zmiany,
4.14.7.47. data dodania,
4.14.8. Widok listy użytkowników musi mieć możliwość utworzenia indywidualnego filtru widoku.
4.14.9. Moduł musi umożliwiać na przypisanie indywidualnych uprawnień do wybranego użytkownika.
4.14.10. Moduł musi umożliwiać na przypisanie uprawnień do odczytu, zapisu i kasowania w obrębie:

	4.14.10.1. menu (raporty, wnioski o zmiany, kartoteki, ustawienia, pomoc, wyloguj), 4.14.10.2. raporty (wszystkie, okresowe, raporty do widoków, reakcji, rozwiązania, statystyczne parametryczne, statystyczne), 4.14.10.3. akcje/skrypty (wszystkie, utworzone przez zamawiającego). 4.14.10.4. Widok musi prezentować historię użytkownika. Historia musi zawierać następujące dane: data, autor, element, wartość.
4.15	Nieobecności. 4.15.1. Moduł musi umożliwiać na skonfigurowanie Nieobecności – zastępstw - funkcjonalność pozwalająca na automatyczne wskazanie zastępcy przez użytkownika, wskazania przez administratora nieobecności pracownika i ustanowienie zastępcy. 4.15.2. Interfejs musi umożliwiać rejestrację następujących informacji: 4.15.2.1. Typ nieobecności - typ nieobecności definiowany jest w sekcji Typy nieobecności 4.15.2.2. Dotyczy osoby - osoba, która będzie nieobecna: - pracownik: domyślnie wyłącznie jego dane; - administrator: domyślnie jego dane z możliwością zmiany na podstawie listy 4.15.2.3. Początek - początek nieobecności– kalendarz: domyślnie: jutro 4.15.2.4. Koniec - koniec nieobecności- kalendarz: domyślnie jutro 4.15.2.5. Bezterminowo- bezterminowo – wybór pola bezterminowo blokuje możliwość wskazania koniec - domyślnie: jutro 4.15.2.6. Zastępca - osoba zastępująca – wybór z list, domyślnie ograniczenie widoku użytkowników: pracownik departamentu > lista pracowników departamentów; pracownik oddziału > lista pracowników oddziału 4.15.2.7. Komentarz - komentarz do nieobecności. 4.15.3. Moduł musi współpracować z widokami: 4.15.3.1. Karta żądania zmian > w przypadku nieobecności akceptanta danego wniosku – wniosek musi zostać przekierowany do osoby wskazanej na zastępstwo, a w przypadku nieobecności osoby zastępującej do jego zastępcy. 4.15.4. Moduł musi posiadać podział na nieobecności: 4.15.4.1. aktualne/przyszłe, 4.15.4.2. aktualne, 4.15.4.3. przyszłe, 4.15.4.4. przeszłe, 4.15.4.5. wszystkie 4.15.5. Moduł musi obsługiwać powiadomienia mailowe oraz pop up’y informujące o nieobecnościach. Powiadomienia muszą zawierać następujące informacje: 4.15.5.1. Liczba minut, 4.15.5.2. Tytuł powiadomienia, 4.15.5.3. Treść powiadomienia, 4.15.5.4. Stopka powiadomienia,
4.16	Reguły przypisywania. 4.16.1. Widok musi zawierać zapisane w systemie eHelpDesk reguły, które zostaną aktywowane w przypadku zaistnienia określonego zdarzenia. 4.16.2. Widok musi umożliwiać na skonfigurowanie następujących kolumn: 4.16.2.1. etap, 4.16.2.2. kolejność, 4.16.2.3. włączony, 4.16.2.4. nazwa reguły, 4.16.2.5. źródło: e-mail, obszar, obszar (edycja), obszar (nowe), system zewn. (edycja zgł.), system zewn. (nowe zgł.), system zewn. (zgłoszenie), zgłoszenie, zgłoszenie (edycja), zgłoszenie (nowe), zgłoszenie (nowe) – przed zapisaniem, 4.16.2.6. filtr: od (e-mail), 4.16.2.7. filtr: temat, 4.16.2.8. filtr: treść, 4.16.2.9. filtr ogólny, 4.16.2.10. min. Liczba wystąpień, 4.16.2.11. w czasie (minuty), 4.16.2.12. cel: zgłoszenie, problem, 4.16.2.13. przypisz obszar, 4.16.2.14. przypisz proces, 4.16.2.15. przypisz kateg. zgł.,

	4.16.2.16. ustaw status, 4.16.2.17. przypisz umowę SLA, 4.16.2.18. przypisz grupę wsp., 4.16.2.19. przypisz serwisanta, 4.16.2.20. ustaw poziom błędu, 4.16.2.21. ustaw priorytet, 4.16.2.22. ustaw powiad. zgł.
4.18	Serwer pocztowy: Ustawienia SMTP 4.18.1. Widok musi zawierać zestawienie dodanych do systemu eHelpDesk serwerów pocztowych. 4.18.2. Włączone serwery mogą być wykorzystywane do korespondencji w zgłoszeniach oraz do wysyłania powiadomień. 4.18.3. Konfiguracja serwera SMTP musi umożliwiać na wprowadzenie następujących danych: 4.18.3.1. włączony, 4.18.3.2. SMTP serwer, 4.18.3.3. SMTP port, 4.18.3.4. typ aktualizacji: Basic, XOAUTH2, 4.18.3.5. SMTP login, 4.18.3.6. SMTP hasło, 4.18.3.7. opcje autoryzacji przy XOAUTH2, 4.18.3.8. SMTP SSL 4.18.3.9. SMTP TLS, 4.18.3.10. mail od, 4.18.3.11. link w mailu
4.19	Serwer pocztowy: Ustawienia importu. 4.19.1. Widok musi zawierać opisane ustawienia, według których importowane będą maile do systemu eHelpDesk, z których mogą być tworzone zgłoszenia. 4.19.2. Konfiguracja musi umożliwiać na wprowadzenie następujących danych: 4.19.2.1. nazwa, 4.19.2.2. włączony, 4.19.2.3. serwer, 4.19.2.4. port, 4.19.2.5. typ aktualizacji: Basic, XOAUTH2, 4.19.2.6. login, 4.19.2.7. hasło, 4.19.2.8. SSL 4.19.2.9. TLS, 4.19.2.10. protokół, 4.19.2.11. folder, 4.19.2.12. folder z zaimport., 4.19.2.13. folder z niezaimp.
4.20.	Wymagane kolumny w Zgłoszeniu. 4.20.1. Widok musi prezentować listę zdefiniowanych wymaganych kolumn, które w każdym nowym zgłoszeniu muszą zostać uzupełnione 4.20.2. Widok musi umożliwiać na wskazanie w obrębie kolumn następujących danych: 4.20.2.1. pole, 4.20.2.2. widoczny (nowe zgł.), 4.20.2.3. widoczny (istniejące zgł.), 4.20.2.4. wymagany, 4.20.2.5. edycja (nowe zgł.), 4.20.2.6. edycja (istniejące zgł.), 4.20.2.7. tryb zalogowania, 4.20.2.8. typ obszaru (filtr), 4.20.2.9. proces (filtr), 4.20.2.10. opis procesu (filtr), 4.20.2.11. kategoria (filtr), 4.20.2.12. podkategoria (filtr), 4.20.3. Widok musi wyświetlać następujące kolumny: 4.20.3.1. Czas otw. w nast. pracującym dniu,

