ZAŁĄCZNIK NR 2

OPIS PRZEDMIOTU ZAMÓWIENIA

„Podniesienie poziomu cyberbezpieczeństwa systemów IT i OT w Miejskim Zakładzie Wodociągów i Kanalizacji Sp. z o.o. w Złotowie”

Spis treści

1 CENTRALNY SYSTEM EDR (ENDPOINT DETECTION & RESPONSE) (20 SZT.)....4
2 WDROŻENIE SYSTEMU EDR (20 SZT.)....4
3 PUNKTY DOSTĘPOWE KLASY ENTERPRISE Z OBSŁUGĄ WPA3 I CENTRALNĄ KONTROLĄ (4 SZT.)....4
4 WDROŻENIE URZĄDZEŃ ACCESS POINT (4 SZT.)....5
5 SERWER NAS....5
6 WDROŻENIE SERWERA NAS....7
7 OPROGRAMOWANIE DO OBSŁUGI MFA....8
8 WDROŻENIE OPROGRAMOWANIA MFA....11
9 SERWER ENTERPRISE....12
10 WDROŻENIE I URUCHOMIENIE SERWERA ENTERPRISE....21
11 SYSTEM WIRTUALIZACJI....21
12 WDROŻENIE WIRTUALIZACJI SERWERA....22
13 OPROGRAMOWANIE DO MONITOROWANIA SERWERÓW, STACJI ROBOCZYCH, URZĄDZEŃ SIECIOWYCH....22
14 WDROŻENIE OPROGRAMOWANIA DO MONITOROWANIA INFRASTRUKTURY INFORMATYCZNEJ....23
15 SYSTEM AUTOMATYCZNEGO SKANOWANIA SIECI, SERWERÓW, APLIKACJI I URZĄDZEŃ POD KĄTEM PODATNOŚCI BEZPIECZEŃSTWA....24
16 WDROŻENIE SYSTEMU AUTOMATYCZNEGO SKANOWANIA SIECI, SERWERÓW, APLIKACJI I URZĄDZEŃ POD KĄTEM PODATNOŚCI BEZPIECZEŃSTWA....24
17 URZĄDZENIE UTM....24
18 WDROŻENIE URZĄDZENIA UTM....25
19 PRZEŁĄCZNIKI ZARZĄDZALNE Z OBSŁUGĄ VLAN I PROTOKOŁU 802.1X. (4 SZT.)....26
20 WDROŻENIE PRZEŁĄCZNIKÓW ZARZĄDZALNYCH Z OBSŁUGĄ VLAN I PROTOKOŁU 802.1X....26
21 ZAPORA SIECIOWA UTM KLASY PRZEMYSŁOWEJ DLA SEGMENTACJI I OCHRONY SIECI OT/ICS....27
22 WDROŻENIE ZAPORY SIECIOWEJ UTM KLASY PRZEMYSŁOWEJ DLA SEGMENTACJI I OCHRONY SIECI OT/ICS....28
23 EDR DO OCHRONY STACJI ROBOCZYCH I SERWERÓW OT (3 SZT.)....28
24 WDROŻENIE SYSTEMU EDR DO OCHRONY STACJI ROBOCZYCH I SERWERÓW OT....29
25 SYSTEM MONITOROWANIA INFRASTRUKTURY OT DO ANALIZY LOGÓW, ZDARZEŃ I ANOMALII W ŚRODOWISKU PRZEMYSŁOWYM....29
26 WDROŻENIE SYSTEMU MONITOROWANIA INFRASTRUKTURY OT....29
27 SONDY/SENSORY DO PASYWNEGO MONITOROWANIA RUCHU I PROTOKOŁÓW PRZEMYSŁOWYCH W SIECIACH OT....30
28 WDROŻENIE SOND/SENSORÓW DO PASYWNEGO MONITOROWANIA RUCHU I PROTOKOŁÓW PRZEMYSŁOWYCH W SIECIACH OT....31
29 INSTALACJA, KONFIGURACJA I WSPARCIE TECHNICZNE SYSTEMU UWIERZYTELNIANIA I AUTORYZACJI DOSTĘPU DO SIECI RADIUS....31
30 INSTALACJA, KONFIGURACJA, WDROŻENIE I URUCHOMIENIE SYSTEMU LOG MANAGER DO SCENTRALIZOWANEGO GROMADZENIA, PRZECHOWYWANIA,

WYSZUKIWANIA, ANALIZY I ALARMOWANIA ZDARZEŃ LOGOWYCH Z INFRASTRUKTURY IT/OT.....34

1 Centralny system EDR (Endpoint Detection & Response) (20 szt.)

Obecnie Zamawiający użytkuję oprogramowanie ESET PROTECT ENTRY o identyfikatorze licencji 3A2-PSA-XNU Dostarczone oprogramowanie musi zostać przedłużone o rok oraz podniesione przynajmniej do wersji ESET PROTECT Enterprise oraz chronić minimum 20 komputery

2 Wdrożenie systemu EDR (20 szt.)

Usługa obejmuje podniesienie obecnie użytkowanego rozwiązania z wersji ESET Endpoint Antivirus do co najmniej ESET PROTECT Enterprise dla 20 chronionych urządzeń. W ramach wdrożenia Wykonawca:

- zweryfikuje aktualne środowisko ESET oraz stan istniejącej licencji,
- przeprowadzi migrację i aktywację licencji ESET PROTECT Enterprise,
- skonfiguruje funkcjonalności EDR dostępne w nowej wersji,
- przypisze ochronę do wszystkich 20 urządzeń objętych licencją,
- zweryfikuje poprawność komunikacji agentów z konsolą zarządzającą,
- przeprowadzi test poprawności działania oraz potwierdzi prawidłowe funkcjonowanie systemu po migracji.

Wdrożenie zostanie wykonane z zachowaniem ciągłości ochrony stacji roboczych oraz z wykorzystaniem istniejącej infrastruktury Zamawiającego.

3 Punkty dostępowe klasy enterprise z obsługą WPA3 i centralną kontrolą (4 szt.)

Funkcjonalność	**Wymagania minimalne**
Ogólne	Punkt dostępowy WiFi przeznaczony do montażu sufitowego lub ściennego, zgodny ze standardem WiFi 7 (IEEE 802.11be). Urządzenie wyposażone w sześć strumieni przestrzennych (2×2 MIMO dla pasm 2,4 GHz, 5 GHz oraz 6 GHz), umożliwiające jednoczesną obsługę ponad 300 klientów. Zasilanie poprzez PoE+.
Parametry techniczne	• Wymiary: Ø206 × 46 mm • Waga: maks. 680 g • Interfejs sieciowy: minimum 1 × RJ45 1/2.5 Gigabit Ethernet • Standard bezprzewodowy: WiFi 7 (802.11be) z kompatybilnością wsteczną z WiFi 6/6E, WiFi 5 i WiFi 4 • Liczba strumieni: 6 (2×2 MIMO dla każdego pasma) • Maksymalna przepustowość: do 5,8 Gb/s (6 GHz), 4,3 Gb/s (5 GHz), 688 Mb/s (2,4 GHz) • Maksymalna moc nadawcza: min. 23 dBm (2,4 GHz i 6 GHz), min. 26 dBm (5 GHz) • Zysk anten: minimum 4 dBi (2,4 GHz), 6 dBi (5 GHz), 5,8 dBi (6 GHz) • Pokrycie sygnałem: minimum 140 m² • Obsługa minimum 300 klientów jednocześnie • Maksymalny pobór mocy: 21 W • Zakres napięcia zasilania: 44–57 V DC (PoE+) • Zestaw montażowy do montażu sufitowego lub ściennego w komplecie
Funkcjonalność	• Obsługa Wireless Mesh• Band Steering • 802.11r Fast Roaming, 802.11k oraz 802.11v

