Załącznik nr.10 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa i wdrożenie systemów IT/OT ”
w ramach realizacji projektu Wzmocnienie Cyberodporności GZUW Fredropol”

Cyberbezpieczne Wodociągi

Zamawiający

GMINNY ZAKŁAD USŁUG WODNYCH W FREDROPOLU
Fredropol 15
37-734 Fredropol

Główne części zamówienia

1. Pakiet sieciowy, UTM/NGFW, segmentacja i kontrola dostępu do sieci
2. Pakiet zarządzania podatnościami i testów bezpieczeństwa IT/OT
3. Pakiet inwentaryzacji, CMDB, ITSM, monitoringu i zarządzania zmianą
4. Zintegrowana ochrona punktów końcowych, centralne monitorowanie bezpieczeństwa oraz zarządzana detekcja i reakcja
5. Pakiet infrastruktury serwerowej, wirtualizacji, macierzy, NAS i kopii zapasowych
6. Pakiet zarządzania tożsamością, dostępem i hasłami
7. Pakiet bezpiecznego dostępu do środowiska OT/ICS
8. Pakiet zasilania awaryjnego dla produktów i rozwiązań bezpieczeństwa
9. Pakiet usług wdrożeniowych, dokumentacyjnych, szkoleniowych i utrzymaniowych

Zintegrowany system bezpieczeństwa obszaru IT/OT

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. Zamówienie obejmuje następujące pakiety funkcjonalne, które mogą być realizowane jako wzajemnie zintegrowane rozwiązania, pod warunkiem spełnienia wymagań minimalnych określonych w OPZ.

1. Pakiet sieciowy, UTM/NGFW, segmentacja i kontrola dostępu do sieci

Przedmiotem pakietu jest dostawa, wdrożenie i integracja wielowarstwowego systemu bezpieczeństwa sieciowego dla środowiska IT oraz OT/ICS Zamawiającego.
Ze względu na istniejącą infrastrukturę Zamawiającego, dostępność urządzeń, wymagany termin realizacji projektu oraz konieczność racjonalnego wykorzystania dostępnego budżetu przyjmuje się architekturę wielo-producentową , w której poszczególne komponenty współpracują z wykorzystaniem standardowych protokołów i mechanizmów komunikacyjnych.
Podstawę systemu stanowić będzie klaster dwóch urządzeń klasy UTM/NGFW pracujących w układzie wysokiej dostępności HA, realizujący ochronę styku z Internetem, routing pomiędzy strefami bezpieczeństwa, kontrolę ruchu pomiędzy środowiskiem IT i OT/ICS, VPN, IPS, kontrolę aplikacji, rejestrowanie zdarzeń oraz egzekwowanie centralnych polityk bezpieczeństwa.
Jeden wspólny klaster HA będzie realizował funkcje bezpieczeństwa przewidziane dla obszaru IT oraz OT/ICS, przy zachowaniu logicznego rozdzielenia obu środowisk, wydzielonych stref bezpieczeństwa i niezależnych zestawów reguł komunikacyjnych.
Warstwę przełączającą będą stanowiły zarządzalne przełączniki sieciowe współpracujące z centralnym systemem NAC z wykorzystaniem otwartych standardów, w szczególności IEEE 802.1X, RADIUS, uwierzytelniania urządzeń na podstawie adresu MAC, VLAN, ACL, SNMP i Syslog.
Centralny system NAC będzie odpowiedzialny za identyfikację i uwierzytelnianie użytkowników oraz urządzeń, przydzielanie odpowiednich polityk dostępu, dynamiczne przypisywanie urządzeń do właściwych sieci VLAN oraz izolowanie urządzeń niespełniających ustalonych zasad bezpieczeństwa.
System NAC musi umożliwiać współpracę z urządzeniami sieciowymi różnych producentów i nie może wymagać stosowania jednej, zamkniętej platformy sprzętowej w całej infrastrukturze Zamawiającego.
Architektura musi umożliwiać integrację z usługą katalogową Active Directory, centralnym systemem logowania, systemami monitoringu oraz innymi elementami bezpieczeństwa wdrażanymi w ramach projektu.
W ramach realizacji Wykonawca odpowiada za integrację poszczególnych elementów oraz wykonanie testów współdziałania, w szczególności testów 802.1X, uwierzytelnienia urządzeń bez supplicanta, dynamicznego przydziału VLAN, izolacji urządzenia, ponownego uwierzytelnienia oraz działania mechanizmów awaryjnych w przypadku czasowej niedostępności systemu NAC.
.

1.1. Zakup urządzeń brzegowych klasy UTM (klaster HA) wraz z systemem centralnego zarządzania urządzeniami bezpieczeństwa sieciowego – 1 kpl

Centralna platforma zarządzania UTM/NGFW ma również realizować – w zakresie obsługiwanym przez rozwiązanie – funkcję scentralizowanego zarządzania i orkiestracji polityk bezpieczeństwa OT przewidzianą w O22, bez konieczności zakupu odrębnej platformy.

Architektura systemu UTM/NGFW

Ze względu na skalę infrastruktury Zamawiającego dopuszcza się realizację funkcji ochrony środowiska IT oraz OT/ICS za pomocą jednego wspólnego klastra urządzeń UTM/NGFW pracującego w architekturze wysokiej dostępności HA.

Współdzielenie platformy sprzętowej nie może powodować połączenia logicznego środowisk IT i OT. System musi zapewniać utworzenie odrębnych stref bezpieczeństwa, interfejsów lub sieci VLAN oraz niezależnych zestawów polityk dostępu dla środowiska IT, OT/ICS, strefy DMZ, strefy zarządzającej oraz dostępu serwisowego.
Komunikacja pomiędzy strefami IT i OT/ICS musi być domyślnie zabroniona i dopuszczana wyłącznie dla udokumentowanych przepływów komunikacyjnych wymaganych do realizacji procesów Zamawiającego.
Architektura musi zapewniać co najmniej separację logiczną środowisk, zasadę minimalnych uprawnień, rejestrowanie komunikacji pomiędzy strefami, kontrolę dostępu administracyjnego oraz możliwość zastosowania odrębnych profili ochrony IPS/Application Control dla ruchu IT oraz OT/ICS.
Wykonawca zobowiązany jest wykonać analizę przepływów IT/OT i przygotować przed uruchomieniem produkcyjnym macierz komunikacji obejmującą źródło, cel, protokół, port, kierunek komunikacji oraz uzasadnienie biznesowe.
Ochrona OT musi być dedykowana logicznie i funkcjonalnie: Wykonawca skonfiguruje odrębne strefy i polityki bezpieczeństwa OT, odrębne profile IDS/IPS dla ruchu OT, inspekcję wykorzystywanych protokołów przemysłowych, centralne logowanie i monitoring zdarzeń OT oraz integrację z mechanizmami identyfikacji aktywów i zarządzania podatnościami OT. Odbiór obejmie odrębne testy działania ochrony dla środowiska IT i dla środowiska OT.

1. Wymagania Ogólne Systemu
Dostawa, wdrożenie i konfiguracja systemu centralnego zarządzania urządzeniami klasy UTM/NGFW, kompatybilnego z dostarczonymi urządzeniami bezpieczeństwa sieciowego. System musi zapewniać centralne zarządzanie konfiguracją, politykami bezpieczeństwa, obiektami sieciowymi, regułami filtrowania i translacji, połączeniami VPN, uprawnieniami administratorów oraz kopiami konfiguracji urządzeń.

2. Zakres wdrożenia
W ramach zamówienia Wykonawca wykona co najmniej:

1. Dostawę wymaganych licencji i subskrypcji.
2. Instalację maszyny wirtualnej w środowisku Zamawiającego.
3. Konfigurację adresacji, DNS, NTP, routingu i certyfikatu HTTPS.
4. Podłączenie wszystkich dostarczonych urządzeń UTM/NGFW.
5. Utworzenie struktury urządzeń i lokalizacji obejmującej co najmniej:
    - siedzibę główną;
    - lokalizację oddziałową;
    - obszar IT;
    - obszar OT;
    - styk IT/OT.
6. Konfigurację wspólnych obiektów i polityk bezpieczeństwa.
7. Konfigurację zarządzania tunelami VPN.
8. Konfigurację kont i ról administratorów.
9. Integrację z centralnym systemem logowania.
10. Konfigurację wykonywania kopii zapasowych.
11. Konfigurację monitorowania stanu urządzeń i wdrożeń.
12. Wykonanie testów działania i odtworzenia konfiguracji.
13. Przeprowadzenie instruktażu administratorów Zamawiającego

1.1.2. Zakup 2 urządzeń brzegowych klasy UTM zapewniających wysoką dostępność (HA), do lokalizacji siedziby głównej:
OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.

4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).

26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

27. Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania).
28. Po rozbudowie administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
29. Skaner antywirusowy ma pochodzić od europejskiego producenta.
30. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
31. Po rozbudowie administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP.
    W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

32. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
33. Ochrona antyspam ma działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. Skaner heurystyczny.
34. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
35. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

36. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub siteto-site (lokalizacja-lokalizacja).
37. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    a. IPSec VPN,
    b. SSL VPN.
38. SSL VPN ma działać w trybie tunelu.
39. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
40. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
41. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
42. W ramach licencji dostępny jest klient SSLVPN pod systemy: Windows, Linux, macOS objęty gwarancją i wsparciem równolegle ze wsparciem dla rozwiązania UTM.
43. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
44. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
45. Rozwiązanie ma umożliwiać wykorzystanie algorytmów post-kwantowej kryptografii w szyfrowaniu IPSec w standardzie ML-KEM.

FILTR DOSTĘPU DO STRON WWW

46. Rozwiązanie ma umożliwiać wykorzystanie filtra URL w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
47. Administrator ma mieć możliwość dodawania własnych kategorii URL.
48. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:

   a. blokowanie dostępu do adresu URL,
   b. zezwolenie na dostęp do adresu URL,
   c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
49. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
50. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
51. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
52. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
53. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
54. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

55. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
   a. lokalną bazę użytkowników (wewnętrzny LDAP),
   b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
   c. usługę katalogową Microsoft Active Directory.
   d. Microsoft Entra ID, opartej na protokole OpenID Connect.
56. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
57. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
   a. SSL,
   b. Radius,
   c. Kerberos.
58. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
59. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
60. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
61. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
62. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
63. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
64. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

65. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
66. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
   a. równoważenie względem adresu źródłowego,
   b. równoważenie względem połączenia.
67. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
68. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
69. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.

70. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
71. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

72. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
73. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
74. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
75. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
76. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

ADMINISTRACJA URZĄDZENIEM

77. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
78. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
79. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
80. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
81. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
82. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
83. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
84. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
85. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
86. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
87. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
88. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
89. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
90. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
91. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
92. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
93. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    a. manualnego eksportu do pliku w dowolnym momencie czasu,
    b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
94. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
95. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.

96. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

97. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
98. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
99. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
100. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
101. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
102. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
103. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
104. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 2 i 3.
105. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

106. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
107. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
108. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
109. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
110. Urządzenie ma posiadać usługę DNS Proxy.
111. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
112. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
113. Urządzenie musi mieć możliwość wykorzystania REST API.
114. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
115. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
116. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.

GWARANCJA I SERWIS

117. Urządzenie ma być **objęte 36-miesięczną gwarancją producenta** na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
118. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

119. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.

120. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
121. Liczba portów Ethernet 2,5Gbps – min. 8.
122. Liczba portów światłowodowych 1Gbps – min. 1.
123. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
124. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps.
125. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 6Gbps.
126. Przepustowość typu Threat Prevention – minimum 740Mbps.
127. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 3Gbps.
128. Liczba tuneli VPN IPSec – minimum 300.
129. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 300.
130. Obsługa interfejsów 802.11q (VLAN) – minimum 393.
131. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 39 000 nowych sesji/sekundę.
132. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie ActivePassive.
133. Urządzenie nie ma limitu na liczbę użytkowników.
134. Liczba reguł filtrowania – minimum 8 192.
135. Liczba tras statycznego routingu – minimum 512.
136. Liczba tras dynamicznego routingu – minimum 10 000.

Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. 138. Urządzenie musi być wyposażone w moduł TPM

1.2. Zakup zarządzanych przełączników sieciowych, wraz ze wsparciem technicznym oraz z usługą segmentacji sieci oraz POE.

1.2.1. Przełączniki zarządzalne – łącznie 2 szt. w lokalizacji siedziby głównej, pracujące wspólnie w konfiguracji redundantnej. Obydwa urządzenia muszą obsługiwać wydzielone sieci i VLAN dla środowisk IT oraz OT. Redundancja ma być realizowana przez stackowanie, MLAG lub mechanizm równoważny zapewniający ciągłość komunikacji w przypadku awarii pojedynczego przełącznika. Urządzenia muszą obsługiwać VLAN, 802.1X, SNMP, Syslog, ACL, port mirroring/SPAN oraz mechanizmy bezpiecznego zarządzania; MACsec wymagany jest w zakresie wynikającym z aktualnego WoD i kompatybilności urządzeń końcowych.
Nie dopuszcza się realizacji tego zakresu jako dwóch niezależnych przełączników, z których jeden obsługuje wyłącznie IT, a drugi wyłącznie OT. W formularzu cenowym i dokumentacji odbiorowej należy wskazać sposób przypisania wartości obu urządzeń w obszarach IT i OT.

1.	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2.	Wymagane parametry fizyczne: a) możliwość montażu w stelażu/szafie 19” b) wysokość maksymalna 1U c) głębokość nie większa niż 41 cm d) minimum dwa wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Każde urządzenie musi zostać dostarczone z 2 zasilaczami umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap) e) minimum dwa wymienne moduły wentylatorów f) zakres temperatur pracy ciągłej co najmniej od -5°C do +45 °C g) zakres wilgotności pracy co najmniej 5% - 95% h) waga bez zainstalowanych modułów zasilania nie większa niż 7,1 kg i) minimum 1 port USB

3.	Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie: ● 48 portów 10/100/1000BASE-T PoE++ ● 16 portów 10/100/1000/2500/5000/10000BASE-T PoE++ ● 4 porty 1/10/25GE SFP28 z obsługą modułów 25G-SR, 25G-LR, 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC Budżet PoE minimum 1600W Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
4.	Przełącznik musi mieć możliwość rozbudowy o dodatkowe minimum dwa porty 40G QSFP28 lub minimum cztery porty 25G SFP28
5.	Przełącznik musi posiadać następujące porty służące do zarządzania: ● Port konsoli ze złączem RJ45 ● Port out-of-band RJ45 1000Base-T
6.	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) Zarządzanie stosem poprzez jeden adres IP b) Do min. 9 jednostek w stosie c) Porty do stackowania mogą być współdzielone z portami typu uplink. d) Magistrala stackująca o wydajności minimum 160Gb/s e) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation) f) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree g) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
7.	Układ przełączający o wydajności min. 980 Gbps, wydajność przełączania przynajmniej 655 Mpps
8.	Obsługa min. 320 000 adresów MAC
9.	Wbudowana pamięć RAM min. 2GB. Minimalne taktowanie procesora 1000MHz Bufor pakietów minimum: 4MB
10.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 8GB
11.	Obsługa min. 4092 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
12.	Możliwość skonfigurowania min. 4092 interfejsów vlan interface SVI działających równocześnie
13.	Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad
14.	Obsługa minimum 250 grup LAG
15.	Obsługa ramek jumbo o wielkości min. 13000 bajtów
16.	Obsługa protokołu BFD oraz LACP
17.	Obsługa sFlow
18.	Wsparcie dla G.8032 ERPS
19.	Obsługa protokołu VRRP IPv4 i VRRP IPv6
20.	Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP), 802.1ag, 802.3ah, 802.3ad
21.	Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
22.	Obsługa min. 80 000 tras dla routingu IPv4
23.	Obsługa min. 32 000 tras dla routingu IPv6 Obsługa min. 30 000 IPv6 neighbor discovery (ND)
24.	Obsługa protokołów związanych z obsługą ruchu typu multicast: a) IGMP v3 b) IGMP Snooping v3 c) PIM-SM, PIM-SSM i PIM-DM d) MLDv2 e) MSDP i MLD Snooping f) Multicast VLAN i Multicast VPN g) minimum 7000 tras multicast dla IPv4 i minimum 7000 tras multicast dla IPv6
25.	Minimalny rozmiar tablicy ARP 64 000 wpisów

26.	Obsługa protokołów LLDP i LLDP-MED
27.	Przełącznik musi posiadać funkcjonalność DHCP Serwer, DHCP Snooping, DHCP relay, DHCP klient, DHCPv6 Serwer, DHCPv6 Snooping, DHCPv6 relay, DHCPv6 klient
28.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) min. 3 poziomy dostępu administracyjnego poprzez konsolę b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz przypisania listy ACL c) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC d) obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1700 reguł ACL e) zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2 f) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP g) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, IPv6 RA Guard h) możliwość synchronizacji czasu zgodnie z NTP lub SNTP
29.	Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: ● klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP ● wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ
30.	Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA). Obsługa mechanizmu SPAN i RSPAN
31.	Wymagane opcje zarządzania: a) możliwość lokalnej obserwacji ruchu na określonym porcie b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC) c) wsparcie dla skyptów python uruchamianych na urządzeniu d) wsparcie dla RMON e) dedykowany port konsoli, zgodny ze standardem RS-232 f) dedykowany port zarządzający out-of-band Ethernet Base-T
32.	Wraz z urządzeniami muszą zostać dostarczone: a) pełna dokumentacja w języku polskim lub angielskim b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana
33.	Wsparcie dla funkcjonalności MACsec 802.1ae. Funkcjonalność musi być dostępna na wszystkich portach uplink i downlink. Jeżeli obsługa funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający wymaga jej dostarczenia.
34.	Wsparcie dla funkcjonalności VXLAN L2 i L3 oraz EVPN. Jeżeli obsługa funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający wymaga jej dostarczenia.
35.	Wsparcie dla technologii MPLS L2 i L3 VPN. Jeżeli funkcjonalność MPLS wymaga licencji to należy ją dostarczyć w ramach niniejszego postępowania
36.	Wsparcie dla funkcjonalności MP-BGP
37.	Wsparcie dla technologii Segment Routing
38.	Wsparcie dla funkcjonalności M-LAG lub MC-LAG
39.	Wsparcie dla funkcjonalności PFC, ECN, OpenFlow (minimum 1.3), NETCONF
40.	Wsparcie dla funkcjonalności telemetry: gRPC
41.	Wsparcie dla funkcjonalności tuneli GRE
42.	Wsparcie dla funkcjonalności aktualizacji programowania: ISSU
43.	Zgodność urządzenia ze standardem 802.3az
44.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
45.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.

46.	Zamawiający wymaga, aby urządzenia posiadały **min 3-letni serwis gwarancyjny** świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Wymiana uszkodzonego elementu w trybie 9x5 następnego dnia roboczego wysyłka. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki). W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.
47.	Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń.

1.2.2. Zakup punktów dostępowych WiFi – 4 szt.

Łącznie przewiduje się 4 punkty dostępowe: 3 szt. dla obszaru IT oraz 1 szt. dla kontrolowanego zakresu OT. W projekcie logicznym należy wydzielić co najmniej odrębne SSID/VLAN dla sieci administracyjnej/biurowej oraz dla kontrolowanej komunikacji technicznej OT. Dostęp do OT z WLAN nie może omijać NAC/RADIUS ani polityk UTM/NGFW.

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja, integracja i uruchomienie jednego kompletnego systemu zarządzanej sieci bezprzewodowej Wi-Fi 6, obejmującego łącznie 4 punkty dostępowe. System ma zapewniać bezpieczny dostęp użytkowników i urządzeń do wydzielonych zasobów IT oraz – wyłącznie w uzasadnionym i kontrolowanym zakresie – do wydzielonych stref OT/ICS, z zachowaniem segmentacji ruchu, centralnego zarządzania, uwierzytelniania w standardzie 802.1X i szyfrowania WPA3-Enterprise.

Lp.	**parametr**	**Wymagania minimalne**
1	Typ urządzenia	Wewnętrzny, sufitowy lub ścienny punkt dostępowy klasy enterprise, przeznaczony do pracy ciągłej i centralnego zarządzania.
2	Standard sieci bezprzewodowej	Obsługa IEEE 802.11ax (Wi-Fi 6) oraz zgodność wsteczna co najmniej z IEEE 802.11a/b/g/n/ac.
3	Pasma radiowe	Obsługa pasm 2,4 GHz i 5 GHz, z co najmniej dwoma niezależnymi torami radiowymi.
4	Klasa wydajności	Klasa co najmniej AX1800; maksymalna teoretyczna szybkość warstwy radiowej nie mniejsza niż 574 Mb/s w paśmie 2,4 GHz oraz 1200 Mb/s w paśmie 5 GHz.
5	MIMO	Co najmniej 2x2 MIMO / 2 tory nadawczo-odbiorcze dla każdego pasma.
6	Anteny	Wbudowane anteny dookólne o zysku nie mniejszym niż 5 dBi; urządzenie bez konieczności stosowania zewnętrznych anten w typowej instalacji wewnętrznej.
7	Porty przewodowe	Co najmniej 2 porty Ethernet 10/100/1000 Mb/s.
8	Zasilanie	Zasilanie przez PoE zgodne co najmniej z IEEE 802.3af/at; dopuszcza się dodatkowe wejście zasilania DC.
9	PoE-out	Co najmniej jeden port z możliwością przekazania zasilania PoE do dodatkowego urządzenia lub funkcja równoważna – wymaganie może być realizowane zgodnie z architekturą producenta.
10	Procesor	Procesor co najmniej czterordzeniowy klasy ARM 64-bit, o taktowaniu maksymalnym nie mniejszym niż 1,8 GHz, lub rozwiązanie zapewniające równoważną wydajność funkcjonalną.
11	Pamięć	Co najmniej 1 GB RAM oraz 128 MB pamięci nieulotnej.
12	System operacyjny	Wbudowany, licencjonowany system operacyjny producenta, umożliwiający lokalne i centralne zarządzanie, aktualizację oraz wykonywanie kopii konfiguracji.
13	Chłodzenie	Pasywne, bez wentylatorów.
14	Warunki pracy	Temperatura pracy co najmniej od -20°C do +55°C; urządzenie referencyjne dopuszcza szerszy zakres
15	Klasa wydajności	Klasa co najmniej AX1800; maksymalna teoretyczna szybkość warstwy radiowej nie mniejsza niż 574 Mb/s w paśmie 2,4 GHz oraz 1200 Mb/s w paśmie 5 GHz.

16	MIMO	Co najmniej 2x2 MIMO / 2 tory nadawczo-odbiorcze dla każdego pasma.
17	Anteny	Wbudowane anteny dookólne o zysku nie mniejszym niż 5 dBi; urządzenie bez konieczności stosowania zewnętrznych anten w typowej instalacji wewnętrznej.
18	Porty przewodowe	Co najmniej 2 porty Ethernet 10/100/1000 Mb/s.
19	Zasilanie	Zasilanie przez PoE zgodne co najmniej z IEEE 802.3af/at; dopuszcza się dodatkowe wejście zasilania DC.
20	Gwarancja	**min. 36 miesięcy.**

1.3 Dostawa szafy rack wraz z wyposażeniem dla urządzeń zakresu bezpieczeństwa (siedziba główna)
Przedmiotem zamówienia jest dostawa nowej szafy rack do głównej wraz z kompletnym systemu monitoringu parametrów środowiskowych, przeznaczonego do nadzorowania m.in. wystąpienia zalania, zadymienia, temperatury oraz wilgotności, wraz z jednostką centralną, elementami montażowymi, komunikacją LTE oraz niezbędnym okablowaniem. Wszystkie dostarczone elementy muszą być fabrycznie nowe, wzajemnie kompatybilne oraz umożliwiać pracę jako jeden zintegrowany system. Dopuszcza się rozwiązania równoważne, spełniające co najmniej poniższe wymagania funkcjonalne i techniczne

1.3.1. Dostawa Szafy rack z akcesoriami
Przedmiotem zamówienia jest dostawa fabrycznie nowej szafy serwerowej RACK 19” o wysokości min 22U, do siedziby głównej Zamawiajacego, przeznaczonej do montażu serwerów, przełączników, urządzeń bezpieczeństwa sieciowego, zasilaczy UPS, paneli krosowych oraz pozostałych elementów infrastruktury teleinformatycznej.
Szafa musi spełniać co najmniej następujące wymagania:

- wysokość robocza: minimum 22U;
- standard montażowy: RACK 19”;
- głębokość zewnętrzna: minimum 1200 mm;
- konstrukcja stalowa, stabilna, przeznaczona do montażu urządzeń serwerowych i sieciowych;
- drzwi przednie perforowane lub przeszklone z możliwością zamknięcia na klucz;
- drzwi tylne perforowane lub pełne, zamykane na klucz;
- zdejmowane lub otwierane panele boczne, zamykane lub zabezpieczone przed nieautoryzowanym dostępem;
- regulowane profile montażowe 19” z przodu i z tyłu szafy;
- możliwość wprowadzenia okablowania od góry i od dołu szafy;
- możliwość montażu listew zasilających PDU, organizerów kabli, półek, paneli wentylacyjnych i innych akcesoriów rack;
- szafa musi zapewniać odpowiednią wentylację urządzeń zamontowanych wewnątrz;
- nośność statyczna dostosowana do montażu urządzeń serwerowych, nie mniejsza niż 600 kg;
- wyposażenie w komplet elementów montażowych niezbędnych do instalacji urządzeń, w tym śruby i nakrętki koszykowe;
- kolor czarny lub inny uzgodniony z Zamawiającym;
- szafa musi być dostarczona jako kompletne rozwiązanie gotowe do montażu i użytkowania w serwerowni Zamawiającego.
- Gwarancja: Minimum 24 miesiące, gwarancja producenta

1.3.2 Listwa zasilająca PDU do szafy 19"
Listwa, wyposażona w min. 12 gniazd z uziemieniem typu Schuko, podzielonych na 2 niezależne obwody po 6 gniazd, każdy o parametrach znamionowych 250 V AC, 50/60 Hz, 16 A. Każdy obwód wyposażony w zabezpieczenie przeciążeniowe. Obudowa wykonana z aluminium. Gniazda/wyjścia obrócone o 45°, ułatwiające podłączanie urządzeń. Listwa wyposażona w 2 przewody zasilające o długości min. 2 m, o przekroju min. 3 × 1,5 mm², zakończone wtykami z uziemieniem. Instalacja pionowa w szafie 19", wraz z kompletem niezbędnych uchwytów montażowych

1.4 Wdrożenie mechanizmów RADIUS, VPN, segmentacji IT/OT oraz kontroli dostępu do sieci

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. wdrożenie odrębnego systemu kontroli dostępu do sieci klasy NAC;
5. integrację systemu NAC z usługami katalogowymi, urządzeniami sieciowymi, punktami dostępowymi, UTM/NGFW oraz systemem centralnego logowania.
   Rozwiązanie powinno zostać wdrożone z uwzględnieniem podziału na strefy bezpieczeństwa, lokalizacje, typy użytkowników, typy urządzeń, role administracyjne oraz wymagania środowiska IT i OT/ICS.