	4.20.3.2. Czas poświęcony na rozwiązanie, 4.20.3.3. Czas zamkn. w dniu przyj. Zgłoszenia, 4.20.3.4. Czas zamkn. w nast. pracującym dniu, 4.20.3.5. Data przyjęcia/wpłynięcia zgłoszenia reklamacyjnego, 4.20.3.6. Data rozpatrzenia zgłoszenia reklamacyjnego, 4.20.3.7. Data wystąp. błędu, 4.20.3.8. Decyzja, 4.20.3.9. Dostawca/Operator, 4.20.3.10. Grupa wsparcia, 4.20.3.11. Kategoria, 4.20.3.12. Kategoria / podkategoria, 4.20.3.13. Kogo dotyczy, 4.20.3.14. Kolektor, 4.20.3.15. Korespondencja 4.20.3.16. Kwota rozpatrzenia, 4.20.3.17. Modyfikował, 4.20.3.18. Modyfikował (ost. użytkownik), 4.20.3.19. Nazwa firmy realizującej naprawę, 4.20.3.20. Nowy adres, 4.20.3.21. Nr zgłoszenia w Jira, 4.20.3.22. Obserwatorzy: grupy wsp., 4.20.3.23. Obserwatorzy: osoby, 4.20.3.24. Obszar, 4.20.3.25. Ocena zgłoszenia, 4.20.3.26. Opis, 4.20.3.27. Podkategoria, 4.20.3.28. Podkategoria II, 4.20.3.29. Poziom błędu, 4.20.3.30. Priorytet, 4.20.3.31. Problemy powiązane, 4.20.3.32. Proces, 4.20.3.33. Rekomend. data rozw., 4.20.3.34. Rozwiązania, 4.20.3.35. Serwisant, 4.20.3.36. Start zlecenia, 4.20.3.37. Stary adres, 4.20.3.38. Status, 4.20.3.39. System krytyczny, 4.20.3.40. Szablon urządzeń, 4.20.3.41. Temat, 4.20.3.42. Typ, 4.20.3.43. Typ obszaru, 4.20.3.44. Umowa SLA, 4.20.3.45. Utworzył, 4.20.3.46. Waluta naprawy, 4.20.3.47. Wartość naprawy, 4.20.3.48. Wprowadź notatkę, 4.20.3.49. Włącz powiad. zgł., 4.20.3.50. Zasoby, 4.20.3.51. Załączniki, 4.20.3.52. Zestaw klienta, 4.20.3.53. Zgłoszenia powiązane, 4.20.3.54. Źródło kontaktu.
4.21.	Zablokowany dostęp 4.21.1. Widok musi umożliwiać administratorowi wyświetlenie listy zablokowanych kont. 4.21.2. Lista musi zawierać następujące dane: 4.21.2.1. typ, 4.21.2.2. element, 4.21.2.3. czas blokady (s),

	4.21.2.4. ost. aktywność.
4.22.	Zgłoszenia cykliczne. 4.22.1. Funkcjonalność musi pozwalać na zdefiniowanie cyklicznych zgłoszeń, które będą przypisywane do konkretnego użytkownika z uwzględnieniem interwału 4.22.2. Widok musi zawierać następujące kolumny: 4.22.2.1. nazwa zgł. Cykl., 4.22.2.2. włączony, 4.22.2.3. częstotliwość, 4.22.2.4. obszar, 4.22.2.5. kogo dotyczy, 4.22.2.6. zasób, 4.22.2.7. proces, 4.22.2.8. kategoria/podkategoria, 4.22.2.9. temat, 4.22.2.10. opis, 4.22.2.11. umowa SLA, 4.22.2.12. grupa wsparcia, 4.22.2.13. serwisant, 4.22.2.14. status 4.22.2.15. poziom błędu, 4.22.2.16. system krytyczny, 4.22.2.17. priorytet, 4.22.2.18. włącz powiad. zgł.,
5.	Bezpieczeństwo.
5.1.	System musi być wyposażony w mechanizmy definicji praw dostępu do poszczególnych widoków danych i opcji w konsoli administracyjnej.
5.2.	System musi umożliwiać na zablokowanie komunikacji z serwerem producenta w celu wyłączenia aktualizacji.
5.3.	System musi umożliwiać na dostarczenie aktualizacji w formie offline.
5.4.	Uwierzytelnianie do systemu musi być możliwe do zrealizowania: - z wykorzystaniem imiennego konta użytkownika i hasła, - z wykorzystaniem imiennego konta administratorów aplikacji i hasła, - z wykorzystaniem hasła w systemie i bazach danych nie mogą w żadnym z przypadków występować w formie jawnej, - za pośrednictwem jednokrotnego uwierzytelniania poprzez Active Directory, - za pośrednictwem kont LDAP, - za pośrednictwem kont CAS, - za pośrednictwem uwierzytelniania dwuskładnikowego 2FA, - za pośrednictwem weryfikacji dwuetapowej z użyciem e-mail,
5.5.	System musi umożliwiać na definiowanie poziomu uprawnień dla grupy oraz użytkownika (odczyt, zapis, kasowanie) do wszystkich widoków danych oraz wybranych elementów struktury organizacyjnej, wyposażony musi być w opcję dziedziczenia uprawnień. Odebranie praw do widoku lub zakładki na widoku musi powodować ukrycie opcji.
5.6.	Lista użytkowników / administratorów systemu musi być importowana i aktualizowana zgodnie z harmonogramem w oparciu o mechanizm RBAC (Role Base Access Control) z wybranego obiektu Active Directory. Użytkownik wyłączony/usunięty/zablokowany w Active Directory automatycznie musi traci prawa do korzystania z konsoli administracyjnej systemu.
5.7.	System musi posiadać mechanizmy automatycznego wykonywania kopii bezpieczeństwa w zadanych interwałach czasowych w formie kopii przyrostowej i nie przyrostowej oraz musi udostępniać informacje o rezultacie wykonania kopii.
5.8.	System musi pobierać dane z widoków (ang. View) zdefiniowanych w bazie danych a nie bezpośrednio z tabel bazy danych.
5.9.	W przypadku wystąpienia awarii systemu i konieczności instalacji systemu na nowo system musi automatycznie z serwera aktualizacji producenta w ciągu 24 godzin dokonać aktualizacji wszystkich komponentów (konsola administracyjna, serwer, baza danych, bazy wiedzy).
5.10.	System musi zapewniać mechanizmy zapewniające integralność, poufność i dostępność przechowywanych informacji.

5.11.	System musi posiadać możliwość definiowania dozwolonych ścieżek do backupu bazy.
5.12.	System musi mieć zaimplementowane zabezpieczenia chroniące przed Broken Access Control.
5.13.	System musi mieć możliwość definiowania dozwolonych serwerów baz danych, z których można importować dane.
5.14.	System musi mieć możliwość definiowania dozwolonych serwerów, z których można importować maile do eHelpDesk.
5.15.	System musi mieć możliwość definiowania dozwolonych serwerów, do których można wysyłać maile.
5.16.	System musi mieć możliwość blokowania adresu IP lub użytkownika po x nieudanych prób logowania.
5.17.	System musi mieć zaimplementowane zabezpieczenia chroniące przed atakami Reflected Cross-site Scripting w punktach końcowych wykorzystujących parametr ID.
5.18.	System musi mieć zaimplementowany mechanizm pozwalający na monitorowanie zablokowanych adresów IP/użytkowników.
5.19.	System musi mieć wprowadzone wewnętrzne zabezpieczenia chroniące przed ujawnieniem lokalizacji katalogu domowego oraz wersji zainstalowanego oprogramowania przy przesyłaniu pliku na serwer.
5.20.	System musi mieć możliwość wprowadzenia limitowania błędów związanych z operacjami dot. SMTP, AD, Importu maili, importu danych z innej bazy (dotyczy blokowania po IP).
5.21.	System musi mieć zaimplementowaną możliwość definiowania dozwolonych rozszerzeń plików (załączników) wysyłanych na serwer.
5.22.	System musi mieć ustawione flagi HttpOnly i Secure dla ciasteczek sesyjnych i wszystkich innych zawierających wrażliwe dane.
5.23.	System musi mieć wprowadzone wewnętrzne zabezpieczenie chroniące przed ujawnieniem wersji używanej bazy danych.
5.24.	System musi wykorzystywać mechanizm SRI w stosunku do niezaufanych domen.
6.	Wsparcie i pomoc
6.1.	Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
6.2.	System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim.