	• Obsługa sieci gościnnej (Captive Portal) • Izolacja klientów i sieci gościnnej • Dynamiczne przypisywanie VLAN (Dynamic VLAN) • Obsługa PPSK (Private Pre-Shared Key) • Integracja z serwerem RADIUS oraz RadSec • Harmonogramy działania sieci WiFi • Ograniczanie przepustowości klientów
Odporność i zgodność	• Temperatura pracy: od -30°C do +40°C • Wilgotność pracy: 5–95% bez kondensacji • Obudowa z poliwęglanu z elementami metalowymi • Zgodność z normami CE, FCC, IC oraz NDAA Compliant
Gwarancja producenta	Minimum 12 miesięcy

4 Wdrożenie urządzeń Access Point (4 szt.)

Usługa obejmuje dostawę, montaż, konfigurację oraz uruchomienie 4 punktów dostępowych WiFi. W ramach wdrożenia Wykonawca:

- zamontuje urządzenia w lokalizacjach wskazanych przez Zamawiającego,
- skonfiguruje urządzenia w systemie centralnego zarządzania,
- utworzy i skonfiguruje sieci bezprzewodowe zgodnie z wymaganiami Zamawiającego,
- skonfiguruje parametry bezpieczeństwa oraz dostęp do sieci,
- zweryfikuje poprawność działania urządzeń, roamingu oraz łączności bezprzewodowej,
- przeprowadzi test poprawności działania i przekaże urządzenia do eksploatacji.

5 Serwer NAS

Funkcjonalność	**Wymagania minimalne**
Procesor	Procesor czterordzeniowy 64-bitowy o taktowaniu nie niższym niż 2.2GHz
Obudowa	RACK 19" 2U – wraz z kompletem szyn umożliwiającym zamontowanie w szafie RACK
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	1. Minimum 4GB DDR4 ECC - RAM tego samego producenta, co serwer NAS. 2. Pamięć RAM zgodna z listą kompatybilności producenta oferowanego serwera. 3. Możliwość rozszerzenia RAM do 32GB.
Całkowita liczba gniazd pamięci	Minimum 2 – jeden slot musi zostać wolny
Liczba zatok na dyski twarde	Minimum 8
Obsługiwane dyski twarde	1. 3.5" SATA HDD / 2.5" SATA SSD 2. Zamawiający wymaga dostarczenia minimum 8dysków 3.5” SATA HDD o pojemności 4TB każdy o parametrach nie gorszych niż: 3. Prędkość obrotowa: 7200 RPM 4. MTTF/MTBF: 2 000 000 5. Obciążenie roczne: 550 TB 6. Gwarancja producenta dysku: 5 lat 7. Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera. 8. Dyski zgodne z listą kompatybilności producenta oferowanego serwera.
Możliwość podłączenia	Tak

modułu rozszerzającego	
Minimalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż:	12
Porty na karty rozszerzeń	Minimum 1 x Gen3 x8 slot (x4 link)
Porty LAN	Wbudowane min. 4 x RJ-45 1GbE Min. 2x SFP+ 10GbE, możliwe przez zastosowanie karty rozszerzeń
Porty USB 3.2	Minimum 2
Port eSATA	Minimum 1
Zasilanie	Redundantny zasilacz o mocy minimalnej 350W
Mechanizm szyfrowania sprzętowego	Tak, min AES-NI
Wewnętrzny system plików	BTRFS, EXT4
Obsługiwane tryby RAID	JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny
Uprawnienia	Uprawnienia listy kontroli dostępu systemu Windows (ACL)
Usługa katalogowa	Łączy się z serwerami Windows® AD/LDAP, umożliwiając użytkownikom domeny logowanie za pośrednictwem protokołów SMB/FTP/WebDAV/File Station
Bezpieczeństwo	1. Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zapora sieciowa, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania), 2. dwuetapowa weryfikacja logowania (2FA), 3. adaptacyjna metoda logowania dla konta administratora (AMFA), 4. możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, 5. grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.
Oprogramowanie do kopii zapasowej	1. Oferowany serwer musi mieć oprogramowanie do kopii zapasowej bez konieczności ponoszenia dodatkowych kosztów. 2. Minimalne wymagane funkcje oprogramowania do backupu: a. kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal, b. kopia zapasowa środowisk MacOS c. kopia zapasowa maszyn wirtualnych (VMware, Hyper-V) d. kopia zapasowa serwerów fizycznych (Windows, Linux) e. obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania, f. obsługa wielu wersji i retencji, g. możliwość wyzwalania kopii zapasowej według harmonogramu, h. obsługa klastra przełączania awaryjnego Microsoft Hyper-V min. 2022 i. automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego

	nagrania wideo z odtworzenia w formie maszyny wirtualnej, j. centralne zarządzanie, k. konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań, l. portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora), m. delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla użytkowników bez uprawnień administratora, n. kopia zapasowa usług chmur publicznych Microsoft 365 i Google Workspace
Oprogramowanie	1. Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych 2. Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników. 3. Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. 4. Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync 5. Obsługa minimum 256 migawek na folder współdzielony i 4096 6. Funkcja serwera VPN (OpenVPN, L2TP/IPSec i PPTP) dla minimum 30 jednoczesnych połączeń
Gwarancja producenta serwera	Minimum 3 lata gwarancji świadczonej przez autoryzowany serwis producenta

6 Wdrożenie Serwera NAS

Usługa obejmuje dostawę, montaż, konfigurację oraz uruchomienie serwera NAS wraz z zainstalowanymi dyskami twardymi. W ramach wdrożenia Wykonawca:

- zamontuje serwer w szafie RACK Zamawiającego wraz z kompletem szyn montażowych,
- zainstaluje oraz skonfiguruje dostarczone dyski twarde,
- skonfiguruje przestrzeń dyskową oraz macierz RAID zgodnie z wymaganiami Zamawiającego,
- skonfiguruje woluminy, foldery współdzielone oraz uprawnienia dostępu,
- zintegruje serwer z usługą katalogową Active Directory lub LDAP (jeżeli jest wykorzystywana przez Zamawiającego),
- skonfiguruje podstawowe mechanizmy bezpieczeństwa, w tym szyfrowanie, migawki, zaporę sieciową oraz uwierzytelnianie wieloskładnikowe, jeżeli będą wykorzystywane,

- skonfiguruje oprogramowanie do wykonywania kopii zapasowych oraz harmonogramy backupu zgodnie z wymaganiami Zamawiającego,
- przeprowadzi aktualizację oprogramowania systemowego i firmware do aktualnych wersji producenta,
- wykona test poprawności działania urządzenia, macierzy RAID, usług sieciowych oraz dostępu do zasobów,
- przekaże urządzenie do eksploatacji wraz z podstawową dokumentacją powdrożeniową.

