Załącznik nr.10 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i wdrożenie rozwiązań IT/OT z zakresu cyberbezpieczeństwa w Zakładzie Usług Komunalnych Sp. z o.o. w Szczucinie

Cyberbezpieczne Wodociągi

Zamawiający

Zakład Usług Komunalnych Sp. z o.o. w Szczucinie
Wola Szczucińska 142
33-230 Wola Szczucińska

Założenia architektury i integracji

Przedmiot Zamówienia obejmuje dostawę i wdrożenie wzajemnie powiązanych komponentów infrastruktury IT/OT, które po zakończeniu realizacji mają tworzyć spójne, centralnie zarządzane, monitorowane i audytowalne środowisko bezpieczeństwa.
Poszczególne pakiety funkcjonalne nie powinny być traktowane jako niezależne wyspy technologiczne. Wykonawca zobowiązany jest zapewnić ich współpracę w zakresie określonym w OPZ, w szczególności wymianę informacji o aktywach, stanie infrastruktury, podatnościach, zdarzeniach bezpieczeństwa oraz incydentach.
Przyjęty model zakłada wykorzystanie otwartych standardów integracyjnych, w szczególności API, Syslog/TLS, SNMPv3, RADIUS, LDAP/Active Directory, SMTP/Webhook oraz innych udokumentowanych mechanizmów właściwych dla dostarczonych rozwiązań. W odniesieniu do centralnego systemu SIEM/SOAR zakres bieżącego licencjonowania i podłączenia obejmuje wyłącznie pięć źródeł określonych w pkt 4.2; pozostałe źródła przewiduje się do przyszłej rozbudowy.
Wdrożenie uważa się za zakończone nie z chwilą dostarczenia urządzeń lub oprogramowania, lecz po ich instalacji, konfiguracji, integracji, wykonaniu wymaganych testów odbiorowych, przekazaniu dokumentacji powdrożeniowej oraz przeprowadzeniu instruktażu administratorów.
W przypadku zastosowania komponentów open source Wykonawca odpowiada za ich prawidłowe wdrożenie, konfigurację, aktualizację i integrację oraz zapewnia wsparcie techniczne w wymaganym w OPZ okresie. Brak komercyjnej licencji producenta nie może ograniczać funkcjonalności wymaganych przez Zamawiającego.

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

Celem Pakietu 1 jest utworzenie spójnej warstwy bezpieczeństwa sieciowego dla środowiska IT oraz OT Zamawiającego. W ramach pakietu należy zapewnić wysokodostępną ochronę brzegu sieci IT, kontrolowany styk IT/OT, segmentację infrastruktury na wydzielone strefy bezpieczeństwa, bezpieczny dostęp zdalny oraz centralną kontrolę dostępu użytkowników i urządzeń do sieci.
Docelowe rozwiązanie obejmuje klaster dwóch urządzeń UTM/NGFW pracujących w trybie HA, przemysłowy firewall zabezpieczający granicę IT/OT, centralne zarządzanie urządzeniami bezpieczeństwa, zarządzalne przełączniki i punkty dostępowe, system NAC/RADIUS oraz mechanizmy VPN i MFA.
System NAC ma stanowić centralny punkt podejmowania decyzji o dostępie, natomiast przełączniki, punkty dostępowe i urządzenia UTM/NGFW będą realizowały egzekwowanie tych decyzji poprzez 802.1X/MAB, przypisanie VLAN, ACL oraz odpowiednie polityki bezpieczeństwa.
Urządzenia UTM/NGFW i firewall IT/OT muszą przekazywać zdarzenia do centralnego systemu logowania w zakresie pięciu źródeł określonych w pkt 4.2. Pozostałe urządzenia i systemy zachowują wymagane funkcje logowania we własnych konsolach oraz monitorowania eksploatacyjnego; ich podłączenie do SIEM przewiduje się do przyszłej rozbudowy.

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

1. Wymagania Ogólne Systemu
System zostanie wykorzystany do zarządzania co najmniej trzema urządzeniami fizycznymi tworzącymi dwa logiczne elementy bezpieczeństwa: klastrem HA dwóch urządzeń UTM/NGFW oraz przemysłowym firewallem zabezpieczającym styk IT/OT, z możliwością rozbudowy o kolejne urządzenia..

System zostanie wykorzystany do zarządzania co najmniej:

- klastrem dwóch urządzeń UTM/NGFW w siedzibie głównej;

- urządzeniem UTM/NGFW w części przemysłowej OT;
- przemysłowym firewallem zabezpieczającym styk IT/OT;
- dodatkowymi urządzeniami, które mogą zostać wdrożone w okresie realizacji projektu.

2. Minimalne wymagania funkcjonalne

System musi:

1. Być dostarczony jako kompletna maszyna wirtualna typu appliance, zawierająca system operacyjny i oprogramowanie zarządzające.
2. Umożliwiać wdrożenie w środowisku wirtualnym Zamawiającego, w szczególności VMware, Hyper-V, KVM, Proxmox lub środowisku równoważnym.
3. Posiadać licencję pozwalającą na zarządzanie minimum pięcioma urządzeniami, węzłami lub klastrami HA, liczonymi zgodnie z zasadami licencyjnymi producenta.
4. Zapewniać centralne zarządzanie co najmniej:
   - regułami filtrowania ruchu;
   - politykami bezpieczeństwa;
   - regułami NAT;
   - obiektami sieciowymi i usługami;
   - interfejsami i strefami bezpieczeństwa;
   - routingiem;
   - konfiguracją VPN;
   - certyfikatami wykorzystywanymi przez urządzenia;
   - aktualizacjami oprogramowania urządzeń;
   - kopiami konfiguracji urządzeń.
5. Umożliwiać tworzenie wspólnych polityk i szablonów konfiguracji dla wielu urządzeń oraz stosowanie indywidualnych parametrów dla poszczególnych lokalizacji.
6. Umożliwiać grupowanie urządzeń według lokalizacji, przeznaczenia oraz obszaru IT lub OT.
7. Zapewniać centralne tworzenie i zarządzanie tunelami VPN site-to-site pomiędzy siedzibą główną, oddziałem oraz chronionymi strefami OT.
8. Prezentować co najmniej:
   - stan połączenia zarządzanych urządzeń;
   - status klastra HA;
   - model i wersję oprogramowania urządzenia;
   - stan licencji i subskrypcji;
   - wynik ostatniego wdrożenia konfiguracji;
   - podstawowy status tuneli VPN.
9. Zapewniać weryfikację konfiguracji przed jej wdrożeniem oraz prezentowanie różnic pomiędzy konfiguracją aktualną i planowaną.
10. Umożliwiać:
    - grupowe wdrażanie zmian;
    - rejestrowanie wyników wdrożenia;
    - przechowywanie historii konfiguracji;
    - przywrócenie wcześniejszej wersji konfiguracji;
    - wykrywanie zmian wykonanych lokalnie na zarządzanym urządzeniu.
11. Zapewniać indywidualne konta administratorów oraz role obejmujące co najmniej:
    - administratora głównego;
    - administratora urządzeń lub grupy urządzeń;
    - użytkownika z dostępem wyłącznie do odczytu.
12. Umożliwiać integrację z usługą katalogową LDAP/Active Directory, RADIUS lub rozwiązaniem równoważnym.
13. Prowadzić dziennik audytowy obejmujący co najmniej:
    - logowania administratorów;
    - zmiany konfiguracji;
    - wdrożenia polityk;
    - zmiany kont i uprawnień;
    - operacje wykonywania i odtwarzania kopii konfiguracji.
14. Umożliwiać eksport logów audytowych do centralnego systemu logowania, platformy SIEM/SOAR lub serwera Syslog.

15. Zapewniać wykonywanie automatycznych i ręcznych kopii konfiguracji systemu centralnego oraz zarządzanych urządzeń.
16. Posiadać udokumentowany interfejs API lub równoważny mechanizm integracji.
17. Zapewniać dostęp administracyjny przez szyfrowany interfejs WWW oraz możliwość zastosowania certyfikatu Zamawiającego.

3. 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 i firewalli przemysłowych.
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. Przygotowanie dokumentacji sposobu przyszłego podłączenia logów audytowych systemu zarządzania do centralnego systemu logowania. Uruchomienie tej integracji i zakup dodatkowych licencji SIEM nie są objęte bieżącym zamówieniem.
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: ul. Wola Szczucińska 142 33-230 Wola Szczucińska

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. 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 być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.
28. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).
29. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
30. Skaner antywirusowy ma pochodzić od europejskiego producenta.

31. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
32. 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

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

WIRTUALNE SIECI PRYWATNE (VPN)

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

FILTR DOSTĘPU DO STRON WWW

47. Urządzenie ma posiadać wbudowany filtr URL.
48. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
49. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.
50. Administrator ma mieć możliwość dodawania własnych kategorii URL.
51. 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.
52. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
53. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.

54. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
55. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
56. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
57. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

UWIERZYTELNIANIE

58. 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.
59. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
60. 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.
61. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
62. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
63. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
64. 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).
65. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
66. 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.
67. 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)

68. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
69. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
a. równoważenie względem adresu źródłowego,
b. równoważenie względem połączenia.
70. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
71. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
72. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
73. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
74. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

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

ADMINISTRACJA URZĄDZENIEM

80. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
81. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
82. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
83. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
84. 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.
85. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
86. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
87. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
88. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
89. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
90. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
91. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
92. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
93. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
94. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
95. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
96. 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
97. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
98. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
99. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

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

POZOSTAŁE USŁUGI I FUNKCJE

109. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
110. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
111. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
112. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
113. 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).
114. Urządzenie ma posiadać usługę DNS Proxy.
115. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
116. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
117. Urządzenie musi mieć możliwość wykorzystania REST API.
118. 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.
119. 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

120. Urządzenie ma być objęte 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
121. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
122. Urządzenie ma być objęte rozszerzoną gwarancją **typu NBD (36 miesięcy**) tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny.

PARAMETRY SPRZĘTOWE

122. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
123. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.

124. Liczba portów Ethernet 2,5Gbps – min. 8.
125. Liczba portów światłowodowych 1Gbps – min. 1.
126. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
127. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps.
128. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 6Gbps.
129. Przepustowość typu Threat Prevention – minimum 740Mbps.
130. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 3Gbps.
131. Liczba tuneli VPN IPSec – minimum 300.
132. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 300.
133. Obsługa interfejsów 802.11q (VLAN) – minimum 393.
134. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 39 000 nowych sesji/sekundę.
135. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie ActivePassive.
136. Urządzenie nie ma limitu na liczbę użytkowników.
137. Liczba reguł filtrowania – minimum 8 192.
138. Liczba tras statycznego routingu – minimum 512.
139. Liczba tras dynamicznego routingu – minimum 10 000.
140. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. 141. Urządzenie musi być wyposażone w moduł TPM.

1.1.3. Zakup 1 urządzenia brzegowych klasy UTM przemysłowej dla części OT

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. 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 być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.
28. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).
29. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
30. Skaner antywirusowy ma pochodzić od europejskiego producenta.
31. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
32. 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

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

WIRTUALNE SIECI PRYWATNE (VPN)

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

FILTR DOSTĘPU DO STRON WWW

47. Urządzenie ma posiadać wbudowany filtr URL.
48. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
49. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.
50. Administrator ma mieć możliwość dodawania własnych kategorii URL.
51. 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.
52. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
53. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
54. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
55. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
56. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
57. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

UWIERZYTELNIANIE

58. 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.
59. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
60. 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.
61. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
62. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
63. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
64. 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).
65. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
66. 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.
67. 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)

68. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
69. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
a. równoważenie względem adresu źródłowego,
b. równoważenie względem połączenia.
70. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
71. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
72. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
73. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
74. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

75. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
76. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

77. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
78. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
79. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

ADMINISTRACJA URZĄDZENIEM

80. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
81. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
82. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
83. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
84. 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.
85. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH).
86. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
87. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
88. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
89. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
90. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
91. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
92. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
93. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
94. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
95. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
96. 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
97. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
98. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
99. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

100. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
101. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
102. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.

103. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
104. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
105. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
106. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
107. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 2 i 3.
108. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

109. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
110. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
111. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
112. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
113. 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).
114. Urządzenie ma posiadać usługę DNS Proxy.
115. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
116. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
117. Urządzenie musi mieć możliwość wykorzystania REST API.
118. 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.

GWARANCJA I SERWIS

119. Urządzenie ma być **objęte 36-miesięczną gwarancją** producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
120. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
121. Urządzenie ma być objęte rozszerzoną gwarancją typu NBD (36 miesięcy) tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny.