Pakiet 5 Centralne logowanie, monitorowanie infasturktury i wykrywanie oraz obsługa zagrożeń

5.1. System centralnego gromadzenia, przechowywania, przeszukiwania i korelowania logów bezpieczeństwa, posiadający funkcjonalności klasy SIEM/SOAR

Zakres obejmuje dostawę i wdrożenie centralnego systemu gromadzenia, przechowywania, przeglądania, raportowania i analizy logów z kluczowych elementów infrastruktury IT i OT Zamawiającego.
Rozwiązanie powinno umożliwiać zbieranie zdarzeń co najmniej z urządzeń bezpieczeństwa sieciowego, przełączników, punktów dostępowych, systemów serwerowych, systemów ochrony końcówek, systemów zarządzania podatnościami oraz innych systemów wskazanych przez Zamawiającego na etapie analizy przedwdrożeniowej. System powinien zapewniać raporty techniczne i zarządcze, możliwość wyszukiwania zdarzeń, filtrowania, eksportu danych oraz retencję zgodną z wymaganiami Zamawiającego
Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz wdrożenie systemu w infrastrukturze Zamawiającego, wraz ze szkoleniem administratorów oraz zapewnieniem aktualizacji i wsparcia serwisowego na **okres min 12 miesiecy** .
System ma służyć do centralnego gromadzenia, przechowywania, analizy i korelacji logów oraz zdarzeń bezpieczeństwa z urządzeń i systemów teleinformatycznych Zamawiającego
Wymagania ogólne:

1. W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
2. Rozwiązanie musi zostać dostarczone w postaci maszyny wirtualnej instalowanej w środowisku Vmware lub Windows Hyper-V.
3. Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
4. Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
5. Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.

6. Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.
7. Rozwiązanie musi posiadać predefiniowane panele dla informacji z urządzeń pracujących w sieci OT.

Zarządzanie Logami:

8. Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
9. Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.
10. Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).
11. Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.

Rodzaje wyszukiwani

12. Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
13. Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).
14. Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.
15. Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).
16. Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów).
17. Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.

Raportowanie

18. Rozwiązanie musi umożliwiać tworzenie statycznych raportów.
19. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
20. Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.
21. Rozwiązanie musi umożliwiać tworzenie własnych raportów.
22. Rozwiązanie musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) z funkcjonalnością „drill-down”.

Zarządzanie incydentami

23. Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.
24. Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.
25. Rozwiązanie ma posiadać moduł SOAR

Wymagania systemowe

26. Liczba zdarzeń na sekundę (EPS): min. 10 000
27. Zarządzanie logami: min 1 rok
28. Liczba obsługiwanych urządzeń min. 500
29. Liczba zapisu zdarzeń na dobę: min 13000 MB

System logów musi wspierać hiperwizory: Vmware ESXi oraz Microsoft HyperV.

5.2. Rozszerzenie funkcjonalności system monitorowania infrastruktury IT - oprogramowanie do monitorowania infrastruktury teleinformatycznej

W ramach realizacji zadania Wykonawca ma dostarczyć, zainstaluje, skonfiguruje system objęty gwarancją i wsparciem technicznym przez okres min. 12 miesięcy, dokona podłączenia wszystkich wymaganych systemów będących przedmiotem zamówienia a w szczególności systemów kopii zapasowej lub uczestniczących w procesie tworzenia kopii zapasowych w sposób pośredni. System musi spełniać poniższe wymagania minimalne:

Użytkownicy

1	▪ Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat. ▪ Zapewnienia równoległego dostępu do systemu dla wielu użytkowników. ▪ Ograniczania użytkownikom dostępu do wybranych grup hostów.
Monitorowanie	
2	Monitorowanie serwerów fizycznych. Monitorowanie urządzeń sieciowych. Monitorowanie stanu połączeń. Monitorowanie interfejsów sieciowych przełączników, routerów i serwerów. Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux. Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych. Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń. Automatyczne wykrywanie usług na urządzeniach oraz powiadamianie o wykryciu nowych usług na urządzeniu. Grupowanie hostów. Definiowanie planowanych przerw serwisowych dla hostów i usług. Możliwość zaznaczenia reakcji na awarię — odpowiadanie na alerty (ACK). Wykonywanie operacji na grupach hostów, w tym: włączanie i wyłączanie monitorowania; włączanie i wyłączanie powiadomień; konfigurowanie przerw serwisowych. Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych, dostępnych przez interfejs WWW. Monitorowanie serwerów za pomocą agentów. Monitorowanie serwerów aplikacji: Tomcat; Oracle WebLogic Server. Monitorowanie Active Directory. Monitorowanie serwerów plików i udziałów sieciowych. Monitorowanie statusu serwerów Apache. Monitorowanie baz danych: Oracle; MySQL; PostgreSQL; Microsoft SQL Server; DB2. Monitorowanie urządzeń z wykorzystaniem następujących protokołów i mechanizmów: SNMP; SNMP traps; WMI; IPMI. Konfiguracja oprogramowania systemu monitorowania poprzez interfejs WWW. Monitorowanie poprawności działania DNS. Monitorowanie środowiska VMware. Monitorowanie środowiska Hyper-V. Monitorowanie środowiska Proxmox. Monitorowanie działania serwera czasu NTP. Monitorowanie offsetu czasu na serwerach. Monitorowanie dostępności za pomocą protokołu ICMP, w tym czasu odpowiedzi i strat pakietów. Monitorowanie zajętości miejsca na poszczególnych partycjach. Monitorowanie obciążenia dysków. Monitorowanie wykorzystania pamięci RAM. Monitorowanie obciążenia CPU. Monitorowanie logów systemowych Windows w zakresie wykrywania określonych błędów i zdarzeń operacyjnych. Monitorowanie macierzy dyskowych, w tym statusu urządzenia i statusu dysków. Dodawanie własnych wtyczek lub agentów dla urządzeń i usług, które standardowo nie są obsługiwane.