1.4.1 Wdrożenie Centralnego uwierzytelnianie RADIUS - Centralne uwierzytelnianie powinno być realizowane przez serwer RADIUS stanowiący integralny element systemu NAC albo przez odrębny komponent dostarczony w ramach tego samego rozwiązania.
Nie dopuszcza się sytuacji, w której system NAC i serwer RADIUS funkcjonują jako niespójne, niezależnie zarządzane rozwiązania, chyba że Wykonawca zapewni ich pełną integrację i jednolite zarządzanie politykami dostępu.
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. przekazywanie logów do centralnego systemu gromadzenia i analizy zdarzeń

1.4.2. Bezpieczny dostęp zdalny VPN - Wykonawca zobowiązany jest skonfigurować bezpieczny dostęp VPN dla użytkowników, administratorów, personelu technicznego oraz podmiotów serwisowych.
System VPN powinien zostać zintegrowany z:

1. Active Directory;
2. centralnym serwerem RADIUS;
3. mechanizmem uwierzytelniania wieloskładnikowego;
4. systemem centralnego logowania;
5. politykami dostępu wynikającymi z roli użytkownika.
   Należy wydzielić odrębne profile dostępu dla:

1. użytkowników zdalnych;
2. administratorów IT;
3. administratorów OT;
4. firm serwisowych;
5. dostępu do stacji przesiadkowych;
6. innych grup wskazanych przez Zamawiającego.
   Dostęp VPN powinien być ograniczony do zasobów niezbędnych dla danej roli, a dostęp serwisowy powinien posiadać możliwość czasowego aktywowania i automatycznego wyłączenia po zakończeniu zatwierdzonego okresu.

1.4.3. Segmentacja sieci IT/OT - Wykonawca zobowiązany jest opracować i wdrożyć projekt segmentacji sieci obejmujący co najmniej:

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 analizę istniejącej adresacji, VLAN, tras, reguł firewall i przepływów komunikacyjnych, a następnie konfigurację docelowych VLAN, stref bezpieczeństwa, routingu, reguł firewall i polityk komunikacji.

    Komunikacja pomiędzy strefami powinna zostać ograniczona do niezbędnych adresów, protokołów i portów, zgodnie z zasadą minimalnych uprawnień.

1.4.4. Kontrola dostępu do sieci NAC - Zamawiający wymaga dostarczenia systemu klasy NAC (Network Access Control) wraz z wsparciem technicznym i dostępem do najnowszych wersji i poprawek **przez okres min. 12 miesięcy**. Zamawiający wymaga wdrożenia oferowanego systemu w taki sposób, aby możliwe było używanie systemu z wymaganą poniżej funkcjonalnością. W ramach wdrożenia Wykonawca musi skonfigurować wszystkie urządzenia sieciowe Zamawiającego do prawidłowej współpracy z wdrażanym systemem.
System do kontroli dostępu musi charakteryzować się następującymi cechami:

1. Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
2. System musi odsługiwać minimum 150 urządzeń klienckich (w tym gości) w trybie HA – klaster dwóch maszyn wirtualnych pracujących w trybie wysokiej dostępności (redundancja). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia
3. Musi posiadać wbudowany serwer Radius
4. Musi wspierać RADIUS VSA co najmniej niżej wymienionych producentów, w tym:
   - Cisco Systems
   - D-Link
   - Alcatel-lucent
   - AlliedTelesis
   - HPE Aruba / ProCurve
   - Huawei Networks
   - Fortinet
   - PaloAlto Networks
   - Mikrotik
   - Juniper
   - Netgear
5. System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN.
6. System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.
7. Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
8. Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych
   - Microsoft Active Directory
   - Radius
   - LDAP
   - Google Workspace
   - Azure Active Directory
   - OAuth 2
   - SAML
   - Eduroam
9. Musi obsługiwać metody profilowania (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie):
   - DHCP
   - TCP
   - MAC OUI
   - SNMP

10. Wspierać min poniższe protokoły:
    - Radius, Radius CoA, web authentication, SAML
    - EAP-FAST (EAP-MSCHAPv2, EAP-TLS)
    - PEAP (EAP-MSCHAPv2, EAP-TLS, EAP-PEAP)
    - EAP-TLS
    - 802.1X
    - NAC
    - Windows machine authentication
    - MAC Auth
    - WPA2-Enterprise
    - OCSP (Online Certificate Status Protocol)
    - SNMP (BRIDGE-MIB, Q-BRIDGE-MIB, IF-MIB, IEEE8021-PAE-MIB
11. Funkcja integracji z systemem monitorowania sieci oraz analizy zdarzeń bezpieczeństwa w celu śledzenie ewentualnych niezgodności oraz naruszeń bezpieczeństwa.(dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie)
12. Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:
    - Co najmniej ESXi 7.0
    - Co najmniej Windows 2016 i 2019 z Hyper-V
    - Co najmniej KVM on CentOS 7.7. Ubuntu 18.04, and Ubuntu 20.04
    - Co najmniej Amazon AWS (EC2)
    - Co najmniej Microsoft Azure
    - - Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (150). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.
    - System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności
13. Samodzielna rejestracja klientów gościnnych w oparciu o:
    - Adres e-mail
    - Numer telefonu (wiadomość SMS)
14. Logowanie w oparciu o portale społecznościowe (Google,Facebook,Github,LinkedIn)
15. Funkcja integracji z systemami trzecimi poprzez API
16. Wspieranie rozwiązań mobilnych poprzez skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
17. Funkcja personalizacji strony gościnnej
    - - Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.
18. System musi wspierać obsługę następujących systemów operacyjnych
    - MS Windows
    - Mac OS X
    - iOS
    - Android
    - Chromebook
    - Ubuntu
19. Umożliwienie klientowi samorejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
20. Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
21. Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID
22. Funkcja dostępu sponsorowanego opartego na rejestracji klienta oraz przesłanie odpowiedniego formularza do administratora systemu celem weryfikacji i zaakceptowania podanego żądania.

Na dostarczony system NAC należy udzielić Zamawiającemu 12 miesiące gwarancji. Gwarancja musi zapewniać dostęp do poprawek oprogramowania oraz wsparcia technicznego w trybie 24x7x365 na wszystkie elementy systemu. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta lub jego partnera. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego. Zamawiający musi mieć możliwość tworzenia zgłoszeń serwisowych na dedykowanym portalu oraz poprzez dedykowaną polskojęzyczną infiolinię zgłoszeniową.

Do oferowanego rozwiązania musi być dostępna publicznie dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu)

(nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.

1.4.5. Usługa przeprojektowania i konfiguracji sieci lokalnej – segmentacja logiczna

Zakres prac obejmuje wykonanie i realiazację kompleksowego projektu sieciowego, którego celem jest podniesienie poziomu bezpieczeństwa i uporządkowanie komunikacji wewnętrznej poprzez wdrożenie segmentacji logicznej sieci, przy jednoczesnym zachowaniu ciągłości pracy infrastruktury teleinformatycznej.:

1. Wykonanie audytu obecnej infrastruktury sieciowej LAN, w tym identyfikacja wszystkich aktywnych urządzeń, punktów dystrybucyjnych, urządzeń końcowych.
2. Zebranie danych konfiguracyjnych z przełączników i urządzeń brzegowych, w tym zrzuty konfiguracji, schematy VLANów, zidentyfikowane porty trunk/uplink, adresacja IP.
3. Opracowanie mapy logiczno-fizycznej sieci LAN, uwzględniającej aktualną topologię oraz planowane zmiany w związku z wdrożeniem segmentacji.
4. Zaprojektowanie szczegółowego planu segmentacji sieci z wykorzystaniem technologii VLAN, obejmującego:
   - rozdzielenie ruchu pomiędzy różnymi strefami funkcjonalnymi
   - przypisanie VLAN ID, zakresów adresów IP, adresów bram domyślnych oraz polityk dostępowych
5. Przygotowanie Analizy Przedwdrożeniowej (AP) i Projektu Technicznego (PT) zawierającego:
   - mapę VLANów i przypisanie do urządzeń i portów,
   - strukturę routingu między VLANami,
   - listę niezbędnych zmian fizycznych i logicznych,
   - wytyczne do konfiguracji firewalli oraz przełączników
6. Przekazanie AP oraz PT do zatwierdzenia przez Zamawiającego. W przypadku konieczności Zamawiający zgłasza konieczności wyjaśnienia oraz uzupełnienia dokumentacji. Wykonawca w przeciągu trzech dni dostarczy poprawioną dokumentację bądź udzieli wyjaśnień. Warunkiem przystąpienia do dalszych prac jest akceptacja AP i PT przez Zamawiającego.
7. Rekonfiguracja przełączników warstwy 2:
   - przypisanie portów do odpowiednich VLANów (access i trunk),
   - konfiguracja Spanning Tree, loop protection, SNMP, DHCP snooping,
   - wykonanie aktualizacja firmware,
   - integracja z systemem NAC w celu dynamicznej zmiany vlanów oraz utworzenie polityk ACL,
   - dokładny opis portów na przełącznikach.
8. Konfiguracja przełączników warstwy 3:
   - utworzenie interfejsów vlan i nadanie adresów IP,
   - konfiguracja routingu pomiędzy podsieciami,
   - konfiguracja statycznych wpisów w tablicy routingu,
   - utworzenie polityk ACL,
   - konfiguracja IPHELPER.
9. Konfiguracja dynamicznego routingu pomiędzy przełącznikiem CORE pracującym w warstwie L3, a urządzeniem UTM w oparciu o OSPF.
10. Utworzenie puli dynamicznej dla każdej adresacji na serwerze DHCP.
11. Indywidualne podejście do urządzeń końcowych podczas zmian adresów IP.
12. Test komunikacji między VLANami zgodnie z założonymi regułami – zapewnienie separacji tam, gdzie wymagane, oraz dostępności usług zgodnie z wymaganiami Zamawiającego.
13. Weryfikacja polityk bezpieczeństwa na firewallu – kontrola aplikacji, inspekcja pakietów, segmentacja stref, polityki DPI/AV/IPS/Content Filter.
14. Opracowanie pełnej dokumentacji powdrożeniowej:
   - aktualne konfiguracje urządzeń (firewalle i przełączniki),
   - końcowa mapa sieci VLAN,
   - zestawienie adresacji, rezerwacji DHCP i przypisań portów,
   - dokumentacja dostępów administracyjnych
15. Przeprowadzenie szkolenia technicznego (transfer wiedzy) dla administratorów Zamawiającego w zakresie:
   - zarządzania VLANami na przełącznikach,
   - administracji firewallami,

- modyfikacji reguł międzysegmentowych,
- diagnozy problemów sieciowych.

16. Całość konfiguracji i wdrożenia musi być zgodna z dobrymi praktykami producentów sprzętu używanego przez Zamawiającego, w tym szczególnie w zakresie wysokiej dostępności, separacji stref, monitorowania i audytowalności konfiguracji.
17. Transfer wiedzy w tym szkolenia /instruktarze szkolenia dla administratorów Zamawiającego z wdrożonego rozwiązania. Szkolenia /instruktarze prowadzone będą **dla 2 osób** w dwóch turach . Ilość godzinowa oraz forma szkolenia (on-line/ stacjonarnie) zostanie ustalona wspólnie przez Zamawiającego i Wykonawcę . Zamawiający zastrzega wymóg przeprowadzenia co najmniej 16 godzin szkolenia/instruktażu na jedną turę osób oddzielnie dla zadania 4
18. Dokumentacja Powdrożeniowa (DP) : DP zawierać musi opis wdrożonych rozwiązań oraz instrukcje konfiguracji wdrożonych rozwiązań do wykorzystania przez administratorów Zamawiającego.
19. Zamawiający wymaga od Wykonawcy minimum 12 miesięcy wsparcia technicznego dla wdrożonych konfiguracji i komponentów programowych, o ile dla konkretnego urządzenia lub licencji OPZ nie określa dłuższego okresu..
    - bieżące wsparcie w zakresie utrzymania poprawnej konfiguracji segmentacji sieci,
    - nadzór nad integralnością reguł routingu i polityk bezpieczeństwa pomiędzy segmentami sieci,
    - konsultacje techniczne i rekomendacje dotyczące optymalizacji segmentacji sieci,
    - interwencje serwisowe w przypadku błędów lub incydentów związanych z konfiguracją VLAN,
    - przygotowywanie dokumentacji powdrożeniowej i aktualizacja schematów logicznych sieci w przypadku modyfikacji zapewnienie systemu zgłoszeniowego (np. w formie portalu serwisowego lub dedykowanego adresu e-mail) umożliwiającego rejestrowanie zgłoszeń serwisowych

2. Pakiet zarządzania podatnościami i testów bezpieczeństwa IT/OT

Pakiet obejmuje wdrożenie zintegrowanego procesu identyfikacji, oceny, priorytetyzacji i ponownej weryfikacji podatności środowiska IT oraz uzgodnionego zakresu OT/ICS. Proces będzie realizowany za pomocą systemu skanowania podatności, mechanizmu zarządzania cyklem życia podatności, lokalnej platformy BAS/AEV wykorzystywanej do bezpiecznej walidacji wdrożonych zabezpieczeń oraz usług testów bezpieczeństwa. Nie wymaga się dostawy odrębnej komercyjnej platformy CTI; systemy mogą korzystać z danych MITRE ATT&CK, CVE oraz zewnętrznych źródeł informacji o zagrożeniach.

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

System do skanowania podatności i zarządzania bezpieczeństwem systemów teleinformatycznych

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).

2.2. 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:

2.3. System automatycznej walidacji zabezpieczeń BAS/AEV – 1 kpl.

Przedmiotem zamówienia jest instalacja, konfiguracja i wdrożenie lokalnego systemu służącego do kontrolowanej walidacji skuteczności wdrożonych mechanizmów cyberbezpieczeństwa poprzez wykonywanie bezpiecznych scenariuszy testowych odwzorowujących wybrane techniki MITRE ATT&CK.
System powinien umożliwiać co najmniej:

- tworzenie i wykonywanie scenariuszy testowych;
- mapowanie testów do MITRE ATT&CK;
- wykonywanie testów atomowych lub sekwencji testowych;
- harmonogramowanie testów;
- sprawdzanie reakcji EDR/XDR, SIEM, firewalli i innych wdrożonych mechanizmów bezpieczeństwa;
- prezentację wyników testów;
- ocenę pokrycia mechanizmami detekcji i prewencji;
- raportowanie wykrytych luk;
- działanie on-premise;
- integrację poprzez REST API, Syslog lub inne otwarte mechanizmy;
- wdrożenie w środowisku wirtualnym lub kontenerowym Zamawiającego**.**
- System może korzystać z zewnętrznych lub lokalnych źródeł informacji o zagrożeniach oraz danych MITRE ATT&CK. Integracja z platformą CTI jest dopuszczalna, ale nie stanowi wymagania minimalnego i nie może generować dodatkowego obowiązkowego kosztu licencyjnego po stronie Zamawiającego.

2.4. usługa testów bezpieczeństwa IT/OT

1. Przedmiot i cel usługi

Przedmiotem usługi jest przeprowadzenie testów bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego, obejmujących środowisko IT oraz uzgodniony zakres środowiska OT wykorzystywanego do realizacji procesów związanych ze zbiorowym zaopatrzeniem w wodę lub odprowadzaniem ścieków.
Celem testów jest:

a. weryfikacja bezpieczeństwa infrastruktury po zakończeniu wdrożenia;
b. identyfikacja podatności, błędów konfiguracji i nadmiernej ekspozycji zasobów;
c. ocena skuteczności zastosowanej segmentacji, kontroli dostępu i zabezpieczeń komunikacji;
d. wskazanie działań naprawczych ograniczających zidentyfikowane ryzyka.

Usługa powinna uwzględniać wymagania ustawy o krajowym systemie cyberbezpieczeństwa oraz specyfikę i krytyczność procesów realizowanych przez Zamawiającego.

2. Termin realizacji

Testy zostaną przeprowadzone po zakończeniu dostawy, konfiguracji i uruchomieniu rozwiązań objętych zamówieniem, nie później niż w terminie 30 dni kalendarzowych od dnia zgłoszenia przez Zamawiającego gotowości środowiska do rozpoczęcia testów.
Szczegółowy termin, zakres oraz harmonogram testów zostaną uzgodnione z Zamawiającym przed rozpoczęciem prac.

3. Zakres testów środowiska IT

Testy środowiska IT powinny obejmować co najmniej:

a. ocenę zasobów i usług dostępnych z sieci Internet;
b. identyfikację podatności systemów, serwerów, stacji roboczych i urządzeń sieciowych;
c. weryfikację konfiguracji urządzeń bezpieczeństwa, sieci LAN, WLAN, VPN i dostępu zdalnego;
d. ocenę segmentacji sieci i możliwości nieuprawnionego dostępu pomiędzy jej wydzielonymi obszarami;
e. weryfikację podstawowych ustawień bezpieczeństwa systemów operacyjnych, usług katalogowych i kont uprzywilejowanych;
f. sprawdzenie występowania zbędnych usług, nieaktualnego oprogramowania, domyślnych ustawień oraz nadmiernych uprawnień;

g. ręczne potwierdzenie istotnych podatności wskazanych przez narzędzia skanujące.

Samo przekazanie automatycznego raportu ze skanera podatności, bez analizy i weryfikacji wyników przez Wykonawcę, nie będzie uznane za wykonanie usługi.

4. Zakres testów środowiska OT

Ze względu na wrażliwość systemów sterowania i konieczność zachowania ciągłości procesów technologicznych testy środowiska OT powinny obejmować przede wszystkim:

1. analizę architektury i sposobu połączenia środowisk IT i OT;
    a. ocenę segmentacji sieci OT oraz zabezpieczenia komunikacji pomiędzy poszczególnymi strefami;
    b. weryfikację konfiguracji urządzeń pośredniczących w komunikacji, w szczególności firewalli, routerów, przełączników, bram komunikacyjnych i rozwiązań dostępu zdalnego;
    c. ocenę ekspozycji systemów SCADA, stacji operatorskich, stacji inżynierskich, serwerów OT i systemów telemetrycznych;
    d. identyfikację znanych podatności na podstawie wersji oprogramowania, oprogramowania układowego i dostępnej dokumentacji;
    e. ocenę zabezpieczenia dostępu administracyjnego i serwisowego do środowiska OT;
    f. ocenę możliwości nieuprawnionego przejścia z sieci IT do sieci OT.

W odniesieniu do sterowników PLC, RTU, urządzeń pomiarowych, wykonawczych i innych elementów bezpośrednio uczestniczących w sterowaniu procesem technologicznym należy stosować przede wszystkim metody pasywne, analizę konfiguracji, dokumentacji i ruchu sieciowego.

Aktywne skanowanie lub próby wykorzystania podatności wobec tych urządzeń mogą być wykonane wyłącznie po uzyskaniu pisemnej zgody Zamawiającego, na podstawie odrębnie uzgodnionego zakresu i po potwierdzeniu, że test nie stwarza zagrożenia dla ciągłości procesu technologicznego.

5. Warunki i zasady prowadzenia testów

Przed rozpoczęciem prac Wykonawca przedstawi Zamawiającemu uproszczony plan testów zawierający:

a. wykaz systemów i obszarów objętych testami;
b. rodzaj planowanych czynności;
c. harmonogram i wymagane okna serwisowe;
d. zasady komunikacji i zgłaszania zagrożeń;
e. warunki przerwania testów.

Testy muszą być prowadzone w sposób kontrolowany, z zachowaniem poufności informacji oraz z minimalnym wpływem na dostępność systemów i procesów Zamawiającego.

Bez pisemnej zgody Zamawiającego niedopuszczalne jest:

a. prowadzenie testów typu DoS lub DDoS;
b. wyłączanie urządzeń, usług lub systemów;
c. dokonywanie zmian w konfiguracji produkcyjnej;
d. usuwanie albo modyfikowanie danych;
e. prowadzenie testów mogących spowodować zatrzymanie lub zakłócenie procesu technologicznego;
f. wykonywanie ataków siłowych powodujących blokowanie kont;
g. przekazywanie danych lub wyników testów do nieuzgodnionych usług zewnętrznych.

Przed rozpoczęciem testów aktywnych Zamawiający potwierdzi dostępność aktualnych kopii zapasowych lub konfiguracji umożliwiających odtworzenie badanych systemów.

Testy należy przerwać, jeżeli wystąpi ryzyko:

a. utraty albo uszkodzenia danych;
b. uszkodzenia urządzenia lub systemu;
c. ograniczenia dostępności usług;
d. zakłócenia procesu technologicznego;
e. wystąpienia incydentu bezpieczeństwa.

W przypadku wykrycia podatności krytycznej lub bezpośredniego zagrożenia dla ciągłości działania Wykonawca niezwłocznie poinformuje Zamawiającego, bez oczekiwania na sporządzenie raportu końcowego.

6. Raport z testów

W terminie do 10 dni roboczych od zakończenia testów Wykonawca przekaże Zamawiającemu raport w języku polskim, obejmujący co najmniej:

a. zakres i sposób przeprowadzenia testów;
b. wykaz zidentyfikowanych podatności i nieprawidłowości;

c. ocenę poziomu ryzyka z uwzględnieniem znaczenia badanego zasobu;
d. wskazanie podatności krytycznych, wysokich, średnich i niskich;
e. opis możliwego wpływu podatności na bezpieczeństwo i ciągłość działania;
f. rekomendacje techniczne i organizacyjne dotyczące usunięcia lub ograniczenia ryzyka;
g. proponowaną kolejność realizacji działań naprawczych;
h. podsumowanie przeznaczone dla kierownictwa Zamawiającego.

Wyniki automatycznych skanów powinny zostać przeanalizowane przez Wykonawcę oraz oczyszczone z wyników fałszywie dodatnich.

7. Omówienie wyników i test sprawdzający

Po przekazaniu raportu Wykonawca przeprowadzi spotkanie podsumowujące, podczas którego przedstawi wykryte nieprawidłowości oraz rekomendowany sposób ich usunięcia.
W ramach wynagrodzenia Wykonawca przeprowadzi jeden test sprawdzający dotyczący podatności oznaczonych jako krytyczne lub wysokie, po wdrożeniu przez Zamawiającego działań naprawczych.
Test sprawdzający zostanie wykonany w terminie uzgodnionym z Zamawiającym, nie później niż w ciągu 30 dni od zgłoszenia gotowości do ponownej weryfikacji.