PARAMETRY SPRZĘTOWE

121. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
122. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
123. Liczba portów Ethernet 10/100/1000Mbps – min. 2, z możliwością rozszerzenia do 4.
124. Urządzenie ma pozwalać na dodanie min. 2 portów światłowodowych 1Gbps.
125. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
126. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
127. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2.6Gbps.
128. Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 0,8 Gbps.
129. Liczba tuneli VPN IPSec – minimum 200.

130. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
131. Obsługa interfejsów 802.11q (VLAN) – minimum 393.
132. Liczba równoczesnych sesji – minimum 500 000 i nie mniej niż 20 000 nowych sesji/sekundę.
133. Liczba reguł filtrowania – minimum 8 192.
134. Liczba tras statycznego routingu – minimum 2 048.
135. Liczba tras dynamicznego routingu – minimum 10 000.
136. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
137. Urządzenie musi być wyposażone w moduł TPM.
138. Urządzenie ma posiadać pasywny system chłodzenia.
139. Urządzenie ma posiadać redundantne zasilanie DC, 2x12-48VDC.
140. Urządzenie ma być przystosowane do pracy w temperaturach od -40oC do +70oC przy wilgotności od 0% do 95% (bez kondensacji).
141. Obudowa urządzenia ma zapewniać ochronę wg. kodów IP – IP30.
142. Urządzenie ma pozwalać na aktywowanie funkcjonalności tzw. hardware bypass, tj. zapewnienie ciągłości transmisji pomiędzy dwoma dedykowanymi interfejsami Ethernet pomimo awarii sprzętowej lub programowej urządzenia.
143. Średni czas bezawaryjnej pracy (MTBF) w temperaturze 25 oC ma być nie mniejszy niż 35.1 lat.
144. Urządzenie nie ma limitu na liczbę użytkowników.
145. Urządzenie ma umożliwiać bezpośredni montaż na szynie typu DIN (35mm).

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

1.2.1. Przełącznik zarządzany PoE+ - 2 szt.

	Minimalne wymaganie dotyczące jednej sztuki przełącznika dostępowego PoE. W ramach postępowania należy dostarczyć 2 zestawy.
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) minimum jeden zasilacz 230V AC d) zakres temperatur pracy ciągłej co najmniej od -5°C do +50°C e) zakres wilgotności pracy co najmniej 5% - 95% f) maksymalny pobór mocy wliczając budżet PoE nie większy niż: 515W
3.	Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie: ● 48 portów 10/100/1000BASE-T PoE+ zgodne z 802.3at (budżet PoE minimum 385W) ● 4 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T, kabli DAC Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
4.	Przełącznik musi posiadać następujące porty służące do zarządzania: ● Port konsoli RS232 ze złączem RJ45 ● Port out-of-band RJ45 ● Port konsoli USB typ C
5.	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 80Gb/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.
6.	Układ przełączający o wydajności min. 176 Gbps, wydajność przełączania przynajmniej 130 Mpps
7.	Obsługa min. 16 000 adresów MAC
8.	Wbudowana pamięć RAM min. 2 GB. Minimalne taktowanie procesora 1100MHz Bufor pakietów minimum: 1.5MB
9.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1 GB
10.	Obsługa min. 4094 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
11.	Możliwość skonfigurowania min. 32 interfejsów vlan interface SVI działających równocześnie
12.	Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad
13.	Obsługa minimum 120 grup LAG
14.	Obsługa ramek jumbo o wielkości min. 9992 bajtów
15.	Obsługa sFlow
16.	Wsparcie dla G.8032 ERPS i RRPP lub równoważnego
17.	Obsługa protokołu VRRPv2 i VRRPv3
18.	Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP). Obsługa Voice VLAN, Private VLAN
19.	Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
20.	Obsługa min. 3 000 tras dla routingu IPv4
21.	Obsługa min. 700 tras dla routingu IPv6 Obsługa min. 700 IPv6 neighbor discovery (ND)
22.	Obsługa protokołów związanych z obsługą ruchu typu multicast: a) IGMPv3 i IGMP Snooping b) MLDv2 I MLD Snooping c) minimum 900 tras multicast d) Multicast VLAN i Multicast VPN
23.	Minimalny rozmiar tablicy ARP 2 000 wpisów
24.	Obsługa protokołów LLDP i LLDP-MED
25.	Przełącznik musi posiadać funkcjonalności dla IPv4 i IPv6: DHCP Serwer, DHCP Snooping, DHCP Relay, DHCP Klient
26.	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 1000 reguł ACL e) zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 i SSHv2 f) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP g) obsługa mechanizmów Port Security, IP Source Guard, IPv6 RA Guard h) możliwość synchronizacji czasu zgodnie z NTP lub SNTP
27.	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
28.	Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA). Urządzenie musi wspierać funkcjonalność gRPC i NETCONF

29.	Obsługa standardów i protokołów: 802.3az, 802.1ak, 802.1ax, 802.1v, RFC4022, RFC4113, RFC5280, RFC6987
30.	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
31.	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
32.	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
33.	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.
34.	Zamawiający wymaga, aby urządzenia posiadały 5-letni serwis gwarancyjny świadczony przez producenta lub Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. 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.
35.	Urządzenie musi pochodzić od tego samego producenta co oferowane **Access Point** w celu zapewnienia spójnego zarządzania siecią
36.	Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń.

1.2.3.. Zakup punktów dostępowych WiFi – 2 szt

	Minimalne wymagania dotyczące punktu dostępowego – w ramach postępowania należy dostarczyć 2 zestawy.
1.	Punkt dostępowy musi być dedykowanym urządzeniem sieciowym przystosowanym do zamontowania na suficie i na ścianie. Wymagane dostarczenie z zestawu montażowego. System operacyjny (firmware) musi być dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej. Oprogramowanie do pracy w trybie tzw „lekkiego AP", możliwość pracy jako tzw "grubego AP (FAT AP)" oraz możliwość pracy w trybie Cloud.
2.	Wymagane parametry fizyczne: a) możliwość montażu na suficie oraz ścianie (wraz z urządzeniem należy dostarczyć elementy do montowania) b) wysokość maksymalna 3,5 cm c) możliwość zasilania przez zasilacz DC d) zakres temperatur pracy ciągłej co najmniej 0°C – +50°C e) zakres wilgotności pracy co najmniej 5% - 95% f) waga nie większa niż 0,55kg
3.	Punkt dostępowy musi posiadać: a) port konsolowy RJ45 zgodny z RS-232 musi stanowić stały element konstrukcji urządzenia, instalowany fabrycznie przez producenta. Zamawiający nie akceptuje portów realizowanych w formie adapterów, przejściówek, kart opcjonalnych ani modułów wymiennych - wymagany jest dedykowany, wbudowany port konsolowy RJ45 b) minimum 1 port 100/1000Mbit BaseT PoE zgodny ze standardem 802.3af i 802.3at c) port fizyczny zabepieczający urządzenie przed kradzieżą - Kensington

4.	Obsługiwane standardy radiowe: 802.11a/b/g/n/ac/ac Wave 2/ax, jednoczesna obsługa minimum 4 SSID dla każdego radia
5.	Wbudowane anteny minimum 4dBi dla 2,4GHz oraz 5dBi dla 5GHz z pracą w standardzie minimum MIMO: 2.4G: 2x2, 5G: 2x2
6.	Wsparcie dla standardów/funkcjonalności bezpieczeństwa: WPA, WPA2, WPA3, 802.1x oraz tworzenie ACL
7.	Wsparcie dla roamingu zgodnego z 802.11k, 802.11v, 802.11r
8.	Obsługa minimum 250 równocześnie podłączonych użytkowników do punktu dostępowego
9.	Wydajność minimum 1,5Gbps w tym minimum 300Mbps dla 2,4GHz oraz 1,2Gbps dla 5GHz
10.	Zużycie mocy nie większe niż 13W
11.	Możliwość zarządzania poprzez: a) WWW over HTTPS b) kontroler tego samego producenta c) SNMP v1, v2c, v3, d) Dedykowany port konsoli e) SSHv2
12.	Kompatybilność dla protokołów oraz standardów sieciowych takich jak: IPv6, LLDP, mDNS, NAT, IPsec
13.	Urządzenie musi posiadać standard bezpieczeństwa EN62368-1
14.	Tunel CAPWAP dla komunikacji z kontrolerem muszą być zaszyfrowane celem ochrony przed możliwością podsłuchania transmisji w sieci kablowej
15.	Wsparcie dla protokołów i standardów: a) 802.11e b) 802.11i c) 802.11d d) 802.11h e) 802.11u f) 802.11w g) 802.15.1 h) LLDP i) DFS j) DTLS encryption k) A-MPDU i A-MSDU
16.	Obsługa NTP lub SNTP
17.	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
18.	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.
19.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski
20.	Zamawiający wymaga, aby urządzenia posiadały 5-letni serwis gwarancyjny świadczony przez producenta lub Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. 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.

21.	Urządzenie musi pochodzić od tego samego producenta co oferowany **przełącznik dostępowy** w celu zapewnienia spójnego zarządzania siecią.
22.	Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.

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 i UTM/NGFW; integrację NAC z SIEM przewiduje się do przyszłej rozbudowy zgodnie z pkt 4.2.

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 Centralne 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. zapewnienie technicznej możliwości przyszłego przekazywania logów do centralnego systemu gromadzenia i analizy zdarzeń; w bieżącym zamówieniu logi NAC/RADIUS pozostają dostępne w jego własnym systemie, bez uruchamiania dodatkowego źródła SIEM.

1.4.2. 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 poprzez logi VPN eksportowane przez urządzenia UTM/NGFW objęte zakresem pkt 4.2, bez tworzenia dodatkowego źródła SIEM;
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:

- Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
- 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
- Musi posiadać wbudowany serwer Radius
- 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
- System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN.
- 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.
- Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
- 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

- Musi obsługiwać metody profilowania (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie):
  - DHCP
  - TCP
  - MAC OUI
  - SNMP
- 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
- 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)
- 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
  - Samodzielna rejestracja klientów gościnnych w oparciu o:
  - Adres e-mail
  - Numer telefonu (wiadomość SMS)
  - Logowanie w oparciu o portale społecznościowe (Google,Facebook,Github,LinkedIn)
  - Funkcja integracji z systemami trzecimi poprzez API
  - Wspieranie rozwiązań mobilnych poprzez skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
  - Funkcja personalizacji strony gościnnej
    - Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.
- System musi wspierać obsługę następujących systemów operacyjnych
  - MS Windows
  - Mac OS X
  - iOS
  - Android
  - Chromebook
  - Ubuntu
- Umożliwienie klientowi samorejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
- Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
- Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID
- 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 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.

2. Pakiet zarządzania podatnościami i testów bezpieczeństwa IT/OT

Zakres obejmuje wdrożenie narzędzi i usług umożliwiających identyfikację, ocenę, priorytetyzację, raportowanie i obsługę podatności w środowisku IT oraz OT/ICS Zamawiającego.
Rozwiązanie powinno umożliwiać cykliczne skanowanie wskazanych zasobów, tworzenie raportów technicznych i zarządczych, klasyfikację podatności według uznanej metodyki oceny ryzyka, wskazywanie rekomendacji naprawczych oraz ewidencję statusu obsługi podatności. W zakresie środowiska OT/ICS testy aktywne mogą być wykonywane wyłącznie po uprzednim uzgodnieniu z Zamawiającym, w zaakceptowanych oknach serwisowych i z wyłączeniem działań mogących zakłócić ciągłość procesów technologicznych.
Pakiet obejmuje również wykonanie usług testów bezpieczeństwa, weryfikację konfiguracji kluczowych elementów infrastruktury, ocenę ekspozycji zasobów oraz przygotowanie raportów zawierających opis zidentyfikowanych ryzyk, rekomendacje działań naprawczych i priorytety ich wdrożenia.

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

1. Przedmiot i cel wdrożenia

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i wdrożenie centralnego systemu przeznaczonego do aktywnego wykrywania, identyfikowania, oceny, priorytetyzowania i raportowania podatności występujących w zasobach teleinformatycznych Zamawiającego.
System musi umożliwiać prowadzenie aktywnych skanów infrastruktury IT niezależnie od instalacji agentów systemów bezpieczeństwa na skanowanych urządzeniach.
System powinien obejmować skanowaniem co najmniej:

- serwery fizyczne;
- serwery i maszyny wirtualne;
- stacje robocze;
- urządzenia sieciowe;
- urządzenia UTM/NGFW i inne urządzenia bezpieczeństwa;
- urządzenia pamięci masowej NAS;
- systemy operacyjne Windows i Linux/Unix;
- usługi i aplikacje dostępne poprzez sieć;
- inne urządzenia posiadające stos TCP/IP wskazane przez Zamawiającego.