	Możliwość rozszerzania zakresu monitorowania przez własne skrypty, programy wykonywalne, pluginy, parametry użytkownika oraz udokumentowane API, bez konieczności modyfikowania kodu źródłowego systemu. Agregacja usług niskiego poziomu do procesów biznesowych. Modelowanie zależności pomiędzy elementami infrastruktury i usługami biznesowymi oraz prezentowanie wpływu rzeczywistej lub kontrolowanej testowej niedostępności elementu na usługi nadrzędne. Monitorowanie rozproszone, umożliwiające podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji lub oddziałów. Wykrywanie niestabilnie działających usług. Monitorowanie dostępności stron internetowych. Konfiguracja hierarchiczna, w tym dziedziczenie konfiguracji dla grup urządzeń
Prezentacja	
3	▪ Prezentację stanu urządzeń na mapie. ▪ Prezentację danych na dashboardach. ▪ Elastyczną konfigurację dashboardów, wybór elementów. ▪ Wizualizację stanu działania całej infrastruktury na jednym dashboardzie. ▪ Tworzenie indywidualnych dashboardów przez użytkowników
Powiadomienia	
4	▪ Globalne wyłączanie powiadomień. ▪ Powiadamianie użytkownika o problemach przez e-mail. ▪ Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie. ▪ Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników. ▪ Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług
Konfiguracja	
5	▪ Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW ▪ Automatyczna konfiguracja i działanie z REST-API ▪ Centralne zarządzanie agentami ▪ Integracja danych z różnych źródeł danych (JSON, XML, SNMP)
Monitoring bazy danych systemu HIS	
6	Możliwość monitorowania bazy danych systemu HIS w zakresie co najmniej: – Instance state – Version – Jobs – Locks – Processes – Number of active sessions – Recovery area – Log switch activity – General tablespace information – Tablespaces performance – Long active sessions – Undo retention – Checkpoint and online backup state – Custom SQLs – RMAN backup status – RMAN backups – ASM disk groups – Apply and transport lag of Oracle Data-Guard – Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości

Monitorowanie urządzeń bezpieczeństwa	
7	System monitoruje urządzenia klasy UTM/NGFW minimum w zakresie: stanu synchronizacji klastra High-Availability; ogólnego stanu urządzenia i alarmów czujników sprzętowych; aktualnej liczby sesji; liczby i stanu tuneli IPsec VPN; poziomu wykorzystania procesora i pamięci operacyjnej; stanu interfejsów sieciowych i podstawowych parametrów transmisji; czasu pracy urządzenia oraz stanu wymaganych usług; progów ostrzegawczych i krytycznych definiowanych przez administratora. Analiza logów bezpieczeństwa, zdarzeń IPS/IDS, antywirusa, EDR/XDR oraz ich korelacja jest realizowana przez centralny system logowania/SIEM w Pakiecie 4 i nie stanowi funkcji systemu monitorowania infrastruktury.

5.3 Usługa MDR (WoD U11 OT) — wykrywanie i reagowanie w oparciu o WithSecure EPP/EDR

Przedmiotem zamówienia jest świadczenie usługi MDR (Managed Detection and Response) dla uzgodnionych zasobów IT/OT, wykorzystującej sygnały i funkcje posiadanych lub wdrażanych rozwiązań WithSecure EPP/EDR. Zakres nie obejmuje zakupu odrębnej platformy MDR innego producenta. Wykonawca potwierdzi na etapie analizy przedwdrożeniowej liczbę i typy endpointów oraz dostępność licencji, sensorów i telemetrii wymaganej do realizacji usługi.

- Usługa ma być świadczona od jej uruchomienia i odbioru, nie dłużej niż do dnia 31 grudnia 2026 r., tj. do końca wskazanego przez Zamawiającego okresu kwalifikowalności. Wymagana jest obsługa analityczna co najmniej 8×5 (dni robocze, godz. 8:00–16:00), automatyczne zbieranie alertów przez system EPP/EDR przez całą dobę oraz uzgodniony kanał eskalacji zdarzeń krytycznych do Zamawiającego. Analityk MDR weryfikuje alerty generowane przez WithSecure EPP/EDR, ocenia ich wiarygodność, wpływ i priorytet, przedstawia rekomendacje i eskaluje incydenty do wskazanych osób. Reakcje wymagające izolacji hosta lub zmiany konfiguracji OT mogą być podejmowane tylko po uzyskaniu zatwierdzenia i w granicach przyznanych uprawnień oraz uzgodnionych okien serwisowych.

- Wykonawca dostarcza miesięczny raport z obsługi alertów, incydentów, podjętych działań, czasu reakcji oraz zaleceń. Zdarzenia istotne dla bezpieczeństwa podlegają ewidencji w ITSM lub innym uzgodnionym rejestrze Zamawiającego.
- Wykonawca określi miejsce przetwarzania telemetrii WithSecure, zakres dostępu analityków, zasady zdalnego dostępu, bezpieczeństwa informacji i zakończenia świadczenia usługi. Zamawiający zachowuje dostęp do własnych danych, raportów i dokumentacji incydentów. Wykonawca nie jest uprawniony do samodzielnego uruchamiania backupu danych w chmurze.
- Usługa MDR objęta ceną zamówienia kończy się 31 grudnia 2026 r. Zamawiający zastrzega możliwość jej przedłużenia po tym terminie na podstawie odrębnej decyzji i zamówienia, po przedstawieniu przez Wykonawcę warunków technicznych, zakresu i ceny kontynuacji. opcja ta nie jest automatycznie uruchamiana ani wliczana do wynagrodzenia podstawowego. Dalszy okres finansowania nie jest objęty deklaracją kwalifikowalności w niniejszym OPZ.

Odbiór usługi MDR obejmie potwierdzenie integracji z WithSecure EPP/EDR, odbierania i interpretacji alertów z zatwierdzonych źródeł, testowy incydent z analizą i eskalacją, raport przykładowy, opis ścieżki kontaktu oraz potwierdzenie daty zakończenia świadczenia usługi 31.12.2026 r. Weryfikacja dostępności źródeł OT nie może naruszać ciągłości procesu technologicznego.

Pakiet 6 Pakiet zarządzania podatnościami i testowanie zabezpieczeń

Zakres obejmuje wdrożenie narzędzi i usług umożliwiających identyfikację, ocenę, priorytetyzację, raportowanie i obsługę podatności w środowisku IT oraz OT/ICS Zamawiającego.
Rozwiązanie powinno umożliwiać cykliczne skanowanie wskazanych zasobów, tworzenie raportów technicznych i zarządczych, klasyfikację podatności według uznanej metodyki oceny ryzyka, wskazywanie rekomendacji naprawczych oraz ewidencję statusu obsługi podatności. W zakresie środowiska OT/ICS testy aktywne mogą być wykonywane wyłącznie po uprzednim uzgodnieniu z Zamawiającym, w zaakceptowanych oknach serwisowych i z wyłączeniem działań mogących zakłócić ciągłość procesów technologicznych.

Pakiet obejmuje również wykonanie usług testów bezpieczeństwa, weryfikację konfiguracji kluczowych elementów infrastruktury, ocenę ekspozycji zasobów oraz przygotowanie raportów zawierających opis zidentyfikowanych ryzyk, rekomendacje działań naprawczych i priorytety ich wdrożenia.

6.1 System do skanowania podatności – dostawa ,konfiguracja i wdrożenie 1kpl.

Przedmiotem zamówienia jest dostawa, konfiguracja i wdrożenie zintegrowanej platformy do identyfikowania, oceny, priorytetyzowania, monitorowania oraz obsługi procesu usuwania podatności w zasobach teleinformatycznych Zamawiającego.

1. Cel wdrożenia

Celem wdrożenia systemu jest zapewnienie ciągłego monitorowania i zarządzania podatnościami w infrastrukturze IT Zamawiającego. System ma umożliwiać identyfikację, analizę i raportowanie luk bezpieczeństwa w zasobach sieciowych (serwerach, stacjach roboczych, urządzeniach sieciowych, usługach sieciowych itp.).