3. Pakiet inwentaryzacji, CMDB, ITSM, monitoringu i zarządzania zmianą

3.1. Oprogramowanie klasy ITSM

Wymagania ogólne dla centralnego systemu zarządzania komputerami

Oprogramowanie musi posiadać polski oraz angielski interfejs językowy.
Oprogramowanie musi posiadać architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji, Agenta/Konsoli zarządzającej.
Oprogramowanie musi umożliwiać obsługę dedykowanych kluczy szyfrujących podczas komunikacji pomiędzy agentami, serwer aplikacji i konsolą zarządzającą.
Odczyt informacji dotyczących parametrów sprzętowych komputera musi odbywać się za pośrednictwem agenta systemu instalowanego na komputerach użytkowników.
Agent systemu nie może nasłuchiwać na żadnym porcie sieciowym po stronie stanowiska komputerowego użytkownika.
Oprogramowanie musi umożliwiać wybór instalacji agenta w trybie standardowym oraz bezpiecznym tj. braku wkompilowanych funkcji takich jak zdalne zarządzanie, transfer plików, zdalny pulpit.
Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji kont operatorów w konsoli zarządzającej poprzez fizyczne zabezpieczenie sprzętowe (lokalne lub sieciowe) wraz z hasłem, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej musi umożliwiać integrację z kontami Active Directory. Wymagane zabezpieczenie sprzętowe musi posiadać mechanizm szyfrowania danych AES w obrębie przechowywania danych wrażliwych.
Oprogramowanie musi posiadać dodatkową autoryzację użytkownika konsoli zarządzającej za pomocą usługi Google Authenticator oraz Microsoft Authenticator.
Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do poszczególnych funkcjonalności systemu dla operatorów konsoli zarządzającej zgodny z modelem RBAC (Role Based Access Control).
Oprogramowanie musi umożliwiać nadawanie oraz odbieranie uprawnień w czasie rzeczywistym (brak konieczności przelogowania użytkownika konsoli systemu).
Oprogramowanie musi umożliwiać blokadę wybranych uprawnień konkretnego użytkownika niezależnie od uprawnień wynikających z przypisanych ról.
Oprogramowanie musi współpracować z serwerem MSSQL Server od wersji 2017
Oprogramowanie, w zakresie wszystkich warstw, nie może wymagać do prawidłowej pracy komponentów Java.
Oprogramowanie serwera aplikacji musi posiadać funkcjonalność centralnego wysyłania wybranych powiadomień mailowych.
Oprogramowanie musi posiadać moduł zarządzania uprawnieniami do danych w zakresie wybranych jednostek organizacyjnych oraz typów zasobów poszczególnych użytkowników konsoli. Wszelkie raporty, zestawienia oraz funkcje obejmują wtedy tylko wynikowe obiekty.
Oprogramowanie musi być podpisane cyfrowo przez Producenta ważnym certyfikatem, z prawidłową ścieżką certyfikacji, w której główny urząd certyfikacji (Root CA) jest uczestnikiem programu certyfikatów głównych

systemu Windows. Podpis cyfrowy dotyczy składników Producenta systemu w zakresie plików wykonywalnych (*.exe), plików bibliotek współdzielonych (*.dll), plików sterowników (*.sys) oraz pakietów instalacyjnych oprogramowania (*.msi).
Oprogramowanie agentów musi posiadać obsługę sesji terminalowych Windows.
Oprogramowanie musi zapewniać dowolną konfigurację pracy wszystkich agentów, jednostek organizacyjnych, pojedynczego agenta, poprzez dziedziczenie definiowanych przez administratora parametrów. Zmiany konfiguracji agentów następują w trybie natychmiastowym (online).
Oprogramowanie musi posiadać raport przedstawiający różnice w konfiguracji poszczególnych agentów w stosunku do konfiguracji globalnej.
Oprogramowanie musi posiadać mechanizm logowania zmian w konfiguracji agentów przez użytkowników konsoli (data, czas, login, poprzednia i nowa wartość).
Oprogramowanie musi posiadać mechanizm analizy czasu pracy komputera, informujący użytkownika (alert oraz wymuszone działanie – restart) o przekroczeniu zadanego czasu pracy bez restartu systemu operacyjnego.
Oprogramowanie musi zapewniać automatyczny import drzewiastej struktury organizacyjnej zamawiającego (bez ograniczeń ilości zagnieżdżeń z kontenera Active Directory/OpenLDAP), kont użytkowników i komputerów z zachowaniem ich oryginalnego położenia wg. OU.
Oprogramowanie musi zapewniać w obrębie synchronizacji z Active Directory/OpenLDAP tworzenie listy filtrów zawężających węzły danych wraz z możliwością wskazania docelowej gałęzi struktury organizacyjnej lub lokalizacyjnej Zamawiającego.
Oprogramowanie musi posiadać kreator powiązań (mapowanie atrybutów) dowolnych atrybutów obiektów z usługi katalogowej do wskazanych atrybutów zasobów systemowych.
Oprogramowanie musi umożliwiać współpracę z nieograniczoną ilością kontrolerów domen z zachowaniem podległej struktury drzewiastej.
Oprogramowanie musi umożliwiać automatyczny import informacji dotyczących przynależności użytkowników oraz stanowisk komputerowych do grup struktury katalogowej.
Oprogramowanie musi posiadać raport przedstawiający informacje nt. grup struktury katalogowej wraz przynależącymi do nich użytkownikami.
Oprogramowanie musi umożliwiać tworzenie dynamicznych grup stanowisk w oparciu o kreator zawierający filtry (AND, OR) w zakresie min. wersja OS, nazwa oraz wersja wybranej aplikacji, RAM, CPU, HDD, jednostka organizacyjna, jednostka lokalizacyjna, architektura (x32, x64), zainstalowane oprogramowanie, wersja oprogramowania, lista usług systemowych, producent oraz model komputera, poziom uprawnień użytkownika, zainstalowana usługa systemowa, ostatnie uruchomienie systemu, obecność pliku EXE na dysku, predefiniowane atrybuty komputera (np. dostawca, numer faktury, data zakupu).
Oprogramowanie musi umożliwiać prezentację widoku zarządzanych stanowisk komputerowych w postaci listy stanowisk, drzewiastej struktury wg jednostek organizacyjnych, jednostek lokalizacyjnych, struktury Active Directory, struktury sieciowej (pule IP) oraz grup dynamicznych.
Oprogramowanie musi umożliwiać dynamiczne zawężanie wyników wyszukiwania ww. widoków na podstawie prezentowanych w nich atrybutów.
Oprogramowanie musi umożliwiać graficzną prezentację aktualnego stanu aktywności agenta (online/offline) z dokładnością do 1 minuty.
Oprogramowanie musi umożliwiać zapisywanie w bazie danych informacji o uruchomieniu i wyłączeniu komputera oraz zalogowaniu i wylogowaniu użytkownika.

Inwentaryzacja konfiguracji komputerów

Oprogramowanie musi umożliwiać wydruk kartoteki sprzętowej stanowiska komputerowego.
Oprogramowanie musi umożliwiać samodzielną edycję wyglądu kartoteki sprzętowej, protokołów przekazania oraz zwrotu zasobów za pomocą graficznego kreatora wyglądu.
Oprogramowanie musi umożliwiać zapisywanie edytowanych szablonów (min. kartoteka sprzętowa, protokoły przekazania/zwrotu zasobów) w kontekście zalogowanego operatora konsoli zarządzającej.
Oprogramowanie musi umożliwiać projektowanie, generowanie oraz wydruk etykiet inwentaryzacyjnych w zakresie: model, nr inwentaryzacyjny, data zakupu, jednostka, wraz z obsługą kodów kreskowych w standardzie EAN128 oraz PDF417

Oprogramowanie musi umożliwiać okresową automatyczną inwentaryzację parametrów sprzętowych stanowiska: HDD, RAM, CPU, karta sieciowa, system operacyjny, karta graficzna itp.
Oprogramowanie Agenta musi umożliwiać audyt off-line, poprzez uruchomienie skanera (z GUI) bez konieczności instalacji, oraz zapis wyników do pliku w postaci zaszyfrowanej.
Oprogramowanie musi umożliwiać analizę sprzętową: - płyty głównej w zakresie model, producent, nr. seryjny, - CPU w zakresie nazwy, modelu, producenta, częstotliwości, - HDD w zakresie numeru seryjnego dysku, numeru seryjnego partycji, rozmiaru pamięci, - RAM w zakresie wielkości pamięci, - karty sieciowej w zakresie model, adres IP, adres MAC, - karty graficznej w zakresie model.
Oprogramowanie musi umożliwiać odczyt informacji dotyczących systemu operacyjnego w zakresie nazwy, wersji, daty instalacji, zainstalowanych poprawek, dostępnych kluczy licencyjnych, produkt ID.
Oprogramowanie musi umożliwiać odczyt informacji sieciowych w zakresie adresu IO, adresu MAC, nazwy sieciowej.
Oprogramowanie musi umożliwiać odczyt informacji sprzętowych z BIOS w zakresie nazwy BIOS, daty, producenta.
Oprogramowanie musi umożliwiać przegląd historii zmian parametrów sprzętowych komputerowych.
Oprogramowanie musi umożliwiać globalny przegląd stanowisk komputerowych pod względem parametrów sprzętowo-systemowych.
Oprogramowanie musi zawierać raport stanowisk komputerowych posiadających co najmniej jedno konto z uprawnieniami administratora.
Oprogramowanie musi umożliwiać odczyt urządzeń podłączonych do stanowiska komputerowego przez interfejs USB, z możliwością odczytania nazwy urządzenia, producenta, modelu oraz numeru seryjnego (o ile urządzenie dostarcza ww. informacji)
Oprogramowanie musi umożliwiać globalną analizę urządzeń podłączonych do stanowisk komputerowych przez interfejs USB
Oprogramowanie musi umożliwiać integrację z zewnętrzną usługą Dell API w celu automatycznego odczytania informacji na temat okresu gwarancji stanowiska komputerowego na podstawie odczytanego przez agenta identyfikatora (ServiceTag)
Oprogramowanie musi umożliwiać okresowe próbkowanie obciążenia procesora oraz zajętości pamięci RAM z możliwością zapisu odczytanych wyników do bazy w celu późniejszej analizy (historia obciążenia komputera).

Inwentaryzacja oprogramowania

Oprogramowanie musi umożliwiać automatyczną inwentaryzację zainstalowanego na komputerach oprogramowania.
Oprogramowanie musi umożliwiać globalny przegląd wszystkich programów zainstalowanych na komputerach.
Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych typów programów (freeware, shareware itp.).
Oprogramowanie musi umożliwiać tworzenie wykazów z zainstalowanym, dowolnie wybranym programem.
Oprogramowanie musi umożliwiać tworzenie zestawień zainstalowanych systemów operacyjnych na komputerach.
Oprogramowanie musi umożliwiać tworzenie wykazów stanowisk z brakiem zainstalowanego, dowolnie wybranego, programu.
Oprogramowanie musi posiadać wbudowany mechanizm umożliwiający, poprzez GUI konsoli, zdalną grupową dezinstalację oprogramowania np. pakietów MS Office.
Oprogramowanie musi umożliwiać oznaczanie kolorem aplikacji zabronionych oraz zgodnych ze standardem wraz z możliwością raportowania wg w/w klasyfikacji.
Oprogramowanie musi umożliwiać zablokowanie na stacji roboczej wybranych procesów celem uniemożliwienia ich uruchomienia przez użytkownika.
Oprogramowanie musi posiadać globalne zestawienie pozwalające na zdalne usunięcie nielegalnych danych np. plików AVI, MP3, MP4 bez konieczności fizycznej obecności użytkownika przy stacji.

Zdalny pulpit, zdalne zarządzanie komputerem

Oprogramowanie musi umożliwiać interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy).
Oprogramowanie musi umożliwiać wybór monitora, którego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu.
Oprogramowanie musi umożliwiać zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta).
Oprogramowanie musi umożliwiać wysyłanie polecenia Wake-on LAN.
Oprogramowanie musi umożliwiać zdalną dwukierunkową linię poleceń.
Oprogramowanie musi umożliwiać przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet).
Oprogramowanie musi umożliwiać konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora.
Oprogramowanie musi umożliwiać wybór aktywnych sesji terminalowych, do których chcemy się podłączyć.
Oprogramowanie musi umożliwiać zbiorczy podgląd zdalnych pulpitów stacji.
Oprogramowanie musi posiadać zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets.
Oprogramowanie musi zapewniać zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode.
Oprogramowanie musi umożliwiać zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe
Oprogramowanie musi umożliwiać zdalne wykonywanie zapytań WQL
Oprogramowanie musi umożliwiać zdalny odczyt oraz modyfikację rejestru Windows
Oprogramowanie musi umożliwiać pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN
Oprogramowanie musi umożliwiać przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji.
Oprogramowanie musi umożliwiać prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Monitoring komputerów

Oprogramowanie umożliwia zestawienie najpopularniejszych adresów (jakie stanowiska je wywoływały, kiedy) z możliwością zapisu całego adresu lub tylko głównej strony.
Oprogramowanie umożliwia zestawienie najaktywniejszych stanowisk (pod kątem WWW), jakie adresy odwiedzały, kiedy, wszystkie zestawienia do poziomu: jednostka organizacyjna, stanowisko, zalogowany użytkownik.
Oprogramowanie umożliwia analizę uruchamianych aplikacji (aktywność stanowisk wg aplikacji oraz wykorzystanie zainstalowanych aplikacji wg stanowisk).
Oprogramowanie umożliwia analizę efektywności pracy użytkowników na poszczególnych aplikacjach
Oprogramowanie umożliwia blokadę stron www (biała i czarna lista adresów, blokada pełna lub selektywna) z możliwością automatycznego zamykania przeglądarki lub konkretnej karty przeglądarki (w przypadku wykrycia adresu zabronionego).
Oprogramowanie umożliwia tworzenie statystyk aktywności stron WWW oraz aktywności stanowisk.
Oprogramowanie umożliwia podział stron na dozwolone i zabronione.
Oprogramowanie umożliwia wydruki tabelaryczne oraz graficzne (wykresy aktywności).
Oprogramowanie umożliwia okresowe tworzenie zrzutu ekranu użytkownika z możliwością przesłania go na serwer.
Oprogramowanie umożliwia rozróżnienie stanów monitorowanego komputera w szczególności stan aktywności (focus okna), hibernacji, uśpienia oraz wylogowania
Oprogramowanie umożliwia odczyt aktywności użytkownika w czasie rzeczywistym w zakresie min. tytuł okna, adres www przeglądanej strony z dokładnością do 1 sekundy.

Oprogramowanie umożliwia analizę aktywności myszy oraz klawiatury dla poszczególnych monitorowanych aplikacji oraz stron internetowych (ilość kliknięć).
Oprogramowanie umożliwia monitorowanie wszystkich prac drukowania generowanych na urządzeniach sieciowych udostępnionych przez centralny serwer wydruków i udostępnionych lokalnie przez port TCP/IP
Oprogramowanie umożliwia monitorowanie wszystkich prac drukowania generowanych na urządzeniach lokalnych udostępnionych przez port LPT, USB. Monitorowanie tych wydruków odbywa się poprzez agenta aplikacji zainstalowanego na stacji roboczej będącej serwerem wydruków dla drukarki lokalnej.
Oprogramowanie po zainstalowaniu przesyła do serwera aplikacji następujące informacje: nazwa stacji roboczej, nazwa zainstalowanego sterownika drukarki, nazwa portu z jakiego dany sterownik korzysta, opis sterownika drukarki, format drukowanych stron oraz nazwę drukowanego dokumentu.

Backup danych użytkownika

Oprogramowanie umożliwia tworzenie dowolnej ilości automatycznych zadań w zakresie archiwizacji danych – globalnie z poziomu głównej konsoli zarządzającej.
Oprogramowanie umożliwia globalną zmianę parametrów zadań archiwizacji (ilość archiwów, kompresja, okres, zakres).
Oprogramowanie umożliwia definiowanie rozszerzeń plików, które mają być pomijane podczas procesu archiwizacji oraz rozszerzeń plików np. *.doc, które mają być archiwizowane.
Oprogramowanie Agenta umożliwia kopię całościową danych oraz przesyłanie plików z archiwizacji na wskazany serwer FTP.
Mechanizm archiwizacji danych realizowany jest przez Agenta systemu bez udziału zdalnych sesji (typu zdalny pulpit, wywoływanie skryptów)
Oprogramowanie umożliwia definiowanie cyklu archiwizacji.
Oprogramowanie umożliwia automatyczne usuwanie starszych plików kopii całościowej, definiowanie globalnego zadania archiwizacji.

Automatyzacja

Oprogramowanie musi umożliwiać zdalną instalację pakietów *.msi, plików *.cmd, *.bat, *.reg, *.ps1 poprzez utworzenie zadań dystrybucji aplikacji oraz wskazanie docelowych komputerów lub grup komputerów za pomocą dedykowanego GUI użytkownika. Zadanie dystrybucji musi umożliwiać określenie okresu aktywności, godziny rozpoczęcia oraz przedstawiać status instalacji na wybranych stanowiskach.
Oprogramowanie musi umożliwiać tworzenie zadań dystrybucji polegające na jednorazowym uruchomieniu wybranego szablonu akcji na wybranych stanowiskach komputerowych.
Oprogramowanie musi umożliwiać tworzenie polis uruchamianych cyklicznie na wybranych stanowiskach komputerowych wg aktualnej przynależności do struktury organizacyjnej, lokalizacyjnej lub wybranych grup dynamicznych.
Oprogramowanie musi umożliwiać tworzenie dystrybucji zadań oraz polis dla wybranych stanowisk komputerowych poprzez interaktywny kreator (krok po kroku). Wybór odbiorców musi uwzględniać listę stanowisk, strukturę organizacyjną, strukturę lokalizacyjną oraz dynamiczne grupy stanowisk.
Oprogramowanie musi umożliwiać globalną dystrybucję plików oraz folderów do wskazanych lokalizacji do wybranych stanowisk komputerowych wg przynależności do struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej wraz z automatycznym (polisa) odtworzeniem brakujących danych w przypadku wykrycia niespójności.
Oprogramowanie musi umożliwiać szyfrowanie plików źródłowych dla zadań instalacji.
Oprogramowanie musi umożliwiać globalny przegląd postępu wykonania wybranych zadań oraz polis wraz z odczytem standardowego wyjścia (stdout) oraz standardowego wyjścia błędów (stderr).
Oprogramowanie musi umożliwiać tworzenie własnych szablonów akcji zawierających zdefiniowaną listę akcji pozwalających na warunkowe uruchamianie akcji zależnych (oczekiwanie na zakończenie akcji, praca w tle).
Oprogramowanie musi umożliwiać konfigurację typów akcji co najmniej w zakresie: dystrybucja i uruchomienie plików wsadowego BAT, dystrybucja plików rejestru REG, dystrybucja i instalacja pakietu MSI, dystrybucja i instalacja poprawki MSP, dystrybucja i uruchomienie aplikacji EXE, dystrybucja i uruchomienie skryptu PowerShell, dystrybucja plików i folderów, uruchomienie/wyłączenie/restart usługi systemowej, zakończenie procesu systemowego, wywołanie polecenia CMD.
Oprogramowanie musi umożliwiać konfigurowanie dedykowanych parametrów dla każdej z ww. akcji.

Oprogramowanie musi umożliwiać uruchomienie na prawach administracyjnych pliku instalacyjnego EXE (z GUI) w sesji użytkownika z ograniczonymi uprawnieniami do instalacji aplikacji. Proces instalacji jest manualnie kontynuowany przez użytkownika.
Oprogramowanie musi umożliwiać ograniczenie zakresu działania zadania, polisy oraz zawężenie wszelkich raportów systemowych do stanowisk spełniających kryteria wybranej dynamicznej grupy stanowisk.
Oprogramowanie w zakresie automatyzacji musi realizować m.in. następujące przypadki użycia z wykorzystaniem mechanizmu grup dynamicznych dla zadań oraz polis: Automatyczną instalacji aplikacji na komputerach spełniających warunki: stanowiska z Windows 10 z pamięcią RAM>4GB i zainstalowaną wybraną aplikacją w wersji mniejszej (np. 7.0) Automatyczne odinstalowanie aplikacji na komputerach spełniających warunki: stanowiska z Windows 7 gdzie producentem komputera jest np. Dell i zainstalowaną wybraną aplikacją w wersji większej niż (np. 8.0) Dystrybucję plików oraz folderów (ze wskazaną zawartością np. dokumenty, skróty do aplikacji) na pulpity stanowisk komputerowych spełniających warunki: stanowiska z Windows 10 z brakiem zainstalowanej wybranej aplikacji oraz nie posiadające konta użytkownika z prawami administracyjnymi Uruchomienia wybranego skryptu PowerShell dla komputerów spełniających warunki: stanowiska z Windows 10 w architekturze 32 bitowej, zainstalowaną aplikacją X w wersji większej niż (np. 6.0) i brakiem zainstalowanej aplikacji Y. Uruchomienia wybranych szablonów akcji w przypadku wykrycia zmiany jednostki organizacyjnej stanowiska komputerowego. W przypadku wcześniej zdefiniowanych polis wymagane jest, aby zostały one automatycznie uruchomione dla nowych stanowisk komputerowych po spełnieniu warunków przynależności do określonych grup dynamicznych.
Oprogramowanie musi umożliwić instalację oprogramowania z plików exe, które nie posiadają instalacji w trybie cichym poprzez automatyzację procesu manualnej instalacji (nagrywanie makr w zakresie wyborów typu zaznaczenie checkbox, wybór pozycji z listy, kliknięcie przycisku, wpisanie parametru/ścieżki itp.)
Oprogramowanie musi posiadać repozytorium szablonów makr automatyzacji do późniejszego wykorzystania podczas procesów instalacji
Oprogramowanie musi zawierać funkcję testowania nagranych makr z poziomu interfejsu użytkownika
Oprogramowanie musi wznawiać instalację, w przypadku przerwania procesu instalacji (np. z powodu wyłączenia komputera)
Nagrywanie makr musi być realizowane przez wybranie/wskazanie elementu okna, na którym ma zostać wykonana akcja (np. kliknięcie, wprowadzenie tekstu, zaznaczenie)
Oprogramowanie musi umożliwiać wysyłanie komunikatów (Windows Notification) do wskazanych stanowisk komputerowych (wybór manualny, wg struktury organizacyjnej, lokalizacyjnej lub grupy dynamicznej)
Oprogramowanie musi umożliwiać wysyłanie komunikatów przed każdą zdefiniowaną akcją automatyzacji (np.: przed rozpoczęciem instalacji pakietu MSI, przed dystrybucją plików, przed uruchomieniem skryptu PowerShell)
Oprogramowanie musi umożliwiać automatyzację procesu konfiguracji dowolnej aplikacji Windows w celu odtworzenia zapamiętanych akcji (makr) dla wskazanych stanowisk komputerowych.

System wewnętrznego komunikatora dla użytkowników

Oprogramowanie musi zawierać wewnętrzny komunikator pracujący w sieci LAN, integrujący się z usługą katalogową w zakresie kont użytkowników (dane osobowe, avatar), jednostek organizacyjnych.
Oprogramowanie komunikatora musi umożliwiać automatyczne logowanie użytkowników pochodzących z usługi katalogowej.
Oprogramowanie komunikatora musi umożliwiać konwersację grupową oraz prywatną pomiędzy użytkownikami
Oprogramowanie komunikatora musi umożliwiać wysyłanie wiadomości powitalnych; komunikatów grupowych z raportowaniem doręczenia oraz odczytania.
Oprogramowanie komunikatora musi umożliwiać generowanie raportów doręczenia/odczytania wiadomości wymagających potwierdzenia.
Oprogramowanie komunikatora musi umożliwiać określenie maksymalnego rozmiaru transferowanego pliku (przez administratora).
Oprogramowanie komunikatora musi umożliwiać wysyłanie powiadomień e-mail o utworzeniu/modyfikacji użytkowników, którzy nie pochodzą z usługi katalogowej.
Oprogramowanie komunikatora musi umożliwiać automatyczną aktualizację wg. zadanej konfiguracji danych synchronizowanych (ze szczególnym uwzględnieniem danych o użytkownikach, jednostkach organizacyjnych z usługi katalogowej).

Oprogramowanie komunikatora musi umożliwiać archiwizację starych rozmów między użytkownikami.
Oprogramowanie komunikatora musi umożliwiać administratorowi wyłączenie globalnie możliwości zamknięcia/wylogowanie/zapisywanie poświadczeń dla klientów końcowych.
Oprogramowanie komunikatora musi umożliwiać administratorowi bezpieczeństwa wgląd do rozmów pracowników, wyłączenie wybranych funkcjonalności dla klienta końcowego (np. transferu plików, konferencji audio-video).
Oprogramowanie komunikatora musi umożliwiać wymianę plików pomiędzy zalogowanymi użytkownikami
Oprogramowanie komunikatora musi umożliwiać nawiązanie sesji audio oraz wideo pomiędzy zalogowanymi użytkownikami wraz z obsługą konferencji grupowych.

Wymagania dla oprogramowania w zakresie zarządzania procesami i usługami.

ServiceDesk – Zarządzanie zgłoszeniami

Oprogramowanie w części HelpDesk musi być oparte na zasadach ITIL w szczególności: ● Zarządzanie problemem ● Zarządzanie incydentem ● Obsługa procesów poprzez WorkFlow (wnioski o usługi, uprawnienia, zakupy) ● Zarządzanie umowami serwisowymi ● Definicje poziomów SLA (reakcja, naprawa)
Oprogramowanie musi umożliwiać zgłaszania przez użytkowników z poziomu przeglądarki WWW (dedykowany portal) awarii sprzętu, usług, oprogramowania i innych typów awarii zdefiniowanych przez administratora.
Portal ServiceDesk musi mieć możliwość obsługi przez wiodące przeglądarki WWW
Portal ServiceDesk musi umożliwiać wybór wersji językowej interfejsu (co najmniej polski i angielski).
Obsługa listy zgłoszeń serwisowych musi być realizowana przez portal ServiceDesk z zachowaniem nadanego poziomu uprawnień.
Oprogramowanie musi umożliwiać kontrolę obciążenia działu IT, optymalizację podziału pracy pomiędzy pracowników działu IT oraz przegląd awaryjności sprzętu.
Oprogramowanie musi umożliwiać uwierzytelnianie użytkowników wykorzystując bazę Active Directory poprzez protokół LDAP.
Oprogramowanie musi umożliwiać automatyczne autoryzowanie określonych stanowisk i użytkowników (z wykorzystaniem mechanizmu SSO), aby uniknąć każdorazowego uwierzytelniania przed korzystaniem z systemu zgłoszeń.
Oprogramowanie musi umożliwiać sortowanie listy zgłoszeń awarii, wg daty zgłoszenia, priorytetu, statusu.
Oprogramowanie musi umożliwiać filtrację zgłoszeń wg priorytetu oraz statusów zgłoszeń, stanowisk oraz inżynierów obsługujących zgłoszenia.
Oprogramowanie musi umożliwiać tworzenie dedykowanych list zgłoszeń z różnymi danymi, domyślnym filtrowaniem i sortowaniem.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych list zgłoszeń w zależności od zalogowanego użytkownika.
Oprogramowanie musi umożliwiać określenie widoczności zgłoszeń w zależności od kategorii i lokalizacji zgłoszeń przypisanych do zalogowanego użytkownika.
Oprogramowanie musi umożliwiać dostęp do zgłoszeń swoich podwładnych przez przełożonego.
Oprogramowanie musi umożliwiać dodawanie przez administratora nowych wpisów (komentarzy) w zgłoszeniu, jak i umożliwiać zmianę statusu sprawy. Użytkownik także ma możliwość dodawania nowych wpisów do zgłoszonego problemu wraz ze zmianą statusu.
Oprogramowanie musi umożliwiać tworzenie zadań w ramach konkretnego zgłoszenia z możliwością przekazania do realizacji przez innych użytkowników.
Oprogramowanie musi umożliwiać tworzenie globalnych zadań do realizacji przez zalogowanego użytkownika.
Oprogramowanie musi umożliwiać tworzenie szablonów zadań.
Oprogramowanie musi umożliwiać rejestrację czasu pracy poświęconego na realizację zgłoszenia przez opiekuna.