System określony w niniejszym punkcie stanowi uzupełnienie agentowego mechanizmu wykrywania podatności hostów określonego w pkt 4.4 OPZ.
Funkcjonalność systemu określonego w pkt 4.4 nie może zastępować aktywnego skanera podatności określonego w niniejszym punkcie.

2. Wymagania funkcjonalne

System musi umożliwiać co najmniej:

1. wykonywanie aktywnych skanów wskazanych hostów, zakresów adresów IP i podsieci;
2. wykonywanie skanów bez konieczności instalowania dedykowanego agenta na skanowanym urządzeniu;
3. wykonywanie skanów nieuwierzytelnionych;
4. wykonywanie skanów uwierzytelnionych;
5. definiowanie zakresu portów podlegających skanowaniu;
6. definiowanie hostów, adresów IP, usług lub portów wyłączonych ze skanowania;
7. tworzenie różnych profili skanowania;
8. uruchamianie skanów ręcznych;
9. definiowanie cyklicznych harmonogramów skanowania;
10. wykonywanie skanów o różnym zakresie i intensywności.

3. Skanowanie uwierzytelnione

System musi umożliwiać wykonywanie skanów uwierzytelnionych z wykorzystaniem mechanizmów właściwych dla skanowanych systemów, w szczególności:

- SSH dla systemów Linux/Unix i wspieranych urządzeń sieciowych;
- mechanizmów umożliwiających uwierzytelnione skanowanie systemów Microsoft Windows;
- SNMP, w tym SNMPv3, dla wspieranych urządzeń infrastruktury;
- innych bezpiecznych mechanizmów dostępnych w zaoferowanym rozwiązaniu.

Poświadczenia wykorzystywane podczas skanowania muszą być przechowywane w sposób zabezpieczony przed nieuprawnionym dostępem.

4. Wykrywanie hostów i usług

System musi umożliwiać:

1. wykrywanie aktywnych hostów;
2. identyfikację dostępnych portów i usług;
3. identyfikację, w zakresie technicznie możliwym:
    - systemu operacyjnego;
    - rodzaju urządzenia;
    - wersji dostępnych usług;
    - aplikacji i komponentów dostępnych poprzez sieć;
4. tworzenie i ponowne wykorzystywanie zdefiniowanych celów skanowania;
5. grupowanie zasobów podlegających skanowaniu.

5. Identyfikacja i ocena podatności

System musi:

1. identyfikować znane podatności występujące w systemach, usługach i komponentach;
2. korzystać z regularnie aktualizowanego repozytorium testów i informacji o podatnościach;
3. prezentować identyfikatory CVE, jeżeli zostały przypisane do wykrytej podatności;
4. prezentować poziom krytyczności podatności;
5. wykorzystywać klasyfikację CVSS, jeżeli jest dostępna dla danej podatności;
6. umożliwiać filtrowanie wyników co najmniej według:
    - hosta;
    - poziomu ryzyka;
    - identyfikatora podatności;
    - portu lub usługi;
    - daty wykrycia;
7. prezentować opis podatności;
8. prezentować informacje lub rekomendacje pomocne w jej usunięciu albo ograniczeniu ryzyka, jeżeli są dostępne;
9. przechowywać wyniki wcześniejszych skanów.

6. Repozytorium testów podatności

System musi wykorzystywać aktualizowane repozytorium obejmujące co najmniej:

- informacje o podatnościach;
- identyfikatory CVE;
- informacje pozwalające identyfikować podatne wersje systemów i usług;
- testy wykorzystywane przez silnik aktywnego skanowania;
- konfiguracje niezbędne do realizacji skanów.

System musi umożliwiać automatyczną aktualizację repozytorium testów i informacji o podatnościach.

7. Raportowanie

System musi posiadać centralny interfejs webowy oraz zapewniać co najmniej:

1. prezentację wyników według hostów;
2. prezentację wyników według poziomu ryzyka;
3. wyszukiwanie i filtrowanie wyników;
4. generowanie raportów technicznych;

5. eksport wyników do powszechnie stosowanych formatów umożliwiających dalsze przetwarzanie danych;
6. prezentowanie co najmniej:
    - adresu/nazwy hosta;
    - portu i usługi;
    - nazwy podatności;
    - identyfikatora CVE, jeśli jest dostępny;
    - poziomu krytyczności;
    - opisu wyniku;
    - informacji pomocnych przy działaniach naprawczych.

8. Integracja

System musi umożliwiać przekazywanie informacji o wykrytych podatnościach do innych systemów wdrażanych w ramach zamówienia za pomocą API, eksportu danych lub innego udokumentowanego mechanizmu integracyjnego.

Wykonawca skonfiguruje, w zakresie wspieranym przez zastosowane rozwiązania, przekazywanie istotnych wyników do:

- centralnego systemu SIEM/SOAR wyłącznie w ramach przyszłej rozbudowy; w bieżącym zamówieniu wymagana jest możliwość techniczna eksportu, bez uruchamiania integracji i bez zakupu licencji SIEM dla skanera;
- systemu ITSM/CMDB.

System ITSM może być wykorzystywany do dalszej obsługi procesu remediacji podatności, w tym rejestrowania zadań naprawczych, odpowiedzialności, statusu realizacji oraz terminów.

9. Architektura

System musi umożliwiać instalację lokalną w infrastrukturze Zamawiającego.

System musi umożliwiać wdrożenie w środowisku wirtualizacyjnym opartym o **Proxmox VE/KVM** lub środowisko równoważne.

Dopuszcza się realizację systemu jako:

- maszyny wirtualnej;
- systemu Linux;
- zestawu kontenerów;
- rozwiązania appliance;
- innego równoważnego modelu spełniającego wymagania OPZ.

Dopuszcza się zastosowanie rozwiązania open source.

W przypadku zastosowania rozwiązania open source odpowiedzialność za instalację, konfigurację, aktualizację, integrację i wsparcie techniczne rozwiązania ponosi Wykonawca.

10. Zakres zasobów

W ramach wdrożenia Wykonawca skonfiguruje system do skanowania co najmniej **50 zasobów/aktywów** wskazanych przez Zamawiającego.

Za pojedynczy zasób należy rozumieć w szczególności serwer, stację roboczą, maszynę wirtualną, urządzenie sieciowe, firewall, urządzenie NAS lub inne urządzenie posiadające własny adres IP.

Ostateczna lista zasobów oraz zakresów adresacji zostanie uzgodniona podczas analizy przedwdrożeniowej.

11. Środowisko OT/ICS

Aktywne skanowanie środowiska OT/ICS może być wykonywane wyłącznie:

- po uzyskaniu zgody Zamawiającego;
- po przeprowadzeniu oceny ryzyka;
- w uzgodnionym oknie serwisowym;
- przy zastosowaniu profilu skanowania ograniczającego ryzyko zakłócenia działania urządzeń.

Zamawiający musi mieć możliwość wyłączenia wskazanych urządzeń, portów lub usług ze skanowania.

Niedopuszczalne jest prowadzenie bez odrębnej zgody Zamawiającego testów powodujących zmianę konfiguracji, restart, zatrzymanie usług lub inne zakłócenie pracy urządzeń OT/ICS.

12. Zakres wdrożenia

Wykonawca wykona co najmniej:

1. instalację i konfigurację systemu;
2. konfigurację aktualizacji repozytorium testów podatności;
3. konfigurację minimum 50 wskazanych zasobów;
4. konfigurację skanów nieuwierzytelnionych;
5. konfigurację skanów uwierzytelnionych dla wskazanych systemów;
6. utworzenie wymaganych profili skanowania;
7. utworzenie harmonogramów skanowania;
8. konfigurację raportowania;
9. konfigurację wymaganych integracji;
10. wykonanie skanu bazowego infrastruktury;
11. przygotowanie raportu początkowego z wykrytych podatności;
12. konfigurację backupu rozwiązania;
13. przeprowadzenie testów odbiorowych;
14. przekazanie dokumentacji powdrożeniowej;
15. instruktaż dla minimum 2 administratorów.

13. Testy odbiorowe

Wykonawca musi wykazać co najmniej:

1. wykonanie aktywnego skanu wskazanego zasobu bez instalacji agenta;
2. identyfikację dostępnych usług;
3. wykrycie i prezentację przykładowej podatności lub wyniku testu;
4. wykonanie skanu uwierzytelnionego wskazanego systemu, jeśli Zamawiający udostępni system testowy;
5. działanie harmonogramu skanowania;
6. wygenerowanie raportu;
7. poprawną aktualizację repozytorium testów;
8. działanie skonfigurowanej integracji lub eksportu danych.

14. Wsparcie techniczne

Wykonawca zapewni minimum **12 miesięcy wsparcia technicznego**.

Wsparcie musi obejmować co najmniej pomoc w:

- diagnozowaniu problemów;
- aktualizacji systemu;
- aktualizacji repozytorium testów;
- konfiguracji skanów;
- odtwarzaniu rozwiązania;
- utrzymaniu wykonanych integracji.

2.2. Testy 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 ITSM/ITAM/CMDB i inwentaryzacji aktywów

Celem pakietu jest wdrożenie centralnego systemu ITSM/ITAM/CMDB stanowiącego podstawowy rejestr zasobów teleinformatycznych oraz centralny system obsługi zgłoszeń, incydentów, problemów i zmian.

System powinien umożliwiać automatyczną oraz ręczną inwentaryzację zasobów, obejmującą w szczególności stacje robocze, serwery fizyczne i wirtualne, urządzenia sieciowe, urządzenia bezpieczeństwa, urządzenia peryferyjne oraz inne aktywa wskazane przez Zamawiającego.

Informacje o aktywach powinny być utrzymywane w CMDB wraz z historią zmian i relacjami pomiędzy zasobami, użytkownikami, lokalizacjami, usługami oraz komponentami infrastruktury.

System ITSM powinien zapewnić co najmniej obsługę zgłoszeń i incydentów, problemów, zmian, bazy wiedzy oraz powiązanie zgłoszenia z konkretnym zasobem CMDB. Powinien umożliwiać przyjmowanie zdarzeń lub zgłoszeń z systemu monitorowania, systemu zarządzania podatnościami i pozostałych systemów bezpieczeństwa poprzez API, webhook, pocztę elektroniczną lub równoważny mechanizm.

Efektem wdrożenia ma być jeden aktualny rejestr aktywów oraz jeden centralny proces ewidencjonowania i obsługi zdarzeń wymagających interwencji administratora

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

ServiceDesk – Zarządzanie rezerwacjami

Oprogramowanie musi umożliwiać rezerwację dowolnego aktywnego zasobu w systemie.
Oprogramowanie musi umożliwiać kategoryzowanie rejestrowanych rezerwacji.
Oprogramowanie musi umożliwiać określenie widoczności poszczególnych kategorii rezerwacji w zależności od zalogowanego użytkownika.
Oprogramowanie musi informować o możliwych konfliktach podczas tworzenia/edycji rezerwacji z zasobem.
Oprogramowanie musi prezentować informacje o rezerwacjach w formie graficznej – kalendarza.
Oprogramowanie musi umożliwiać akceptację, odrzucenie lub anulowanie rezerwacji przez upoważnionych użytkowników.

ServiceDesk – Automatyzacja operacji za pomocą sztucznej inteligencji

Oprogramowanie dla realizacji wymagań związanych z automatyzacją z wykorzystaniem sztucznej inteligencji musi umożliwiać integrację z usługą OpenAI (ChatGPT) za pomocą indywidualnego klucza API
Oprogramowanie musi umożliwiać automatyczne sugerowanie rozwiązań użytkownikom na etapie rejestracji nowego zgłoszenia. Potencjalna odpowiedź sztucznej inteligencji musi bazować na analizie treści zgłoszenia, kategorii oraz historii wszystkich wewnętrznych rozwiązanych zgłoszeń.
Oprogramowanie musi umożliwiać wzbogacanie odpowiedzi inżynierów o sugerowane rozwiązania sztucznej inteligencji oparte na opisie zgłoszenia.
Oprogramowanie musi umożliwiać automatyczne tworzenie artykułów w bazie wiedzy przez generator treści AI na podstawie historii rozwiązanych zgłoszeń.
Oprogramowanie musi umożliwiać tworzenie automatycznych podsumowań tematyki wybranego zgłoszenia bazując na analizie historii komentarzy oraz przedstawiać najbardziej prawdopodobne rozwiązanie problemu.
Oprogramowanie musi umożliwiać automatyczne tworzenie okresowych podsumowań opisujących aktualny stan techniczny i kondycję krytycznych elementów zarządzanej infrastruktury IT.
Oprogramowanie musi umożliwiać automatyczne generowanie sugestii dotyczących zalecanych działań mogących korzystnie wpłynąć na stabilność i bezpieczeństwo infrastruktury IT.