2. Wymagania funkcjonalne systemu

System oferowany przez Wykonawcę musi spełniać następujące wymagania funkcjonalne:

2.1. Skanowanie podatności

- Umożliwia wykonywanie aktywnych skanów sieci w celu wykrywania podatności systemów operacyjnych, usług sieciowych, aplikacji webowych i komponentów.
- Obsługuje skanowanie zgodne z aktualną bazą podatności CVE oraz zgodne z klasyfikacjami CVSS v3.
- Umożliwia definiowanie harmonogramów skanowania (skany cykliczne, skany ad-hoc).
- Wspiera różne typy skanów (pełny, szybki, pasywny, niestandardowy).

2.2. Wykrywanie urządzeń

- Umożliwia automatyczne wykrywanie hostów w sieci oraz identyfikację ich systemów operacyjnych i uruchomionych usług.
- Obsługuje protokoły SNMP, SSH, SMB, HTTP/S i inne powszechnie stosowane.

2.3. Raportowanie i analiza

- Generowanie raportów z wynikami skanów w formatach: HTML, PDF, CSV, XML.
- Klasyfikacja podatności wg krytyczności (np. niski, średni, wysoki, krytyczny).
- Możliwość filtrowania wyników wg hosta, typu podatności, poziomu ryzyka.
- Eksport wyników do systemów SIEM i narzędzi zewnętrznych (opcjonalnie REST API).

2.4. Zarządzanie i integracja

- Interfejs webowy do zarządzania konfiguracją i przeglądania wyników.
- Możliwość integracji z LDAP/Active Directory.
- Uwierzytelnianie wieloskładnikowe (MFA) do konsoli administracyjnej (opcjonalnie).

3. Wymagania techniczne

- System może być wdrożony jako maszyna wirtualna lub kontener (np. Docker).
- System działa na systemach Linux (rekomendowane: Debian/Ubuntu lub CentOS/RHEL).
- System powinien być oparty na otwartym oprogramowaniu (Open Source), zgodnie z licencją GPL lub równoważną.
- Komponenty systemu muszą być utrzymywane i rozwijane przez aktywną społeczność lub organizację.
- Dostarczony system nie wymaga zakupu licencji komercyjnych.

4. Wymagania wdrożeniowe i eksploatacyjne

- Instalacja i konfiguracja rozwiązania we wskazanym środowisku Zamawiającego.
- **Wsparcie technicznie w zakresie zaoferowanego rozwiązania - min 12 mieś**.
- Przeprowadzenie testów poprawności działania.
- Dokumentacja użytkownika i administratora w języku polskim lub angielskim.
- Przeszkolenie wskazanych pracowników (min. 2 osoby).

6.2. Oprogramowania do zarządzania podatnościami w infrastrukturze Zamawiającego.

Obsługiwane rodzaje skanów:

- Nieuwierzytelnione skanowanie: Sprawdza systemy bez logowania, idealne do początkowego skanowania i wykrywania widocznych luk.
- Uwierzytelnione skanowanie: Loguje się na systemy, aby przeprowadzić bardziej dokładne testy i wykryć wewnętrzne zagrożenia.

2.Podstawowe funkcje:

- Wykrywanie luk: Analiza systemów i sieci, aby znaleźć znane luki, błędne konfiguracje i inne zagrożenia.
- Ocena ryzyka: Klasyfikuje wykryte luki według ich potencjalnego wpływu na system.
- Raportowanie: Generuje raporty zawierające szczegóły na temat wykrytych luk, ich opis i rekomendacje naprawcze.
- Integracja: Może być zintegrowany z innymi systemami i narzędziami bezpieczeństwa.

3.Architektura:

- Frontend: Interfejs użytkownika do zarządzania skanami i raportami.
- Backend: Serwer, który wykonuje skanowanie i analizę.
- NASL: obsługa języka NASL (Nessus Automatic Scripting Language) do tworzenia skryptów skanujących.

4.Platformy i systemy operacyjne:

- możliwość uruchamiania na różnych platformach, w tym na Linux, Windows (poprzez kontener Docker lub WSL) i Mac OS.

5.Dodatkowe funkcje:

- Skanowanie sieci: możliwość skanowania całych sieci, a nie tylko poszczególnych systemów.
- Automatyczne aktualizacje: możliwość automatycznego pobierania nowych testów i aktualizacji danych o podatnościach.

Wsparcie techniczne na 12 miesięcy, 50 zasobów:

6.3 Testy bezpieczeństwa (U02) i (O28) BAS

Testy bezpieczeństwa IT/OT Zintegrowana platforma zarządzania informacją o cyberzagrożeniach CTI oraz automatycznej walidacji zabezpieczeń BAS/AEV – 1 kpl

1. Przedmiot zamówienia jest dostawa, instalacja, konfiguracja i wdrożenie zintegrowanej platformy przeznaczonej do:

a. gromadzenia, strukturyzowania i analizowania informacji o cyberzagrożeniach;
b. zarządzania wskaźnikami kompromitacji i wiedzą o technikach działania napastników;
c. modelowania cyberzagrożeń zgodnie z MITRE ATT&CK;
d. przygotowywania i wykonywania kontrolowanych symulacji ataków;
e. przeprowadzania testów atomowych zabezpieczeń;
f. weryfikowania skuteczności systemów ochronnych;
g. oceny poziomu detekcji, prewencji i ogólnego poziomu bezpieczeństwa;
h. identyfikowania luk w konfiguracji i działaniu mechanizmów bezpieczeństwa.

System może zostać dostarczony jako jedna platforma albo jako zestaw dwóch wzajemnie zintegrowanych modułów, pod warunkiem zapewnienia ich spójnego działania, wspólnej wymiany danych i jednolitego procesu realizacji testów.

2. Cel wdrożenia jest zwiększenie odporności infrastruktury IT i OT Zamawiającego przez przejście od pasywnego monitorowania zagrożeń do regularnej, kontrolowanej i mierzalnej weryfikacji skuteczności zastosowanych zabezpieczeń.
Platforma ma umożliwiać wykorzystanie aktualnej wiedzy o zagrożeniach do przygotowywania realistycznych scenariuszy testowych, odpowiadających technikom i procedurom stosowanym przez rzeczywistych napastników.
Wdrożenie powinno umożliwić Zamawiającemu:

a. uporządkowanie informacji o zagrożeniach;
b. identyfikowanie zagrożeń istotnych dla przedsiębiorstwa wodociągowo-kanalizacyjnego;
c. powiązanie informacji o podatnościach, wskaźnikach kompromitacji, kampaniach i grupach przestępczych;
d. odwzorowanie technik ataków w modelu MITRE ATT&CK;
e. przygotowywanie scenariuszy odpowiadających rzeczywistym zagrożeniom;
f. wykonywanie bezpiecznych i kontrolowanych testów systemów ochronnych;
g. sprawdzanie, czy wdrożone systemy wykrywają i blokują symulowane działania;
h. ocenę pokrycia technik ATT&CK przez posiadane zabezpieczenia;
i. identyfikowanie luk w zakresie detekcji i prewencji;

j. formułowanie zaleceń dotyczących poprawy konfiguracji EDR/XDR, SIEM, firewalli, IPS i pozostałych mechanizmów bezpieczeństwa;
k. cykliczne potwierdzanie skuteczności zabezpieczeń po aktualizacjach i zmianach konfiguracji.

3. Model wdrożenia - Platforma musi być wdrożona lokalnie w infrastrukturze Zamawiającego i umożliwiać działanie bez konieczności przekazywania danych CTI, wyników testów i informacji o infrastrukturze do publicznej chmury producenta.

Dopuszcza się wdrożenie:
a. w środowisku Docker;
b. w środowisku Kubernetes;
c. w postaci maszyn wirtualnych z uruchomionymi kontenerami;
d. w innym równoważnym środowisku kontenerowym zapewniającym wymagane bezpieczeństwo i trwałość danych.