7 Oprogramowanie do obsługi MFA

Funkcjonalność	Wymagania minimalne
Ogólne	• System musi zawierać konsolę administracyjną dostępną z poziomu przeglądarki internetowej umożliwiającą administratorowi jego konfigurację oraz zarządzanie. • Dostęp do konsoli administracyjnej systemu musi być chroniony uwierzytelnianiem wieloskładnikowym, z możliwością ograniczenia konieczności potwierdzania żądania uwierzytelnienia wieloskładnikowego czynnikiem niepodatnym na ataki phishingowe (np. kluczem sprzętowym typu FIDO2/U2F). • System musi umożliwiać samodzielną rejestrację i zarządzanie uwierzytelniaczami (tokenami uwierzytelniającymi) przez użytkowników. • System musi umożliwiać w konsoli administracyjnej rejestrację przez administratora uwierzytelniaczy w postaci sprzętowych kluczy typu FIDO2/U2F dla określonych użytkowników. System musi również umożliwiać zarządzanie zarejestrowanymi uwierzytelniaczami tego typu oraz wyświetlanie szczegółowych informacji na ich temat, w tym adresu IP, z którego dokonano rejestracji, AAGUID, algorytmu COSE oraz licznika podpisów. • System musi umożliwiać potwierdzenie żądania uwierzytelnienia wieloskładnikowego poprzez zareagowanie na spersonalizowane powiadomienie wysyłane na urządzenie mobilne użytkownika (mobilne systemy operacyjne iOS, Android oraz Harmony OS). • System musi umożliwiać potwierdzenie żądania uwierzytelnienia wieloskładnikowego poprzez wpisanie kodu jednorazowego pochodzącego z dowolnej aplikacji generującej kody jednorazowe zgodnie ze standardem TOTP (RFC 6238). Przykładami takich aplikacji są Microsoft Authenticator oraz Google Authenticator. • System musi umożliwiać potwierdzenie żądania uwierzytelniania wieloskładnikowego poprzez wpisanie kodu jednorazowego wysłanego na numer telefonu użytkownika w postaci wiadomości SMS. • System musi wspierać możliwość potwierdzenia żądania uwierzytelnienia wieloskładnikowego poprzez kliknięcie w link wysłany na numer telefonu użytkownika w postaci wiadomości SMS. • System musi umożliwiać zebranie zgody użytkownika na wysyłkę

	wiadomości uwierzytelniających poprzez SMS na numer telefonu użytkownika. • System musi umożliwiać wyświetlanie w konsoli administracyjnej informacji o udzielonej zgodzie od użytkownika na wysyłkę wiadomości uwierzytelniających poprzez SMS na wskazany numer telefonu. • System musi wspierać możliwość potwierdzenia żądania uwierzytelnienia wieloskładnikowego przy pomocy mobilnej aplikacji uwierzytelniającej, do której dostęp może być zabezpieczony przy pomocy blokady biometrycznej w postaci odcisku palca lub skanu twarzy, jeśli urządzenie mobilne użytkownika posiada taką techniczną możliwość. • System musi wspierać możliwość potwierdzenia żądania uwierzytelniania wieloskładnikowego poprzez zareagowanie na połączenie telefoniczne nawiązane przez System na stacjonarny lub mobilny numer telefonu użytkownika. • System musi umożliwiać zakładanie kont administratorów mających dostęp do konsoli administracyjnej wraz z przypisaniem im roli stosownej do zakresu obowiązków danego administratora. • System musi umożliwiać identyfikowanie użytkowników po aliasach. • System musi umożliwiać udzielanie dostępu do określonych chronionych rozwiązań informatycznych tylko wybranym grupom użytkowników. • System musi wygaszać sesję administratora w konsoli administracyjnej w przypadku nieaktywności administratora. • System musi umożliwiać przeszukiwanie list zarejestrowanych przez użytkowników numerów telefonów oraz kluczy sprzętowych. • System musi zapewnić reguły lub polityki zarządzania żądaniami uwierzytelnienia użytkowników w oparciu o zdefiniowane parametry, co najmniej takie jak: grupa, chroniony zasób, lokalizacja (kraj) użytkownika oraz adres IP użytkownika. System powinien umożliwiać przypisywanie różnych reguł lub polityk indywidualnie do każdej chronionej aplikacji, w zależności od przynależności użytkownika do określonej grupy użytkowników. • System musi umożliwiać wygenerowanie tymczasowego kodu dostępowego dla wskazanego użytkownika w przypadku niedostępności uwierzytelniacza, np. zagubienia klucza uwierzytelniającego. • System musi zapewnić logowanie żądań uwierzytelniania użytkowników. System musi umożliwiać pobieranie logów w formacie CSV lub poprzez API. • System musi zapewnić logowanie zdarzeń związanych z obsługą Systemu (wprowadzanie zmian w konfiguracji i politykach, logowanie działań administratorów). System musi umożliwiać pobieranie logów w formacie

	CSV lub poprzez API. • System musi posiadać API (pol.: Interfejs Programowania Aplikacji) umożliwiające zarządzanie co najmniej użytkownikami oraz pobieranie logów. • System musi zapewnić interfejs użytkownika dokonującego uwierzytelniania do chronionych aplikacji w j. polskim.
Integracje	• System musi zapewniać możliwość uruchomienia uwierzytelniania wieloskładnikowego dla rozwiązań uwierzytelniających użytkowników ze źródeł Active Directory (LDAP, LDAPS) i RADIUS. • System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego dla logowania do stacji roboczych z systemem operacyjnym Microsoft Windows 7 i nowszymi wersjami, oraz do serwerów z systemem operacyjnym Microsoft Windows Server 2008 R2 i nowszymi wersjami. W przypadku braku połączenia z Internetem musi być możliwe wykonanie uwierzytelnienia wieloskładnikowego przynajmniej w postaci jednorazowego hasła (One-Time Password, OTP). • System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego przy pomocy sprzętowego klucza zgodnego ze standardem FIDO2 dla logowania do stacji roboczych z systemem operacyjnym Microsoft Windows, oraz poprzez RDP do serwerów z systemem operacyjnym Microsoft Windows Server. • System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego przy użyciu karty RFID dla logowania do stacji roboczych z systemem operacyjnym Microsoft Windows oraz dla logowania poprzez RDP do serwerów z systemem operacyjnym Microsoft Windows Server. • System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla technologii: Microsoft Outlook Web App (OWA), Microsoft Remote Desktop Gateway/Web Access/Web Client/Web Feed oraz Microsoft Active Directory Federation Services (AD FS). • System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla połączeń przez protokół Remote Desktop Protocol (RDP). • System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla połączeń SSH do systemów Linux. • System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla dostępu do rozwiązań VPN w oparciu o protokoły RADIUS i LDAP. • System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla dostępu do urządzeń sieciowych (routery,

	switche, zapory sieciowe) w oparciu o protokoły RADIUS i LDAP. • System musi umożliwiać integrację z oprogramowaniem własnym poprzez zastosowanie Software Development Kit (SDK), np. dla oprogramowania .NET, Java, PHP, które umożliwi wykonywanie uwierzytelniania wieloskładnikowego w tym oprogramowaniu. • System musi umożliwiać jednostronną synchronizację użytkowników ze źródeł Microsoft Active Directory, OpenLDAP oraz Microsoft Entra ID.
Wymagania licencyjne oraz gwarancyjne	• Oferent jest zobowiązany do dostarczenia oświadczenia Producenta Systemu potwierdzającego, że Oferent jest Autoryzowanym Partnerem Producenta Systemu. • Oferent jest zobowiązany do dostarczenia oświadczenia Producenta Systemu potwierdzającego, że w przypadku zaprzestania działalności Oferenta (likwidacji, upadłości lub innych przyczyn uniemożliwiających realizację wsparcia technicznego), Producent przejmie zobowiązanie wsparcia technicznego na rzecz Zamawiającego. • Oferowany System musi istnieć na rynku co najmniej przez okres 3 lat oraz posiadać wsparcie techniczne w języku polskim. • Producentem Systemu musi być podmiot posiadający siedzibę w Unii Europejskiej. • Producent Systemu musi posiadać wdrożony system zarządzania bezpieczeństwem informacji, potwierdzony ważnym certyfikatem zgodności z normą ISO/IEC 27001:2023 lub normą równoważną, obejmujący projektowanie i wytwarzanie oprogramowania, bezpieczeństwo informacji oraz ciągłość działania. • W ramach przedmiotu zamówienia Wykonawca zobowiązuje się udzielić lub zapewnić udzielenie wszelkich licencji wymaganych do prawidłowego działania Systemu, jako całości, jak i poszczególnych jego elementów, dla maksymalnie 20 użytkowników, na okres 12 miesięcy, oraz dostarczyć Oprogramowanie niezbędne do uruchomienia Systemu.