Oprogramowanie musi umożliwiać przesyłanie użytkownikom powiadomień pocztą elektroniczną o nowych wpisach i zmianach w zgłoszeniu.
Oprogramowanie musi umożliwiać edycję szablonów powiadomień email.
Oprogramowanie musi umożliwiać tworzenie wielopoziomowych list kategorii zawierających nazwę i opis kategorii.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii w zależności od zalogowanego użytkownika.
Oprogramowanie musi umożliwiać tworzenie pól dodatkowych na formularzu rejestracji zgłoszenia.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych pól dodatkowych w zależności od zalogowanego użytkownika.
Rozwiązania w bazie wiedzy muszą posiadać znacznik określający czy są dostępne dla użytkowników, czy są wewnętrznymi uwagami działu IT. Panel www użytkownika musi zawierać wyszukiwarkę tematów wg słów kluczowych oraz wewnętrznej treści.
Oprogramowanie musi umożliwiać edycję bazy wiedzy z poziomu przeglądarki WWW wraz z możliwością formatowania tekstu oraz wstawiania załączników.
Oprogramowanie musi umożliwiać administratorowi wprowadzenie do systemu zgłoszenia użytkownika, który nie ma dostępu do PC (np. telefoniczna informacja o awarii komputera).
Oprogramowanie musi umożliwiać delegowanie zgłoszenia innemu administratorowi (technikowi), jak również przejęcie innego zgłoszenia (np. w przypadku nieplanowanej nieobecności pracownika).
Oprogramowanie musi umożliwiać obsługę tzw. Linii wsparcia poprzez samodzielne tworzenie nowych linii wraz z przypisywaniem do nich dowolnej ilości kont operatorów HelpDesk. Zgłoszenie serwisowe musi mieć możliwość przekazania do dowolnej linii wsparcia lub dedykowanego operatora HelpDesk. Linia wsparcia musi mieć możliwość przypisania powiązanych z nią kategorii zgłoszeń.
Oprogramowanie musi umożliwiać informowanie pracowników o planowanych działaniach, awariach za pomocą komunikatów wprowadzanych na stronę główną panelu zgłaszania usterki, bądź do poszczególnych kategorii.
Oprogramowanie musi umożliwiać określenie widoczności komunikatów o planowanych działaniach, awariach w zależności od zalogowanego użytkownika.
Oprogramowanie musi umożliwiać tworzenia baz umów serwisowych powiązanych z bazami firm serwisowych (dostawców sprzętu, oprogramowania, lokalnych serwisów). lub z zakupionym sprzętem.
Oprogramowanie w oparciu o bazę firm/umów serwisowych musi umożliwiać zapis przekazania zgłoszenia do serwisu zewnętrznego.
Oprogramowanie musi umożliwiać przesyłanie powiadomień do firm serwisowych powiązanych ze zgłoszeniem.
Oprogramowanie musi posiadać możliwość rejestracji w historii zgłoszenia, korespondencji mailowej między opiekunami zgłoszenia a firmami serwisowymi powiązanymi ze zgłoszeniem.
Oprogramowanie musi posiadać dedykowane panele WWW w zależności od aktywnie zalogowanego użytkownika końcowego (panel dla użytkownika tj. zgłaszanie incydentów, panel dla operatora serwisowego – obsługa zgłoszeń)
Oprogramowanie musi umożliwiać wyświetlenie w panelu WWW użytkownika informacji nt. powiązanych z użytkownikiem zasobów (przypisane stanowiska PC, przydzielone licencje aplikacji, wydane urządzenia).
Oprogramowanie musi umożliwiać wybranie zasobu w określonej kategorii powiązanego z użytkownikiem podczas rejestracji zgłoszenia.
Oprogramowanie musi umożliwiać tworzenie zgłoszeń cyklicznych z możliwością definiowania częstości występowania oraz typu okresu (codziennie, co tydzień, co miesiąc)
Oprogramowanie musi umożliwiać tworzenie reguł w celu automatyzacji obsługi zgłoszeń. Reguły muszą uruchamiać się w odpowiedzi na określone zdarzenia w systemie i wykonywać akcje w zależności od spełnionych warunków. W zakresie reguł ServiceDesk musi realizować m.in. następujące przypadki użycia: ● Zmiana statusu po przejęciu zgłoszenia przez opiekuna. ● Przejmowanie zadań po przejęciu zgłoszenia przez opiekuna. ● Dodawanie zadań w zgłoszeniu w zależności od parametrów zgłoszenia. ● Wznawianie zgłoszenia po odpowiedzi przez zgłaszającego użytkownika. ● Zamykanie zgłoszenia po upływie czasu bez odpowiedzi użytkownika. ● Zamykanie zgłoszenia po upływie czasu reklamacji. ● Dodawanie wpisów (komentarzy) w zgłoszeniu na podstawie szablonów. ● Zmiana parametrów zgłoszenia po znalezieniu wybranej frazy w treści komentarza.

● Walidacja zamkniętych zadań w zamykanym zgłoszeniu. ● Systemowe potwierdzanie realizacji zgłoszenia. ● Wysyłanie dodatkowych powiadomień cyklicznych ze zgłoszeniami, np. zgłoszenia wymagające reakcji, zgłoszenia do realizacji lub zgłoszenia wstrzymane/wznowione.
Oprogramowanie musi umożliwiać tworzenie szablonów komentarzy wykorzystywanych przez opiekunów zgłoszeń.
Oprogramowanie musi posiadać możliwość rejestracji zgłoszeń i komentarzy drogą mailową, zarówno przez zarejestrowanych użytkowników systemu jak i niezarejestrowanych użytkowników.
Oprogramowanie musi umożliwiać obsługę dowolnej ilości kont pocztowych do wysyłania powiadomień i generowania zgłoszeń/komentarzy przez email.
Oprogramowanie musi posiadać wbudowane raporty prezentujące m.in. realizację obsługi zgłoszeń w zakładanym SLA (statystyka miesięczna, kwartalna, roczna).
Oprogramowanie musi umożliwiać definiowanie własnych widoków oraz zestawień dla każdego zalogowanego użytkownika
Oprogramowanie musi umożliwiać zdefiniowanie własne macierzy priorytetów na podstawie pilności oraz wpływu zgłoszenia
Oprogramowanie musi umożliwiać zamodelowanie trzy zmianowego trybu pracy inżynierów (opiekunów zgłoszeń)
Oprogramowanie musi umożliwiać informowanie użytkowników o nowych zdarzeniach systemowych za pomocą notyfikacji podczas pracy z systemem
Oprogramowanie musi umożliwiać tworzenie obiegu procesu decyzyjnego dla wniosków o uprawnienia lub elementy konfiguracji w oparciu o bazę CMDB
Oprogramowanie musi umożliwiać zaprojektowanie dowolnego formularza do wprowadzania danych z wykorzystaniem własnych atrybutów (wraz ze zmianą układu/położenia atrybutów w projektowanym widoku)
Oprogramowanie musi umożliwiać definicję czasów SLA w oparciu o matrycę priorytetów, statusy, kategorie lub dowolne warunki i atrybuty zgłoszenia
Oprogramowanie musi umożliwiać dodanie Akceptacji do już istniejącego zgłoszenia
Oprogramowanie musi umożliwiać definiowanie własnych reguł zarządzania w oparciu o warunki i akcje dla Prawdy i Fałszu (zdarzenie -> warunek -> akcja)
Oprogramowanie musi umożliwiać tworzenie wielu zgłoszeń poprzez wybór kilku użytkowników w zgłoszeniu
Oprogramowanie musi umożliwiać tworzenie słowników wartości dla atrybutów w oparciu o strukturę płaską lub drzewiastą
Oprogramowanie musi umożliwiać tworzenie atrybutów zależnych poprzez określone warunki widoczności
Oprogramowanie musi umożliwiać definiowanie formularzy zamykających zgłoszenie oraz zatwierdzające zmiany w zgłoszeniu
Oprogramowanie musi umożliwiać definiowanie reguł biznesowych za pomocą graficznego/blokowego kreatora.
Oprogramowanie musi umożliwiać definiowanie obiegów za pomocą graficznego/blokowego kreatora.
Oprogramowanie musi umożliwiać tworzenie niestandardowych raportów za pomocą kreatora.
Oprogramowanie musi umożliwiać definiowanie poziomu dostępu do zgłoszeń dla dynamicznych grup użytkowników.
Oprogramowanie musi umożliwiać definiowanie formularzy dla zgłoszeń w danej kategorii za pomocą kreatora Drag&Drop z możliwością określenia układu kolumn.
Oprogramowanie musi umożliwiać tworzenie dowolnej liczby Dashboard-ów dla użytkownika za pomocą kreatora Drag&Drop.
Oprogramowanie musi umożliwiać zmianę układu szczegółów zgłoszenia za pomocą kreatora Drag&Drop.
Oprogramowanie musi umożliwiać udostępniania ogłoszeń w formie Widget-u oraz okienka modalnego z wymaganym potwierdzeniem dla użytkownika.
Oprogramowanie musi umożliwiać zaprojektowanie dowolnego szablonu protokołu zgłoszenia.
Oprogramowanie musi udostępniać matrycę(wpływ/pilność) dla obliczania priorytetu zgłoszeń.
Oprogramowanie musi umożliwiać zmianę koloru dla statusu/priorytetu/wpływu/pilności zgłoszenia prezentowanego na liście zgłoszeń.

Oprogramowanie musi umożliwiać definiowanie dowolnych kolejek zgłoszeń.	
Oprogramowanie musi umożliwiać rejestrację nieobecności administratorów z możliwością wybrania zastępstwa.	
Oprogramowanie musi umożliwiać wybór trybu ciemnego(nocnego)	
Oprogramowanie musi umożliwiać obsługę zgłoszeń w widoku Kanban z możliwością jego konfiguracji w zakresie grupowania, sortowania oraz nakładania filtrów w logice AND/OR	

ServiceDesk – Zarządzanie wnioskami

Oprogramowanie musi zapewnić obsługę Workflow w zgłoszeniach serwisowych poprzez zdefiniowanie logicznych ścieżek (zbiór węzłów logicznych).
Oprogramowanie musi umożliwiać wybór wielu zasobów na jednym formularzu wniosku. Przykładowo dla wniosku o nadanie uprawnień musi istnieć możliwość wskazania wielu systemów/zbiorów danych z podziałem na moduły lub poziomy uprawnień użytkownika.
Na poziomie każdego węzła logicznego w workflow musi być możliwość edycji/modyfikacji zawartości danych w szczególności statusu, uwag, załączników (o dowolnym typie pliku) wraz z utworzeniem wpisu w historii przetwarzanego obiegu.

ServiceDesk – Zarządzanie uprawnieniami

Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych
Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych
Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)
Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych
Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek
Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych
Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)
Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku
Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)
Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób
Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych
Oprogramowanie w zakresie modułu ServicDesk musi umożliwiać integracje z systemami trzecimi poprzez REST API
Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika

CMDB

Oprogramowanie musi umożliwiać tworzenie własnych typów elementów konfiguracji (CI)
Oprogramowanie musi umożliwiać dodawanie dowolnych atrybutów dla typów CI w szczególności: wartości logiczne, data/czas, numeryczne, tekstowe, słownikowe
Oprogramowanie musi umożliwiać tworzenie podrzędnych i nadrzędnych typów CI
Oprogramowanie musi umożliwiać dziedziczenie atrybutów przez elementy konfiguracji posiadające typ nadrzędny
Oprogramowanie musi umożliwiać tworzenie dowolnych typów relacji do obsługi połączeń pomiędzy różnymi typami CI

Oprogramowanie musi umożliwiać tworzenie atrybutów dla relacji
Oprogramowanie musi umożliwiać prezentowanie powiązań pomiędzy elementami konfiguracji w formie struktury płaskiej (grid z możliwością jego modyfikacji w zakresie widoczności kolumn, ich szerokości oraz kolejności) oraz graficznej (wizualizacja sieci połączeń między elementami CI, z możliwością rozwijania widoku o dalsze poziomy relacji poszczególnych obiektów. Manualnie stworzony widok musi umożliwiać zapamiętanie pozycji elementów oraz widoczności poszczególnych jego elementów)
Oprogramowanie musi umożliwiać zbiorczy podgląd relacji pomiędzy poszczególnymi elementami konfiguracji
Oprogramowanie musi umożliwiać modelowanie struktury relacji pomiędzy elementami bazy CMDB w tym m.in. usługami, sprzętem, organizacją oraz pracownikami
Oprogramowanie musi umożliwiać nadzór nad wpływem zmian na poszczególne elementy konfiguracji
Oprogramowanie musi umożliwiać import elementów konfiguracji ze źródeł takich jak usługa katalogowa, skaner sieci, zewnętrzne pliki płaskie (CSV)
Oprogramowanie musi umożliwiać tworzenie oraz edycję własnych list elementów konfiguracji
Oprogramowanie musi umożliwiać wyszukiwanie i analizę elementów konfiguracji wg posiadanych atrybutów
Oprogramowanie musi umożliwiać tworzenie własnych typów relacji z określaniem nazwy relacji podstawowe i odwrotnej
Oprogramowanie w zakresie modułu CMDB musi umożliwiać integracje z systemami trzecimi poprzez REST API
Oprogramowanie musi umożliwiać tworzenie własnych formularzy dla wszystkich elementów konfiguracji

Zarządzanie zasobami oraz użytkownikami
Oprogramowanie musi umożliwiać tworzenie własnych szablonów widoków zasobów z określeniem analizowanych typów zasobów, widocznych atrybutów oraz informacji nt. powiązań pomiędzy zasobami.
Oprogramowanie musi umożliwiać tworzenie własnych atrybutów o typach co najmniej: tekst, liczba, bit, data, wartość słownikowa dla wybranego typu zasobu.
Oprogramowanie musi umożliwiać zapis oraz przegląd historii zmian dowolnego atrybutu zasobu w zakresie: operator, data, czas, poprzednia oraz nowa wartość.
Oprogramowanie musi umożliwiać zdefiniowanie dowolnych relacji pomiędzy zasobami (np. powiązania komputera z pracownikiem, licencją, dowolnym innym zasobem) wraz z zapisem historii relacji zasobów.
Oprogramowanie musi umożliwiać przypisywanie do każdego z zarządzanych w systemie zasobów dokumentów typu: faktura zakupu, gwarancja, umowa serwisowa. Bazą dokumentów musi być centralne repozytorium umożliwiające powiazania dokumentów z zasobami w relacji 1:N wraz z podglądem przypisanych zasobów oraz wydrukiem.
Oprogramowanie musi umożliwiać zdefiniowanie dowolnego typu zasobu inwentaryzacyjnego (np. telefon, drukarka, komputer) w strukturze drzewiastej wraz z kreatorem widocznych/wymaganych atrybutów edycyjnych.
Oprogramowanie musi posiadać dedykowaną (zintegrowaną z systemem) aplikację na platformę Android umożliwiającą spis z natury zinwentaryzowanych zasobów oraz bieżący podgląd atrybutów poszczególnego zasobu po jego zeskanowaniu
Oprogramowanie musi umożliwiać import danych z pliku CSV zawierającego dowolne informacje inwentaryzacyjne z wprowadzanych do systemu urządzeń w zakresie m.in.: numer faktury, numer seryjny, model, nazwa, data zakupu.
Oprogramowanie musi umożliwiać zaprojektowanie własnego schematu importu danych z zewnętrznego pliku CSV.
Oprogramowanie musi umożliwiać automatyczne tworzenie relacji pracownik-komputer na podstawie atrybutów obiektu w usłudze katalogowej.
Oprogramowanie musi zawierać wbudowany kreator wydruków w zakresie protokołów przekazania, zwrotu, likwidacji wraz z możliwością utworzenia dowolnego typu dokumentu
Oprogramowanie musi umożliwiać export ww. protokołów w formacie PDF

Oprogramowanie musi umożliwiać obsługę kodów kreskowych oraz QR w obrębie ww. kreatora wydruków
Oprogramowanie musi umożliwiać użycie w kreatorze wydruków własnego logotypu organizacji
Oprogramowanie musi umożliwiać użycie w kreatorze wydruków dowolnego atrybutu zasobu
Oprogramowanie musi umożliwiać przypisanie dowolnej firmy serwisowej z bazy organizacji do zasobu
Oprogramowanie musi umożliwiać przypisanie załącznika do zasobu
Oprogramowanie musi umożliwiać pogląd wszystkich zgłoszeń serwisowych dotyczących danego zasobu
Oprogramowanie musi umożliwiać podgląd zasobów (przypisanych do danego pracownika) z poziomu jego portalu użytkownika końcowego
Oprogramowanie musi umożliwiać zarządzanie cyklem życia zasobu
Oprogramowanie musi umożliwiać tworzenie niestandardowych reguł biznesowych dla zarządzania zasobami
Oprogramowanie musi umożliwiać seryjne dodawanie zasobów
Oprogramowanie musi umożliwiać automatyczne nadawanie numerów inwentaryzacyjnych dla zasobów
Oprogramowanie musi udostępniać kreator raportów dla zasobów
Oprogramowanie musi udostępniać możliwość kopiowania widoku dla określonego typu(ów) zasobu z innego typ zasobu
Oprogramowanie musi udostępniać możliwość kopiowania formularz dla określonego typu(ów) zasobu z innego typ zasobu
Oprogramowanie musi umożliwiać ewidencję magazynów
Oprogramowanie musi umożliwiać ewidencję lokalizacji magazynowych
Oprogramowanie musi umożliwiać ewidencję produktów magazynowych
Oprogramowanie musi udostępniać informację o stanie magazynowym(ilościowo)
Oprogramowanie musi umożliwiać generowanie dokumentów PZ/PW/RW/MM
Oprogramowanie musi umożliwiać przyjęcie zasobów ewidencjonowanych i eksploatacyjnych na magazyn
Oprogramowanie musi umożliwiać wydawanie zasobów ewidencjonowanych i eksploatacyjnych z magazynu
Oprogramowanie musi umożliwiać zwrot zasobów na magazyn
Oprogramowanie musi umożliwiać zmianę szablonów dokumentów PZ/PW/RW/MM
Oprogramowanie musi umożliwiać wyszukiwanie dokumentów po dowolnym atrybucie
Oprogramowanie musi umożliwiać zarządzanie organizacjami/typami organizacji (np. klient, podwykonawca)
Oprogramowanie musi umożliwiać dowolne przypisanie osoby do organizacji
Oprogramowanie musi umożliwiać tworzenia dynamicznych grup użytkowników
Oprogramowanie musi umożliwiać zarządzanie kontaktami osób/organizacji
Oprogramowanie musi umożliwiać zarządzanie nieobecnościami użytkowników
Oprogramowanie musi umożliwiać zarzadzanie uprawnieniami i poziomami dostępu do danych w zakresie zarządzania zasobami
Oprogramowanie w zakresie modułu Zasobów musi umożliwiać integracje z systemami trzecimi poprzez REST API
Oprogramowanie musi umożliwiać automatyczne pobieranie danych rejestrowych kontrahentów z bazy GUS

Zarządzanie dokumentami

Oprogramowanie musi umożliwiać centralną ewidencję dokumentów
Oprogramowanie musi umożliwiać zawierać dedykowany formularz dodawania nowego dokumentu z możliwością edycji widocznych oraz wymaganych atrybutów dokumentu
Oprogramowanie musi umożliwiać dołączenie skanu dokumentu (m.in.: skany faktur, umów)
Oprogramowanie musi umożliwiać stworzenie dedykowanego zbioru ról i uprawnień w zakresie obsługi rejestru dokumentów
Oprogramowanie musi umożliwiać utworzenie pomocniczych rejestrów oraz słowników

Oprogramowanie musi umożliwiać przeszukiwanie bazy dokumentów oraz kontrahentów po dowolnie wskazanym atrybucie opisującym
Oprogramowanie musi umożliwiać utworzenie rejestru osób reprezentujących
Oprogramowanie musi umożliwiać analizę zmian wartości dowolnych atrybutów opisujących dokument w zakresie daty zmiany, aktualnej/poprzedniej wartości oraz osoby dokonującej zmiany

Wymagania formalne:

W okresie 12 miesięcy od wdrożenia wymagany jest dostęp do nowych wersji systemu oraz wsparcia technicznego producenta.
Obsługa serwisowa musi być realizowana przez Producenta oprogramowania, w dni robocze w godzinach 8-16 w języku polskim, zgodnie z poniższymi parametrami:

Typ zgłoszenia	Opis	Czas Reakcji (godziny robocze)	Czas Realizacji (godziny robocze)
Błąd Krytyczny	Nieprawidłowości, która uniemożliwia dalsze korzystanie z Systemu - awaria	2h	8h
Usterka Ważna	Nieprawidłowości utrudniającej korzystanie z Systemu, ale w stopniu umożliwiającym dalsze korzystanie	8h	40h
Usterka	Nieprawidłowości utrudniająca korzystanie z Systemu, ale w stopniu umożliwiającym i nieutrudniającym w sposób znaczny dalsze korzystanie	24h	144h

Dostarczone licencje na oprogramowanie muszą objąć co najmniej **25 stanowisk komputerowych** z systemem klasy Microsoft Windows. Licencje nie mogą mieć ograniczeń ilościowych dotyczących liczby obsługiwanych innych zasobów (np. drukarki, skanery, monitory itp). Ponadto musi posiadać co najmniej 2 licencji dostępowych do konsoli zarządzającej.
Zamawiający wymaga od wykonawcy, aby w terminie do 30 dni od podpisania umowy przeprowadził wdrożenie systemu
Zamawiający wymaga od wykonawcy, aby w terminie 5 dni od zakończenia prac wdrożeniowych przeprowadził szkolenie administracyjne z obsługi systemu (wymagane co najmniej 20 sesje szkoleniowe po 1,5 godziny każda)
Zamawiający wymaga, aby producent oferowanego oprogramowania przedstawił ważny certyfikat potwierdzający, że proces wytwarzania oprogramowania odbywa się zgodnie z międzynarodową normą ISO/IEC 27001. W celu potwierdzenia zgodności, do oferty należy dołączyć kopię certyfikatu ISO/IEC 27001.

Zamawiający wymaga, aby oferowane oprogramowanie w zakresie:
Zarządzanie incydentami (Incident Management),
Zarządzanie problemami (Problem Management),
Zarządzanie bazą wiedzy (Knowledge Management),
Zarządzanie zasobami (Asset Management).
posiadało aktualny certyfikat zgodności z najlepszymi praktykami IT Service Management, wydany przez niezależną organizację certyfikującą (np. Pink Elephant). Do oferty należy dołączyć kopię stosownego certyfikatu oraz wskazać link do strony internetowej organizacji certyfikującej, na której potwierdzona jest zgodność oferowanego rozwiązania z ww. procesami ITSM.

3.2. Wdrożenie zintegrowanej usługi zarządzania aktualizacjami, monitoringu infrastruktury i ewidencji aktywów IT/OT – 1 usł.

1. W ramach niniejszej pozycji Wykonawca zaprojektuje, skonfiguruje, zintegruje i uruchomi **zintegrowaną usługę zarządzania aktualizacjami, monitoringu infrastruktury oraz ewidencji aktywów IT/OT**, wykorzystując funkcjonalności systemów dostarczanych lub wdrażanych w ramach niniejszego zamówienia.
Celem usługi jest zapewnienie Zamawiającemu jednego, spójnego procesu obejmującego:

- identyfikację i ewidencję aktywów IT oraz OT/ICS;
- monitorowanie ich dostępności, stanu i podstawowych parametrów technicznych;
- identyfikację brakujących aktualizacji i poprawek bezpieczeństwa;
- kontrolowane wdrażanie aktualizacji na obsługiwanych stacjach roboczych i serwerach;
- utrzymywanie aktualnej informacji o stanie aktywów;
- powiązanie danych o aktywach, podatnościach, aktualizacjach i zdarzeniach infrastrukturalnych;
- raportowanie stanu infrastruktury Zamawiającego.

2. Sposób realizacji

Zamawiający **nie wymaga dostarczenia w ramach niniejszej pozycji jednego, odrębnego produktu informatycznego ani trzech niezależnych systemów**.
Wykonawca może wykorzystać w szczególności funkcjonalności:

- systemu ITSM/CMDB,
- systemu ochrony i monitorowania bezpieczeństwa,
- systemu zarządzania stacjami roboczymi i serwerami,
- systemu monitoringu infrastruktury,
- systemu NAC,
- urządzeń UTM/NGFW,
- zarządzalnych urządzeń sieciowych,
- systemów katalogowych,
- innych komponentów dostarczanych lub istniejących u Zamawiającego,

o ile łącznie zapewnią realizację wszystkich wymagań określonych w niniejszym punkcie.
Jeżeli do realizacji wymaganych funkcji niezbędne będzie zastosowanie dodatkowego komponentu programowego, licencji lub modułu, Wykonawca zobowiązany jest uwzględnić go w cenie niniejszej pozycji.