4. Opis cech funkcjonalno użytkowych platformy:

1. Platforma musi być rozwiązaniem umożliwiającym zarządzanie informacją o cyberzagrożeniach (CTI).
2. Platforma musi umożliwiać:
    - gromadzenie IOC,
    - gromadzenie TTP,
    - Campaign,
    - Malware,
    - Threat Actor,
    - Intrusion Set,
    - Vulnerability (CVE),
    - Indicators,
    - Observables,
    - Reports,
    - Identities,
    - Relationships pomiędzy obiektami.
4. Platforma musi umożliwiać modelowanie wiedzy zgodnie z MITRE ATT&CK.
5. Platforma musi posiadać graficzną wizualizację relacji pomiędzy obiektami CTI.
6. Platforma musi wspierać standard STIX 2.1 oraz TAXII 2.1 do wymiany informacji o zagrożeniach.
7. Platforma musi posiadać interfejs webowy
8. Platforma musi udostępniać GraphQL API.
9. Platforma musi umożliwiać wielożytkownikową pracę z kontrolą uprawnień.
10. Platforma musi umożliwiać import i eksport danych minimum w formatach:
    - STIX
    - CSV
    - JSON
    - PDF.

10. Platforma musi posiadać mechanizm konektorów umożliwiających integrację z:
    - MISP
    - CVE
    - NVD
    - MITRE ATT&CK
    - AlienVault OTX
    - Mandiant
    - Shodan
    - VirusTotal
    - AbuseIPDB
    - Splunk
    - Elastic
    - QRadar
    - Microsoft Sentinel
    - własnymi źródłami danych.
11. Platforma musi umożliwiać automatyczne wzbogacanie informacji (Enrichment).
12. Platforma musi umożliwiać automatyczne importowanie danych z wielu źródeł.
13. Platforma musi umożliwiać prowadzenie analiz i korelację informacji o zagrożeniach.

14. Platforma musi być rozwiązaniem umożliwiającym planowanie oraz wykonywanie kampanii symulujących ataki.
15. Platforma musi umożliwiać:
    - tworzenie scenariuszy,
    - harmonogramowanie kampanii,
    - wykonywanie testów atomowych,
    - testowanie bezpieczeństwa infrastruktury.
16. Platforma musi posiadać:
    - Executor,
    - Injectory,
    - Collectory.
17. Platforma musi umożliwiać integrację z:
    - SIEM,
    - SOAR,
    - XDR,
    - EDR,
    - Firewall,
    - Mail Gateway,
    - NAC.
18. Platforma musi umożliwiać automatyczne sprawdzenie czy:
    - EDR wykrył zagrożenie,
    - SIEM wygenerował alarm,
    - Firewall zablokował ruch,
    - IPS zablokował exploit,
    - Mail Gateway zatrzymał wiadomość.
19. Platforma musi umożliwiać automatyczne generowanie scenariuszy na podstawie danych z OpenCTI.
20. Platforma musi umożliwiać mapowanie testów do MITRE ATT&CK.
21. Platforma musi umożliwiać ocenę:
    - Detection Coverage,
    - Prevention Coverage,
    - Security Posture.
22. Platforma musi umożliwiać prezentację wyników poprzez interfejs web
23. Platforma musi posiadać REST API.
24. Platforma musi umożliwiać pracę całkowicie wewnątrz infrastruktury Zamawiającego (On-Premises).
25. Platforma musi umożliwiać uruchomienie w środowisku Docker oraz Kubernetes.
26. Platforma musi umożliwiać automatyczne budowanie scenariuszy testowych na podstawie ATT&CK,
27. Platforma musi automatyczne uruchamianie testów,
28. Platforma musi umożliwiać prezentację poziomu pokrycia zabezpieczeń

5. Bezpieczeństwo wykonywania testów

Platforma musi umożliwiać prowadzenie testów w sposób kontrolowany i ograniczający ryzyko zakłócenia działania infrastruktury.

W szczególności musi umożliwiać:

- wskazanie dokładnego zakresu testowanych zasobów;
- stosowanie list dozwolonych i wykluczeń;
- określenie czasu wykonania testu;
- uruchamianie testów w oknach serwisowych;
- zatwierdzanie kampanii przed uruchomieniem;
- zatrzymanie trwającej kampanii;
- rejestrowanie wszystkich wykonanych czynności;
- rozróżnienie testów bezpiecznych od potencjalnie zakłócających;
- przeprowadzenie testu pilotażowego;
- ograniczenie testów w środowisku OT do zasobów zatwierdzonych przez Zamawiającego.

Na sterownikach PLC, RTU, urządzeniach embedded i innych krytycznych urządzeniach przemysłowych testy aktywne mogą być wykonywane wyłącznie po pisemnym zatwierdzeniu scenariusza i potwierdzeniu bezpieczeństwa takiego działania.

Pakiet 7.- Zarzadzanie tożsamością i centralny manager haseł

7. System Zarządzanie tożsamością i dostępem, centralny menadżer haseł

Pakiet obejmuje zarządzanie tożsamością, cyklem życia kont i uprawnieniami, natomiast centralne, szyfrowane repozytorium poświadczeń. Menedżer haseł nie jest automatycznie pełnym systemem PAM z proxy i nagrywaniem sesji, o ile takie funkcje nie zostały jawnie wymagane.
Przedmiotem zamówienia w niniejszym zakresie jest dostawa, wdrożenie, konfiguracja, integracja, uruchomienie i udokumentowanie rozwiązań służących do zarządzania tożsamością, dostępem, uprawnieniami oraz hasłami użytkowników i administratorów Zamawiającego, z wykorzystaniem istniejącej usługi katalogowej Active Directory jako podstawowego źródła tożsamości.
Celem wdrożenia jest uporządkowanie zarządzania kontami i uprawnieniami w Active Directory, ograniczenie liczby kont nadmiarowych, i nieaktywnych, wdrożenie okresowego przeglądu uprawnień, zapewnienie rozliczalności działań administracyjnych oraz utworzenie centralnego, bezpiecznego repozytorium haseł wykorzystywanych w środowisku IT i wybranych elementach OT Zamawiającego
Przedmiotem rozwiązania jest dostawa i wdrożenie centralnego systemu zarządzania hasłami oraz danymi uwierzytelniającymi opartymi o lekką, samodzielnie hostowaną implementację platformy do przechowywania danych. Okres świadczonego wsparcia i **aktualizacji systemu – min 12 mieś**.

1. Wymagania ogólne

1. System musi być rozwiązaniem, przeznaczonym do bezpiecznego przechowywania oraz współdzielenia poświadczeń między użytkownikami.
2. System musi umożliwiać instalację lokalną w infrastrukturze Zamawiającego, bez obowiązku korzystania z chmury producenta.
3. System nie może posiadać ograniczenia czasowego ani limitu liczby użytkowników
4. System musi posiadać interfejs administracyjny i użytkowy dostępny przez przeglądarkę internetową.
5. Dostęp do systemu musi być możliwy przez połączenie szyfrowane HTTPS.

2. Przechowywanie poświadczeń

7. System musi umożliwiać tworzenie i przechowywanie co najmniej:

- nazw zasobów,
- nazw użytkowników,
- adresów URL,
- haseł,
- zaszyfrowanych opisów i notatek,
- kodów TOTP,
- dodatkowych pól niestandardowych.

System rozdziela dane na metadane zasobu oraz zaszyfrowaną część sekretu; typy zasobów mogą obejmować hasła, TOTP i pola dodatkowe.