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 **15 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.

W przypadku wątpliwości Zamawiający zastrzega sobie prawo (w przeciągu do 7 dni od terminu otwarcia ofert) do wezwania wykonawcy do prezentacji zaoferowanego rozwiązania celem weryfikacji zgodności z wymaganiami stawianymi przez zamawiającego w niniejszym postępowaniu.

Pakiet 4. Zintegrowana ochrona punktów końcowych, centralnego logowania i monitorowania bezpieczeństwa. – 1 kpl.

Celem pakietu jest zapewnienie centralnej widoczności stanu bezpieczeństwa i dostępności infrastruktury ZUK poprzez połączenie ochrony punktów końcowych, centralnego gromadzenia i korelacji logów, monitorowania infrastruktury oraz detekcji zdarzeń na hostach.
Pakiet obejmuje migrację istniejącego środowiska ochrony końcówek do rozwiązania klasy EPP/EDR/XDR, centralny system logowania i korelacji zdarzeń klasy SIEM/SOAR oraz system monitorowania infrastruktury IT/OT.
System monitorowania powinien obejmować w szczególności urządzenia UTM/NGFW, firewall IT/OT, przełączniki, punkty dostępowe, serwery fizyczne i wirtualne, platformę Proxmox, system backupu, NAS, UPS, oraz kluczowe usługi systemowe.
Do centralnego systemu logowania i korelacji trafiają zdarzenia wyłącznie z pięciu źródeł określonych w pkt 4.2. Pozostałe systemy zachowują własne logi i konsole, a zdarzenia wymagające obsługi administratora powinny być możliwe do przekazania do systemu ITSM zgodnie z wymaganiami szczegółowymi.
Wykonawca skonfiguruje zestaw dashboardów, progów alarmowych, powiadomień oraz scenariuszy testowych pozwalających potwierdzić prawidłowe działanie integracji.
Pakiet ma umożliwić:

- ochronę stacji roboczych, serwerów i wspieranych stacji operatorskich przed złośliwym oprogramowaniem, ransomware, phishingiem i zagrożeniami typu zero-day;
- wykrywanie nietypowych zachowań procesów, użytkowników, aplikacji i połączeń sieciowych;
- gromadzenie w jednym miejscu logów z pięciu krytycznych źródeł: dwóch urządzeń UTM/NGFW w HA, jednego firewalla IT/OT, centralnej instancji ESET oraz jednego serwera Windows Server AD/DNS, zgodnie z pkt 4.2;
- korelowanie zdarzeń pochodzących z wielu systemów;
- identyfikowanie incydentów niewidocznych na poziomie pojedynczego urządzenia;
- automatyzację wybranych czynności analitycznych i reakcyjnych;
- zapewnienie wsparcia specjalistów MDR w ocenie alertów, kwalifikowaniu incydentów oraz przygotowaniu i koordynacji reakcji;
- skrócenie czasu wykrycia zagrożenia i czasu podjęcia działań;
- ograniczenie możliwości rozprzestrzeniania się incydentów pomiędzy systemami i segmentami sieci;
- zapewnienie materiału dowodowego, historii zdarzeń i raportów na potrzeby audytów, obsługi incydentów i realizacji obowiązków wynikających z SZBI, KRI i KSC;
- zwiększenie ciągłości działania systemów wspierających dostawy wody i odbiór ścieków.

Przedmiotem zamówienia jest dostawa licencji, wdrożenie, konfiguracja i integracja zintegrowanego pakietu bezpieczeństwa obejmującego:

1. system ochrony punktów końcowych i serwerów klasy EPP/EDR/XDR;
2. system centralnego gromadzenia, przechowywania, przeszukiwania i korelowania logów bezpieczeństwa, posiadający funkcjonalności klasy SIEM/SOAR;
3. integrację powyższych elementów w zakresie właściwym dla ich funkcji; obowiązek dostawy licencji i podłączenia źródeł do SIEM ogranicza się do pięciu źródeł wskazanych w pkt 4.2.

4.1. **System ochrony stacji roboczych i serwerów** przed szkodliwym oprogramowaniem z wykorzystaniem narzędzia EDR/XDR.

Zakres obejmuje migrację do pakietu ESET PROTEC ELITE i 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. Migracja istniejącego środowiska ESET do ESET PROTECT Elite, wdrożenie centralnego zarządzania w formie Virtual Appliance/Linux, migracja polityk, urządzeń, grup, konfiguracji i agentów, uruchomienie EDR/XDR oraz Vulnerability & Patch Management. bezpieczeństwa.

Dostarczone licencje na oprogramowanie muszą objąć co najmniej : 15 aktywnych użytkowników/ 15 stacji roboczych, liczba urządzeń mobilnych 13, liczba serwerów 2 szt, liczba maszyn wirtualnych 4., liczba stacji

OT/SCADA 2 szt , liczba serwerów OT/SCADA - 2szt,. Ponadto musi posiadać co najmniej 2 licencji dostępowych do konsoli zarządzającej.
Wykonawca zaoferuje nowe licencje i zapewni jej ważność min do dnia 31.12.2026 r. (zakończenie projektu)

Aktualna licencja; ESET Endpoint & Server Security for ESET PROTECT Advanced, ważna do: 07.2027, nr licencji Nr certyfikatu: NL2026/045248 Liczba stanowisk: 10 (w tym maksymalnie serwerów: 10)

4.2. system centralnego gromadzenia, przechowywania, przeszukiwania i korelowania logów bezpieczeństwa, posiadający funkcjonalności klasy SIEM/SOAR;

Zakres obejmuje dostawę i wdrożenie centralnego systemu gromadzenia, przechowywania, przeglądania, raportowania i analizy logów w wariancie krytycznym, obejmującym pięć źródeł zdarzeń wskazanych poniżej. Bieżące zamówienie obejmuje licencjonowanie, instalację, konfigurację i uruchomienie integracji wyłącznie pięciu źródeł. System musi zapewniać raporty techniczne i zarządcze, wyszukiwanie, filtrowanie i eksport zdarzeń oraz retencję określoną w niniejszym punkcie. Analiza przedwdrożeniowa służy wskazaniu adresów, instancji i zakresu logowania tych źródeł i nie rozszerza liczby źródeł objętych zamówieniem.
Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz wdrożenie systemu w infrastrukturze Zamawiającego, wraz ze szkoleniem administratorów oraz zapewnieniem **aktualizacji i wsparcia serwisowego na okres min 12 miesiecy .**
System ma służyć do centralnego gromadzenia, przechowywania, analizy i korelacji logów oraz zdarzeń bezpieczeństwa z pięciu źródeł objętych bieżącym wdrożeniem. Wymagania logowania, integracji i odbioru w pozostałych częściach OPZ należy stosować z uwzględnieniem tego zakresu.

Źródła objęte bieżącą dostawą i integracją
1) UTM/NGFW nr 1 w klastrze HA – 1 źródło; 2) UTM/NGFW nr 2 w klastrze HA –1 źródło 3) firewall przemysłowy na styku IT/OT – 1 źródło; 4) centralna instancja ESET PROTECT/EDR/XDR – 1 zbiorcza integracja ; 5) jedna maszyna Windows Server realizująca AD/DNS – 1 źródło .
Zakres logów obejmuje: dla firewalli – zdarzenia ruchu i bezpieczeństwa, w tym IPS/IDS, VPN i filtrowanie WWW, stosownie do funkcji urządzenia; dla ESET – dostępne w oferowanej integracji alerty i zdarzenia ochrony zarządzanych końcówek; dla AD/DNS – co najmniej zdarzenia uwierzytelniania, zmiany kont i grup oraz uprawnień administracyjnych. Szczegółowe polityki zbierania należy uzgodnić i udokumentować podczas wdrożenia.
Integracja ESET obejmuje zdarzenia z centralnej instancji zarządzającej ochroną końcówek, bez odrębnego bezpośredniego podłączania ich logów systemowych do SIEM. Wykonawca zapewni w cenie oferty wszystkie wymagane uprawnienia i konektory oraz potwierdzi sposób rozliczania zbiorczej integracji zgodnie z zasadami producenta. Jedna VM nie oznacza automatycznie jednego węzła licencyjnego; dostarczone uprawnienia muszą pokrywać cały wskazany zakres bez dodatkowych opłat przy odbiorze.
Zakres pięciu źródeł nie ogranicza ochrony końcówek przez ESET ani zakresu monitorowania infrastruktury i HIDS/FIM określonego w innych punktach OPZ. Licencje i integracje tych rozwiązań pozostają wymagane w ich własnym zakresie; nie oznaczają automatycznego podłączenia ich wszystkich do SIEM.

Wymagania ogólne:

1. W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
2. Rozwiązanie musi umożliwiać wdrożenie w środowisku wirtualnym Zamawiającego opartym o Proxmox VE/KVM lub zostać dostarczone w formie wspieranej przez producenta maszyny/appliance możliwej do uruchomienia na tej platformie..
3. Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
4. Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
5. Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.
6. Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.

7. Rozwiązanie musi posiadać predefiniowane panele dla informacji z urządzeń pracujących w sieci OT.

Zarządzanie Logami:

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

Rodzaje wyszukiwani

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

Raportowanie

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

Zarządzanie incydentami

23. Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.
24. Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.
25. Rozwiązanie ma posiadać moduł SOAR. Należy dostarczyć uprawnienia do modułu SOAR umożliwiające pracę co najmniej jednego operatora i realizację wymaganych powyżej funkcji; licencja SOAR nie oznacza rozszerzenia liczby źródeł logów.

Wymagania systemowe

26. Wydajność zbierania, przetwarzania i korelacji zdarzeń musi zapewniać obsługę rzeczywistego strumienia logów z pięciu źródeł objętych wdrożeniem, także przy przełączeniu klastra HA. Wykonawca dobierze zasoby i wykaże podczas odbioru brak utraty zdarzeń w uzgodnionych scenariuszach testowych
27. Retencja logów z pięciu źródeł: **minimum 12 miesięcy**, z możliwością ich przeszukiwania i analizy w okresie ważności licencji. Wykonawca określi wymaganą pojemność na podstawie analizy przedwdrożeniowej i udokumentuje przyjęte założenia.
28. Liczba źródeł objętych dostawą licencji i integracją: 5. W modelu licencjonowania węzłowego należy zapewnić min 5 licencji lub równoważny zakres uprawnień zgodny z zasadami producenta.. System musi umożliwiać późniejsze dodawanie źródeł poprzez rozszerzenie licencji i zasobów, bez wymiany całej platformy
29. Przestrzeń i przepustowość zapisu należy dobrać do rzeczywistej liczby i wielkości zdarzeń z pięciu źródeł oraz wymaganej retencji. Nie wymaga się deklarowanej zdolności zapisu xxx MB na dobę niezależnie od faktycznego obciążenia. Dobór zasobów, konfiguracja retencji i sposób monitorowania zajętości muszą zostać udokumentowane.

System musi być wspierany przez producenta w środowisku Proxmox VE/KVM , o, zgodnie z wymaganiem powyżej. Obsługa VMware ESXi i Microsoft Hyper-V może stanowić dodatkową możliwość produktu, lecz nie wymaga dostawy ani licencjonowania tych hiperwizorów.