8 Wdrożenie oprogramowania MFA

Usługa obejmuje instalację, konfigurację oraz uruchomienie systemu uwierzytelniania wieloskładnikowego (MFA). W ramach wdrożenia Wykonawca:

- zainstaluje i skonfiguruje system MFA,
- zintegruje rozwiązanie z usługą katalogową wykorzystywaną przez Zamawiającego (np. Active Directory lub LDAP), jeżeli jest stosowana,
- skonfiguruje polityki uwierzytelniania wieloskładnikowego zgodnie z wymaganiami Zamawiającego,

- skonfiguruje metody uwierzytelniania dla użytkowników oraz administratorów,
- przeprowadzi rejestrację i aktywację użytkowników objętych wdrożeniem,
- skonfiguruje mechanizmy zabezpieczeń dostępu do wskazanych usług i systemów,
- przeprowadzi testy poprawności logowania oraz działania mechanizmów MFA,
- zaktualizuje oprogramowanie do aktualnej wersji producenta oraz przekaże system do eksploatacji.

9 Serwer Enterprise

Funkcjonalność	Wymagania minimalne
Obudowa	• Obudowa Rack o wysokości max 1U • 8 slotów na dyski 2.5” SAS/SATA • Obudowa wyposażona w ramkę chroniącą dyski przed nieuprawnionym dostępem.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 144 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	• Zainstalowane dwa procesory min. 16-rdzeniowe, min. 2.3GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 245 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej oferowanego serwera.
RAM	• 512GB DDR5 RDIMM 6400MT/s,

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  ○ Wsparcie dla dysków samoszyfrujących
	  ○ Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS

Dyski twarde	• Zainstalowane:
	  ○ dyski SSD SATA o przepustowości interfejsu minimum 6 Gb/s, skonfigurowane w macierzy RAID 6, zapewniającej odporność na jednoczesną awarię co najmniej dwóch dysków oraz przestrzeń użytkową o pojemności minimum 5 TB,
	  ○ dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.

Gniazda PCI	• Min. dwa sloty PCIe LP x16
Interfejsy sieciowe/FC/SAS	• 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

	• 4 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Wbudowane porty	• 4 portów USB w tym min:
	  ○ 1 port USB 2.0 Type-C
	  ○ 2 porty USB 3.1
	  ○ 1 port USB 3.0 wewnątrz obudowy
	• Port VGA z tyłu obudowy

Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 800W klasy Titanium • 2x przewód C13/C14 o dl. min. 2 m.
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych

Rozwiązanie operacyjny	Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w postaci **2 wirtualnych środowisk SSO** za pomocą wbudowanych mechanizmów wirtualizacji.
	Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta.
	SSO musi posiadać następujące, wbudowane cechy:
	a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,
	b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,
	c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych,
	d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,
	e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
	f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,
	g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,
	h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),
	i) wbudowane wsparcie instalacji i pracy na wolumenach, które:
	  I. pozwalają na zmianę rozmiaru w czasie pracy systemu,
	  II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
	  III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
	  IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL),
	j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
	k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających

	min. certyfikat FIPS 140-2 l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków,

	4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, • z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Licencje dostępowe	• Należy dostarczyć **20 licencji dostępowych** na użytkownika tzw. USER CAL
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika ○ możliwość podmontowania zdalnych wirtualnych napędów ○ wirtualną konsolę z dostępem do myszy, klawiatury ○ wsparcie dla IPv6 ○ wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer ○ integracja z Active Directory ○ możliwość obsługi przez sześciu administratorów jednocześnie

	○ Wsparcie dla automatycznej rejestracji DNS ○ wsparcie dla LLDP ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej ○ możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. ○ Monitorowanie zużycia dysków SSD ○ Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ Automatyczne update firmware dla wszystkich komponentów serwera ○ Możliwość przywrócenia poprzednich wersji firmware ○ Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON ○ Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych ○ Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. ○ Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera ○ kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania ○ możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień ○ możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera ○ możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer ○ możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe możliwość rozszerzenia funkcjonalności o: ○ możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch ○ możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej ○ Automatyczne odświeżanie certyfikatów SSL ○ monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów

	○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz

	automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów o Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo o Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. o Musi istnieć możliwość tworzenia własnych polityk

	bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. o Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia o Urządzenie Producenta dostarczane w ramach postępowania o Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent o Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności o Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Okres gwarancji **minimum 60 miesięcy** gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego – dokumenty potwierdzające należy załączyć do oferty. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – dokumenty potwierdzające należy załączyć do oferty. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru

	zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. • Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. • Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty. • Wskazana firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny dokument np. certyfikat lub deklaracją producenta, potwierdzającą autoryzację dla wskazanej firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku gdy dany producent nie posiada takiego ogólnodostępnego dokumentu, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski – dokumenty potwierdzające należy załączyć do oferty.

10 Wdrożenie i uruchomienie serwera Enterprise

Usługa obejmuje dostawę, montaż, konfigurację oraz uruchomienie serwera klasy Enterprise w infrastrukturze Zamawiającego. W ramach wdrożenia Wykonawca:

- zamontuje serwer w szafie RACK wraz z kompletem szyn montażowych,
- zainstaluje i skonfiguruje wszystkie dostarczone podzespoły, w tym procesory, pamięć operacyjną, kontroler RAID oraz dyski,
- skonfiguruje macierz RAID zgodnie z wymaganiami Zamawiającego,
- zaktualizuje firmware serwera oraz wszystkich komponentów do aktualnych wersji producenta,
- skonfiguruje kontroler zarządzania serwerem oraz podstawowe parametry monitorowania i zdalnego dostępu,
- zainstaluje i skonfiguruje system operacyjny, jeżeli jest objęty przedmiotem zamówienia,
- skonfiguruje interfejsy sieciowe oraz podstawowe parametry pracy serwera,
- przeprowadzi testy poprawności działania podzespołów, macierzy dyskowej oraz komunikacji sieciowej,
- zweryfikuje poprawność działania systemu po wdrożeniu i przekaże serwer do eksploatacji,
- przekaże podstawową dokumentację powdrożeniową obejmującą konfigurację serwera oraz zastosowane ustawienia.