8. System musi umożliwiać organizowanie wpisów w folderach.
9. System musi umożliwiać oznaczanie najczęściej używanych wpisów jako ulubione.
10. System musi posiadać generator haseł umożliwiający tworzenie losowych poświadczeń.
11. System musi umożliwiać kopiowanie loginu, hasła lub kodu jednorazowego do schowka.
12. System musi umożliwiać automatyczne wypełnianie danych uwierzytelniających w obsługiwanych przeglądarkach.

3. Współdzielenie i uprawnienia

13. System musi umożliwiać współdzielenie pojedynczych poświadczeń oraz folderów:

- z pojedynczym użytkownikiem,
- z grupą użytkowników.

14. System musi umożliwiać nadawanie uprawnień co najmniej na poziomach:

- odczyt,
- edycja,
- właściciel.

System definiuje uprawnienia Read, Update i Owner na poziomie zasobów oraz folderów.

15. Użytkownik posiadający uprawnienia właściciela musi mieć możliwość zarządzania sposobem udostępnienia zasobu.
16. System musi umożliwiać tworzenie grup użytkowników oraz przypisywanie użytkowników do grup.
17. System musi umożliwiać wyznaczanie osób zarządzających składem grupy.

4. Kryptografia i bezpieczeństwo

18. System musi realizować szyfrowanie end-to-end, w którym odszyfrowanie sekretu następuje po stronie uprawnionego klienta użytkownika.
19. System musi wykorzystywać standard OpenPGP lub równoważny mechanizm kryptograficzny do:

- szyfrowania sekretów,
- odszyfrowywania sekretów,
- podpisywania danych,
- weryfikacji tożsamości użytkownika.

OpenPGP jest podstawowym mechanizmem kryptograficznym System.

20. Każdy użytkownik musi posiadać własną parę kluczy kryptograficznych.
21. Serwer aplikacyjny nie może przechowywać haseł użytkowników w postaci jawnej.
22. System musi umożliwiać uwierzytelnianie wieloskładnikowe z wykorzystaniem co najmniej kodów TOTP. MFA z TOTP.
23. Administrator musi mieć możliwość włączenia lub wyłączenia MFA dla organizacji.
24. System musi umożliwiać generowanie i przechowywanie kodów TOTP związanych z chronionymi kontami.
25. System musi umożliwiać sprawdzenie tożsamości serwera na podstawie klucza kryptograficznego lub jego odcisku.

5. Dostęp użytkowników

26. System musi posiadać rozszerzenie przeglądarkowe umożliwiające co najmniej:

- wyszukiwanie poświadczeń,
- tworzenie wpisów,
- edycję wpisów,
- współdzielenie wpisów,
- automatyczne wypełnianie formularzy logowania,
- import i eksport danych.

Funkcje te są dostępne w interfejsie rozszerzenia przeglądarkowego System CE.

27. System musi posiadać aplikację mobilną co najmniej dla:

- Android,
- iOS.

28. Aplikacje mobilne muszą umożliwiać dostęp do przechowywanych poświadczeń oraz kodów TOTP.

6. Import i eksport

29. System musi umożliwiać import danych co najmniej z formatów:

- CSV,
- KDBX.

30. System musi umożliwiać eksport danych co najmniej do:

- CSV,
- KDBX.

31. Zalecanym formatem eksportu zaszyfrowanego powinien być KDBX lub format równoważny. System obsługuje import i eksport CSV/KDBX; producent wskazuje KDBX jako bezpieczniejszy format przenoszenia poświadczeń.
32. Administrator musi mieć możliwość wyłączenia eksportu danych w postaci jawnej.

7. Administracja

33. System musi umożliwiać:

- tworzenie użytkowników,
- aktywowanie użytkowników,
- blokowanie lub usuwanie użytkowników,
- tworzenie grup,
- zarządzanie członkostwem w grupach,
- nadawanie roli administratora.

34. System musi umożliwiać wysyłanie użytkownikom wiadomości aktywacyjnych za pośrednictwem serwera SMTP.
35. System musi udostępniać mechanizm kontroli poprawności konfiguracji i stanu działania aplikacji.
36. System musi prowadzić dzienniki zdarzeń co najmniej dla:

- uwierzytelnienia,
- dostępu do sekretów,
- tworzenia i modyfikacji wpisów,
- współdzielenia zasobów,
- operacji administracyjnych.

Dokumentacja API wskazuje, że dostęp do sekretów jest rejestrowany.

37. System musi umożliwiać wykonywanie kopii zapasowej co najmniej:
- bazy danych,
- klucza prywatnego serwera,
- konfiguracji aplikacji,
- plików przechowywanych przez aplikację.

8. Integracja i automatyzacja

38. System musi udostępniać interfejs API umożliwiający automatyzację operacji na użytkownikach, grupach, zasobach i uprawnieniach.
39. API powinno być opisane w standardzie OpenAPI lub równoważnym. Wymagana platforma musi udostępniać REST API oraz publiczną specyfikację OpenAPI.
40. System musi umożliwiać uwierzytelnianie klientów API przy użyciu mechanizmu kryptograficznego opartego na OpenPGP lub tokenów JWT.

9. Wymagania wdrożeniowe

41. System musi umożliwiać instalację co najmniej:
- na systemie Linux,
- w środowisku kontenerowym Docker.

42. Baza danych musi pracować lokalnie w infrastrukturze Zamawiającego.
43. System musi umożliwiać pracę bez połączenia z chmurą producenta.
44. Wykonawca musi dostarczyć:
- instalację i konfigurację systemu,
- konfigurację HTTPS,
- konfigurację SMTP,
- konfigurację kopii zapasowych,
- dokumentację powdrożeniową,
- instrukcję odtwarzania systemu,
- instrukcję tworzenia użytkowników i grup.

45. System musi zostać dostarczony w najnowszej wersji wraz z wsparciem technicznym przez okres min. 12 miesięcy

.

8. Wdrożenie utrzymanie warunki odbioru

Pakiet usług wdrożeniowych, dokumentacyjnych, szkoleniowych i utrzymaniowych

8.1. Wymagania ogólne dla całości zamówienia

Wykonawca zobowiązany jest dostarczyć rozwiązanie kompletne, zintegrowane i gotowe do pracy produkcyjnej, obejmujące wszystkie urządzenia, licencje, subskrypcje, moduły, elementy montażowe, okablowanie, wkładki, zasilacze, szyny, oprogramowanie, dokumentację oraz usługi niezbędne do prawidłowego uruchomienia i eksploatacji przedmiotu zamówienia.
Wszystkie elementy przedmiotu zamówienia muszą być dobrane w sposób zapewniający wzajemną kompatybilność, możliwość integracji, centralne zarządzanie w zakresie właściwym dla danej klasy rozwiązania, zachowanie ciągłości działania oraz możliwość bezpiecznej eksploatacji przez Zamawiającego po zakończeniu wdrożeni

8.2. Opis wdrożenia rozwiązań infrastruktury serwerowej, sieciowej i cyberbezpieczeństwa

Kompleksowe wdrożenie zintegrowanego środowiska infrastruktury IT i cyberbezpieczeństwa, obejmującego dostawę, instalację, konfigurację, integrację, uruchomienie oraz udokumentowanie rozwiązań serwerowych, macierzowych, sieciowych i bezpieczeństwa, zgodnie z wymaganiami Zamawiającego oraz standardami cyberbezpieczeństwa.
Wdrożenie musi zostać przeprowadzone w sposób zapewniający wysoką dostępność usług, odporność na awarie, segmentację sieci, centralne zarządzanie, kontrolę dostępu, monitorowanie zdarzeń bezpieczeństwa oraz możliwość dalszej rozbudowy środowiska. Rozwiązanie po zakończeniu wdrożenia musi być kompletne, spójne funkcjonalnie, przetestowane i gotowe do pracy produkcyjnej w środowisku Zamawiającego.