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

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

Użytkownicy	
1	Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat. Zapewnienia równoległego dostępu do systemu dla wielu użytkowników. Ograniczania użytkownikom dostępu do wybranych grup hostów.
Monitorowanie	
2	Monitorowanie serwerów fizycznych. Monitorowanie urządzeń sieciowych. Monitorowanie stanu połączeń. Monitorowanie interfejsów sieciowych przełączników, routerów i serwerów. Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux. Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych. Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń. Automatyczne wykrywanie usług na urządzeniach oraz powiadamianie o wykryciu nowych usług na urządzeniu. Grupowanie hostów. Definiowanie planowanych przerw serwisowych dla hostów i usług. Możliwość zaznaczenia reakcji na awarię — odpowiadanie na alerty (ACK). Wykonywanie operacji na grupach hostów, w tym: włączanie i wyłączanie monitorowania; włączanie i wyłączanie powiadomień; konfigurowanie przerw serwisowych. Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych, dostępnych przez interfejs WWW. Monitorowanie serwerów za pomocą agentów. Monitorowanie serwerów aplikacji: Tomcat; Oracle WebLogic Server. Monitorowanie Active Directory. Monitorowanie serwerów plików i udziałów sieciowych. Monitorowanie statusu serwerów Apache. Monitorowanie baz danych: Oracle; MySQL; PostgreSQL; Microsoft SQL Server; DB2. Monitorowanie urządzeń z wykorzystaniem następujących protokołów i mechanizmów: SNMP; SNMP traps; WMI;

	IPMI. Konfiguracja oprogramowania systemu monitorowania poprzez interfejs WWW. Monitorowanie poprawności działania DNS. Monitorowanie środowiska VMware. Monitorowanie środowiska Hyper-V. Monitorowanie środowiska Proxmox. Monitorowanie działania serwera czasu NTP. Monitorowanie offsetu czasu na serwerach. Monitorowanie dostępności za pomocą protokołu ICMP, w tym czasu odpowiedzi i strat pakietów. Monitorowanie zajętości miejsca na poszczególnych partycjach. Monitorowanie obciążenia dysków. Monitorowanie wykorzystania pamięci RAM. Monitorowanie obciążenia CPU. Monitorowanie logów systemowych Windows w zakresie wykrywania określonych błędów i zdarzeń operacyjnych. Monitorowanie macierzy dyskowych, w tym statusu urządzenia i statusu dysków. Dodawanie własnych wtyczek lub agentów dla urządzeń i usług, które standardowo nie są obsługiwane. Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działających w systemach Linux i Unix. Agregacja usług niskiego poziomu do procesów biznesowych. Symulacja awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe. Monitorowanie rozproszone, umożliwiające podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji lub oddziałów. Wykrywanie niestabilnie działających usług. Monitorowanie dostępności stron internetowych. Konfiguracja hierarchiczna, w tym dziedziczenie konfiguracji dla grup urządzeń
Prezentacja	
3	Prezentację stanu urządzeń na mapie. Prezentację danych na dashboardach. Elastyczną konfigurację dashboardów, wybór elementów. Wizualizację stanu działania całej infrastruktury na jednym dashboardzie. Tworzenie indywidualnych dashboardów przez użytkowników
Powiadomienia	
4	Globalne wyłączanie powiadomień. Powiadamianie użytkownika o problemach przez e-mail. Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie. Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników. Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług
Konfiguracja	
5	Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW Automatyczna konfiguracja i działanie z REST-API Centralne zarządzanie agentami Integracja danych z różnych źródeł danych (JSON, XML, SNMP)
Monitoring bazy danych	
6	Możliwość monitorowania bazy danych w zakresie co najmniej: Instance state Version

	Jobs Locks Processes Number of active sessions Recovery area Log switch activity General tablespace information Tablespaces performance Long active sessions Undo retention Checkpoint and online backup state Custom SQLs Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości
Kolektor logów	
7	System posiada własny kolektor logów syslog Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event Klasyfikuje wiadomości bazując zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.
Cyberbezpieczeństwo	
8	System monitoruje urządzenia klasy UTM minimum w zakresie: wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany” jest uważany za OK, a status „niezsynchronizowany” CRIT. monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz” (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda” (1). monitoruje aktualną liczbę sesji na urządzeniu monitoruje liczbę dostępnych tuneli IPSec VPN monitoruje wykrywanie wirusów i szybkość blokowania systemów UTM, AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika. monitoruje poziom wykorzystania procesora Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne. System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog.

4.4. System HIDS/FIM oraz agentowego wykrywania podatności hostów – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja i wdrożenie centralnego systemu klasy HIDS lub rozwiązania równoważnego, przeznaczonego do monitorowania bezpieczeństwa serwerów, maszyn wirtualnych oraz wskazanych stacji administracyjnych i technicznych.

System ma stanowić uzupełnienie systemu EPP/EDR/XDR, centralnego systemu logowania/SIEM/SOAR oraz systemu monitorowania infrastruktury.

System musi zapewniać co najmniej:

- centralne zarządzanie agentami lub równoważnym mechanizmem monitorowania hostów;
- obsługę systemów Windows Server oraz Linux;
- analizę logów systemowych i zdarzeń bezpieczeństwa;
- monitorowanie integralności plików i katalogów (FIM), w tym wykrywanie ich utworzenia, modyfikacji i usunięcia;
- wykrywanie zmian konfiguracji systemów, kont użytkowników, grup, uprawnień i usług;
- wykrywanie zdarzeń takich jak nieudane logowania, użycie kont uprzywilejowanych, zmiany uprawnień oraz wyłączenie mechanizmów bezpieczeństwa;
- klasyfikację i priorytetyzację alertów;

- możliwość tworzenia lub modyfikowania reguł detekcyjnych;
- centralny interfejs webowy umożliwiający przeglądanie i wyszukiwanie zdarzeń;
- techniczna możliwość przekazywania zdarzeń i alertów do centralnego systemu logowania/SIEM/SOAR za pomocą Syslog, API lub mechanizmu równoważnego; uruchomienie tej integracji przewiduje się do przyszłej rozbudowy zgodnie z pkt 4.2;
- możliwość przekazywania wybranych alertów do systemu ITSM;
- bezpieczną, szyfrowaną i uwierzytelnioną komunikację pomiędzy agentami a systemem centralnym;
- centralną inwentaryzację systemów operacyjnych, zainstalowanych pakietów i aplikacji na monitorowanych hostach;
- korelację informacji o systemie operacyjnym oraz wersjach zainstalowanych pakietów i aplikacji z aktualizowanym repozytorium informacji o podatnościach, obejmującym identyfikatory CVE;
- centralny wykaz wykrytych podatności wraz z możliwością przypisania ich do poszczególnych monitorowanych hostów;
- prezentowanie poziomu krytyczności wykrytych podatności, w tym informacji o klasyfikacji CVSS, jeżeli jest dostępna dla danej podatności;
- funkcjonalność Security Configuration Assessment (SCA) lub równoważną, umożliwiającą ocenę konfiguracji bezpieczeństwa monitorowanych hostów względem zdefiniowanych polityk;
- możliwość przyszłego przekazywania istotnych alertów bezpieczeństwa i informacji o podatnościach do nadrzędnego systemu SIEM/SOAR za pomocą udokumentowanego interfejsu; w bieżącym zamówieniu dane pozostają w systemie HIDS/FIM, z zachowaniem wymaganej możliwości przekazywania wybranych alertów do ITSM.

System centralny musi umożliwiać uruchomienie w środowisku wirtualizacyjnym Zamawiającego opartym o **Proxmox VE/KVM** lub środowisko równoważne.
Zamawiający dopuszcza zastosowanie rozwiązania open source, pod warunkiem zapewnienia wszystkich wymaganych funkcjonalności. W przypadku rozwiązania open source wymagane wsparcie techniczne może być świadczone przez Wykonawcę i nie musi obejmować zakupu komercyjnej subskrypcji producenta.
Zakres wdrożenia
W ramach wdrożenia Wykonawca wykona co najmniej:

1. instalację i konfigurację systemu centralnego;
2. instalację i rejestrację agentów na wskazanych hostach;
3. konfigurację monitorowania logów, FIM, inwentaryzacji hostów, agentowego wykrywania podatności, Security Configuration Assessment oraz wymaganych reguł detekcyjnych;
4. konfigurację centralnej prezentacji informacji o stanie agentów, zdarzeniach bezpieczeństwa i wykrytych podatnościach;
5. udokumentowanie sposobu przyszłej integracji z centralnym systemem SIEM/SOAR, bez jej uruchamiania i bez zakupu dodatkowych licencji SIEM w bieżącym zamówieniu;
6. konfigurację przekazywania wybranych zdarzeń i alertów do systemu ITSM;
7. przeprowadzenie testów poprawności działania, obejmujących co najmniej wykrycie zmiany chronionego pliku, wygenerowanie zdarzenia bezpieczeństwa oraz identyfikację przykładowej podatności na monitorowanym hoście;
8. przekazanie dokumentacji powdrożeniowej obejmującej co najmniej architekturę systemu, wykaz objętych monitoringiem hostów, zastosowane polityki i integracje;
9. zapewnienie minimum 12 miesięcy wsparcia technicznego.

System określony w pkt 4.4 nie zastępuje systemu EPP/EDR/XDR ani systemu monitorowania infrastruktury, lecz zapewnia dodatkową warstwę detekcji zdarzeń bezpieczeństwa, kontroli integralności plików, oceny konfiguracji bezpieczeństwa, inwentaryzacji oraz agentowego wykrywania podatności monitorowanych hostów.
Funkcjonalność agentowego wykrywania podatności nie zastępuje systemu aktywnego skanowania podatności określonego w Pakiecie 2. System aktywnego skanowania podatności musi umożliwiać niezależne od instalacji agenta badanie wskazanych zasobów sieciowych, w tym urządzeń, systemów i usług dostępnych poprzez sieć.

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

Celem pakietu jest utworzenie jednego, centralnego i redundantnie wyposażonego hosta wirtualizacyjnego dla systemów IT i cyberbezpieczeństwa oraz dwóch niezależnych repozytoriów NAS realizujących funkcje wykonywania, przechowywania, replikacji i odtwarzania kopii zapasowych. Architektura rozdziela logicznie i sieciowo środowisko produkcyjne od warstwy backupu. Zakupiony serwer będzie jedynym fizycznym hostem wirtualizacyjnym. Na serwerze zostaną uruchomione wymagane maszyny wirtualne Windows Server oraz Linux/appliance. Lokalna przestrzeń dyskowa serwera służy środowisku produkcyjnemu; trwałe kopie zapasowe muszą być kierowane do niezależnych repozytoriów NAS.

Nie przewiduje się odrębnego fizycznego serwera backupowego. Funkcja wykonywania i zarządzania kopiami jest realizowana przez mechanizmy backupu środowiska VE oraz oprogramowanie backupowe zintegrowane z urządzeniami NAS. Dwa urządzenia NAS stanowią odrębne od hosta produkcyjnego repozytoria kopii zapasowych.
Rozwiązanie backupowe musi zapewnić wykonywanie kopii maszyn wirtualnych i kontenerów bez ich wyłączania, kopie przyrostowe, kompresję, deduplikację na poziomie systemu backupowego lub repozytorium, polityki retencji, weryfikację integralności, wersjonowanie oraz testowe odtwarzanie. Dla systemów Windows wymagany jest backup pełnego systemu/dysków/plików z możliwością odtworzenia bare-metal lub funkcjonalnością równoważną.

Dwa urządzenia NAS pełnią odpowiednio rolę repozytorium podstawowego NAS-1 i repozytorium wtórnego/DR NAS-2. NAS-2 musi znajdować się w odrębnej lokalizacji lub co najmniej odrębnej domenie awarii i posiadać odseparowane poświadczenia administracyjne. Należy skonfigurować automatyczną, wersjonowaną replikację/kopiowanie NAS-1 -> NAS-2 oraz archiwizację wybranych krytycznych kopii do repozytorium online.

5.1. Zakup serwera fizycznego (1 szt) niezbędnego do zainstalowania i wdrożenia rozwiązań z zakresu bezpieczeństwa wraz z oprogramowaniem systemowym i licencjami dostępowymi oraz oprogramowaniem do wirtualizacji.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji 8 dysków SAS/SATA 2,5”. Możliwość rozbudowy o dodatkowe min. 8 wnęk na dyski SAS/SATA/NVMe 2.5”. Serwer musi mieć możliwość wyposażenia w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający: - wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS - wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy - wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera - wyświetlanie w czasie rzeczywistym temperatury procesorów - konfigurowanie ustawień sieciowych modułu zarządzania. Serwer wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Możliwość dokupienia z oficjalnego kanału sprzedaży producenta przedniego panelu zamykanego na klucz, chroniącego dyski przed nieuprawnionym wyjęciem z serwera.