11 System Wirtualizacji

Nazwa	Minimalne wymagania dla sprzętu
Ogólne	System kopii zapasowych klasy enterprise oparty o komponenty Open Source, przeznaczony do centralnego zarządzania kopiami bezpieczeństwa środowisk fizycznych oraz wirtualnych. Rozwiązanie umożliwia wdrożenie w środowisku wirtualnym Zamawiającego oraz zapewnia skalowalną architekturę umożliwiającą dalszą rozbudowę systemu backupowego wraz ze wzrostem infrastruktury. System realizuje mechanizmy wykonywania kopii pełnych oraz przyrostowych z wykorzystaniem deduplikacji blokowej, kompresji danych oraz mechanizmów syntetycznych kopii bezpieczeństwa. Rozwiązanie umożliwia definiowanie polityk retencji danych, harmonogramów backupu, wykonywanie kopii lokalnych i

	wynaszanych (off-site), a także szybkie odtwarzanie danych na poziomie pojedynczych plików, katalogów, obrazów systemów oraz środowisk wirtualnych. Rozwiązanie zapewnia: • centralne zarządzanie z poziomu interfejsu WWW oraz CLI, • szyfrowanie komunikacji oraz danych backupowych, • monitorowanie procesów backupu i odtwarzania, • obsługę polityk retencji i harmonogramów, • ograniczanie wykorzystania pasma sieciowego, • mechanizmy integralności danych, • możliwość replikacji danych pomiędzy lokalizacjami, • obsługę środowisk fizycznych oraz wirtualnych, • możliwość rozbudowy o dodatkowe repozytoria danych, • zabezpieczenie dostępu do interfejsu administracyjnego z wykorzystaniem SSL/TLS. W ramach wdrożenia wykonana zostanie instalacja, konfiguracja oraz uruchomienie systemu kopii zapasowych wraz z konfiguracją repozytoriów danych, harmonogramów, polityk retencji oraz mechanizmów bezpieczeństwa. Wykonane zostaną testy poprawności działania oraz procedury odtworzeniowe potwierdzające poprawność działania rozwiązania. W ramach realizacji przewidziane jest również szkolenie administratora obejmujące konfigurację systemu, zarządzanie zadaniami backupowymi, procedury odtwarzania danych, monitorowanie pracy systemu oraz podstawowe czynności administracyjne i eksploatacyjne.

12 Wdrożenie wirtualizacji serwera

W ramach realizacji zamówienia Wykonawca:

1. zainstaluje i skonfiguruje system kopii zapasowych w środowisku Zamawiającego,
2. skonfiguruje repozytoria danych przeznaczone do przechowywania kopii zapasowych,
3. zaktualizuje oprogramowanie systemowe do aktualnej stabilnej wersji producenta/projektu,
4. skonfiguruje harmonogramy wykonywania kopii zapasowych oraz polityki retencji danych,
5. skonfiguruje mechanizmy deduplikacji, kompresji, szyfrowania oraz weryfikacji integralności kopii zapasowych,
6. skonfiguruje wykonywanie kopii zapasowych wskazanych maszyn wirtualnych, serwerów oraz danych zgodnie z wymaganiami Zamawiającego,
7. skonfiguruje mechanizmy replikacji lub wykonywania kopii poza lokalizację podstawową (off-site), jeżeli będą wykorzystywane,
8. skonfiguruje monitorowanie procesów wykonywania kopii zapasowych oraz powiadamianie o błędach i zakończonych zadaniach,
9. wykona testowe kopie zapasowe oraz przeprowadzi testy odtworzenia danych, potwierdzające poprawność działania rozwiązania,
10. przygotuje i przekaże dokumentację powdrożeniową obejmującą konfigurację systemu, harmonogramy, polityki retencji oraz procedury wykonywania i odtwarzania kopii zapasowych,

13 Oprogramowanie do monitorowania serwerów, stacji roboczych, urządzeń sieciowych

System monitoringu infrastruktury	
Nazwa parametru	Minimalna wartość parametru
Ogólne	System monitorowania infrastruktury IT klasy Open Source przeznaczony do centralnego nadzoru nad dostępnością, wydajnością i stanem technicznym urządzeń oraz usług teleinformatycznych. Rozwiązanie umożliwia monitorowanie serwerów fizycznych i wirtualnych, stacji roboczych, urządzeń sieciowych, systemów operacyjnych, aplikacji, baz danych, usług sieciowych oraz środowisk chmurowych. System powinien zapewniać: * centralne zbieranie danych eksploatacyjnych i wydajnościowych z urządzeń oraz systemów, * monitorowanie dostępności usług, aplikacji, serwerów, urządzeń sieciowych oraz zasobów infrastruktury, * monitorowanie parametrów pracy takich jak wykorzystanie procesora, pamięci RAM, przestrzeni dyskowej, interfejsów sieciowych i usług systemowych, * obsługę standardów monitorowania, w tym m.in. SNMP, ICMP, IPMI, JMX, Syslog oraz mechanizmów agentowych, * automatyczne wykrywanie urządzeń sieciowych, interfejsów, usług i zasobów infrastruktury, * budowę map topologii sieci oraz wizualizację zależności pomiędzy monitorowanymi zasobami, * definiowanie progów alarmowych, reguł korelacji zdarzeń oraz automatycznych działań reakcyjnych, * generowanie powiadomień o awariach, przekroczeniu parametrów lub utracie dostępności usług, * wysyłanie powiadomień za pomocą poczty elektronicznej oraz integrację z zewnętrznymi systemami komunikacji, * tworzenie dashboardów prezentujących stan infrastruktury w czasie rzeczywistym, * budowę raportów historycznych i analiz trendów wykorzystania zasobów, * planowanie pojemności infrastruktury na podstawie danych historycznych, * przechowywanie danych historycznych wraz z możliwością definiowania okresów retencji, * zarządzanie monitorowanymi zasobami z wykorzystaniem szablonów konfiguracyjnych, * delegowanie uprawnień użytkownikom oraz integrację z usługami katalogowymi, * dostęp do systemu za pomocą interfejsu WWW, * integrację z systemami zarządzania bezpieczeństwem, systemami klasy SIEM oraz platformami automatyzacji. Architektura rozwiązania powinna umożliwiać pracę rozproszoną z wykorzystaniem serwerów pośredniczących zbierających dane z lokalizacji zdalnych, zapewniając skalowalność i możliwość monitorowania infrastruktury wielooddziałowej. Rozwiązanie powinno być dostarczone na licencji Open Source i nie może wymagać ponoszenia kosztów licencyjnych za monitorowanie urządzeń, serwerów, usług lub użytkowników.

14 Wdrożenie oprogramowania do monitorowania infrastruktury informatycznej

Usługa obejmuje instalację, konfigurację oraz uruchomienie centralnego systemu monitorowania infrastruktury IT. W ramach wdrożenia Wykonawca:

- zainstaluje i skonfiguruje serwer systemu monitorowania,
- skonfiguruje bazę danych oraz interfejs administracyjny,
- doda do monitorowania wskazane serwery, stacje robocze, urządzenia sieciowe oraz usługi,
- skonfiguruje mechanizmy monitorowania z wykorzystaniem protokołów SNMP, ICMP, agentów systemowych oraz innych obsługiwanych metod monitorowania,
- skonfiguruje automatyczne wykrywanie urządzeń i usług w infrastrukturze,
- przygotuje dashboardy prezentujące stan monitorowanych zasobów,
- skonfiguruje progi alarmowe, reguły powiadomień oraz kanały powiadamiania,
- skonfiguruje zbieranie danych historycznych oraz retencję danych,
- skonfiguruje mapy infrastruktury oraz podstawowe wizualizacje zależności pomiędzy monitorowanymi urządzeniami,
- zweryfikuje poprawność działania monitoringu poprzez przeprowadzenie testów działania i generowania alarmów,
- przekaże system do eksploatacji wraz z podstawową dokumentacją powdrożeniową.