8.3. Zakres prac wdrożenia

Wykonawca zobowiązany jest do wykonania co najmniej następujących prac:

1. Przeprowadzenia analizy przedwdrożeniowej środowiska Zamawiającego, obejmującej inwentaryzację istniejącej infrastruktury serwerowej, macierzowej, sieciowej, bezpieczeństwa oraz zależności pomiędzy systemami.
2. Dostawy, montażu i fizycznej instalacji urządzeń w szafach rack, wraz z podłączeniem zasilania, okablowania LAN/SAN/management oraz oznaczeniem połączeń.
3. Instalacji i konfiguracji serwerów fizycznych, systemów operacyjnych, oprogramowania zarządzającego, licencji dostępowych oraz komponentów niezbędnych do pracy środowiska.
4. Instalacji i konfiguracji macierzy dyskowej, w tym utworzenia wymaganych grup dyskowych, wolumenów, mechanizmów RAID, cache, snapshotów, thin provisioning oraz prezentacji zasobów do hostów.
5. Utworzenia klastra wysokiej dostępności HA dla środowiska serwerowego i/lub usług objętych wdrożeniem, wraz z konfiguracją mechanizmów przełączania awaryjnego, testami failover/failback oraz weryfikacją ciągłości dostępu do danych.
6. Uruchomienia i integracji mechanizmów RADIUS w istniejącym systemie zarządzania dostępem Alcatel-Lucent Enterprise OmniVista/UPAM albo zgodnym komponencie RADIUS, bez dostawy nowej platformy NAC.
7. Konfiguracji i integracji posiadanych urządzeń UTM/NGFW WatchGuard z natywnymi narzędziami WatchGuard System Manager/Management Server oraz Dimension. W zakres pakietu zarządzania politykami nie wchodzi ponowna dostawa klastra WatchGuard ani odrębna platforma NSPM/SOAR.
8. Konfiguracji funkcji bezpieczeństwa, w szczególności: firewall, NAT, IPS, antywirus, kontrola aplikacji, filtrowanie WWW/DNS, ochrona przed malware, VPN IPsec/SSL, inspekcja ruchu szyfrowanego, logowanie zdarzeń oraz integracja z mechanizmami uwierzytelniania.
9. Instalacji i konfiguracji przełączników zarządzalnych, w tym VLAN, trunk/access, LACP, STP/RSTP/MSTP, routingu, DHCP Snooping, Dynamic ARP Inspection, port security, 802.1X, ACL, mirroring, SNMP, syslog oraz integracji z urządzeniami UTM/NGFW.
10. Zachowania istniejącej segmentacji sieci Zamawiającego, w tym aktualnego podziału VLAN i stref IT/OT. Wykonawca odwzoruje polityki sieciowe na dostarczonych urządzeniach i w istniejącym OmniVista; zmiany struktury stref, adresacji lub reguł separacji wprowadzi tylko po pisemnej akceptacji Zamawiającego.
11. Wdrożenia i udokumentowania polityk dostępu NAC/UNP w posiadanym Alcatel-Lucent Enterprise OmniVista/UPAM, wraz z testami RADIUS, 802.1X, MAB i przypisywania profili dostępowych. Nie dopuszcza się zastąpienia OmniVista nową platformą NAC.
12. Integracji rozwiązania z usługami katalogowymi Zamawiającego, w szczególności Active Directory/LDAP/RADIUS, w celu centralnego uwierzytelniania administratorów i użytkowników.
13. Pełne wdrożenie Active Directory w oparciu o oprogramowanie Microsoft Windows Server.
14. Konfiguracji centralnego monitorowania i logowania zdarzeń, w tym przekazywania logów do wskazanych systemów Zamawiającego lub systemów dostarczonych w ramach zamówienia.
15. Wdrożenia polityk bezpieczeństwa uzgodnionych z Zamawiającym, z uwzględnieniem zasady minimalnych uprawnień, rozdziału ról administracyjnych, MFA oraz ograniczenia dostępu administracyjnego wyłącznie z uprawnionych adresów lub stref.
16. Przeprowadzenia testów funkcjonalnych, wydajnościowych i bezpieczeństwa, w szczególności poprawności działania posiadanej segmentacji IT/OT, autoryzacji NAC/OmniVista, RADIUS i VPN, polityk WatchGuard w WSM/Dimension, odtwarzania lokalnych kopii PBS, separacji wspólnego NAS, logowania oraz monitoringu. Testy mogące wpływać na OT wymagają wcześniejszej zgody Zamawiającego.
17. Usunięcia wykrytych nieprawidłowości i ponownego wykonania testów w zakresie niezbędnym do potwierdzenia prawidłowości działania rozwiązania.
18. Przygotowania dokumentacji powykonawczej, instrukcji administracyjnych, oraz zaleceń eksploatacyjnych.
19. Przeprowadzenia instruktażu powdrożeniowego dla administratorów Zamawiającego, obejmującego obsługę, monitorowanie, podstawową diagnostykę oraz zarządzanie politykami bezpieczeństwa

8.4. Wymagania dotyczące organizacji prac

Wszystkie prace wdrożeniowe muszą być prowadzone w sposób minimalizujący ryzyko zakłócenia pracy Zamawiającego, z uwzględnieniem **ciągłości działania jego krytycznych procesów/funkcji**. Działania mogące wpływać na dostępność systemów produkcyjnych muszą być realizowane wyłącznie w uzgodnionych z Zamawiającym oknach serwisowych..

Wykonawca zobowiązany jest do bieżącej współpracy z przedstawicielami Zamawiającego, raportowania postępu prac, zgłaszania ryzyk oraz uzyskiwania akceptacji dla kluczowych etapów wdrożenia. Przed rozpoczęciem prac produkcyjnych Wykonawca musi przedstawić plan wdrożenia oraz plan wycofania zmian.

8.5. Dokumentacja i odbiór

Wykonawca zobowiązany jest do przekazania Zamawiającemu kompletnej dokumentacji powykonawczej, obejmującej co najmniej:

1. opis architektury wdrożonego rozwiązania;
2. schematy logiczne i fizyczne;
3. zestawienie urządzeń, numerów seryjnych, wersji firmware i licencji;
4. konfigurację istniejących VLAN i segmentacji IT/OT, RADIUS, VPN, NAC/OmniVista, polityk WatchGuard, zarządzania WSM/Dimension oraz macierzy dozwolonych przepływów;
5. opis kont administracyjnych, ról i mechanizmów uwierzytelniania;
6. procedury awaryjne i odtworzeniowe dla lokalnego Proxmox Backup Server oraz wspólnego NAS IT/OT, w tym testy odtwarzania i plan zabezpieczenia kluczy;
7. raport z testów funkcjonalnych, wydajnościowych i bezpieczeństwa;
8. instrukcję eksploatacyjną dla administratorów Zamawiającego.

Odbiór wdrożenia nastąpi po zakończeniu wszystkich prac, przekazaniu dokumentacji, przeprowadzeniu testów z wynikiem pozytywnym oraz podpisaniu protokołu odbioru przez upoważnionych przedstawicieli Zamawiającego i Wykonawcy.