Płyta główna	Płyta główna przeznaczona do serwera klasy enterprise, obsługująca co najmniej dwóch procesorów wymaganej klasy oraz umożliwiająca dalszą rozbudowę pamięci i interfejsów zgodnie z OPZ.
Chipset	Chipset serwerowy zgodny z zaoferowanym procesorem i platformą serwerową.
Procesor	Zainstalowany min jeden procesor x86 posiadający minimum 12 fizycznych rdzeni, o taktowaniu bazowym minimum 2,2 GHz, umożliwiający osiągnięcie w oferowanym modelu serwera wyniku SPECrate2017_int_base nie mniejszego niż 295 pkt. Dopuszcza się większą liczbę rdzeni. Wynik musi być opublikowany w oficjalnej bazie SPEC CPU2017.
Pamięć RAM	Minimum 128 GB ECC RDIMM DDR5 6400MT/s. Platforma musi umożliwiać rozbudowę pamięci do co najmniej 4 TB bez wymiany wszystkich zainstalowanych modułów. Wymaga się minimum 32 slotów RDIMM, pod przyszłą rozbudowę
Zabezpieczenie pamięci	DRAM ECC, POST PPR, Runtime PPR, DRAM thermal throttling, DRAM SDDC, ADDDC Multiple Region, Memory mirroring, DDR command/address parity check and retry.
Pamięć masowa i kontroler RAID	Zainstalowanie minimum 2 × 480 GB enterprise SSD/NVMe przeznaczone na system/hiperwizor, skonfigurowane w RAID1 lub równoważnym zabezpieczeniu. Dodatkowo minimum 2 × 3,84 TB enterprise SSD przeznaczone na datastore maszyn wirtualnych, skonfigurowane w RAID1, zapewniające odporność na awarię jednego dysku oraz pojemność użytkową minimum 3,84 TB p. Kontroler/HBA musi być zgodny z przyjętym sposobem realizacji pamięci masowej;
Wbudowane porty	3 x USB z czego nie mniej niż 2 x USB 3.0. Port USB TYP-C lub microUSB na przednim panelu obudowy. 1 x VGA na tylnym panelu obudowy oraz 1 x VGA na tylnym panelu obudowy. Złącze USB TYP-C / microUSB na przednim panelu musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS. Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
Sloty PCIE	Minimum 3 aktywne sloty PCIe, w tym co najmniej jeden x16, oraz możliwość rozbudowy o dodatkowe interfejsy sieciowe/pamięci masowej. Serwer powiniń posiadać min.dwa slotów PCIe OCP 3.0, jeżeli oferowana konfiguracja zapewnia wszystkie wymagane interfejsy.
Interfejsy sieciowe	Minimum: 1 x dedykowany port zarządzający RJ-45, 4 x 1 GbE Base-T oraz 2 x 10 GbE SFP+ lub 10GBase-T. Interfejsy 10 GbE należy wykorzystać do ruchu serwerowego i sieci backupu; dopuszcza się ich realizację kartą rozszerzeń.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wentylatory	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla oferowanej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
Zasilanie	Minimum dwa identyczne zasilacze klasy Titanium zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza nie więcej niż 1600W.
Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta. Możliwość instalacji modułu TPM 2.0.
Zarządzanie	Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca: • monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.),

	• monitorowanie w czasie rzeczywistym poboru prądu przez serwer, • zbieranie logów błędów hardware, • przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, • montowanie wirtualnych napędów, • zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, • wysyłanie zawiadomień droga mailową i poprzez SNMP • wsparcia dla IPMI, SSH, Redfish • wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows, • nadawanie ról użytkownikom, • możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, • możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.
Dodatkowe oprogramowanie do zarządzania i monitorowania	Wraz z serwerem dostarczone powinno zostać oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne monitorowanie i zarządzanie serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na: włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów. tworzenie szablonów instalacyjnych dla systemów operacyjnych. tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów. zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera. aktualizacja sterowników i BIOS serwerów. zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.
Kompatybilność	Producent serwerów musi posiadać certyfikat jakości według normy ISO 9001 na produkcję oferowanego asortymentu lub równoważny certyfikat jakości oraz certyfikat według normy ISO-14001 Systemu Zarządzania Środowiskowego lub równoważną normę zarządzania środowiskowego. Należy dołączyć do oferty dokumenty potwierdzające spełnianie wymogów w zakresie opisanym powyżej. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2022, Windows Server 2025. Serwer wraz ze wszystkimi oferowanymi komponentami muszą być kompatybilne z systemem Microsoft Windows Server 2022 i 2025, Vmware 8.0 U3 i 9.0, Red Hat Enterprise Linux 9.5 oraz Oracle Linux 9.5, a producent serwera powinien udostępniać na swojej stronie internetowej wszystkie wymagane sterowniki do tych komponentów dla wskazanych systemów.
System operacyjny/dodatkowe oprogramowanie	Systemem bazowym hosta będzie Proxmox VE lub rozwiązanie równoważne. W ramach zamówienia należy dostarczyć Microsoft Windows Server 2025 Standard w liczbie licencji rdzeniowych wystarczającej do objęcia wszystkich fizycznych rdzeni oferowanego serwera, nie mniej niż 16 rdzeni, zapewniającej prawo do uruchomienia co najmniej 2 maszyn wirtualnych Windows Server, oraz 15 licencji Windows Server User CAL.
Gwarancja	1. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP. 2. Urządzenie objęte **minimum 36 miesięcznym okresem gwarancji** w trybie 9x5 onsite z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. 3. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.

	4. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych.. 5. Możliwość darmowego pobierania aktualizacji firmware i sterowników bezpośrednio ze strony producenta serwera po ustaniu wsparcia serwisowego. Przy braku takiej możliwości, dopuszcza się spełnienie tego wymogu poprzez zaoferowanie wsparcia serwisowego dla serwera na minimum 7 lat od momentu dostawy serwera do Zamawiającego. 6. 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 lub autoryzowanego partnera serwisowego producenta, ● otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.

5.2. Wirtualizacja wraz z mechanizmami wykonywania kopii do repozytoriów NAS

Dostawa i wdrożenie systemu wirtualizacji w środowisku Zamawiającego wraz ze wsparciem technicznym o parametrach minimalnych jak niżej lub oprogramowanie równoważne

Licencja na minimum 1 gniazd procesorów - Należy zapewnić wymagane prawa do użytkowania/subskrypcję/wsparcie dla jednego fizycznego hosta systemu wirtualizacji przez okres 36 miesięcy, zgodnie z zasadami licencyjnymi oferowanego rozwiązania.”.
Rozwiązanie musi zapewnić możliwość natywnej obsługi wielu instancji maszyn wirtualnych i kontenerów na każdym serwerze fizycznym. Na etapie realizacji zamówienia wymagany jest jeden fizyczny host wirtualizacyjny. Rozwiązanie musi umożliwiać późniejszą rozbudowę o kolejne hosty bez konieczności zmiany 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 firewall natywnie konfigurowalny w GUI na poziomie hosta i maszyn wirtualnych.
Rozwiązanie musi umożliwiać wykonywanie kopii maszyn wirtualnych i kontenerów do zewnętrznego repozytorium NAS przez NFS/CIFS lub mechanizm równoważny, z zachowaniem konfiguracji VM/CT.
Rozwiązanie musi umożliwiać eksport, import i odtworzenie maszyn wirtualnych na zgodnym hoście Proxmox VE lub równoważnym. Wymóg migracji live pomiędzy wieloma fizycznymi hostami nie obowiązuje na etapie obecnego wdrożenia.
Rozwiązanie wirtualizacyjne musi zapewniać funkcjonalność z poziomu konsoli graficznej przypisywania dla konkretnej maszyny wirtualnej wybranych rdzeni konkretnego procesora lub grupy rdzeni procesorów w serwerze.
Wysoka dostępność warstwy serwerowej w obecnym wariancie jest realizowana przez redundancję komponentów pojedynczego hosta (zasilanie, pamięć masowa, interfejsy sieciowe), kopie konfiguracji i maszyn wirtualnych na dwóch niezależnych NAS oraz procedury szybkiego odtworzenia. Nie wymaga się klastra HA wielu hostów.
Należy dostarczyć licencję dla oferowanego środowiska wirtualnego z wsparciem technicznym na **min. 36 miesięcy**. Wsparcie producenta oprogramowania umożliwiające dostępu do poprawek i uaktualnień w wersji dla środowisk produkcyjnych. Dla tego samego okresu, wsparcie serwisowe musi być świadczone przez dostawcę

rozwiązania, ze zgłoszeniami w trybie dni roboczych i czasem reakcji do 1 dnia roboczego. Wdrożenie wymaga przedstawienia końcowej dokumentacji opisującej infrastrukturę, jej konfigurację i wszelkie dane dostępowe do wszystkich elementów systemu. Warstwa pamięci masowej Serwer musi wykorzystywać mechanizm Software Defined Storage (SDS) oparty o system plików działający z zaoferowanym rozwiązaniem wirtualizacji , zapewniający programową realizację funkcji pamięci masowej bez konieczności stosowania dedykowanych macierzy dyskowych. Rozwiązanie powinno umożliwiać tworzenie odpornych na awarie pul dyskowych, realizację mechanizmów RAID programowego, wykonywanie migawek (snapshotów), klonowania danych, kompresji oraz deduplikacji blokowej, zwiększając efektywność wykorzystania przestrzeni dyskowej. Zastosowanie SDS ma zapewniać integralność danych poprzez sumy kontrolne, automatyczne wykrywanie i naprawę błędów oraz wysoką dostępność i skalowalność zasobów pamięci masowej.

Minimalne wymagania techniczne dla systemu backupu środowiska wirtualnego

Wymagane minimalne parametry techniczne
System wspiera kopie zapasowe maszyn wirtualnych i kontenerów uruchomionych na hoście VE oraz pełne kopie wskazanych systemów Windows/końcówek do repozytorium NAS.
Repozytorium online/chmurowe musi komunikować się z systemem backupowym/NAS przez szyfrowane i uwierzytelnione połączenie (VPN, TLS lub mechanizm równoważny). Nie wymaga się istnienia klastra wielu hostów fizycznych.
System uruchomiony z licencją lub subskrypcją, lub w abonamencie, zapewniający dostęp w trybie ‘online’ do repozytorium o przestrzeni roboczej min. 2TB, dla archiwum skonfigurowanych kopii zapasowych, na okres minimum 36 miesięcy.
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 musi umożliwiać zautomatyzowaną, regularną replikację lub synchronizację kopii pomiędzy NAS-1 i NAS-2 oraz archiwizację wybranych kopii do repozytorium online, tak aby kopie znajdowały się w niezależnych domenach awarii.
System wspiera bezpieczeństwo logowania przy pomocy technologii “Two Factor Authentication (2FA)” przez GUI oraz “Time-based One Time Passwords (TOTP)”.
Obsługa archiwizacji na taśmy LTO nie jest wymagana. Dopuszcza się jej zaoferowanie jako funkcjonalności dodatkowej bez wpływu na cenę i ocenę spełnienia wymagań minimalnych.
Dla systemu wirtualizacji oraz urządzeń NAS należy zapewnić aktualizacje i wsparcie techniczne przez **minimum 36** miesięcy. W przypadku oprogramowania open source wsparcie może być realizowane przez producenta, autoryzowanego partnera lub Wykonawcę, pod warunkiem zachowania wymaganych funkcjonalności i czasu reakcji do 1 dnia roboczego w dni robocze.
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. **System wykonywania kopii zapasowych i deduplikacji realizowany z wykorzystaniem dwóch urządzeń NAS - 1 kpl.**

5.3.1. Zakup urządzeń NAS - 2 szt.

Celem wdrożenia dwóch urządzeń NAS jest utworzenie podstawowego repozytorium kopii zapasowych NAS-1 oraz odseparowanego repozytorium wtórnego/DR NAS-2. Urządzenia mają przechowywać kopie maszyn wirtualnych, kontenerów, systemów Windows, konfiguracji urządzeń i wybranych danych IT/OT, zapewniając snapshoty, wersjonowanie, szyfrowanie, replikację oraz mechanizmy deduplikacji/kompresji w zakresie dostarczonego oprogramowania.

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 producenta NAS lub rozwiązanie równoważne umożliwiające wykonywanie pełnych i przyrostowych kopii systemów Windows PC/Server na NAS, obejmujących system operacyjny, dyski, foldery i pliki, z harmonogramem i możliwością odtworzenia bare-metal. Dodatkowo NAS musi udostępniać NFS i/lub CIFS/SMB jako repozytorium kopii VE.
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 Wymagane dodatkowo: odrębne konta administracyjne, możliwość MFA dla administracji lub równoważnego silnego uwierzytelniania, filtrowanie dostępu do usług backupu oraz szyfrowana replikacja między NAS-1 i NAS-2.
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	3 lata

6. Pakiet centralnego zarządzania hasłami i poświadczeniami

Przedmiotem zamówienia w ramach Pakietu 6 jest dostawa, instalacja, konfiguracja, integracja, uruchomienie oraz udokumentowanie **centralnego systemu zarządzania hasłami i poświadczeniami**, przeznaczonego do bezpiecznego przechowywania, organizowania oraz kontrolowanego udostępniania danych uwierzytelniających wykorzystywanych w środowisku IT i OT Zamawiającego.
Celem wdrożenia jest ograniczenie wykorzystywania haseł przechowywanych w sposób niekontrolowany, zapewnienie centralnego i bezpiecznego repozytorium poświadczeń oraz umożliwienie nadawania użytkownikom i administratorom dostępu do przechowywanych danych zgodnie z posiadanymi uprawnieniami.
System powinien umożliwiać w szczególności bezpieczne przechowywanie haseł i innych danych uwierzytelniających, zarządzanie użytkownikami i grupami, kontrolowane współdzielenie poświadczeń, rejestrowanie operacji związanych z dostępem do przechowywanych danych oraz integrację z istniejącymi mechanizmami uwierzytelniania Zamawiającego w zakresie przewidzianym w dalszych wymaganiach OPZ

6.1. 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.