3.2.1. Centralne zarządzanie aktualizacjami

W ramach usługi Wykonawca zapewni mechanizm centralnego zarządzania aktualizacjami systemów operacyjnych oraz oprogramowania na stacjach roboczych i serwerach Zamawiającego.
Mechanizm musi umożliwiać co najmniej:

- inwentaryzację wersji systemów operacyjnych i zainstalowanego oprogramowania;
- identyfikację brakujących aktualizacji i poprawek bezpieczeństwa;
- prezentację statusu aktualizacji urządzeń;
- tworzenie grup urządzeń;
- definiowanie harmonogramów i okien serwisowych;
- zatwierdzanie lub odraczanie wybranych aktualizacji;
- stopniowe wdrażanie aktualizacji, w tym możliwość zastosowania grupy testowej;
- raportowanie powodzenia i niepowodzenia wdrożeń;
- wskazywanie urządzeń wymagających interwencji;
- możliwość wyłączenia określonej aktualizacji z procesu automatycznego wdrożenia;
- w przypadku, gdy dana aktualizacja i system operacyjny to umożliwiają – jej wycofanie lub odinstalowanie.

Dla urządzeń sieciowych, systemów bezpieczeństwa i innych urządzeń infrastrukturalnych, których aktualizacji nie obsługuje centralny system aktualizacji stacji i serwerów, Wykonawca opracuje i udokumentuje sposób aktualizacji z wykorzystaniem mechanizmów producenta danego urządzenia.
Aktualizacje urządzeń OT/ICS mogą być wykonywane wyłącznie po wcześniejszej analizie wpływu na proces technologiczny i po uzyskaniu akceptacji Zamawiającego

3.2.2. Monitoring infrastruktury IT/OT

W ramach usługi Wykonawca wdroży mechanizm centralnego monitorowania kluczowych elementów infrastruktury IT oraz, w zakresie technicznie bezpiecznym i obsługiwanym, OT/ICS.
Monitoring powinien obejmować co najmniej:

- dostępność urządzeń;
- dostępność kluczowych usług;

- wykorzystanie procesora;
- wykorzystanie pamięci RAM;
- wykorzystanie przestrzeni dyskowej;
- stan interfejsów sieciowych;
- podstawowe parametry komunikacyjne;
- stan urządzeń sieciowych;
- stan serwerów fizycznych i wirtualnych;
- stan systemu backupu;
- stan urządzeń bezpieczeństwa;
- stan UPS i innych urządzeń infrastrukturalnych posiadających obsługiwany interfejs monitorowania;
- monitorowanie wybranych zasobów OT, jeżeli może być ono realizowane bez ingerencji w proces technologiczny.

System musi umożliwiać:

- definiowanie progów alarmowych;
- generowanie alertów;
- klasyfikację zdarzeń według poziomu istotności;
- powiadamianie administratorów;
- przechowywanie historii parametrów;
- prezentację bieżącego stanu infrastruktury;
- tworzenie raportów;
- powiązanie monitorowanych elementów z ewidencją aktywów.

3.2.3. Ewidencja i inwentaryzacja aktywów IT/OT

Wykonawca utworzy i zasili centralną ewidencję aktywów sprzętowych i programowych IT oraz OT/ICS. Centralnym repozytorium informacji o aktywach może być wdrażany system CMDB lub inne centralne repozytorium informacji zapewniające wymagane funkcje ewidencyjne.

Dla każdego aktywa należy w zakresie dostępnych informacji gromadzić co najmniej:

- unikalny identyfikator;
- nazwę urządzenia lub systemu;
- kategorię aktywa;
- lokalizację;
- producenta i model;
- numer seryjny, jeżeli jest dostępny;
- adres IP;
- adres MAC, jeżeli jest dostępny;
- system operacyjny / firmware;
- wersję oprogramowania;
- środowisko: IT / OT / DMZ / zarządzanie;
- właściciela lub opiekuna;
- status eksploatacyjny;
- poziom krytyczności;
- datę ostatniej aktualizacji informacji;
- powiązania z innymi urządzeniami lub usługami, jeżeli są dostępne.

Inwentaryzacja IT

Dane dotyczące środowiska IT mogą być pozyskiwane automatycznie m.in. z:

- systemu zarządzania endpointami;
- agentów bezpieczeństwa;
- systemów monitorowania;
- NAC;
- UTM/NGFW;
- Active Directory;
- urządzeń sieciowych;
- systemów wirtualizacyjnych;
- innych źródeł dostępnych w środowisku Zamawiającego.

Inwentaryzacja OT

Inwentaryzacja OT/ICS musi być wykonywana metodami bezpiecznymi dla procesów technologicznych.
W pierwszej kolejności należy wykorzystywać:

- istniejącą dokumentację techniczną;
- konfiguracje SCADA, HMI, PLC i RTU;
- dane dostępne z systemów zarządzających;
- informacje z urządzeń sieciowych;
- tablice MAC i ARP;
- VLAN;
- informacje z UTM/NGFW;
- dane z monitoringu;
- dane uzyskane od administratorów i automatyków;
- pasywną obserwację ruchu, jeżeli jest dostępna.

3.2.4. Integracja i przepływ informacji

W ramach wdrożenia Wykonawca zapewni, aby informacje pozyskiwane przez poszczególne komponenty mogły być wykorzystane w spójnym procesie operacyjnym.
Wykonawca musi w ramach usługi:

- skonfigurować wszystkie wymagane integracje pomiędzy dostarczonymi systemami;
- zapewnić przepływ informacji niezbędnych do realizacji funkcji pkt 3.2;
- wskazać źródła danych dla poszczególnych typów aktywów;
- skonfigurować harmonogramy synchronizacji;
- skonfigurować konta techniczne z minimalnym zakresem uprawnień;
- zapewnić bezpieczne przechowywanie danych uwierzytelniających;
- przygotować dokumentację opisującą sposób integracji;
- skonfigurować mechanizmy kontroli błędów synchronizacji.

3.2.5. Raportowanie

Usługa musi umożliwiać przygotowanie co najmniej następujących zestawień:

- lista aktywów IT;
- lista aktywów OT;
- aktywa według lokalizacji;
- aktywa według statusu;
- urządzenia nieaktualne;
- urządzenia z brakującymi poprawkami;
- urządzenia niedostępne;
- stan aktualizacji systemów;
- historia wdrożonych aktualizacji;

3.2.6. Dokumentacja powdrożeniowa

Wykonawca przekaże dokumentację obejmującą minimum:

- opis architektury usługi;
- wykaz użytych systemów i komponentów;
- wskazanie, które komponenty realizują poszczególne funkcje;
- sposób integracji;
- źródła danych;
- harmonogramy aktualizacji;
- polityki aktualizacji;

4. Pakiet ochrony punktów końcowych oraz centralnego zarządzania logami i zdarzeniami – 1 kpl.

4.1. Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i wdrożenie lokalnego systemu centralnego zarządzania logami i zdarzeniami bezpieczeństwa (O24) z funkcjami korelacji i alertowania, wraz z integracją źródeł IT/OT, instruktażem administratorów oraz minimum 12-miesięcznym wsparciem technicznym.

4.1.1. System SIEM ma służyć do centralnego gromadzenia, przechowywania, analizy i korelacji logów oraz zdarzeń bezpieczeństwa z urządzeń i systemów teleinformatycznych Zamawiającego

Wymagania dla Systemu Analizy Logów

a) W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
b) Rozwiązanie musi być możliwe do uruchomienia jako maszyna wirtualna lub zestaw maszyn wirtualnych w środowisku wirtualizacyjnym Zamawiającego, w tym KVM/Proxmox lub rozwiązaniu równoważnym.
c) Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach.
d) Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
e) Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.
f) Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.
g) Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
h) Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.
i) Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).
j) Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.
k) Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie. –
l) Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).
m) Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.
n) Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).
o) Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów)
p) Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.
q) Rozwiązanie musi umożliwiać tworzenie statycznych raportów.
r) Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF.
s) Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.
t) Rozwiązanie musi umożliwiać tworzenie własnych raportów.
u) 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.
v) 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.

Wymagania systemowe

a) System musi zostać zwymiarowany do rzeczywistej liczby źródeł i wolumenu zdarzeń Zamawiającego, z minimum 30% rezerwą wydajnościową; jako wartość odbiorową należy przyjąć obsługę co najmniej 500 EPS.
b) Retencja logów musi być konfigurowalna. Wymaga się minimum 90 dni retencji online dla logów bezpieczeństwa oraz możliwości archiwizacji długoterminowej na zasobach Zamawiającego.
c) System musi obsługiwać co najmniej 50 aktywnych źródeł logów z możliwością dalszej rozbudowy.
d) Pojemność repozytorium logów należy dobrać na podstawie pomiaru lub szacunku wolumenu danych z uwzględnieniem wymaganej retencji i minimum 30% rezerwy.
e) System logów musi być możliwy do uruchomienia w środowisku KVM/Proxmox lub innym środowisku wirtualizacyjnym wskazanym przez Zamawiającego.

4.1.2. Integracja źródeł IT/OT

System ma przyjmować i korelować logi z urządzeń UTM/NGFW, przełączników, serwerów, Active Directory, systemu NAC/RADIUS, EDR/XDR, systemów backupu, monitoringu infrastruktury oraz – jeżeli udostępniają

odpowiednie interfejsy – systemów i urządzeń OT. Nie wymaga się dostawy odrębnych sond NDR/IDS ani fizycznego urządzenia analizującego ruch sieciowy w ramach tego pakietu.

4.1.3. Wymagania dla konsoli systemu SIEM

Konsola zarządzającą umożliwiająca grupowanie takich samych zdarzeń w ramach jednego wpisu oraz wyświetlająca liczbę wystąpień identycznego zdarzenia.
Konsola posiadającą możliwość tworzenia i śledzenia zgłoszeń.
Konsola umożliwiająca stworzenie zgłoszenia z dowolnego zdarzenia.
Konsola posiadająca dedykowany widok dla utworzonych zgłoszeń.

4.1.4. Poufność, bezpieczeństwo informacji i dane osobowe

1. Wykonawca zobowiązany jest do zachowania w poufności wszelkich informacji uzyskanych w związku z realizacją przedmiotu zamówienia, w szczególności informacji dotyczących infrastruktury teleinformatycznej Zamawiającego, konfiguracji systemów, treści logów, danych osobowych oraz innych informacji stanowiących tajemnicę przedsiębiorstwa lub tajemnicę prawnie chronioną.
2. Przed dopuszczeniem do realizacji prac osoby wyznaczone przez Wykonawcę do udziału w wykonywaniu zamówienia zobowiązane są podpisać oświadczenie/umowę o zachowaniu poufności, zgodnie ze wzorem stanowiącym załącznik nr 1 do niniejszego OPZ lub do umowy.
3. Wykonawca nie jest uprawniony do wykorzystywania informacji uzyskanych w związku z realizacją zamówienia w jakimkolwiek innym celu niż wykonanie umowy, ani do udostępniania tych informacji osobom trzecim bez uprzedniej pisemnej zgody Zamawiającego, chyba że obowiązek udostępnienia wynika wprost z przepisów prawa.
4. Dane (w tym logi i zrzuty ekranów) pozyskane w ramach realizacji usług serwisowych, w szczególności z wykorzystaniem zdalnego dostępu, które zawierają informacje dotyczące środowiska Zamawiającego, nie mogą być przenoszone ani przechowywane poza środowiskiem Zamawiającego, z wyjątkiem przypadków wyraźnie zaakceptowanych przez Zamawiającego na piśmie.
5. W przypadku, gdy w związku z realizacją zamówienia dochodzi do przetwarzania danych osobowych w rozumieniu przepisów o ochronie danych osobowych, strony zawrą odrębną umowę powierzenia przetwarzania danych osobowych, zgodnie z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oraz przepisami krajowymi.
6. Po zakończeniu realizacji zamówienia (lub wcześniej, na żądanie Zamawiającego) Wykonawca zobowiązany jest do zwrotu lub trwałego usunięcia wszelkich danych, informacji i nośników zawierających informacje Zamawiającego, o ile ich dalsze przechowywanie nie wynika z bezwzględnie obowiązujących przepisów prawa. Fakt usunięcia danych Wykonawca potwierdzi stosownym protokołem.
7. Postanowienia niniejszego punktu pozostają w mocy także po wygaśnięciu lub rozwiązaniu umowy, przez okres co najmniej 5 lat, a w zakresie danych osobowych – przez okres wymagany przepisami prawa.

Zakres wdrożenia obejmuje instalację konsoli, wdrożenie agentów, przygotowanie polityk ochrony, integrację z Active Directory oraz centralnym menedżerem logów, test detekcji i izolacji kontrolnego endpointu, dokumentację powdrożeniową i instruktaż administratorów.
1. Wymagane licencje/subskrypcje muszą obejmować okres minimum 12 miesięcy od odbioru, o ile dla zaoferowanego rozwiązania lub urządzenia aktualny WoD nie przewiduje dłuższego okresu.
2. Dla systemów OT agent może być instalowany wyłącznie na urządzeniach wspieranych przez producenta rozwiązania i po potwierdzeniu braku wpływu na proces technologiczny.
3. Raportowanie stanu ochrony, wykrytych zagrożeń, urządzeń nieaktywnych oraz wersji agentów.
4. Możliwość przekazywania zdarzeń i alertów do centralnego menedżera logów/SIEM przy użyciu API, Syslog, webhooków lub innego udokumentowanego mechanizmu.
5. Szyfrowana komunikacja agent–konsola i bezpieczne uwierzytelnianie administratorów.
6. Ochrona musi działać również podczas czasowego braku łączności endpointu z konsolą.
7. Centralne definiowanie polityk, wyjątków, harmonogramów i grup urządzeń oraz zdalne wdrażanie/aktualizowanie agentów.
8. Funkcje XDR lub równoważna korelacja zdarzeń pochodzących z chronionych endpointów i innych obsługiwanych źródeł bezpieczeństwa.
9. Funkcje EDR: rejestracja i analiza aktywności procesów, plików, połączeń sieciowych i logowań; budowa drzewa procesów; wyszukiwanie zdarzeń; możliwość izolacji urządzenia i wykonania działań remediacyjnych.
10. Ochrona antymalware i antyransomware oparta co najmniej na sygnaturach, analizie behawioralnej oraz mechanizmach reputacyjnych.

11. Centralna konsola zarządzająca dostępna przez bezpieczny interfejs WWW, z obsługą ról administracyjnych i MFA.

4.2. System ochrony stacji roboczych i serwerów EPP/EDR/XDR (O01)

Zakres obejmuje dostawę, wdrożenie i konfigurację centralnie zarządzanego systemu ochrony punktów końcowych, obejmującego stacje robocze, serwery oraz wybrane stacje techniczne lub operatorskie środowiska OT, o ile ich charakter i wymagania eksploatacyjne pozwalają na instalację agentów bezpieczeństwa. Dostarczone licencje muszą objąć minimum 25 stanowisk lub urządzeń objętych ochroną i zarządzaniem. Jeżeli rozwiązanie posiada konsolę licencjonowaną według liczby operatorów, należy zapewnić minimum 2 dostępy operatorskie do konsoli administracyjnej.
Wymagane licencje/subskrypcje dla systemu ochrony punktów końcowych muszą obejmować okres minimum 12 miesięcy od daty odbioru, chyba że aktualny WoD albo wymagania dla konkretnego urządzenia lub systemu przewidują okres dłuższy.

1. WYMAGANIA OGÓLNE

1.1. Przedmiotem zamówienia jest dostawa, wdrożenie i utrzymanie rozwiązania zapewniającego kompleksową ochronę przed zagrożeniami w standardzie Endpoint Detection & Response (EDR) w połączeniu z Endpoint Protection Platform (EPP), Network Detection & Response (NDR), Identity Threat Detection & Response (ITDR), Extended Detection and Response (XDR), Email Security, Domain Filtering, Web Content Filtering, SaaS & Cloud Security Posture Management (SSPM/CSPM), External Attack Surface Management (EASM), Centralized Log Management, Deception Technology, User Behavior Analytics (UBA) oraz wbudowaną usługą 24/7 MDR i orkiestrację automatyzacji (SOAR). System musi zapewniać centralne zarządzanie ochroną wszystkich typów urządzeń końcowych (stacje robocze, serwery), automatyzację reakcji na incydenty, integrację z warstwą sieciową, tożsamościową, mailową i chmurową w ramach zapewnienia kompleksowej ochrony zagrożeń wielowarstwowych.

1.2. Wszystkie metadane, telemetria, logi i dane użytkownika muszą być przechowywane wyłącznie na terytorium Unii Europejskiej – zgodnie z RODO i normami UE.

1.3. Platforma musi umożliwiać wdrożenie w modelu:

1.3.1. Cloud (SaaS)

1.3.2. On-premise

1.3.3. Hybrydowym

1.4. Musi być dostępna centralna konsola zarządzająca dostępna przez przeglądarkę, wspierać autentykację wieloskładnikową (MFA) oraz granularne role i uprawnienia dla zarządzania wielowarstwowym i skalowaniem uprawnień.

1.5. System musi obsługiwać automatyczne wykrywanie i instalowanie agentów na nowych urządzeniach oraz zapewniać szybkie, bezobsługowe wdrożenie aktualizacji (bez potrzeby restartów). Niezbędna jest możliwość komunikacji przez publiczne API, integracja z narzędziami do monitorowania, analizowania i reagowania na zagrożenia w czasie rzeczywistym klasy Security Information and Event Management (SIEM), zdalnego monitorowania i zarządzania Remote Monitoring and Management (RMM) oraz integracja z MITRE ATT&CK framework.

1.6. W ramach licencji wymagana jest usługa wsparcia technicznego realizowana przez wykwalifikowany zespół, obejmująca również Menedżera ds. Technicznej Obsługi Klienta – Technical Account Manager, konsultacje cykliczne, onboarding oraz raporty z działalności.

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

1.8.1. 98% skuteczności w zakresie Detection Visibility (widoczność/detekcja wszystkich kroków ataku),

1.8.2. 98% skuteczności w zakresie Protection Rate (blokowanie złośliwych kroków ataku),

1.8.3. 98% skuteczności w zakresie Prevention (blokowanie ataków na etapie pierwszych kroków).

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

2. WYMAGANIA SZCZEGÓŁOWE – MINIMALNA FUNKCJONALNOŚĆ 2.1. OCHRONA STACJI ROBOCZYCH, SERWERÓW I URZĄDZEŃ

2.1.1. Możliwość instalacji agenta ochrony na następujących systemach operacyjnych:

2.1.1.1. Windows XP SP3

2.1.1.2. Windows Vista SP1
2.1.1.3. Windows 7 SP1
2.1.1.4. Windows 8, 8.1
2.1.1.5. Windows 10
2.1.1.6. Windows 11
2.1.1.7. Windows Server 2003
2.1.1.8. Windows Server 2008
2.1.1.9. Windows Server 2012
2.1.1.10. Windows Server 2016
2.1.1.11. Windows Server 2019
2.1.1.12. Windows Server 2022
2.1.1.13. Linux Ubuntu 18.04 i nowsze
2.1.1.14. Linux Red Hat Enterprise 6.10 I nowsze
2.1.1.15. Linux Fedora 35 i nowsze
2.1.1.16. Linux Debian 10.7 i nowsze
2.1.1.17. Linux CentOS 7 i nowsze
2.1.1.18. Linux CentOS Stream 8 i nowsze
2.1.1.19. Linux Rocky 9 I now sze
2.1.1.20. MacOS 10.15 I nowsze

2.1.2. Platforma musi zapewniać kompleksową ochronę przed szeroką gamą zagrożeń, obejmującą:
2.1.2.1. Wirusy i trojany
2.1.2.2. Ransomware
2.1.2.3. Oprogramowanie szpiegujące (spyware) i adware
2.1.2.4. Oprogramowanie typu rootkit
2.1.2.5. Cryptominers
2.1.2.6. Ataki typu fileless
2.1.2.7. Exploity wykorzystujące luki OS
2.1.2.8. Narzędzia hakerskie
2.1.2.9. Phishing
2.1.2.10. Ataki na tożsamość i logowanie (credential attacks)
2.1.2.11. Zagrożenia związane z SaaS i chmurą

2.1.3. Platforma musi posiadać wbudowany zaawansowany antywirus nowej generacji (NGAV) z heurystyką i uczeniem maszynowym:
2.1.3.1. Machine Learning dla statycznej analizy plików
2.1.3.2. Analiza behawioralna procesów i plików w czasie rzeczywistym
2.1.3.3. Integracja z threat intelligence (VirusTotal i niestandardowe źródła)
2.1.3.4. Heurystyka zaawansowana dla wykrywania zagrożeń typu nieznane/zero-day

2.1.4. Rozwiązanie musi mieć w sobie zawarty moduł Storage Device Control do zarządzania dostępem do urządzeń USB:
2.1.4.1. Blokowanie/dozwolenie urządzeń USB i pamięci przenośnych
2.1.4.2. Monitorowanie całego ruchu na USB
2.1.4.3. Tworzenie polityk na poziomie organizacji, grupy i użytkownika
2.1.4.4. Logowanie wszystkich interakcji z urządzeniami USB

2.1.5. Wymaga się, by system posiadał minimum następujące wbudowane mechnizmy odpowiedzi na zagrożenia:
2.1.5.1. Izolację stacji lub hosta z sieci
2.1.5.2. Blokowanie kont użytkowników
2.1.5.3. Zamykanie procesów malware
2.1.5.4. Kwarantannę plików złośliwych
2.1.5.5. Automatyczne wdrażanie akcji remedacyjnych bez interwencji operatora

2.1.6. System także musi posiadać pełną kompatybilność z innymi narzędziami bezpieczeństwa:
2.1.6.1. Brak konfliktów z zainstalowanym oprogramowaniem
2.1.6.2. Obsługa współpracy z Microsoft Defender
2.1.6.3. Możliwość działania równolegle z innymi narzędziami antywirusowymi
2.1.6.4. Brak wymagania deinstalacji innych rozwiązań

2.2. ZARZĄDZANIE PLATFORMĄ I ADMINISTRACJA

2.2.1. Zarządzanie witrynami, grupami, polityką i audytami;

2.2.1.1. Zarządzanie wieloma stanowiskami oraz grupami urządzeń
2.2.1.2. Tworzenie, edycja i wdrażanie polityk zabezpieczenia na poziomie organizacji, grupy i urządzenia
2.2.1.3. Centralizowany audyt wszystkich zmian konfiguracyjnych
2.2.1.4. Ścieżki audytu ze znacznikami czasowymi i identyfikacją użytkownika
2.2.1.5. Zarządzanie wielowitrynowe (multi-tenant)
2.2.2. Zarządzanie użytkownikami, rolami i uwierzytelnianiem wieloskładnikowym (MFA);
2.2.2.1. Zarządzanie kontami użytkowników konsoli administracyjnej
2.2.2.2. Granularne role i uprawnienia (least privilege principle)
2.2.2.3. Autentykacja wieloskładnikowa (MFA) – obsługa TOTP
2.2.2.4. Zarządzanie sesją użytkownika
2.2.3. Zarządzanie licencjami i użytkowaniem;
2.2.3.1. Zarządzanie licencjami min 25 stanowisk
2.2.3.2. **Obsługa licencji terminowych (12 miesięcy)**
2.2.3.3. Raportowanie zgodności licencyjnej
2.2.3.4. Realokacja licencji między urządzeniami
2.2.4. Panel (dashboard) i raporty;
2.2.4.1. Centralna konsola nawigacyjna wyświetlająca stan środowiska
2.2.4.2. Przegląd zagrożeń, zdarzeń bezpieczeństwa i stanu compliance
2.2.4.3. Raportowanie standardowe (wstępnie zdefiniowane raporty biznesowe, raporty zgodności)
2.2.4.4. Harmonogramowanie raportów i automatyczne dostarczanie
2.2.4.5. Eksport raportów w formatach PDF, CSV, XLSX
2.2.5. Integracje API, RMM i PSA:
2.2.5.1. Publiczne API REST dla integracji z systemami trzecich
2.2.5.2. Dokumentacja API i SDK
2.2.5.3. Integracja z platformami zarządzania zdalnymi (RMM)
2.2.5.4. Webhooks dla zdarzeń bezpieczeństwa
2.2.5.5. Obsługa OAuth 2.0
2.2.6. Integracja MITRE ATT&CK:
2.2.6.1. Mapowanie wykrytych zagrożeń na taktyki i techniki MITRE ATT&CK
2.2.6.2. Wizualizacja zagrożeń na mapie ATT&CK (ATT&CK Heat Map)
2.2.6.3. Raportowanie pokrycia i luk w detekcji poszczególnych technik
2.3. WYKRYWANIE I REAGOWANIE NA URZĄDZENIACH KOŃCOWYCH
2.3.1. Ciągłe monitorowanie i widoczność urządzeń końcowych;
2.3.1.1. Pełna widoczność wszystkich procesów uruchomionych na endpoint
2.3.1.2. Drzewo procesów (process tree) z historią
2.3.1.3. Monitoring i logging zmian w rejestrze Windows
2.3.1.4. Śledzenie operacji na systemie plików
2.3.1.5. Monitoring ruchu sieciowego na poziomie procesu
2.3.1.6. Detekcja behawioralna podejrzanych operacji
2.3.1.7. Korelacja zdarzeń z wieloma źródłami
2.3.2. Widoczność zdarzeń systemu Windows
2.3.2.1. Zbieranie dzienników zdarzeń Windows na endpoint
2.3.2.2. Monitoring logów logowania użytkowników
2.3.2.3. Śledzenie zmian polityk bezpieczeństwa
2.3.2.4. Monitoring zmian uprawnień użytkownika
2.3.2.5. Przechowywanie dzienników z konfigurowlanym okresem retencji
2.3.3. Widoczność aplikacji i urządzeń końcowych:
2.3.3.1. Inwentaryzacja wszystkich uruchomionych aplikacji
2.3.3.2. Śledzenie wersji oprogramowania
2.3.3.3. Monitoring zmian w konfiguracji aplikacji
2.3.3.4. Raportowanie bezpieczeństwa aplikacji
2.3.4. Kontrola i panel użytkownika końcowego:
2.3.4.1. Prosta konsola dla użytkownika końcowego
2.3.4.2. Wyświetlanie stanu ochrony na jego urządzeniu
2.3.4.3. Możliwość skanowania na żądanie