15 System automatycznego skanowania sieci, serwerów, aplikacji i urządzeń pod kątem podatności bezpieczeństwa

Nazwa	Minimalne wymagania dla sprzętu
Ogólne	System klasy Vulnerability Management w modelu Open Source przeznaczony do identyfikacji podatności oraz oceny poziomu bezpieczeństwa infrastruktury IT i OT.
Skanowanie	Możliwość wykonywania skanów podatności urządzeń sieciowych, serwerów, stacji roboczych, systemów operacyjnych oraz usług sieciowych z wykorzystaniem skanów uwierzytelnionych i nieuwierzytelnionych.
Baza podatności	Wykorzystanie aktualizowanej bazy testów podatności (VT) obejmującej informacje CVE, CPE, CVSS oraz inne publicznie dostępne źródła informacji o zagrożeniach.
Funkcjonalność	• Harmonogramy automatycznych skanów.• Tworzenie raportów i historii skanowań.• Klasyfikacja podatności według poziomu ryzyka.• Obsługa skanów zgodności (Compliance).• Zarządzanie zasobami (Asset Management).• Eksport raportów do popularnych formatów.• Powiadomienia o zakończonych skanach.• Zarządzanie zadaniami skanowania z poziomu interfejsu WWW.
Integracja	Możliwość integracji z systemami monitorowania, SIEM oraz innymi rozwiązaniami bezpieczeństwa z wykorzystaniem dostępnych interfejsów i mechanizmów eksportu danych.
Licencjonowanie	Rozwiązanie Open Source niewymagające opłat licencyjnych za korzystanie z oprogramowania.
Ogólne	System klasy Vulnerability Management w modelu Open Source przeznaczony do identyfikacji podatności oraz oceny poziomu bezpieczeństwa infrastruktury IT i OT.

16 Wdrożenie systemu automatycznego skanowania sieci, serwerów, aplikacji i urządzeń pod kątem podatności bezpieczeństwa

Usługa obejmuje instalację, konfigurację oraz uruchomienie systemu zarządzania podatnościami. W ramach wdrożenia Wykonawca zainstaluje i skonfiguruje system, zaktualizuje bazę testów podatności, skonfiguruje skanowanie wskazanych zasobów infrastruktury IT i OT, utworzy harmonogramy automatycznych skanów, skonfiguruje raportowanie oraz powiadomienia, zintegruje rozwiązanie z systemem monitorowania infrastruktury oraz systemem SIEM, jeżeli są dostarczane w ramach niniejszego zamówienia, przeprowadzi testy poprawności działania oraz przekaże rozwiązanie do eksploatacji wraz z podstawową dokumentacją powdrożeniową.

17 Urządzenie UTM

Nazwa	Minimalne wymagania dla sprzętu
Typ urządzenia	Urządzenie klasy UTM / Firewall w dedykowanej obudowie producenta umożliwiającej montaż w standardowej rack
Procesor	Urządzenie wyposażone w minimum ośmiordzeniowy procesor zgodny z architekturą x86
Pamięć operacyjna (RAM)	Minimum 32 GB DDR4 lub nowsza
Pamięć masowa (SSD)	Minimum 512 GB w technologii NVMe M.2
Interfejsy sieciowe	Minimum 3 porty RJ-45 o przepustowości 2.5 Gb/s. Minimum 4 porty SFP o przepustowości 1 Gb/s Minimum 4 porty SFP+ o przepustowości 10 Gb/s
Porty	Minimum 2 wolne sloty PCIe do rozbudowy Minimum 2 porty USB Minimum jeden port konsolowy
Wydajność	L3 Forwarding dla IPERF3 Traffic: min 35 Gbps Firewall 10k ACLs dla IPERF3 Traffic: min 25 Gbps IPsec VPN AES dla PERF3 Traffic: min.14 Gbps
Zasilanie	Redundantne zasilacze Hot-Plug
Parametry bezpieczeństwa	Oprogramowanie routera współpracujące z istniejącą infrastrukturą Zamawiającego i zapewniające funkcjonalności typowe dla firewalli klasy enterprise, w tym filtrowanie ruchu na podstawie adresów IP, portów i protokołów) Router w, obsługę reguł NAT (DNAT, SNAT, port forwarding) oraz stateful packet inspection. Urządzenie powinno obsługiwać rozwiązania VPN kompatybilne z posiadaną infrastrukturą Zamawiającego, oraz protokoły tunelowania i wirtualizacji sieci, takie jak IPsec, VLAN i GRE, umożliwiając zestawianie tuneli site-to-site oraz client-to-site z uwierzytelnianiem użytkowników za pomocą certyfikatów, login/hasło lub RADIUS/LDAP. Router musi obsługiwać zarówno trasy statyczne, jak i dynamiczne protokoły routingu, w tym BGP, OSPF i RIP. W przypadku protokołu BGP urządzenie musi umożliwiać obsługę tablicy routingu. Funkcjonalność DHCP dla IPv4 oraz IPv6 (DHCPv6) jest wymagana, w tym przydzielanie adresów IPv6 zarówno w trybie stateless, jak i stateful, wraz z możliwością konfiguracji zakresów adresów, rezerwacji i przydzielania statycznych adresów dla urządzeń sieciowych. Urządzenie musi posiadać mechanizmy QoS i shaping ruchu, umożliwiające priorytetyzację i ograniczanie pasma dla wybranych usług, użytkowników lub interfejsów, wraz z obsługą kolejkowania ruchu. Dodatkowo router musi oferować funkcje bezpieczeństwa i monitorowania, w tym IDS/IPS, obsługę blacklist oraz możliwość wysyłania logów na zewnętrzny serwer (syslog). System musi umożliwiać monitorowanie ruchu sieciowego i obciążenia urządzenia w czasie rzeczywistym. Administracja routera powinna odbywać się zarówno za pomocą graficznego interfejsu WWW (HTTPS), jak i CLI (SSH), z możliwością tworzenia kopii zapasowych i przywracania konfiguracji. Aktualizacje bezpieczeństwa muszą być dostępne bez dodatkowych opłat w okresie gwarancji. Oprogramowanie routera musi być dostępne wraz z kodem źródłowym i umożliwiać niezależnym deweloperom tworzenie i instalowanie dodatkowych funkcjonalności w formie modułów lub wtyczek, zgodnie z zasadami open source, co umożliwia rozwój i integrację z innymi rozwiązaniami.
Gwarancja ~~producenta~~	**Min. 12 miesięcy gwarancji realizowanej przez producenta lub Autoryzowanego Partnera Serwisowego producent.**

18 Wdrożenie urządzenia UTM

Usługa obejmuje dostawę, montaż, konfigurację oraz uruchomienie urządzenia klasy UTM/Firewall w infrastrukturze Zamawiającego. W ramach wdrożenia Wykonawca:

- zamontuje urządzenie w szafie RACK Zamawiającego,
- zainstaluje oraz uruchomi system operacyjny urządzenia,
- zaktualizuje firmware oraz oprogramowanie systemowe do aktualnej stabilnej wersji producenta,
- skonfiguruje podstawową adresację IP oraz interfejsy sieciowe,
- skonfiguruje routing statyczny oraz dynamiczny zgodnie z wymaganiami Zamawiającego,
- skonfiguruje translację adresów NAT (SNAT, DNAT oraz Port Forwarding),
- skonfiguruje polityki zapory sieciowej wraz z kontrolą dostępu pomiędzy segmentami sieci,
- skonfiguruje obsługę sieci VLAN oraz podstawową segmentację ruchu,
- skonfiguruje usługi DHCP dla IPv4 oraz IPv6, jeżeli będą wykorzystywane,
- skonfiguruje tunele VPN typu Site-to-Site oraz/lub Client-to-Site zgodnie z wymaganiami Zamawiającego,
- skonfiguruje mechanizmy IDS/IPS oraz podstawowe mechanizmy ochrony przed zagrożeniami,
- skonfiguruje mechanizmy QoS oraz ograniczania przepustowości dla wskazanych usług lub użytkowników,
- skonfiguruje wysyłanie logów do centralnego systemu monitorowania lub systemu SIEM,
- skonfiguruje monitorowanie stanu urządzenia, wykorzystania zasobów oraz ruchu sieciowego,
- wykona kopię zapasową konfiguracji urządzenia,
- przeprowadzi testy poprawności działania wszystkich skonfigurowanych usług, w tym routingu, zapory sieciowej, translacji NAT, VPN oraz mechanizmów bezpieczeństwa,
- przekaże urządzenie do eksploatacji wraz z podstawową dokumentacją powdrożeniową zawierającą opis konfiguracji oraz procedurę odtworzenia konfiguracji z kopii zapasowej.