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

7.2 Dostawa stacji roboczej przesiadkowej – ilość 1 szt

element	Wymagane minimalne parametry techniczne komputerów
Komputer	Stacja przesiadkowa będzie dedykowanym, utwardzonym stanowiskiem przeznaczonym wyłącznie do kontrolowanego dostępu administracyjnego, serwisowego i diagnostycznego do wskazanych systemów OT/ICS.. 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.

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 zasilacza 1-fazowy, obudowa standard/desktop lub rack 3kVA – 2 szt

Opis wymagań techniczno-funkcjonalnych	**Wymagane wartości /funkcje/**
Technologia	VFI (true on-line, podwójne przetwarzanie energii)
Moc znamionowa	3 kVA / 3 kW
Wyjściowy współczynnik mocy (PF)	1
Wejściowy współczynnik mocy	cosϕ ≥ 0,99
Napięcie wejściowe	208/220/230/240 VAC + N
Tolerancja napięcia wejściowego	176 – 300 VAC
Częstotliwość wejściowa	40-70 Hz
Minimalna sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	≥91%
Minimalna sprawność w trybie ECO	≥96,0% dla 100% obciążenia
Napięcie wyjściowe	208/220/230/240 VAC
Częstotliwość wyjściowa	50/60Hz (programowalna)
Czas podtrzymania	4 minuty dla obciążenia 2000W
Intuicyjny panel graficzny	Wymagane
Stabilizacja napięcia wyjściowego	±1%
Zniekształcenia napięcia wyjściowego	≤ 2% z obciążeniem liniowym ≤ 5% z obciążeniem nieliniowym
Współczynnik szczytu przy obciążeniu znamionowym	3:1
Przeciążenie inwertera	105%-125% przez 1 minutę 125% -150% przez 30 sekund >150% przez 300 milisekund
Złącze interfejsów	RS232 + USB
Interfejs EPO (do wyłącznika ppoż.)	Wymagane
Możliwość pracy jako konwerter częstotliwości	Wymagane
Baterie	Szczelne, bezobsługowe, w technologii AGM o żywotności projektowanej minimum 5 lat w temperaturze 25 stopni Celsjusza
Możliwość zainstalowania akumulatorów wewnątrz modułu zasilacza UPS (bez konieczności użycia modułu bateryjnego)	Wymagane
Test bateryjny	Wymagane

Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane
Poziom hałasu w odległości 1m	≤ 50 dBA
Rejestr zdarzeń	Wymagane
Spełnienie wszystkich obowiązujących norm bezpieczeństwa potwierdzone deklaracją zgodności CE	Wymagane
Maks. wymiary modułu UPS (szer. x gł. x wys.)	191 x 418 x 335 mm
Gwarancja (UPS oraz akumulatory)	Min. 24 miesiące
Zamawiający zastrzega sobie prawo do weryfikacji oczekiwanych parametrów w zainstalowanym urządzeniu. W przypadku niespełnienia któregokolwiek z oczekiwanych parametrów Wykonawca na swój koszt zdemontuje dostarczone urządzenie oraz dostarczy zasilacz spełniający wszystkie parametry zawarte w OPZ.	

9. Pakiet usług wdrożeniowych, dokumentacyjnych, szkoleniowych i utrzymaniowych

9.1. Wymagania ogólne dla całości zamówienia

Wykonawca zobowiązany jest dostarczyć i wdrożyć rozwiązanie kompletne, wzajemnie zintegrowane i gotowe do pracy produkcyjnej, obejmujące wszystkie urządzenia, licencje, subskrypcje, elementy montażowe, okablowanie, moduły, zasilacze, wkładki, oprogramowanie, maszyny wirtualne, konfiguracje oraz usługi niezbędne do prawidłowego uruchomienia i eksploatacji przedmiotu zamówienia.
Wszystkie elementy przedmiotu zamówienia muszą zostać dobrane i skonfigurowane w sposób zapewniający ich wzajemną kompatybilność, bezpieczną komunikację i integrację oraz możliwość centralnego zarządzania, monitorowania i audytowania w zakresie właściwym dla poszczególnych klas rozwiązań.
Wykonawca ponosi odpowiedzialność za prawidłowe współdziałanie wszystkich dostarczanych i wdrażanych w ramach zamówienia komponentów, niezależnie od tego, czy poszczególne rozwiązania pochodzą od jednego czy wielu producentów oraz czy są rozwiązaniami komercyjnymi, czy open source.
W przypadku zastosowania oprogramowania open source Wykonawca odpowiada za jego instalację, konfigurację, aktualizację, zabezpieczenie, integrację oraz zapewnienie wymaganego wsparcia technicznego.
Rozwiązanie po zakończeniu realizacji musi tworzyć spójne funkcjonalnie środowisko bezpieczeństwa IT/OT, a nie zbiór niezależnie działających systemów.

9.2. Cel i zakres wdrożenia

Przedmiotem usług wdrożeniowych jest kompleksowe uruchomienie i integracja środowiska infrastruktury IT/OT oraz cyberbezpieczeństwa Zamawiającego, obejmującego w szczególności:

- urządzenia bezpieczeństwa sieciowego UTM/NGFW i firewall przemysłowy IT/OT;
- zarządzalne przełączniki sieciowe i punkty dostępowe WLAN;
- system kontroli dostępu do sieci NAC wraz z usługą RADIUS;
- mechanizmy segmentacji sieci IT/OT, VPN i MFA;
- środowisko serwerowe i wirtualizacyjne;
- system wykonywania i przechowywania kopii zapasowych;
- systemy Windows Server i usługi Active Directory/DNS;
- ochronę EPP/EDR/XDR;
- centralne gromadzenie i analizę logów bezpieczeństwa
- monitoring infrastruktury IT;
- system detekcji i monitorowania bezpieczeństwa hostów HIDS/FIM;
- system zarządzania podatnościami;
- system ITSM/ITAM/CMDB oraz inwentaryzacji aktywów;
- dostępem i poświadczeniami;
- bezpieczny dostęp administracyjny do środowiska OT/ICS;

- systemy zasilania awaryjnego oraz monitoringu parametrów zasilania i środowiska szaf teleinformatycznych.

Wdrożenie musi zapewnić w szczególności segmentację infrastruktury, kontrolę dostępu, centralne zarządzanie, monitorowanie stanu infrastruktury, wykrywanie zdarzeń bezpieczeństwa, zarządzanie podatnościami, ochronę danych oraz możliwość identyfikacji i obsługi incydentów.

9.3. Zakres prac wdrożeniowych

Wykonawca zobowiązany jest wykonać co najmniej następujące prace:

1. Przeprowadzić analizę przedwdrożeniową, obejmującą inwentaryzację istniejącej infrastruktury IT i OT, adresacji IP, sieci VLAN, systemów serwerowych, urządzeń sieciowych, urządzeń bezpieczeństwa, systemów backupu, usług katalogowych oraz zależności komunikacyjnych pomiędzy systemami.
2. Opracować na podstawie analizy przedwdrożeniowej projekt wykonawczy, obejmujący co najmniej docelową architekturę logiczną i fizyczną, adresację, VLAN, strefy bezpieczeństwa, przepływy komunikacyjne, zasady routingu, dostęp administracyjny, integracje systemów oraz sposób migracji do środowiska docelowego.
3. Dostarczyć, zamontować i uruchomić urządzenia w szafach teleinformatycznych wraz z niezbędnym okablowaniem, elementami montażowymi, wkładkami, przewodami zasilającymi i pozostałymi akcesoriami.
4. Skonfigurować dwa urządzenia UTM/NGFW w układzie wysokiej dostępności HA, obejmującym synchronizację konfiguracji i stanu urządzeń oraz mechanizmy automatycznego przełączenia awaryjnego.
5. Skonfigurować funkcje bezpieczeństwa urządzeń UTM/NGFW, w szczególności firewall, NAT, IPS/IDS, kontrolę aplikacji, ochronę przed szkodliwym oprogramowaniem, filtrowanie ruchu, VPN, logowanie oraz integrację z systemami uwierzytelniania i centralnego logowania.
6. Zainstalować i skonfigurować przemysłowy firewall zabezpieczający styk IT/OT, wraz z politykami komunikacji pomiędzy strefami IT, OT i DMZ oraz mechanizmami kontroli i inspekcji ruchu właściwymi dla środowiska OT.
7. Wdrożyć centralny system zarządzania urządzeniami bezpieczeństwa sieciowego oraz podłączyć do niego urządzenia objęte zamówieniem.
8. Zainstalować i skonfigurować zarządzalne przełączniki sieciowe i punkty dostępowe WLAN, w tym w szczególności VLAN, 802.1X, LACP, STP/RSTP/MSTP, ACL, port security, SNMPv3, Syslog oraz pozostałe funkcje wymagane w OPZ.
9. Opracować i wdrożyć docelową segmentację sieci, obejmującą co najmniej sieć użytkowników, serwerową, administracyjną, zarządzającą, backupu, urządzeń technicznych/IoT, WLAN, sieć gościnną, środowisko OT/ICS, strefę DMZ, strefę dostępu serwisowego oraz strefę kwarantanny.
10. Wdrożyć system NAC wraz z centralnym RADIUS, zintegrowany co najmniej z Active Directory/LDAP, przełącznikami i infrastrukturą WLAN, umożliwiający realizację 802.1X, MAB, dynamiczne przypisywanie VLAN oraz rejestrowanie decyzji dostępowych.
11. Skonfigurować dostęp VPN dla wskazanych grup użytkowników i administratorów oraz dostępu serwisowego, wraz z MFA oraz ograniczeniem dostępu do zasobów wynikających z przydzielonej roli.
12. Zainstalować i skonfigurować na serwerze produkcyjnym środowisko wirtualizacyjne Proxmox VE lub równoważne oraz utworzyć maszyny wirtualne niezbędne do uruchomienia systemów objętych zamówieniem.
13. Utworzyć i skonfigurować co najmniej dwie maszyny wirtualne Windows Server:
    - serwer usług Active Directory/DNS;
    - serwer aplikacyjny.
14. Wdrożyć lub skonfigurować usługę Active Directory, strukturę organizacyjną, DNS, polityki bezpieczeństwa, konta administracyjne oraz wymagane integracje z systemami dostarczanymi w ramach zamówienia.
15. Skonfigurować na hoście VE mechanizmy wykonywania kopii maszyn wirtualnych i kontenerów do NAS-1 oraz skonfigurować na NAS-1 system backupu pełnego dla wskazanych systemów Windows/końcówek.
16. Skonfigurować wykonywanie kopii zapasowych maszyn wirtualnych i innych wskazanych zasobów, deduplikację, kompresję, harmonogramy, polityki retencji, weryfikację integralności kopii oraz procedury odtwarzania.