2.3.4.4. Wyświetlanie historii zagrożeń dla urządzenia
2.3.4.5. Powiadomienia o krytycznych zdarzeniach bezpieczeństwa
2.3.5. Zautomatyzowane działania dochodzeniowo-śledcze:
2.3.5.1. Narzędzia do śledztw cyfrowych (digital forensics)
2.3.5.2. Zbieranie i analiza artefaktów systemu
2.3.5.3. Rekonstrukcja sekwencji zdarzeń
2.3.5.4. Export danych forensycznych w standardowych formatach
2.3.5.5. Zdalne wykonania poleceń diagnostycznych
2.3.5.6. Zbieranie kopii pamięci (memory dump) na żądanie
2.3.5.7. Archiwizacja i długoterminowe przechowywanie danych forensycznych z obsługą natywnych i zewnętrznych źródeł
2.3.6. Niestandardowe zasady wykrywania:
2.3.6.1. Tworzenie zaawansowanych reguł detektowania zagrożeń
2.3.6.2. Edytor reguł oparty na wizualizacji lub kodzie
2.3.6.3. Obsługa wyrażeń regularnych i wzorców behawioralnych
2.3.6.4. Walidacja i testowanie reguł przed wdrożeniem
2.3.7. Automatyzacja reakcji na incydenty (playbooki)
2.3.7.1. Możliwość definiowania predefiniowanych playbooków reakcji na określone typy incydentów (np. ransomware, podejrzenie exfiltracji danych, podejrzana aktywność użytkownika).
2.3.7.2. Możliwość tworzenia własnych, personalizowanych playbooków reakcji przez administratorów Zamawiającego, złożonych z wielu kroków (akcje na endpointach, kontach użytkowników, ruchu sieciowym).
2.3.7.3. Możliwość definiowania i zapisywania własnych akcji remediacyjnych (custom remediation actions), które mogą być wykorzystywane jako kroki w playbookach (np. blokada procesu, blokada domeny/IP, izolacja hosta, wyłączenie konta, usunięcie zadania).
2.3.7.4. Automatyczne uruchamianie playbooków na podstawie zdefiniowanych warunków (typ zagrożenia, poziom ryzyka, źródło incydentu, spełnienie określonych reguł detekcji).
2.3.7.5. Możliwość ręcznego wyzwalania playbooków przez analityka bezpieczeństwa z poziomu konsoli.
2.3.7.6. Rejestrowanie wszystkich wykonanych akcji w ramach playbooków i remediacji (pełna ścieżka audytowa z czasem, użytkownikiem i wynikiem akcji).
2.3.7.7. Obsługa orkiestracji z zewnętrznymi systemami (SIEM, ITSM, RMM) poprzez API i webhooks.
2.3.8. Secure Remote Shell:
2.3.8.1. Bezpieczne zdalne połączenie do urządzeń końcowych
2.3.8.2. Szyfrowana komunikacja z wykorzystaniem TLS
2.3.8.3. Logowanie zdarzeń dostępu zdalnego
2.3.8.4. Historia poleceń wykonanych zdalnie
2.3.8.5. Wykonywanie skryptów zdalnych (PowerShell, Bash)
2.4. WYKRYWANIE I REAGOWANIE NA ZAKŁÓCENIA SIECIOWE
2.4.1. Wykrywanie skanowania sieci:
2.4.1.1. Detekcja aktywności skanowania portów na urządzeniach
2.4.1.2. Identyfikacja źródeł skanowania (wewnętrzne/zewnętrzne)
2.4.1.3. Analiza pakietów sieciowych
2.4.1.4. Alertowanie przy podejrzanym skanowaniu
2.4.2. Wykrywanie zatrucia sieci:
2.4.2.1. Detekcja ataków ARP poisoning
2.4.2.2. Monitorowanie anomalii w protokołach warstwy drugiej
2.4.2.3. Detekcja prób spoofingu adresów IP
2.4.2.4. Alertowanie przy podejrzanych zmianach routingu
2.4.3. Wykrywanie eksfiltracji tunelu:
2.4.3.1. Detekcja tunelowania danych przez DNS (DNS tunneling)
2.4.3.2. Detekcja tunelowania przez ICMP (ICMP tunneling)
2.4.3.3. Detekcja tunelowania przez HTTP/S
2.4.3.4. Monitoring połączeń do znanych serwerów C2
2.4.3.5. Alertowanie przy ekfiltracji danych

2.4.4. Widoczność sieci na poziomie procesu:
2.4.4.1. Pełna widoczność ruchu sieciowego na poziomie procesu
2.4.4.2. Monitorowanie połączeń wychodzących (DNS, HTTP/S, TCP)
2.4.4.3. Monitoring transferu danych
2.4.4.4. Detekcja anomalii w ruchu sieciowym
2.5. ANALIZA ZACHOWAŃ UŻYTKOWNIKÓW (UBA) I WYKRYWANIE ANOMALII
2.5.1. Widoczność aktywności użytkownika:
2.5.1.1. Pełne logowanie działań użytkownika
2.5.1.2. Monitoring czasów pracy użytkownika
2.5.1.3. Śledzenie zalogowania
2.5.1.4. Raportowanie aktywności użytkownika
2.5.2. Wykrywanie ruchu bocznego
2.5.2.1. Detekcja prób SMB relay
2.5.2.2. Monitorowanie ataków pass-the-hash
2.5.2.3. Analiza ruchu sieciowego dla lateral movement
2.5.2.4. Automatyczne tworzenie alertów
2.5.2.5. Wizualizacja łańcucha ataku
2.5.3. Wykrywanie anomalii:
2.5.3.1. Profilowanie normalnego zachowania użytkownika
2.5.3.2. Profilowanie normalnego zachowania procesu
2.5.3.3. Profilowanie normalnego zachowania hosta
2.5.3.4. Detekcja anomalii w wzorcach behawioralnych
2.5.3.5. Machine Learning dla obsługi anomalii
2.5.3.6. Ocena ryzyka (risk scoring)
2.5.3.7. Integracja z SIEM dla korelacji
2.6. DECEPCJA
2.6.1. Urządzenia końcowe i serwery
2.6.1.1. Tworzenie wirtualnych pułapek będących imitacją realnych urządzeń końcowych
2.6.1.2. Automatyczne konfigurowanie wirtualnych pułapek
2.6.1.3. Monitoring dostępu do wirtualnych pułapek
2.6.1.4. Alertowanie przy każdym dostępie
2.6.1.5. Logowanie wszystkich działań na wirtualnych pułapek
2.6.2. Pliki i dokumenty:
2.6.2.1. Tworzenie plików-pułapek (decoy files) we wrażliwych lokalizacjach
2.6.2.2. Monitorowanie dostępu do plików-pułapek
2.6.2.3. Generowanie alertu przy każdym dostępie
2.6.2.4. Śledzenie propagacji pliku-pułapki
2.6.2.5. Logowanie zawartości odczytanej z pliku
2.6.3. Użytkownicy
2.6.3.1. Tworzenie kont użytkowników-pułapek (honeypots)
2.6.3.2. Monitorowanie logowania się na konta pułapki
2.6.3.3. Alertowanie przy logowaniu na pułapkę
2.6.3.4. Śledzenie całej sesji na koncie pułapki
2.6.3.5. Raportowanie aktywności na koncie pułapki
2.7. IDENTITY THREAT DETECTION AND RESPONSE (ITDR)
2.7.1. Monitorowanie tożsamości i dostępu:
2.7.1.1. Monitoring logowań użytkowników i anomalii w logowaniach
2.7.1.2. Detekcja ataków na poświadczenia (credential attacks)
2.7.1.3. Monitoring zmian uprawnień i roli dostępu
2.7.1.4. Śledzenie aktywności kont
2.7.1.5. Detekcja ataków pass-the-hash i pass-the-ticket
2.7.2. Analiza tożsamości:
2.7.2.1. Profilowanie typowego zachowania konta użytkownika
2.7.2.2. Detekcja anomalii w zachowaniu użytkownika
2.7.2.3. Analiza ryzyka związanego z tożsamością (identity risk scoring)
2.7.2.4. Monitoring anomalii dotyczących lokalizacji i czasów dostępu
2.7.2.5. Detekcja kompromitacji kont

2.7.3. Automatyczne reagowanie na zagrożenia tożsamości:
2.7.3.1. Automatyczne wyłączanie podejrzanych kont
2.7.3.2. Zmuszenie do zmiany hasła na podejrzanych kontach
2.7.3.3. Wyłączanie aktywnych tokenów sesji
2.7.3.4. Wycofanie dostępu do aplikacji i zasobów
2.7.3.5. Izolacja konta z sieci w przypadku potwierdzenia zagrożenia 2.8.
EXTENDED DETECTION AND RESPONSE (XDR) I KORELACJA ZDARZEŃ
2.8.1. Korelacja wielowarstwowa:
2.8.1.1. Korelacja zdarzeń z endpointów, sieci, poczty, tożsamości i SaaS/Cloud
2.8.1.2. Budowa incydentów z powiązanych zdarzeń z wielu źródeł
2.8.1.3. Czasowe i logiczne łączenie zdarzeń
2.8.1.4. Automatyczne tworzenie złożonych alertów XDR
2.8.1.5. Wizualizacja pełnego łańcucha ataku (kill chain)
2.8.2. Zaawansowane reguły detekcji XDR:
2.8.2.1. Budowanie zaawansowanych scenariuszy detekcji obejmujących wiele warstw
2.8.2.2. Obsługa wieloetapowych ataków i Advanced Persistent Threats (APT)
2.8.2.3. Tworzenie custom reguł z wykorzystaniem query language
2.8.2.4. Testowanie i walidacja reguł przed wdrożeniem
2.8.3. Threat Intelligence Integration:
2.8.3.1. Integracja z wewnętrznymi i zewnętrznymi źródłami threat intelligence
2.8.3.2. Automatyczne wzbogacenie alertów o dane z threat intel
2.8.3.3. Monitoring znanych IoCs (Indicators of Compromise)
2.8.3.4. Raportowanie aktualnych zagrożeń i kampanii 2.9.
OCHRONA POCZTY ELEKTRONICZNEJ (EMAIL SECURITY)
2.9.1. Wsparcie dla:
2.9.1.1. Microsoft 365 2.9.1.2. Google Workspace
2.9.2. Filtrowanie wiadomości:
2.9.2.1. Detekcja i blokowanie phishingu
2.9.2.2. Detekcja i blokowanie złośliwych załączników
2.9.2.3. Ochrona przed ransomware w poczcie
2.9.2.4. Filtry antyspamowe
2.9.2.5. Obsługa kwarantanny dla podejrzanych wiadomości
2.9.3. Monitoring ruchu poczty:
2.9.3.1. Monitorowanie wszystkich przychodzących i wychodzących wiadomości
2.9.3.2. Detekcja prób exfiltracji danych przez pocztę
2.9.3.3. Analiza załączników w czasie rzeczywistym
2.9.3.4. Logowanie wszystkich zdarzeń poczty
2.10. FILTROWANIE DOMEN I ZAWARTOŚCI INTERNETOWEJ (DOMAIN FILTERING / WEB CONTENT FILTERING)
2.10.1. Filtrowanie i blokowanie:
2.10.1.1. Blokowanie złośliwych domen
2.10.1.2. Blokowanie fałszywych domen (typosquatting)
2.10.1.3. Blokowanie niepożądanych kategorii zawartości
2.10.1.4. Lista białych i czarnych domen
2.10.1.5. Policy-based blocking na poziomie użytkownika/grupy
2.10.2. Analiza ruchu HTTP/HTTPS:
2.10.2.1. Monitoring wszystkich połączeń HTTP/HTTPS
2.10.2.2. Detekcja oraz blokowanie C2 komunikacji
2.10.2.3. SSL/TLS inspection (gdzie aplikowalne)
2.10.2.4. Raportowanie aktywności web
2.11. BEZPIECZEŃSTWO SAAS I CLOUD (SSPM / CSPM) ORAZ EXTERNAL ATTACK SURFACE MANAGEMENT (EASM)
2.11.1. SaaS Security Posture Management (SSPM):
2.11.1.1. Inwentaryzacja aplikacji SaaS używanych w organizacji
2.11.1.2. Monitorowanie konfiguracji bezpieczeństwa aplikacji SaaS

2.11.1.3. Detekcja nieautoryzowanych aplikacji i shadow IT
2.11.1.4. Analiza uprawnień dostępu do aplikacji
2.11.1.5. Monitoring zmian w uprawnieniach aplikacji
2.11.1.6. Alertowanie niepoprawnej konfiguracji bezpieczeństwa
2.11.2. Cloud Security Posture Management (CSPM):
2.11.2.1. Monitoring konfiguracji bezpieczeństwa w chmurze (AWS, Azure, Google Cloud)
2.11.2.2. Detekcja niewłaściwych konfiguracji zasobów chmurnych
2.11.2.3. Monitoring uprawnień dostępu i roli
2.11.2.4. Detekcja i raportowanie niezgodności z best practices
2.11.2.5. Rekomendacje remediacyjne
2.11.3. External Attack Surface Management (EASM):
2.11.3.1. Odkrywanie zewnętrznych zasobów organizacji dostępnych z Internetu
2.11.3.2. Monitoring ekspozycji danych i wrażliwych informacji online
2.11.3.3. Detekcja podatności w zasobach zewnętrznych
2.11.3.4. Monitoring domeny oraz certyfikatów SSL
2.11.3.5. Alerty o nowych zagrożeniach dla powierzchni ataku
2.12. CENTRALIZED LOG MANAGEMENT (CLM) I FORENSICS
2.12.1. Gromadzenie i przechowywanie logów:
2.12.1.1. Centralized zbieranie logów z endpointów, sieci, poczty, tożsamości i aplikacji
2.12.1.2. Konfigurowalny okres retencji logów
2.12.1.3. Obsługa archiwizacji logów dla długoterminowego przechowywania
2.12.1.4. Natywne przechowywanie danych forensycznych
2.12.2. Analiza i przeszukiwanie logów:
2.12.2.1. Zaawansowane przeszukiwanie logów z wykorzystaniem query language
2.12.2.2. Filtrowanie i sortowanie zdarzeń
2.12.2.3. Analiza trendu zdarzeń w czasie
2.12.2.4. Export logów w standardowych formatach
2.12.3. Raportowanie i compliance:
2.12.3.1. Raportowanie zgodności z wymogami regulacyjnymi (PCI-DSS, HIPAA, GDPR, SOC2)
2.12.3.2. Raporty dla audytorów i inspektorów
2.12.3.3. Automatyczne generowanie raportów
2.13. WSPARCIE TECHNICZNE, SERWISOWE I MANAGED DETECTION & RESPONSE (24/7 MDR)
2.13.1. Managed Detection and Response 24/7
2.13.1.1. 24/7 monitoring i zarządzanie zdarzeniami bezpieczeństwa przez wykwalifikowany zespół
2.13.1.2. Triage alertów i eskalacja incydentów krytycznych
2.13.1.3. Rekomendacje remediacyjne i wsparcie w reagowaniu
2.13.1.4. Możliwość zlecania zdalnych działań dochodzeniowych i remediacyjnych zespołowi
2.13.1.5. Raporty z zagrożeń i trendów cyberbezpieczeństwa
2.13.1.6.
2.13.2. Technical Account Manager (TAM):
2.13.2.2. Konsultacje cykliczne dotyczące bezpieczeństwa
2.13.2.3. Pomoc w planowaniu wdrożenia
2.13.2.4. Wsparcie onboardingu dla zespołu Zamawiającego
2.13.2.5. Raporty periodyczne z działalności i wyników
2.13.2.6. Szkolenia dodatkowo dostępne na żądanie
2.13.2.7. Dostęp do portalu wsparcia z bazą wiedzy

3. WYMAGANIA TECHNICZNE

3.1. KOMPATYBILNOŚĆ SYSTEMÓW OPERACYJNYCH

Platforma musi obsługiwać instalację agenta ochrony na następujących systemach operacyjnych:

3.1.1. Windows XP SP3
3.1.2. Windows Vista SP1
3.1.3. Windows 7 SP1
3.1.4. Windows 8, 8.1
3.1.5. Windows 10
3.1.6. Windows 11
3.1.7. Windows Server 2003

3.1.8. Windows Server 2008
3.1.9. Windows Server 2012
3.1.10. Windows Server 2016
3.1.11. Windows Server 2019
3.1.12. Windows Server 2022
3.1.13. Linux Ubuntu 18.04 i nowsze
3.1.14. Linux Red Hat Enterprise 6.10 I nowsze
3.1.15. Linux Fedora 35 i nowsze
3.1.16. Linux Debian 10.7 i nowsze
3.1.17. Linux CentOS 7 i nowsze
3.1.18. Linux CentOS Stream 8 i nowsze
3.1.19. Linux Rocky 9 I now sze
3.1.20. MacOS 10.15 I nowsze 3.2. WYMAGANIA INFRASTRUKTURALNE

3.2.1. Wdrożenie i instalacja:
3.2.1.1. Wdrażanie w modelu SaaS (cloud)
3.2.1.2. Dostęp do konsoli zarządzającej przez przeglądarkę
3.2.1.3. Obsługa przeglądarek: Chrome, Firefox, Safari, Edge (najnowsze wersje)
3.2.1.4. Szybkie i bezobsługowe wdrożenie agenta na urządzeniach końcowych
3.2.1.5. Automatyczne wykrywanie i wdrażanie agenta na nowych urządzeniach

3.2.2. Wydajność i wykorzystanie zasobów:
3.2.2.1. Lekki agent – maksymalne zużycie RAM: ~250 MB na endpoint
3.2.2.2. Zużycie CPU: 2-5% średnio na endpoint
3.2.2.3. Minimalny wpływ na wydajność systemu
3.2.2.4. Brak konieczności restartów dla aktualizacji
3.2.2.5. Obsługa trybu offline – pełna ochrona bez łączności z serwerem

3.2.3. Przechowywanie i komunikacja danych:
3.2.3.1. Szyfrowana komunikacja między agentami a serwerem zarządzającym (TLS 1.2+)
3.2.3.2. Przechowywanie danych wyłącznie na terytorium UE
3.2.3.3. Architektura zarządzania centralizowana
3.2.3.4. Obsługa rozłączenia i ponownego nawiązania połączenia

5. Pakiet infrastruktury serwerowej, wirtualizacji, macierzy, NAS i kopii zapasowych.

Przedmiotem pakietu jest dostawa, instalacja, konfiguracja i wdrożenie infrastruktury serwerowej oraz pamięci masowej przeznaczonej do uruchamiania i utrzymania systemów cyberbezpieczeństwa wdrażanych w środowisku IT oraz OT/ICS Zamawiającego.
Środowisko obejmie **jeden fizyczny serwer przeznaczony do uruchomienia platformy wirtualizacyjnej oraz maszyn wirtualnych i usług wykorzystywanych przez wdrażane systemy bezpieczeństwa**, wraz z wymaganym oprogramowaniem systemowym, licencjami dostępowymi oraz oprogramowaniem do wirtualizacji.
Serwer będzie stanowił platformę obliczeniową w szczególności dla systemów służących do ochrony, monitorowania, zarządzania i integracji środowiska IT/OT, w tym komponentów wykorzystywanych na styku sieci IT i OT oraz systemów wymagających pracy w środowisku wirtualnym lub kontenerowym.
W ramach pakietu przewiduje się również dostawę i wdrożenie infrastruktury pamięci masowej oraz mechanizmów wykonywania i przechowywania kopii zapasowych, obejmujących macierz dyskową, systemy NAS oraz rozwiązania backupu i deduplikacji, zgodnie ze szczegółowymi wymaganiami określonymi w dalszej części OPZ.
Architektura powinna zapewniać właściwą separację zasobów i systemów przeznaczonych dla środowiska IT oraz OT/ICS, możliwość wykonywania kopii zapasowych maszyn wirtualnych, konfiguracji i danych systemów bezpieczeństwa oraz możliwość dalszej rozbudowy środowiska.

5.1. Zakup serwera fizycznego – 1 szt. wraz z oprogramowaniem systemowym, licencjami dostępowymi oraz oprogramowaniem do wirtualizacji

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	Procesor min. dwunasto-rdzeniowy, x86 - 64 bity, osiągający w testach SPECrate2017_int_base wynik nie gorszy niż 280 punktów dla testu oferowanego modelu serwera w konfiguracji z dwoma 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. 385W
Liczba procesorów	Min. 1 procesor
Pamięć operacyjna	Min. 128GB RDIMM DDR5 Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB.
Sloty rozszerzeń	Min. 3 aktywne gniazda 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/ NVMe. Serwer z możliwością rozbudowy do obsługi min. 10 dysków SFF typu Hot Swap, SAS/SATA/SSD/ NVMe. Zainstalowane min. 2 szt. dysków min. 1,92 TB SSD typu Hot-swap w konfiguracji RAID 1 oraz min. 4 dyski, min. 2,4TB HDD 10 tyś obr. Każdy z dysków
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	Zainstalowana min. 1 karta, 2-portowa 10/25Gbps SFP28 oraz jedna karta 4 portowa 1Gbe
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	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe posiadające dedykowany port RJ45, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI. Wymagana jest ochrona przed uruchomieniem nieautoryzowanego oprogramowania podczas uruchamiania serwera.
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019, 2022 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/dodatkowe oprogramowanie	• Licencje Microsoft Windows Server Standard 2025 lub równoważne, w zakresie wymaganym dla uruchamianych w środowisku wirtualnym systemów i usług objętych zamówieniem • Licencje dostępu klienta **CAL typu USER w ilości 25** szt. zapewniające dostęp użytkowników do usług katalogowych, plikowych i aplikacyjnych w środowisku serwerowym. 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.
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.
Element konfiguracji	**Wymagania minimalne**

5.2. Oprogramowanie do wirtualizacji i wykonywania kopii zapasowych środowiska wirtualnego – 1 kpl.
Dostawa i wdrożenie systemu wirtualizacji w środowisku Zamawiającego wraz ze wsparciem technicznym o parametrach minimalnych jak niżej lub oprogramowanie równoważne

Należy zapewnić licencję lub subskrypcję oprogramowania wirtualizacyjnego obejmującą wszystkie procesory/gniazda procesorowe zainstalowane w jednym fizycznym serwerze aplikacyjnym dostarczanym w ramach pkt 5.1, wraz ze wsparciem technicznym i dostępem do aktualizacji przez okres minimum 36 miesięcy.
Rozwiązanie musi zapewnić możliwość natywnej obsługi wielu instancji maszyn wirtualnych i kontenerów na każdym serwerze fizycznym. Oprogramowanie wirtualizacyjne musi umożliwiać przyszłą rozbudowę środowiska o dodatkowe fizyczne hosty bez konieczności wymiany obecnej platformy wirtualizacyjnej. 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.

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
Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć skonfigurowanie od 1 do co najmniej 12 wirtualnych kart sieciowych.
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'.
Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania przekierowania używanych fizycznych urządzeń zainstalowanych w gniazdach PCI/PCIe serwera wraz z przekierowaniem akceleratorów GPU.
Rozwiązanie wirtualizacyjne musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
Rozwiązanie wirtualizacyjne powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
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)
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.
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.
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.
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.
Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
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.
Oprogramowanie do wirtualizacji musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora.
Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi, również w trybie działającej maszyny, która jest klonowana.
Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
Rozwiązanie wirtualizacyjne musi posiadać wbudowany interfejs programistyczny (API) zapewniający integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
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 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. Rozwiązanie wirtualizacyjne musi posiadać mechanizm zapory sieciowej zarządzanej z poziomu interfejsu administracyjnego, umożliwiającej definiowanie reguł dla hosta, maszyn wirtualnych i kontenerów.. Rozwiązanie wirtualizacyjne musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych. Rozwiązanie powinno umożliwiać eksport, import, przenoszenie i odtwarzanie maszyn wirtualnych oraz kontenerów, w tym możliwość ich przeniesienia na inny kompatybilny host w przypadku przyszłej rozbudowy infrastruktury.. Rozwiązanie wirtualizacyjne musi zapewniać funkcjonalność z poziomu konsoli graficznej przypisywania dla konkretnej maszyny wirtualnej wybranych rdzeni konkretnego procesora lub grupy rdzeni procesorów w serwerze. Rozwiązanie wirtualizacyjne musi zapewniać mechanizmy zwiększające odporność środowiska na awarie w zakresie pojedynczego serwera, w szczególności poprzez obsługę redundantnych interfejsów sieciowych, redundantnego zasilania serwera, mechanizmów RAID, wykonywania kopii zapasowych maszyn wirtualnych i kontenerów oraz możliwość ich odtworzenia na tym samym lub innym kompatybilnym serwerze. W ramach niniejszego zamówienia nie wymaga się utworzenia klastra wysokiej dostępności HA pomiędzy fizycznymi serwerami. Należy dostarczyć licencję dla oferowanego środowiska wirtualnego z wsparciem technicznym na min. 12 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. Wdrożenie wymaga przedstawienia końcowej dokumentacji opisującej infrastrukturę, jej konfigurację i wszelkie dane dostępowe do wszystkich elementów systemu.