19 Przełączniki zarządzalne z obsługą VLAN i protokołu 802.1X. (4 szt.)

Ogólne	Zarządzalny przełącznik warstwy L3 przeznaczony do montażu w szafie RACK 19” (1U), wyposażony w porty Gigabit Ethernet z obsługą PoE+, porty Multi-Gigabit 2.5GbE PoE+, porty uplink 10GBase-T oraz 10G SFP+. Urządzenie umożliwia fizyczne i wirtualne stackowanie, routing warstwy 3 oraz centralne zarządzanie siecią.
Parametry techniczne	• Obudowa Rack 19”, wysokość 1U• 44 × port 10/100/1000Base-T PoE+ • 4 × port 2.5GBase-T PoE+• 2 × port 10GBase-T • 2 × port 10G SFP+• Budżet PoE: do 370 W• Przepustowość przełączania: 188 Gbps • Maksymalna szybkość przekazywania pakietów: 139,88 Mpps • Tablica adresów MAC: minimum 16 384 wpisów • Obsługa do 512 statycznych adresów MAC• Obsługa ramek Jumbo do 12 288 B• MTBF: minimum 328 174 godzin• Wymiary: 441 × 308,5 × 44 mm• Masa: maks. 4,8 kg
Funkcjonalność	• Fizyczne stackowanie do 8 urządzeń z przepustowością stosu do 80 Gbps• Wirtualne stackowanie do 32 urządzeń• Obsługa VLAN (802.1Q, Voice VLAN, MAC VLAN, Private VLAN, Q-in-Q, Selective Q-in-Q)• Link Aggregation (LACP 802.1AX/802.3ad)• STP, RSTP, MSTP• ERPS• IGMP Snooping v1/v2/v3 oraz MLD Snooping• Routing IPv4/IPv6, trasy statyczne, RIP/RIPng, OSPF, VRRP• QoS z 8 kolejkami na port• ACL IPv4/IPv6• DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, IPv6 Guard• 802.1X, RADIUS, TACACS+, Dynamic VLAN• Zarządzanie przez WWW, CLI, SNMP v1/v2c/v3, SSH, HTTPS, Syslog, sFlow, LLDP/LLDP-MED• Zero Touch Provisioning (ZTP) oraz D-Link Network Assistant (DNA)
Odporność i zgodność	• Temperatura pracy: od -5°C do +50°C• Wilgotność pracy: 10–95% RH• Temperatura składowania: od -40°C do +70°C• Zgodność z CE Class A, FCC Class A, IC Class A, RCM Class A, VCCI Class A oraz BSMI Class A
Gwarancja	Minimum 5 lat gwarancji producenta lub zgodnie z warunkami producenta.

20 Wdrożenie Przełączników zarządzalnych z obsługą VLAN i protokołu 802.1X.

Usługa obejmuje dostawę, montaż, konfigurację oraz uruchomienie przełącznika sieciowego w infrastrukturze Zamawiającego. W ramach wdrożenia Wykonawca:

- zamontuje urządzenie w szafie RACK Zamawiającego,
- zaktualizuje oprogramowanie systemowe do aktualnej wersji producenta,
- skonfiguruje podstawowe parametry sieciowe, w tym adresację IP oraz dostęp administracyjny,
- skonfiguruje porty dostępowe, trunk, sieci VLAN oraz mechanizmy agregacji łączy zgodnie z wymaganiami Zamawiającego,
- skonfiguruje funkcje bezpieczeństwa przełącznika, w tym mechanizmy kontroli dostępu, zabezpieczenia portów oraz zarządzanie,
- skonfiguruje zasilanie PoE dla urządzeń końcowych, jeżeli będzie wykorzystywane,
- przeprowadzi test poprawności działania, komunikacji sieciowej oraz zasilania PoE,
- przekaże urządzenie do eksploatacji wraz z podstawową dokumentacją powdrożeniową.

21 Zapora sieciowa UTM klasy przemysłowej dla segmentacji i ochrony sieci OT/ICS

Nazwa	Minimalne wymagania dla sprzętu
Typ urządzenia	Urządzenie klasy UTM / Firewall przeznaczone do pracy z systemami Open Source (m.in. pfSense CE, OPNsense, OpenWRT lub równoważnymi), wykonane w kompaktowej obudowie umożliwiającej pracę ciągłą 24/7.
Procesor	Minimum czterordzeniowy procesor x86-64 o taktowaniu do 3,4 GHz, TDP nie większym niż 10 W.
Pamięć operacyjna	Minimum 8 GB DDR5 z możliwością rozbudowy do co najmniej 32 GB.
Pamięć masowa	Minimum 1 × gniazdo M.2 NVMe 2280 umożliwiające instalację dysku SSD.
Interfejsy sieciowe	Minimum 2 × port Ethernet 10 Gb/s SFP+ lub RJ45 oraz minimum 4 × port Ethernet 2.5 Gb/s RJ45.
Interfejsy I/O	Minimum 1 × USB 3.0, minimum 4 × USB 2.0, minimum 1 × USB-C, gniazdo kart pamięci microSD/TF oraz port konsolowy lub równoważny interfejs administracyjny.
Grafika	Wyjście HDMI oraz DisplayPort lub USB-C DisplayPort Alternate Mode umożliwiające lokalną administrację urządzeniem.
Obudowa	Aluminiowa obudowa przystosowana do ciągłej pracy, wyposażona w aktywny układ chłodzenia.
Zasilanie	Zasilacz zewnętrzny 12 V DC.
Funkcjonalność	Obsługa automatycznego uruchamiania po przywróceniu zasilania (Auto Power On).
Warunki pracy	Temperatura pracy minimum od -20°C do +60°C
Parametry bezpieczeństwa	Oprogramowanie routera współpracujące z istniejącą infrastrukturą Zamawiającego i zapewniające funkcjonalności typowe dla firewalli klasy enterprise, w tym filtrowanie ruchu na podstawie adresów IP, portów i protokołów) Router w, obsługę reguł NAT (DNAT, SNAT, port forwarding) oraz stateful packet inspection. Urządzenie powinno obsługiwać rozwiązania VPN kompatybilne z posiadaną infrastrukturą Zamawiającego, oraz protokoły tunelowania i wirtualizacji sieci, takie jak IPsec, VLAN i GRE, umożliwiając zestawianie tuneli site-to-site oraz client-to-site z uwierzytelnianiem użytkowników za pomocą certyfikatów, login/hasło lub RADIUS/LDAP. Router musi obsługiwać zarówno trasy statyczne, jak i dynamiczne protokoły routingu, w tym BGP, OSPF i RIP. W przypadku protokołu BGP urządzenie musi umożliwiać obsługę tablicy routingu. Funkcjonalność DHCP dla IPv4 oraz IPv6 (DHCPv6) jest wymagana, w tym przydzielanie adresów IPv6 zarówno w trybie stateless, jak i stateful, wraz z możliwością konfiguracji zakresów adresów, rezerwacji i przydzielania statycznych adresów dla urządzeń sieciowych. Urządzenie musi posiadać mechanizmy QoS i shaping ruchu, umożliwiające priorytetyzację i ograniczanie pasma dla wybranych usług, użytkowników lub interfejsów, wraz z obsługą kolejkowania ruchu. Dodatkowo router musi oferować funkcje bezpieczeństwa i

	monitorowania, w tym IDS/IPS, obsługę blacklist oraz możliwość wysyłania logów na zewnętrzny serwer (syslog). System musi umożliwiać monitorowanie ruchu sieciowego i obciążenia urządzenia w czasie rzeczywistym. Administracja routera powinna odbywać się zarówno za pomocą graficznego interfejsu WWW (HTTPS), jak i CLI (SSH), z możliwością tworzenia kopii zapasowych i przywracania konfiguracji. Aktualizacje bezpieczeństwa muszą być dostępne bez dodatkowych opłat w okresie gwarancji. Oprogramowanie routera musi być dostępne wraz z kodem źródłowym i umożliwiać niezależnym deweloperom tworzenie i instalowanie dodatkowych funkcjonalności w formie modułów lub wtyczek, zgodnie z zasadami open source, co umożliwia rozwój i integrację z innymi rozwiązaniami.
Gwarancja	12 miesięcy