17. Zainstalować i skonfigurować dwa urządzenia NAS: NAS-1 jako podstawowe repozytorium backupu oraz NAS-2 jako odseparowane repozytorium DR. Skonfigurować automatyczną replikację/kopiowanie NAS-1 -> NAS-2, snapshoty/wersjonowanie oraz kopię wybranych krytycznych danych do repozytorium online.
18. Przeprowadzić migrację istniejącego środowiska ochrony punktów końcowych do wymaganego rozwiązania klasy EPP/EDR/XDR, obejmującą migrację konfiguracji, polityk, grup i agentów oraz uruchomienie wymaganych funkcjonalności ochronnych.
19. Zainstalować i skonfigurować centralny system gromadzenia, przechowywania, przeszukiwania i korelacji logów bezpieczeństwa oraz podłączyć z min pięć źródeł określonych w pkt 4.2. Zapewnić licencje, aktualizacje i wsparcie dla tego zakresu przez minimum 12 miesięcy.
20. Zainstalować i skonfigurować system monitorowania infrastruktury IT, obejmując monitoring co najmniej jednego serwera fizycznego, środowiska VE, maszyn wirtualnych, urządzeń sieciowych, firewalli, obu urządzeń NAS, zadań backupu/replikacji, UPS/PDU oraz kluczowych usług. Monitoring ma obejmować również stan repozytoriów, wolną przestrzeń, błędy dysków/RAID, wyniki zadań backupu i replikacji oraz alerty o nieudanych kopiach.
21. Zainstalować i skonfigurować system HIDS/FIM do detekcji i monitorowania bezpieczeństwa hostów, obejmujący analizę logów systemowych, kontrolę integralności plików, wykrywanie zmian konfiguracji i wybranych zdarzeń bezpieczeństwa oraz przekazywanie wybranych alertów do systemu ITSM. Zdarzenia pozostają dostępne w konsoli HIDS/FIM; integracja HIDS/FIM z SIEM jest przewidziana do przyszłej rozbudowy zgodnie z pkt 4.2.
22. Zainstalować i skonfigurować system zarządzania podatnościami, obejmujący skanowanie wskazanych zasobów, harmonogramy skanowania, klasyfikację podatności, raportowanie oraz przekazywanie wyników wymagających działań naprawczych do właściwych procesów obsługi.
23. Zainstalować i skonfigurować system ITSM/ITAM/CMDB i inwentaryzacji aktywów, obejmujący utworzenie centralnego rejestru zasobów oraz podstawowych procesów obsługi zgłoszeń, incydentów, problemów i zmian.
24. Przeprowadzić początkową inwentaryzację zasobów i zasilić system CMDB informacjami o urządzeniach, serwerach, maszynach wirtualnych, systemach, licencjach oraz innych zasobach wskazanych przez Zamawiającego.
25. Zainstalować i skonfigurować , dostępem i poświadczeniami, w tym integrację z Active Directory, role administracyjne, MFA, mechanizmy zarządzania dostępem oraz centralny menedżer poświadczeń.
26. Skonfigurować stację przesiadkową OT jako dedykowany punkt kontrolowanego dostępu administracyjnego i serwisowego do środowiska OT/ICS, z ograniczeniem dostępu zgodnie z zasadą minimalnych uprawnień oraz rejestrowaniem i udostępnianiem zdarzeń we własnym systemie lub we wdrożonym systemie HIDS/FIM. Bezpośrednie przekazywanie jej zdarzeń do SIEM przewiduje się do przyszłej rozbudowy zgodnie z pkt 4.2.
27. Zainstalować i uruchomić urządzenia UPS, i objąć je centralnym monitoringiem, w szczególności w zakresie stanu zasilania, baterii, obciążenia, temperatury i wilgotności.
28. Skonfigurować synchronizację czasu NTP dla urządzeń i systemów objętych wdrożeniem.
29. Wdrożyć rozdział uprawnień administracyjnych, MFA, zasadę minimalnych uprawnień oraz ograniczenie dostępu administracyjnego do wydzielonych stref i uprawnionych użytkowników.
30. Wykonać konfigurację kopii zapasowych konfiguracji urządzeń i systemów bezpieczeństwa oraz udokumentować procedury ich odtwarzania.

9.4. Wymagania dotyczące integracji systemów

Wykonawca zobowiązany jest zapewnić integrację dostarczanych systemów w zakresie wynikającym z ich funkcji i wymagań szczegółowych. W odniesieniu do SIEM/SOAR obowiązek dostawy licencji i uruchomienia integracji obejmuje min pięć źródeł wskazanych w pkt 4.2. Dla pozostałych systemów wymagana jest techniczna możliwość przyszłej integracji, bez uruchamiania dodatkowych źródeł SIEM w bieżącym zamówieniu.
Wymiana danych pomiędzy systemami powinna być realizowana z wykorzystaniem otwartych i udokumentowanych mechanizmów,
Wykonawca zobowiązany jest skonfigurować integracje oraz wykazać ich prawidłowe działanie podczas odbioru.

9.5. Wymagania dotyczące organizacji prac

Wszystkie prace wdrożeniowe muszą być prowadzone w sposób minimalizujący ryzyko zakłócenia pracy Zamawiającego, ze szczególnym uwzględnieniem ciągłości procesów związanych z dostarczaniem wody i odbiorem ścieków.

Działania mogące wpływać na dostępność infrastruktury produkcyjnej, systemów OT/ICS, usług sieciowych lub serwerowych mogą być wykonywane wyłącznie w terminach i oknach serwisowych uzgodnionych z Zamawiającym.
W szczególności aktywne skanowanie i testowanie urządzeń środowiska OT/ICS musi zostać poprzedzone analizą ryzyka oraz uzyskaniem zgody Zamawiającego.
Przed rozpoczęciem zmian produkcyjnych Wykonawca przedstawi co najmniej:

- plan wdrożenia i kolejność prac;
- zakres przewidywanych zmian;
- wskazanie elementów mogących wpływać na dostępność usług;
- plan wykonania kopii bezpieczeństwa konfiguracji;
- plan wycofania zmian (rollback);
- proponowane okna serwisowe.

Wykonawca zobowiązany jest do bieżącej współpracy z Zamawiającym, raportowania postępu realizacji, zgłaszania wykrytych ryzyk i uzyskiwania akceptacji dla zmian mogących mieć istotny wpływ na środowisko produkcyjne.

9.6. Testy odbiorowe

Po zakończeniu wdrożenia Wykonawca przeprowadzi testy funkcjonalne i integracyjne obejmujące co najmniej:

1. poprawność działania klastra UTM/NGFW, w tym test przełączenia awaryjnego;
2. poprawność routingu, VLAN i segmentacji sieci;
3. blokowanie niedozwolonej komunikacji pomiędzy strefami;
4. działanie firewall IT/OT i polityk komunikacji pomiędzy IT a OT;
5. uwierzytelnianie 802.1X/RADIUS/NAC oraz przydzielanie właściwego dostępu;
6. działanie dostępu VPN i MFA;
7. poprawność działania Active Directory/DNS;
8. uruchomienie i pracę wymaganych maszyn wirtualnych na platformie Proxmox;
9. wykonanie kopii zapasowej oraz testowe odtworzenie co najmniej jednej maszyny wirtualnej i wskazanego pliku lub zasobu;
10. prawidłowe przekazywanie, rozpoznawanie, przeszukiwanie i korelację logów z każdego ze źródeł określonych w pkt 4.2, w tym logi obu urządzeń HA i ich identyfikację po przełączeniu; potwierdzenie zgodności dostarczonych licencji z zakresem integracji ESET; pozostałe systemy nie podlegają testom podłączenia do SIEM w bieżącym zamówieniu;
11. generowanie i odbiór alarmów systemu monitorowania;
12. wykrywanie przykładowego zdarzenia HIDS/FIM;
13. wykonanie przykładowego skanu podatności;
14. przekazanie wybranego zdarzenia lub alertu do systemu ITSM;
15. poprawność działania inwentaryzacji i powiązania zasobu z CMDB;
16. działanie monitoringu UPS;
17. kontrolowany dostęp poprzez stację przesiadkową do wskazanego zasobu OT.

Testy aktywne w środowisku OT/ICS mogą być wykonywane wyłącznie po uzgodnieniu z Zamawiającym oraz w sposób niepowodujący zagrożenia dla ciągłości procesu technologicznego.
Nieprawidłowości stwierdzone podczas testów muszą zostać usunięte przez Wykonawcę przed odbiorem końcowym.

9.7. Dokumentacja powdrożeniowa

Wykonawca zobowiązany jest przekazać Zamawiającemu kompletną dokumentację powdrożeniową as-built, obejmującą co najmniej:

1. opis docelowej architektury środowiska IT i OT;
2. aktualne schematy logiczne i fizyczne infrastruktury;
3. zestawienie dostarczonych urządzeń wraz z modelami, numerami seryjnymi i wersjami firmware;
4. wykaz systemów, licencji, subskrypcji i terminów ich obowiązywania;
5. wykaz maszyn wirtualnych wraz z ich przeznaczeniem, systemami operacyjnymi i podstawową konfiguracją;
6. konfigurację adresacji IP, VLAN, routingu, stref bezpieczeństwa oraz przepływów komunikacyjnych;
7. dokumentację konfiguracji UTM/NGFW, HA, firewall IT/OT i VPN;
8. opis konfiguracji NAC/RADIUS, 802.1X i zasad kontroli dostępu;
9. opis środowiska Proxmox VE i systemu backupowego;

10. harmonogramy, polityki retencji oraz procedury backupu i odtwarzania;
11. wykaz min pięciu źródeł podłączonych do SIEM, ich identyfikatorów i adresów, zakresu zdarzeń, licencji, integracji i reguł korelacji oraz opis sposobu przyszłej rozbudowy o kolejne źródła; Dokumentacja musi wskazywać miejsca dostępu do logów i alertów systemów niepodłączonych do SIEM.
12. opis zakresu monitorowania infrastruktury oraz konfiguracji alarmów;
13. opis wdrożenia HIDS/FIM oraz monitorowanych hostów;
14. opis systemu zarządzania podatnościami i harmonogramów skanowania;
15. opis konfiguracji ITSM/ITAM/CMDB i wykonanej inwentaryzacji;
16. opis integracji pomiędzy systemami;
17. wykaz kont administracyjnych i ról, bez umieszczania haseł w dokumentacji jawnej;
18. sposób bezpiecznego przekazania poświadczeń administracyjnych;
19. procedury awaryjne, odtworzeniowe i eksploatacyjne;
20. raport z wykonanych testów odbiorowych wraz z wynikami.

Dokumentacja musi odzwierciedlać stan faktyczny infrastruktury po zakończeniu wdrożenia, a nie jedynie pierwotny projekt wykonawczy.

9.8. Instruktaż i przekazanie do eksploatacji

Wykonawca przeprowadzi instruktaż powdrożeniowy dla administratorów wskazanych przez Zamawiającego. Instruktaż musi obejmować co najmniej:

- podstawową administrację wdrożonym środowiskiem;
- obsługę urządzeń bezpieczeństwa i systemów centralnego zarządzania;
- obsługę systemu wirtualizacji i backupu;
- wykonywanie i odtwarzanie kopii zapasowych;
- obsługę systemów monitorowania i centralnego logowania;
- analizę podstawowych alertów EDR/XDR i HIDS/FIM;
- obsługę systemu zarządzania podatnościami;
- obsługę NAC/RADIUS;
- obsługę ITSM/CMDB;
- podstawowe procedury reakcji na awarie i incydenty.

Celem instruktażu jest umożliwienie administratorom Zamawiającego samodzielnego wykonywania podstawowych czynności eksploatacyjnych po zakończeniu wdrożenia.

9.9. Wsparcie powdrożeniowe

Wykonawca zapewni wsparcie techniczne i powdrożeniowe dla wdrożonych elementów przez okres wynikający z wymagań szczegółowych poszczególnych pakietów OPZ.

Wsparcie Wykonawcy powinno obejmować co najmniej pomoc w:

- diagnozowaniu problemów konfiguracji;
- analizie błędów integracyjnych;
- aktualizacji wdrożonych komponentów;
- odtwarzaniu konfiguracji;
- obsłudze zgłoszeń dotyczących współpracy pomiędzy systemami;
- usuwaniu nieprawidłowości wynikających z przeprowadzonego wdrożenia.

W przypadku systemów open source wsparcie może być świadczone przez Wykonawcę i nie musi oznaczać zakupu komercyjnego wsparcia producenta lub projektu, o ile szczegółowe wymagania OPZ nie stanowią inaczej.

9.10. Warunki odbioru końcowego

Za zakończenie realizacji przedmiotu zamówienia uważa się nie samo dostarczenie urządzeń, licencji lub instalację oprogramowania, lecz osiągnięcie kompletnego, skonfigurowanego, zintegrowanego i przetestowanego środowiska gotowego do pracy produkcyjnej.

Odbiór końcowy nastąpi po:

- zakończeniu wszystkich wymaganych prac;
- wykonaniu konfiguracji i integracji;
- przeprowadzeniu testów odbiorowych z wynikiem pozytywnym;
- usunięciu stwierdzonych nieprawidłowości;
- przekazaniu kompletnej dokumentacji powdrożeniowej;
- przekazaniu licencji, dostępów i poświadczeń administracyjnych;
- wykonaniu instruktażu;
- podpisaniu protokołu odbioru końcowego przez upoważnionych przedstawicieli stron.