Minimalne wymagania techniczne dla systemu backupu środowiska wirtualnego

Wymagane minimalne parametry techniczne
System wspiera kopie zapasowe maszyn wirtualnych, kontenerów i danych z fizycznych hostów
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.
Wsparcie kompresji standard przed wysyłką kopii do magazynu docelowego
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 pozwala na zautomatyzowaną, regularną synchronizację kopii zapasowych między różnymi instancjami systemu backupu w celu przechowywania kopii w kilku niezależnych lokalizacjach
System wspiera bezpieczeństwo logowania przy pomocy technologii “Two Factor Authentication (2FA)” przez GUI oraz “Time-based One Time Passwords (TOTP)”.
System backupu musi umożliwiać współpracę z dodatkowym odłączanym repozytorium danych albo realizację kontrolowanego eksportu/kopiowania kopii zapasowych na wymienne nośniki offline. Zamawiający dopuszcza zarówno nośniki taśmowe, jak i wymienne nośniki dyskowe, pod warunkiem zapewnienia fizycznego odłączenia kopii od środowiska produkcyjnego, szyfrowania danych oraz udokumentowanej procedury odtworzenia.
Dla oferowanego systemu wymagane jest 12 miesięczne wsparcie producenta oprogramowania w zakresie dostępu do poprawek i uaktualnień. W tym samym okresie, wsparcie serwisowe musi być świadczone przez dostawcę rozwiązania, ze zgłoszeniami w trybie dni roboczych i czasem reakcji do 1 dnia roboczego.
Wdrożenie wymaga przedstawienia finalnej dokumentacji opisującej infrastrukturę, jej konfigurację i wszelkie dane dostępowe na poziomie najwyższym do wszystkich elementów systemu. Wdrożenie zakończone będzie min. 16-godzinnym instruktażem stanowiskowym (2 dni robocze) dla zespołu administratorów**.**

5.3 Serwer backupu z usługa deduplikacji -1 szt

Serwer backupu ma być niezależnym fizycznym urządzeniem, którego podstawową rolą jest wykonywanie, przechowywanie, deduplikacja, weryfikacja i odtwarzanie kopii zapasowych. W normalnym trybie pracy nie stanowi aktywnego drugiego węzła klastra HA serwera aplikacyjnego, jednak musi być sprzętowo i programowo przygotowany do awaryjnego, czasowego uruchomienia najważniejszych maszyn wirtualnych i usług krytycznych po awarii podstawowego hosta wirtualizacyjnego.
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	Procesor min. dwunasto-rdzeniowy, x86 - 64 bity, osiągający w testach SPECrate2017_int_base wynik nie gorszy niż 280 punktów dla testu oferowanego modelu serwera w konfiguracji z dwoma 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. 385W
Liczba procesorów	Min. 1 procesor
Pamięć operacyjna	Min. 128 GB RDIMM DDR5 Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB.
Sloty rozszerzeń	Min. 3 aktywne gniazda 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/ NVMe. Serwer z możliwością rozbudowy do obsługi min. 10 dysków SFF typu Hot Swap, SAS/SATA/SSD/ NVMe. Zainstalowane min. 2 szt. dysków min. 960 GB SSD typu Hot-swap w konfiguracji RAID1, oraz min 2x3,84TB SSD Enterprise RAID6
Kontroler	Serwer z możliwością wyposażenia 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.
Interfejsy sieciowe	Zainstalowana min. 2x karty, 2-portowa 10/25Gbps SFP28 oraz jedna karta 4 portowa 1Gbe
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	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe posiadające dedykowany port RJ45, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI. Wymagana jest ochrona przed uruchomieniem nieautoryzowanego oprogramowania podczas uruchamiania serwera.
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019, 2022 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/dodatkowe oprogramowanie	System operacyjny i dodatkowe oprogramowanie serwera backupu muszą być zgodne z oferowanym systemem backupu i deduplikacji oraz umożliwiać przygotowanie serwera do awaryjnego, czasowego uruchomienia wskazanych maszyn wirtualnych. Wykonawca zapewni wszystkie wymagane licencje i komponenty niezbędne do realizacji funkcji backupu oraz awaryjnego uruchomienia usług krytycznych. Dopuszcza się system Linux, Windows Server lub rozwiązanie równoważne, a mechanizm awaryjnej wirtualizacji musi być zgodny z platformą zastosowaną na hoście podstawowym albo zapewniać udokumentowaną możliwość odtworzenia i uruchomienia kopii maszyn wirtualnych bez konwersji powodującej utratę funkcjonalności.
Wsparcie techniczne	Minimum 3-letnia gwarancja producenta w miejscu instalacji. Czas reakcji NBD.
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.

5.4. Zakup serwera NAS -1 szt

Celem wdrożenia sieciowej pamięci masowej NAS jest zapewnienie bezpiecznego, wydajnego i centralnego repozytorium do przechowywania kopii zapasowych danych, konfiguracji, maszyn wirtualnych, systemów serwerowych oraz wybranych zasobów środowiska IT i OT Zamawiającego

Opis wymagania	**Wymagania minimalne**
Procesor	Procesor 64-bitowy x86 o bazowym taktowaniu nie mniejszym niż 2.0 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8 GB
Pamięć Flash	Nie mniej niż 4GB
Liczba zatok na dyski twarde	Minimum 4
Obsługiwane dyski twarde	3,5-calowe, 2,5-calowe
Złącza M.2	Minimum 2 x M.2 2280 PCIe Gen 3 x1
Pojemność dysków twardych	możliwość stosowania dysków o pojemnościach do 24TB, **zainstalowane min. 4 dyski twarde kompatybilne z oferowanym urządzeniem, każdy o pojemności min. 12 TB**
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2

Porty LAN 2,5 GbE	Minimum 2
Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2 Gen 2	Minimum 2
Porty USB 2.0	Minimum 2
Port PCiE	Tak, minimum 1 Gen 3
Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40℃
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Maksymalnie 90W, 100-240 V
Specyfikacja oprogramowania	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Szyfrowanie wolumenów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box

Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	**Minimum 36 mieś.**

5.5. Zakup macierzy dyskowej -1 szt

Lp	Cecha	Opis Wymagań
1)	Obudowa	Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Obudowa kontrolerów o wysokości nie większej niż 2U musi pozwalać na instalację min 12 dysków 3.5”.

Lp	Cecha	Opis Wymagań
		Obudowa kontrolerów musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów (tego elementu) bez konieczności wyłączania macierzy.
2)	Dyski	**Zainstalowane 6 dysków każdy NL-SAS 8TB 7.2k oraz 5 dysków każdy SSD SAS 480 GB.** **Wymagana możliwość rozbudowy do min. 30 dysków. Rozbudowa musi być wykonywana w sposób online, bez przerwy w dostępie do danych.**
3)	Zabezpieczenia dyskami SPARE	Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.
4)	Pamięć Cache	Co najmniej 32GB pamięci cache RAM na całą macierz (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub podtrzymanie bateryjne min 72h.
5)	Dostępne porty front-end	Razem kontrolery muszą udostępnić do hostów minimum 8 portów 1Gb Eth RJ45, 4 porty 10Gb Eth SFP+ (wymagane wkładki optyczne). Wymagana możliwość rozbudowy o dodatkowe 8 portów 25Gb Eth lub 10Gb Eth tylko poprzez instalację kart sieciowych w oferowanej obudowie kontrolerów. Karty sieciowe muszą być hot-swap, tzn w przypadku awarii muszą umożliwiać wymianę bez konieczności zatrzymywania pracy urządzenia, zatrzymywania dostępu do danych pozostałymi kartami i portami oraz bez konieczności wyjmowania całego kontrolera. Wymóg nie dotyczy portów wbudowanych. Wymagane dostarczenie odpowiedniej liczby 3 metrowych przewodów OM3.
6)	Porty front-end Ethernet	Wymagana możliwość agregowania portów (bond port) oraz tworzenia VLANów na portach.
7)	Obsługiwane protokoły	Wymagane wsparcie dla FC, iSCSI, NFS, CIFS. Nie dopuszcza się wsparcia dla protokołów plikowych poprzez zastosowanie dodatkowego gateway'a / główki NAS. Protokoły NFS i CIFS muszą być natywnie wspierane przez oferowaną macierz.
8)	Obsługiwane typy zabezpieczenia RAID	Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków bez utraty danych. Macierz musi umożliwiać konfigurację RAID tolerującą jednoczesną awarię 3 dysków bez utraty danych.
9)	Prezentacja dysków logicznych	Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Wymagane dostarczenie w/w funkcjonalność na zainstalowana przestrzeń dyskową. Liczba wolumenów blokowych (LUN) obsługiwanych przez macierz nie może być mniejsza niż 2000. Liczba file system'ów (NAS) obsługiwanych przez macierz nie może być mniejsza niż 500.
10)	Zarządzanie	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS. Wymagana możliwość definiowania polityk logowania oraz tworzenia użytkowników w oparciu o role. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane.

Lp	Cecha	Opis Wymagań
		Wymagany min 1 port 1Gb Eth RJ45 per kontroler dedykowany do zarządzania macierzą.
11)	Kopie wewnątrz macierzy	Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) wolumenów blokowych (LUN) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych lub testów. Snapshoty muszą być wykonywanie w technologii ROW (Redirect On Write). Macierz musi umożliwiać utworzenie min 500 snapshotów wolumenów blokowych (LUN) oraz min 500 snapshotów file systemów. Wymagane wsparcie dla snapshotów kaskadowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów których nie można modyfikować ani usunąć przez wybrany okres czasu (zdefiniowany przez administratora) bez odpowiednich uprawnień celem zabezpieczenia i przywrócenia danych w przypadku ataku ransomware. Tworzenie na żądanie pełnej kopii danych źródłowego wolumenu LUN na docelowym wolumenie LUN, w przypadku uszkodzenia danych na źródłowym wolumenie LUN możliwe jest ich odzyskanie z woluminu docelowego. Dostarczenie powyższych funkcjonalności jest wymagane na całą przestrzeń dyskową.
12)	Usuwanie danych	Wykonywanie na żądanie trwałego usuwania danych, uniemożliwiając ich odzyskanie. Funkcjonalność musi wspierać standard DoD 5220.22-M. Dostarczenie licencji powyższych funkcjonalności jest wymagane.
13)	Kontrola zasobów plikowych (NAS)	Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. Dostarczenie licencji powyższych funkcjonalności jest wymagane.
14)	Replikacja danych	Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybach synchroniczna oraz asynchroniczna przy wykorzystaniu portów FC lub IP. Dostarczenie licencji tej funkcjonalności jest wymagane.
15)	Klaster macierzowy	Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). Macierz musi dostarczać funkcjonalność klastra "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych przy wykorzystaniu portów FC lub IP pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodującej dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automated failover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną. Dopuszcza się zastosowanie tzw arbitra czyli serwer quorum w postaci serwera fizycznego lub maszyny wirtualnej.

Lp	Cecha	Opis Wymagań
		Nie dopuszcza się rozwiązań przy użyciu dodatkowych wirtualizatorów lub urządzeń pośredniczących typu Gateway. Dostarczenie licencji na opisaną funkcjonalność jest wymagana.
16)	Priorytety zadań	Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o próg wydajności IOPS. Musi istnieć możliwość określenia polityk QoS na poziomie wolumenów (LUN). Dostarczenie tej funkcjonalności jest wymagane.
17)	Wspierane systemy operacyjne	Wsparcie, dla co najmniej Microsoft Server Windows 2025, VMware 8.x, RedHat Linux, Oracle Linux, CentOS.
18)	Serwis gwarancja	Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż w 2026 roku i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP. Usługi gwarancyjne muszą być świadczone przez producenta lub autoryzowanego przedstawiciela producenta posiadającego co najmniej certyfikat ISO 9001 na świadczenie usług serwisowych. Urządzenie musi zostać objęte **minimum 36 miesięcznym** okresem gwarancji w trybie 9x5 NBD onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. W przypadku awarii dysków uszkodzone nośniki pozostają u Zamawiającego. Macierz musi posiadać możliwość upgradeu firmware-u kontrolerów bez przerywania dostępu do danych. Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania. Urządzenie musi umożliwiać zdalne zarządzanie. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków: • możliwość pobierania najnowszego firmware. • dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń. • dostęp do centrum pomocy technicznej producenta. • otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware. • otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.

5.6. Napęd streamer i/lub kasety do streamera / równoważny system wymiennych nośników offline – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i uruchomienie systemu wykonywania kopii offline. Dopuszcza się pojedynczy napęd taśmowy LTO wraz z nośnikami albo system wymiennych nośników dyskowych klasy RDX jako rozwiązanie równoważne funkcjonalnie. W obu wariantach komplet musi obejmować urządzenie bazowe oraz minimum 5 wymiennych nośników o pojemności użytkowej/natywnej minimum 5 TB każdy, szyfrowanie kopii, możliwość fizycznego odłączenia i przechowywania nośników poza serwerownią, udokumentowaną rotację nośników, trwałość archiwalną minimum 10 lat oraz wykonanie i udokumentowanie testu odtworzenia. Zamawiający nie wskazuje konkretnego producenta.

System będzie stanowił dodatkową, fizycznie odłączaną warstwę ochrony danych, niezależną od podstawowego repozytorium kopii zapasowych oraz pamięci NAS, umożliwiającą przechowywanie części kopii poza systemami stale podłączonymi do sieci.
System musi umożliwiać ręczne wyjęcie nośnika po zakończeniu zadania backupu oraz jego przechowywanie w bezpiecznym miejscu, w tym poza pomieszczeniem serwerowni.

Parametr	**Wymaganie minimalne**
Rodzaj rozwiązania	system wymiennych dyskowych nośników backupowych
Liczba obsługiwanych nośników jednocześnie	min. 1
Sposób wymiany	ręczna wymiana nośnika bez konieczności demontażu urządzenia
Interfejs	**USB 3.0 lub nowszy**
Przepustowość interfejsu	minimum 5 Gb/s
Prędkość transferu danych	minimum **150 MB/s**, zależnie od zastosowanego nośnika
Obsługiwana pojemność pojedynczego nośnika	minimum **5 TB**
Kompatybilność	systemy Linux oraz Windows
Sposób prezentacji nośnika	standardowe urządzenie pamięci masowej dostępne dla systemu operacyjnego
Zasilanie	kompletne, zgodne z oferowanym urządzeniem
Wykonanie	zewnętrzne; dopuszcza się urządzenie desktop/tabletop
Gwarancja	minimum **36 miesięcy**

W ramach kompletu Wykonawca dostarczy:
minimum 5 **szt**. wymiennych nośników o pojemności **minimum 5 TB** każdy.
Każdy nośnik musi:

1. być zgodny z dostarczonym urządzeniem bazowym;
2. posiadać pojemność użytkową/natywną minimum 5 TB;
3. stanowić fizycznie wymienny i odłączalny nośnik danych;
4. być przeznaczony przez producenta do wielokrotnego wykonywania kopii zapasowych i archiwizacji;
5. posiadać obudowę zabezpieczającą nośnik podczas transportu i przechowywania;
6. umożliwiać wielokrotną wymianę pomiędzy kompatybilnymi urządzeniami systemu;
7. umożliwiać przechowywanie offline bez konieczności podłączenia do zasilania;
8. zapewniać możliwość jednoznacznego fizycznego oznakowania nośnika;
9. posiadać deklarowaną przez producenta trwałość archiwalną minimum 10 lat w warunkach przechowywania zgodnych z wymaganiami producenta.

Integracja z systemem kopii zapasowych

- Wykonawca zobowiązany jest skonfigurować rozwiązanie w taki sposób, aby wymienne nośniki mogły być wykorzystywane jako dodatkowa warstwa przechowywania kopii zapasowych tworzonych w środowisku Zamawiającego.
- System musi umożliwiać wykorzystanie nośników przez środowisko Linux i rozwiązanie backupowe zastosowane przez Zamawiającego.
- Kopie przechowywane na wymiennych nośnikach muszą być zabezpieczone przed odczytem przez osoby nieuprawnione.
- Wymagane jest zastosowanie: szyfrowania danych minimum AES-256 lub mechanizmu równoważnego realizowanego przez system backupowy, system operacyjny albo rozwiązanie dostarczane z systemem wymiennych nośników.

Dokumentacja
Wykonawca przekaże dokumentację zawierającą co najmniej:

- opis urządzenia;
- numery seryjne urządzenia i nośników;

- sposób podłączenia do serwera backupowego;
- konfigurację systemu;
- sposób montowania i odmontowywania nośnika;
- procedurę wykonywania kopii;
- procedurę odtworzenia;
- procedurę rotacji;
- sposób szyfrowania;
- sposób zabezpieczenia kluczy;
- zasady przechowywania nośników;
- schemat jednoznacznego oznakowania nośników offline, np. NOŚNIK-01–NOŚNIK-05;
- procedurę postępowania w przypadku uszkodzenia nośnika;
- procedurę okresowego testowania kopii

6. Pakiet zarządzania tożsamością, dostępem i hasłami

Przedmiotem pakietu jest wdrożenie funkcji zarządzania tożsamością, dostępem i poświadczeniami z wykorzystaniem posiadanej usługi katalogowej Active Directory, centralnego menedżera haseł oraz mechanizmów MFA zintegrowanych z UTM/NGFW, NAC/RADIUS i dostępem administracyjnym.
Celem wdrożenia jest w szczególności:

- uporządkowanie procesu zarządzania cyklem życia kont użytkowników;
- ograniczenie liczby kont nieaktywnych, zbędnych i nadmiarowych;
- wdrożenie zasady minimalnych uprawnień;
- zapewnienie kontrolowanego delegowania czynności administracyjnych;
- automatyzacja powtarzalnych operacji związanych z zarządzaniem kontami;
- wdrożenie mechanizmu okresowych przeglądów i recertyfikacji uprawnień;
- zapewnienie rozliczalności czynności wykonywanych przez administratorów i operatorów systemu.

Okres licencji, wsparcia technicznego i prawa do aktualizacji systemu **– minimum 12 miesięcy**.

Wymagane jest co najmniej: centralne zakładanie i wyłączanie kont, przypisywanie użytkowników do grup i ról, delegowanie uprawnień administracyjnych, ewidencja zmian, okresowy przegląd uprawnień, integracja z AD/LDAP oraz możliwość stosowania MFA dla dostępu uprzywilejowanego i zdalnego.

6.2. Centralny menedżer haseł – 1kpl.
Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja, wdrożenie, uruchomienie oraz udokumentowanie centralnego systemu służącego do bezpiecznego przechowywania, organizowania i współdzielenia haseł, poświadczeń oraz innych danych uwierzytelniających wykorzystywanych przez pracowników i administratorów Zamawiającego.
System będzie wykorzystywany przede wszystkim do bezpiecznego przechowywania i kontrolowanego współdzielenia poświadczeń do systemów, urządzeń, usług sieciowych i aplikacji działających w środowisku IT oraz wybranych elementach OT Zamawiającego.
System nie zastępuje usługi katalogowej Active Directory ani systemu zarządzania cyklem życia tożsamości użytkowników.
1. Wymagania ogólne

1. System musi być rozwiązaniem umożliwiającym bezpieczne przechowywanie i współdzielenie haseł i danych uwierzytelniających.
2. System musi być dostępny w wersji open source pozwalającej Zamawiającemu na samodzielne utrzymywanie rozwiązania.
3. System musi umożliwiać instalację lokalną w infrastrukturze Zamawiającego.
4. Korzystanie z podstawowych funkcji systemu nie może wymagać przechowywania haseł i sekretów w chmurze producenta.
5. System musi posiadać interfejs użytkownika i administratora dostępny za pomocą przeglądarki internetowej.
6. Dostęp do systemu musi być zabezpieczony protokołem HTTPS.

7. W przypadku rozwiązania open source Wykonawca będzie odpowiedzialny za wdrożenie, konfigurację oraz świadczenie wsparcia technicznego przez okres wskazany w OPZ.

2. Przechowywanie poświadczeń

8. System musi umożliwiać przechowywanie co najmniej:
- nazwy zasobu;
- nazwy użytkownika;
- adresu URL;
- hasła;
- opisów lub notatek;
- kodów TOTP, jeżeli funkcja ta jest dostępna w zaoferowanej wersji;
- dodatkowych danych związanych z chronionym zasobem.

9. System musi umożliwiać logiczne organizowanie przechowywanych danych, np. za pomocą folderów lub równoważnego mechanizmu.
10. System musi posiadać generator bezpiecznych losowych haseł.
11. System musi umożliwiać wyszukiwanie zapisanych poświadczeń.
12. System musi umożliwiać kopiowanie danych uwierzytelniających do schowka użytkownika.
13. System musi umożliwiać automatyczne wypełnianie formularzy logowania w obsługiwanych przeglądarkach za pomocą rozszerzenia przeglądarkowego lub mechanizmu równoważnego.

3. Współdzielenie i kontrola dostępu

14. System musi umożliwiać współdzielenie wskazanych poświadczeń pomiędzy uprawnionymi użytkownikami.
15. System musi umożliwiać współdzielenie zasobów z:
- pojedynczym użytkownikiem;
- grupą użytkowników.

16. System musi umożliwiać nadawanie zróżnicowanych poziomów uprawnień do współdzielonych zasobów, obejmujących co najmniej możliwość:
- odczytu;
- modyfikacji;
- zarządzania sposobem udostępnienia zasobu.

17. System musi umożliwiać tworzenie grup użytkowników i wykorzystywanie ich podczas udostępniania poświadczeń.
18. Odebranie użytkownikowi uprawnienia do zasobu musi powodować utratę możliwości dalszego pobierania chronionego sekretu z systemu.

4. Bezpieczeństwo i kryptografia

19. System musi realizować szyfrowanie przechowywanych sekretów.
20. Rozwiązanie musi stosować mechanizm szyfrowania end-to-end lub równoważny, w którym dostęp do jawnej postaci sekretu posiada wyłącznie uprawniony użytkownik.
21. System powinien wykorzystywać standardowe i publicznie udokumentowane mechanizmy kryptograficzne.
22. Dla rozwiązania referencyjnego wymagane jest wykorzystanie mechanizmu opartego na OpenPGP.
23. Każdy użytkownik musi posiadać indywidualny mechanizm kryptograficzny pozwalający na uzyskanie dostępu do udostępnionych mu sekretów.
24. Serwer aplikacyjny nie może przechowywać chronionych haseł użytkowników w jawnej postaci.
25. System musi umożliwiać uwierzytelnianie wieloskładnikowe użytkownika co najmniej za pomocą kodów TOTP albo mechanizmu równoważnego dostępnego w zaoferowanej wersji.

5. Dostęp użytkowników

26. System musi posiadać rozszerzenie lub aplikację dla współczesnych przeglądarek internetowych umożliwiającą dostęp do poświadczeń.
27. Rozszerzenie przeglądarkowe musi umożliwiać co najmniej:
- wyszukiwanie poświadczeń;
- korzystanie z zapisanych danych logowania;
- tworzenie i edycję wpisów;
- automatyczne wypełnianie danych uwierzytelniających.

28. System powinien posiadać aplikację mobilną dla systemów Android oraz iOS.
29. Aplikacja mobilna musi umożliwiać bezpieczny dostęp do danych udostępnionych danemu użytkownikowi.

6. Import, eksport i migracja danych

30. System musi posiadać mechanizm importu danych umożliwiający migrację poświadczeń z powszechnie stosowanych systemów lub formatów.
31. System musi umożliwiać wykonanie eksportu danych lub utworzenie kopii pozwalającej Zamawiającemu na migrację do innego systemu.
32. W przypadku dostępności zarówno jawnego, jak i szyfrowanego formatu eksportu, preferowany musi być format szyfrowany.
33. Możliwość wykonania jawnego eksportu danych powinna być ograniczona do uprawnionych użytkowników lub możliwa do wyłączenia przez administratora, jeżeli zaoferowana wersja rozwiązania posiada taką funkcjonalność.

7. Administracja

34. System musi umożliwiać administratorowi co najmniej:

- tworzenie lub zapraszanie użytkowników;
- aktywowanie kont;
- blokowanie lub usuwanie użytkowników;
- tworzenie grup;
- zarządzanie członkostwem grup;
- nadawanie uprawnień administracyjnych.

35. System musi umożliwiać wykorzystanie serwera SMTP Zamawiającego do przesyłania wymaganych wiadomości systemowych.
36. System musi posiadać mechanizm sprawdzania stanu i poprawności działania podstawowych komponentów aplikacji.
37. System musi generować logi umożliwiające diagnostykę oraz analizę zdarzeń związanych z działaniem aplikacji.
38. Jeżeli zaoferowana wersja systemu umożliwia rejestrowanie operacji związanych z dostępem lub modyfikacją sekretów, mechanizm ten musi zostać włączony i skonfigurowany przez Wykonawcę.

8. API i automatyzacja

39. System musi posiadać udokumentowany interfejs API lub równoważny mechanizm integracyjny pozwalający na automatyzację wybranych czynności.
40. API powinno umożliwiać wykonywanie operacji związanych co najmniej z użytkownikami, grupami oraz zasobami, w zakresie udostępnionym przez zaoferowaną wersję systemu.
41. Komunikacja z API musi być zabezpieczona mechanizmami uwierzytelniania oraz szyfrowaną transmisją.

9. Wymagania instalacyjne

42. System musi umożliwiać instalację na systemie Linux.
43. System musi umożliwiać wdrożenie w środowisku kontenerowym Docker lub równoważnym albo w postaci klasycznej instalacji serwerowej.
44. Baza danych systemu musi znajdować się w infrastrukturze Zamawiającego.
45. System musi posiadać możliwość działania bez konieczności wykorzystywania chmurowej usługi przechowywania sekretów producenta.
46. System musi umożliwiać wykonywanie kopii zapasowych obejmujących wszystkie elementy niezbędne do odtworzenia działania aplikacji, w szczególności:

- bazę danych;
- konfigurację;
- klucze kryptograficzne serwera;
- pliki aplikacji wymagające zachowania.

10. Zakres wdrożenia

47. Wykonawca wykona co najmniej:

- instalację systemu w infrastrukturze Zamawiającego;
- instalację i konfigurację wymaganej bazy danych;
- konfigurację HTTPS i certyfikatu;
- konfigurację SMTP;
- konfigurację podstawowej struktury użytkowników i grup;
- konfigurację polityki dostępu;
- konfigurację MFA;
- konfigurację mechanizmu kopii zapasowych;
- wykonanie testu odtworzenia systemu;

- konfigurację logowania zdarzeń;
- aktualizację rozwiązania do aktualnej stabilnej wersji.

48. Wykonawca przygotuje dokumentację powdrożeniową zawierającą co najmniej:
- opis architektury;
- opis konfiguracji;
- procedurę tworzenia użytkowników i grup;
- procedurę nadawania i odbierania dostępu;
- procedurę wykonywania kopii zapasowej;
- procedurę odtworzenia systemu;
- procedurę aktualizacji.

49. Wykonawca przeprowadzi instruktaż administratorów Zamawiającego z obsługi i administracji rozwiązaniem.
50. Wykonawca zapewni minimum **12 miesięcy wsparcia technicznego** dla wdrożonego systemu, obejmującego co najmniej pomoc w diagnozowaniu błędów, instalowaniu aktualizacji i usuwaniu problemów z konfiguracją.
51. W przypadku rozwiązania open source wymagane wsparcie może być świadczone przez Wykonawcę i nie musi oznaczać zakupu komercyjnej subskrypcji producenta.

7. Pakiet bezpiecznego dostępu do środowiska OT/ICS

Zakres obejmuje rozwiązania techniczne i organizacyjne służące zabezpieczeniu dostępu administracyjnego, serwisowego i diagnostycznego do środowiska OT/ICS, w tym stacji operatorskich, systemów SCADA, komputerów inżynierskich, urządzeń telemetrycznych, sterowników, sieci przemysłowych i urządzeń bezpieczeństwa OT. Rozwiązanie powinno obejmować co najmniej mechanizmy separacji dostępu, kontrolowanego połączenia ze środowiskiem OT, stacji przesiadkowej lub równoważnego mechanizmu dostępu pośredniego, rejestrowania i audytowania połączeń, ograniczania dostępu wyłącznie do uprawnionych osób oraz stosowania zatwierdzonych okien serwisowych. Dla styku IT/OT dopuszcza się zastosowanie mechanizmów jednokierunkowego transferu danych lub innych rozwiązań ograniczających ryzyko nieuprawnionej komunikacji do środowiska operacyjnego. Wskazane w części opisowej WoD bramy jednokierunkowe nie posiadają odrębnej pozycji kosztowej w aktualnym budżecie i nie stanowią obowiązkowej dostawy w niniejszym OPZ; architektura powinna jednak umożliwiać ich późniejsze włączenie po formalnym zabezpieczeniu finansowania.

7.1. System stacji przesiadkowych / bezpiecznego dostępu – 2 role: 1 fizyczna stacja OT + 1 wirtualny jump host/bastion IT/DMZ

element	Wymagane minimalne parametry techniczne komputerów
Komputer	Komputer będzie wykorzystywany jako dedykowana stacja przesiadkowa do bezpiecznego, kontrolowanego dostępu administracyjnego i serwisowego do systemów środowiska OT/ICS, w szczególności systemów SCADA, HMI, serwerów i urządzeń infrastruktury technologicznej. Stacja nie jest przeznaczona do standardowej pracy biurowej, korzystania z poczty elektronicznej ani swobodnego dostępu do Internetu. W ofercie należy podać nazwę producenta, typ, model oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.
Obudowa	Obudowa typu tower umożliwiająca montaż minimum trzech dysków SATA. Dioda LED na przednim panelu, sygnalizująca działanie komputera. Obudowa trwale oznaczona nazwą producenta, numerem seryjnym.
Chipset	Dostosowany do zaoferowanego procesora
Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji) oraz wspierająca konfigurację RAID dla dysków HDD i NVMe. Płyta główna wyposażona w złącza: - min. 4x SATA - min. 4x M.2 w tym 3x złącze M.2 obsługujące dyski PCIe oraz 1x dla karty WLAN. Płyta główna zawierająca następujące gniazda PCIe dla kart rozszerzeń: - 1x PCIe 5.0 x16

	- 1x PCIe 4.0 x16 - 2x PCIe 3.0 x1
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych lub stacjach roboczych klasy x86, o wydajności min. 49 000 puntków na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Pamięć operacyjna	Min. 32 GB DDR5 5600 Min. 4 sloty na pamięć RAM Możliwość rozbudowy pamięci RAM do min. 256 GB
Dysk twardy	Min. 1 TB SSD M.2 PCIe 4.0, wspierający sprzętowe szyfrowanie dysku OPAL. Oferowany model urządzenia musi obsługiwać min. 5 dodatkowych dysków HDD lub SSD w dowolnej konfiguracji.
Karta graficzna	Zintegrowana
Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowany głośnik o mocy min. 2W.
Sieć	Karta sieciowa LAN obsługująca prędkości 10/100/1000 z obsługą Wake-on-LAN
Porty/złącza	Z przodu obudowy: - 1x USB 3.2 typu C - 4x USB 3.2 typu A - 1x port audio combo - 1x port audio in (mikrofonowy) - 1x Czytnik kart pamięci Z tyłu obudowy: - 2x USB 2.0 typu A - 2x USB 3.2 typu A - 1x HDMI 2.1 - 2x DisplayPort 1.4 - port sieciowy RJ-45 - port audio out Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
Zasilacz	Energooszczędny zasilacz o mocy nie mniejszej niż 750W oraz sprawności na poziomie min. 92% posiadający certyfikat 80 PLUS.
Klawiatura	Klawiatura USB
Mysz	Mysz optyczna USB z klawiszami oraz rolką (scroll).
System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,

	7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM

	33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera, - numerze seryjnym, - numerze inwentarzowym (AssetTag), - wersji BIOS, - dacie produkcji BIOS - zainstalowanym procesorze wraz z taktowaniem, - zainstalowanej pamięci RAM wraz z taktowaniem, - dyskach podłączonych do złącz M.2 oraz SATA Administrator z poziomu BIOS musi mieć możliwość: - wyłączenia portów USB - wyłączenia karty sieciowej - wyłączenia karty audio - wyłączenia funkcji Wake on LAN - wyłączenia wirtualizacji - wyłączenia modułu TPM - ustawienia hasła: administratora, Power-On, dysku twardego - wyboru trybu uruchomienia komputera po utracie zasilania - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania sekwencji bootowania - załadowania optymalnych ustawień BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych
Zintegrowany System Diagnostyczny	Zaimplementowany w UEFI BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System obsługiwany za pomocą myszy lub

	klawiatury, umożliwiający wykonanie minimum następujących czynności diagnostycznych: 1. Wykonanie testu komponentów w zakresie przyspieszonym lub rozszerzonym z możliwością wyboru algorytmów testowania oraz liczby cykli testowych do przeprowadzenia. System diagnostyczny powinien umożliwiać wykonanie testu następujących komponentów: - pamięci ram, - procesora, - pamięci masowej, - płyty głównej - portów USB. 2. Identyfikację jednostki i jej komponentów w następującym zakresie: - urządzenie (producent, model, numer seryjny), - bios (wersja oraz data wydania), - procesor (nazwa, taktowanie, ilości pamięci L1, L2, L3, liczba rdzeni), - pamięć ram (ilość zainstalowanej pamięci ram, producent oraz numer seryjny), - dysk twardy (producent, model, numer seryjny, pojemność), - płyta główna (liczba złącz USB, liczba złącz PCI)
Certyfikaty i standardy	Dla producenta sprzętu - ISO 9001 - ISO 14001 - ISO 50001 Dla komputera: - EPEAT Gold dla kraju Unii Europejskiej według danych widocznych na stronie https://epeat.net/search-computers-and-displays - TCO min. 10.0 dostępne na stronie https://tcocertified.com/product-finder - Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
Bezpieczeństwo	- Złącze typu Kensington Lock - Oczko na kłódkę zabezpieczającą urządzenie przed nieautoryzowanym otwarciem -Moduł TPM 2.0 z certyfikacją TCG oraz FIPS 140-2
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.
Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji. Oprogramowanie musi być wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane.
Gwarancja i wsparcie techniczne producenta	**Min. 36 miesięcy świadczona w miejscu użytkowania sprzętu (on-site).** Firma serwisująca posiadająca certyfikat ISO 9001:2000 na świadczenie usług serwisowych. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej: - fabrycznej konfiguracji urządzenia, - rodzaju gwarancji, - dacie wygaśnięcia gwarancji,

	- aktualizacjach. Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera.
Oprogramowanie biurowe	Pakiet oprogramowania biurowego Microsoft Office w języku polskim w wersji 64-bit lub równoważny, zawierający co najmniej następujące składniki: edytor tekstu, arkusz kalkulacyjny, oprogramowanie do przygotowywania i prowadzenia prezentacji, klienta poczty elektronicznej, wraz z udzieleniem Zamawiającemu 1 (jednej) licencji komercyjnej na czas nieokreślony na 1 (jedno) stanowisko komputerowe; Za równoważne Zamawiający uzna oprogramowanie biurowe w pełni obsługujące wszystkie istniejące dokumenty Zamawiającego, wytworzone przy użyciu oprogramowania Microsoft Office: 2003, 2007, 2010 i 2013 bez utraty jakichkolwiek ich parametrów i cech użytkowych (odpowiednio dla pakietu oprogramowania: pliki tekstowe, dokumenty, arkusze kalkulacyjne zawierające makra i formularze, prezentacje, itp.), w pełni kompatybilne i zgodne z obecnie zainstalowanym oraz pracującym u Zamawiającego oprogramowaniem biurowym, antywirusowym, narzędziowym, systemowym (dla stacji roboczych i serwerów) pracujących na systemach operacyjnych Microsoft Windows w wersjach 32 i 64 bity, niewymagającym dodatkowych nakładów finansowych ze strony Zamawiającego w celu dostosowania zaoferowanego oprogramowania do ww. systemów. W przypadku złożenia oferty z produktami równoważnymi należy do oferty załączyć dokumenty poświadczające ich równoważność z funkcjonalnością oprogramowania u Zamawiającego. Zaoferowany pakiet oprogramowania biurowego musi spełniać poniższe wymagania minimalne: interfejs użytkownika zaoferowanych pakietów oprogramowania musi być w pełnej polskiej wersji językowej, aktualizacje zabezpieczeń, hot-fixy, services pack'i mają być dostępne z wykorzystaniem wbudowanych, automatycznych narzędzi do ich pobierania z dedykowanej strony internetowej producenta oprogramowania oraz dostępne do pobrania ręcznego z serwerów producenta oprogramowania, zaoferowane oprogramowanie musi być przeznaczone do użytku komercyjnego, Zaoferowany edytor tekstu musi umożliwiać: określenie układu strony (pionowa/pozioma), wydruk dokumentów, wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego, pracę na dokumentach Zamawiającego, utworzonych przy pomocy oprogramowania Microsoft Word 2003, 2007, 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu, zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Zaoferowany arkusz kalkulacyjny musi umożliwiać: tworzenie raportów tabelarycznych, tworzenie wykresów liniowych (wraz z linią trendu), słupkowych, kołowych, tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML), tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, wyszukiwanie i zamianę danych, wykonywanie analiz danych przy użyciu formatowania warunkowego, nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie, nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności, formatowanie czasu, daty i wartości finansowych z polskim formatem,

	zapis wielu arkuszy kalkulacyjnych w jednym pliku, zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, 2007, 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń, zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. Zaoferowane oprogramowanie do przygotowywania i prowadzenia prezentacji multimedialnych musi umożliwiać: drukowanie w formacie umożliwiającym robienie notatek, zapisanie jako prezentacja tylko do odczytu, nagrywanie narracji i dołączanie jej do prezentacji, opatrywanie slajdów notatkami dla prezentera, umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym, możliwość tworzenia animacji obiektów i całych slajdów, prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, zapewniających zgodność z formatami plików utworzonych za pomocą oprogramowania Microsoft PowerPoint 2003, 2007, 2010 i 2013.

Zakres należy zrealizować jako dwie odrębne role odpowiadające: 1) jedna fizyczna stacja przesiadkowa przeznaczona do kontrolowanego dostępu do OT/ICS oraz 2) jedna wirtualna rola jump host/bastion przeznaczona do dostępu administracyjnego do IT/DMZ. Dostęp do OT musi następować wyłącznie przez DMZ, z MFA, rejestracją zdarzeń i możliwością czasowego uruchamiania dostępu serwisowego.

Monitor 27” do stacji przesiadkowej – 1 szt

element	**Wymagania minimalne**
Monitor	Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację monitora
Wielkość ekranu	Przekątna ekranu min. 27”
Matryca	Powłoka matrycy o wykończeniu matowym typu IPS
Nominalna rozdzielczość	Rozdzielczość nie mniejsza niż 2560x1440
Kąty widzenia	Kąty widzenia min. 178 stopni w pionie i w poziomie
Plamka	Wielkość plamki (pojedynczego piksela) nie większa niż 0.24mm
Częstotliwość odświeżania	Minimum w zakresie 50Hz – 115Hz
Jasność	Nie mniejsza niż 350 nitów
Czas reakcji matrycy	Nie większy niż 6 ms
Zakres kolorów	Nie mniejszy niż 99% sRGB Obsługa min. 16,7 miliona kolorów
Kontrast statyczny	Nie mniejszy niż: 1500:1
Porty/złącza	1x HDMI 2.1 1x DisplayPort 1x USB-B Upstream 1x USB-C 15W Power Delivery oraz transfer) downstream 3x USB-A 3.2 gen 1
Waga	Nieprzekraczająca 6.5 kg z podstawą według karty katalogowej producenta
Ergonomia	Możliwość regulacji ustawienia monitora w zakresie: Przód / tył w zakresie min. -5 do 23 stopni Lewo / prawo w zakresie 45 stopni

	Pivot 90 stopni Wysokość do min. 150mm
Obudowa	musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA (100x100)
Bezpieczeństwo	Złącze typu Kensington Lock
Certyfikaty i standardy	Dla producenta sprzętu należy dostarczyć certyfikat: - ISO 9001 - ISO 14001 - ISO 50001 Dla urządzenia: Energy Star TCO min. 10 EPEAT Gold dla kraju Polska według danych widocznych na stronie https://epeat.net/search-computers-and-displays
Ukompletowanie	Kabel HDMI o długości min. 1,8m Kabel zasilający o długości min. 1,8m
Gwarancja na urządzenie	**Minimum 36 miesięcy**

8. Pakiet zasilania awaryjnego dla produktów i rozwiązań bezpieczeństwa

Zakres obejmuje dostawę, montaż, konfigurację i uruchomienie urządzeń zasilania awaryjnego oraz akumulatorów dla kluczowych produktów i rozwiązań z zakresu bezpieczeństwa, w szczególności urządzeń sieciowych, urządzeń UTM/NGFW, przełączników, elementów infrastruktury serwerowej, systemów backupu, urządzeń OT oraz innych komponentów wskazanych przez Zamawiającego.

8.1. Dostawa i uruchomienie mobilnego agregatu prądotwórczego – 1 kpl.

Przedmiotem zamówienia jest dostawa fabrycznie nowego mobilnego agregatu prądotwórczego stanowiącego rezerwowe źródło zasilania dla kluczowych produktów i rozwiązań bezpieczeństwa OT/ICS.

Minimalne wymagania:

1. • **Parametry ogólne**
   - agregat fabrycznie nowy rok produkcji 2026r
   - Moc (zgodnie z ISO8528):
   - Praca podstawowa P.R.P. – nie mniej niż 50 kVA
   - Praca awaryjna ESP/LTP – nie mniej niż 55 kVA
   - Napięcie : 230/400 V, 50 Hz
   - Prąd znamionowy min. 72 A
   - Stopień ochrony prądnicy: IP23
   - Wymiary zewnętrzne maksymalne 2350 x 1020 x 1690 (długość x szerokość x wysokość) mm
   - Podgrzewacz płynu chłodzącego
   - Zintegrowany prostownik baterii rozruchowych
   - Samoczynny start po podaniu sygnału startu
   - Zintegrowany wyłącznik główny prądnicy
   - Wyłącznik awaryjny
   - Pomiar poziomu paliwa w % z odczytem na wyświetlaczu sterownika
   - Zbiornik paliwa zintegrowany z ramą o pojemności min100 l
   - Wersja w obudowie wyciszonej, odpornej na warunki atmosferyczne
   - Gumowe stopy antywibracyjne zamontowane na zewnątrz o spodu obudowy agregatu
   - Dostarczony z płynami eksploatacyjnymi (prócz paliwa)

Agregat musi być wykonany jako rozwiązanie mobilne, bez konieczności wykonywania stałego fundamentu. Zakres dostawy obejmuje komplet przewodów, właściwe złącza, zabezpieczenia, elementy niezbędne do przyłączenia, uruchomienie oraz sprawdzenie współpracy z instalacją Zamawiającego. Przed zamówieniem

urządzenia Wykonawca zweryfikuje w ramach analizy przedwdrożeniowej sposób przyłączenia i bilans mocy. Jeżeli istniejąca instalacja nie posiada właściwego punktu przyłączenia, Wykonawca wskaże ten fakt Zamawiającemu przed zamówieniem agregatu i przedstawi wymagania techniczne niezbędne do wykonania prawidłowego przyłączenia.

8.2. Zestaw zasilania UPS – 2szt UPS 3 kVA oraz wymagane akumulatory

Oferowane urządzenie do bezprzerwowego zasilania musi być fabrycznie nowe i pochodzić z seryjnej produkcji. Producent oferowanego urządzenia powinien posiadać własny certyfikat ISO 9001 oraz 14001 jako potwierdzenie wymagań międzynarodowego standardu jakości. Oferowane urządzenie musi posiadać oznakowanie CE (deklarację zgodności CE załączyć do oferty). Oferent ma obowiązek przedstawienia karty katalogowej producenta urządzenia, karta dystrybutora własnej marki nie jest wystarczającym potwierdzeniem parametrów urządzenia. Nie dopuszczalne urządzenia marki własnej, których paramterów nie można porównać w ogólno-dostepnych materiałach w internecie.

Proponowany UPS 3 kVA musi spełniać poniżej opisane wymagania - nie gorsze niż:

1. Moc wyjściowa UPS 3 kVA / 3 kW
2. Ilość faz wejściowych 1
3. Ilość faz wyjściowych 1
4. Trzy grupy gniazd wyjścioych
   2 grupy programowalne po 2 sztuki x IEC C13
   1 grupa nieprogramowalna 2 x IEC C13; 1 x IEC C19
5. Możliwość instalacji UPS Rack / Tower (akcesoria w zestawie)
6. Wysokość pojedynczego zasilacza UPS powinna wynosić 2U
7. Możliwość opcjonalnej instalacji modułu bypass 2U, ilość gniazd dystrybucyjnych 6 x IEC C13; C19x1; komunikacja z UPS RS232, bypass ze stykiem wyprzedzającym
8. Baterie dobrane dla 3000W obciążenia, wymagany czas podtrzymania min 2,5min / dla 70% obciążenia min 5min
9. Łączna ilość baterii w ramach obudowy UPS min 6 szt. 9Ah.
10. Projektowana żywotność baterii 3-5 lat
11. Zakres napięcia wejściowego: 175V – 280V pełna moc; 120V – 175V obciążenie (70 – 100%)
12. Zniekształcenia harmoniczne prądu wejściowego: <5%
13. Prąd wejściowy 15A
14. Zakres dopuszczalnej częstotliwości wejściowej: 40 – 70Hz
15. Współczynnik szczytu: 3:1
16. Współczynnik mocy wejściowy: >0,99
17. Wyjściowy współczynnik mocy równy: 1
18. Zniekształcenia harmoniczne napięcia wyjściowego: <= 2%
19. Regulacja napięcia wyjściowego: ± 3%
20. Dopuszczalne przeciążenie: < 105% praca ciągła; 106 – 125% 1 min +/- 5 sek; 126 – 150%: 15 +/- 3 sek;
21. Temperatura pracy od 0 do 55 stopni (40 – 50 obniżenie mocy do 90% znamionowej).
22. Urządzenie musi zapewnić ciągłe bezprzerwowe zasilanie w trybie TRUE ON-LINE z podwójną konwersją przy zupełnych lub chwilowych zanikach napięcia i wahaniach częstotliwości w sieci elektrycznej przez cały czas pracy urządzenia.
23. Urządzenie powinno być wyposażone w komunikacyjny wyświetlacz LCD w języku polskim:
    - Napięcie i częstotliwość wejścia
    - Napięcie i częstotliwość wyjścia UPS
    - Obciążenie, prąd, moc kVA,kW wyjścia UPS
    - Status i wynik testu baterii
    - Wartość podtrzymania baterii
24. Zasilacz UPS musi być wyposażony w adapter Web/SNMP IPv6 z Modbus TCP
25. Preferowany kolor obudowy: czarny.

26. Poziom hałasu urządzenia w trybie podwójnego przetwarzania przy obciążeniu znamionowym nie może przekraczać 40 dB w zależności od obciążenia.
27. Stopień ochrony IP20
28. Urządzenie musi mieć możliwość zainstalowania zewnętrznego wyłącznika awaryjnego ppoż. ,który należy dostarczyć wraz z urządzeniem. Miejsce instalacji wyłącznika wskaże Zamawiający.
29. Sprawność w trybie TRUE ONLINE
    min 94% w rybie normalnym do 99% osiągane w ekonomicznym trybie pracy
30. UPS musi posiadać panel komunikacyjny, w którym powinny być zainstalowane:
    - REPO / ROO
    - Gniazda umożliwiającej instalacje karty SNMP/Relay/Modbus
    - USB
    - Gniazdo komunikacji RS-232
    - 4 styki; wejściowy x 1; wyjściowy x 3
31. Oprogramowanie zarządzające z możliwością zamykania systemów operacyjnych poprzez sieć logiczną:
    - Windows 7, 8, 10, 11
    - Windows Server 2012, 2016, 2019
    - Windows Hyper-V Server Core 2016/2019
    - Redhat Linux Exterprise 8.3
    - Orcale Linux 7.1
    - Linux OpenSUSE 11.4
    - Linux ubuntu 10.04, 12.04.5, 16.04, 20.04
    - Citrix XenServer 6.0.0
    - Linux KVM

C) Gwarancja, warunki dostawy i sposób serwisowania

1. **Gwarancja min. 24 miesięcy** od daty uruchomienia urządzeń na obiekcie. Oferent dostarczy pisemną gwarancję producenta urządzenia, gwarancja dystrybutora nie jest wystarczająca. Producent posiada przynajmniej trzech niezależnych partnerów serwisowo – sprzedażowych (potwierdzenie pisemne producenta). Producent posiada oddział na terenie Polski wraz z własnym magazynem części zamiennych oraz serwisem.

9. Pakiet usług wdrożeniowych, dokumentacyjnych, szkoleniowych i utrzymaniowych

9.1. 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 wdrożenia.

9.2. 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 zapewniać odporność na awarie, w szczególności redundancję UTM/NGFW, przełączników, kontrolerów macierzy, zasilania i interfejsów sieciowych oraz wielowarstwowy system kopii zapasowych. Podstawowy zakres obejmuje jeden fizyczny host wirtualizacyjny i oddzielny fizyczny serwer backupu. Serwer backupu musi być przygotowany do awaryjnego, czasowego uruchomienia wskazanych usług krytycznych po awarii hosta podstawowego, zgodnie z przygotowaną i przetestowaną procedurą DR. Nie wymaga się automatycznego dwuwęzłowego klastra hostów, a architektura ma zachować możliwość późniejszej rozbudowy do środowiska wielowęzłowego.

9.3. 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 dwóch serwerów fizycznych o odrębnych rolach: jednego serwera aplikacyjnego/wirtualizacyjnego oraz jednego dedykowanego serwera kopii zapasowych.
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. Instalacji i konfiguracji platformy wirtualizacyjnej na jednym fizycznym serwerze aplikacyjnym oraz konfiguracji mechanizmów kopii zapasowych, odtwarzania, monitorowania i zabezpieczenia środowiska. Architektura ma umożliwiać późniejszą rozbudowę o dodatkowy host bez wymiany platformy wirtualizacyjnej.
6. Instalacja roli RADIUS w systemach zarządzania tożsamością i dostępem.
7. Instalacji i konfiguracji urządzeń brzegowych klasy UTM/NGFW w układzie wysokiej dostępności Active-Passive lub Active-Active, z synchronizacją sesji, monitoringiem stanu urządzeń, łączy i tuneli VPN.
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 dwóch przełączników zarządzalnych pracujących wspólnie w konfiguracji redundantnej (stackowanie, MLAG lub rozwiązanie równoważne), obsługujących wydzielone sieci i VLAN dla IT oraz OT, w tym konfiguracji 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. Wykonania segmentacji sieci zgodnie z uzgodnioną z Zamawiającym polityką bezpieczeństwa, obejmującą separację co najmniej sieci administracyjnej, serwerowej, użytkowników, urządzeń technicznych, Wi-Fi, DMZ, systemów kopii zapasowych oraz stref zarządzania.
11. Stworzenie polityk NAC na urządzeniach sieciowych w oparciu o rozwiązania producenta zapór sieciowych/przełączników.
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 tym odrębnych testów ochrony IT i OT, testów dostępności usług, redundancji UTM/NGFW i przełączników, poprawności routingu i segmentacji, działania polityk firewall/IDS/IPS/VPN, logowania i monitoringu oraz udokumentowanego testu awaryjnego odtworzenia i uruchomienia wskazanej usługi krytycznej na serwerze backupu.
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

9.4. 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.

9.5. 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 VLAN, adresacji IP, routingu, HA, VPN i polityk bezpieczeństwa;
5. opis kont administracyjnych, ról i mechanizmów uwierzytelniania;
6. procedury awaryjne i odtworzeniowe;
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.