22 Wdrożenie zapory sieciowej UTM klasy przemysłowej dla segmentacji i ochrony sieci OT/ICS

Usługa obejmuje dostawę, instalację, konfigurację oraz uruchomienie zapory sieciowej opartej o oprogramowanie Open Source. W ramach wdrożenia Wykonawca:

- zamontuje i uruchomi urządzenie w miejscu wskazanym przez Zamawiającego,
- zainstaluje oraz skonfiguruje system operacyjny zapory sieciowej,
- zaktualizuje BIOS/UEFI urządzenia oraz oprogramowanie systemowe i wszystkie komponenty do aktualnych stabilnych wersji,
- skonfiguruje interfejsy sieciowe, adresację IP oraz podstawowy routing,
- skonfiguruje translację adresów NAT (SNAT, DNAT oraz Port Forwarding),
- skonfiguruje polityki zapory sieciowej wraz z regułami filtrowania ruchu pomiędzy sieciami,
- skonfiguruje sieci VLAN oraz podstawową segmentację ruchu sieciowego,
- skonfiguruje usługi DHCP dla IPv4 oraz IPv6, jeżeli będą wykorzystywane,
- skonfiguruje routing statyczny oraz dynamiczny zgodnie z wymaganiami Zamawiającego,
- skonfiguruje tunele VPN typu Site-to-Site oraz Client-to-Site wraz z mechanizmami uwierzytelniania użytkowników,
- zainstaluje i skonfiguruje moduły rozszerzające realizujące funkcje IDS/IPS, filtrowania ruchu oraz ochrony przed zagrożeniami,
- skonfiguruje mechanizmy QoS oraz Traffic Shaping dla wskazanych usług lub interfejsów,
- skonfiguruje wysyłanie logów do centralnego systemu monitorowania lub systemu SIEM z wykorzystaniem protokołu Syslog,
- skonfiguruje mechanizmy monitorowania stanu urządzenia, wykorzystania zasobów oraz ruchu sieciowego,
- wykona kopię zapasową konfiguracji urządzenia oraz przygotuje możliwość jej odtworzenia,
- przeprowadzi testy poprawności działania obejmujące w szczególności routing, NAT, VPN, polityki bezpieczeństwa, segmentację VLAN, mechanizmy IDS/IPS oraz komunikację z systemem monitorowania,
- przekaże urządzenie do eksploatacji wraz z dokumentacją powdrożeniową zawierającą opis konfiguracji, kopię konfiguracji oraz instrukcję odtworzenia systemu po awarii.

23 EDR do ochrony stacji roboczych i serwerów OT (3 szt.)

Obecnie Zamawiający użytkuję oprogramowanie ESET PROTECT ENTRY o identyfikatorze licencji 3A2-PSA-XNU Dostarczone oprogramowanie musi zostać przedłużone o rok oraz podniesione przynajmniej do wersji ESET PROTECT Enterprise oraz chronić minimum 3 serwery, zachowując przy tym możliwość chronienia minimum 20 komputerów opisanych w punkcie 1 OPZ.

24 Wdrożenie systemu EDR do ochrony stacji roboczych i serwerów OT

Usługa obejmuje rozszerzenie istniejącego środowiska EDR o ochronę trzech serwerów wykorzystywanych w środowisku OT. W ramach wdrożenia Wykonawca:

- zweryfikuje konfigurację istniejącego środowiska EDR,
- rozszerzy licencję o ochronę trzech serwerów,
- zainstaluje i skonfiguruje agenty EDR na wskazanych serwerach,
- przypisze serwery do odpowiednich polityk bezpieczeństwa,
- skonfiguruje mechanizmy wykrywania zagrożeń i raportowania zdarzeń,
- zweryfikuje komunikację z centralną konsolą zarządzającą,
- przeprowadzi test poprawności działania systemu oraz potwierdzi prawidłową ochronę wszystkich wdrożonych serwerów.

25 System monitorowania infrastruktury OT do analizy logów, zdarzeń i anomalii w środowisku przemysłowym

Ogólne	System klasy SIEM w modelu Open Source przeznaczony do centralnego monitorowania bezpieczeństwa infrastruktury IT i OT. Rozwiązanie musi umożliwiać zbieranie, analizę, korelację oraz przechowywanie logów z serwerów, stacji roboczych, urządzeń sieciowych, systemów operacyjnych, aplikacji oraz urządzeń przemysłowych. Licencja nie może ograniczać liczby monitorowanych urządzeń, użytkowników ani serwerów.
Monitorowanie	• Centralne zbieranie logów w czasie rzeczywistym.• Obsługa agentów oraz monitorowania bezagentowego (m.in. Syslog).• Monitorowanie serwerów, stacji roboczych, urządzeń sieciowych oraz usług.• Dashboardy prezentujące stan bezpieczeństwa infrastruktury.• Raportowanie historyczne oraz analiza trendów.• Korelacja zdarzeń pochodzących z wielu źródeł.
Cyberbezpieczeństwo	• Wykrywanie zagrożeń z mapowaniem do MITRE ATT&CK.• Monitorowanie integralności plików (FIM).• Rootcheck.• Monitorowanie konfiguracji systemów.• Ocena zgodności konfiguracji z politykami bezpieczeństwa.• Wykrywanie podatności oraz błędnych konfiguracji.• Inwentaryzacja sprzętu i oprogramowania.• Możliwość tworzenia własnych reguł detekcji oraz dekoderów logów.• Integracja z zewnętrznymi źródłami Threat Intelligence.• Powiadamianie o incydentach bezpieczeństwa.
Integracja	• Integracja z Active Directory/LDAP.• Integracja z rozwiązaniami EDR, XDR, IDS/IPS, firewallami, systemami pocztowymi oraz urządzeniami sieciowymi.• Możliwość integracji z systemami zgłoszeniowymi oraz zewnętrznymi platformami bezpieczeństwa.• Możliwość monitorowania środowisk lokalnych oraz rozproszonych.
Zarządzanie	• Zarządzanie przez interfejs WWW.• Role administratorów i operatorów.• Definiowanie retencji danych.• Konfigurowalne reguły alarmowania.• Możliwość automatycznej reakcji na wybrane incydenty bezpieczeństwa.
Licencjonowanie	Rozwiązanie Open Source niewymagające opłat licencyjnych za liczbę monitorowanych urządzeń, użytkowników ani serwerów oraz umożliwiające swobodną rozbudowę środowiska.

26 Wdrożenie systemu monitorowania infrastruktury OT

Usługa obejmuje dostawę, instalację, konfigurację oraz uruchomienie systemu klasy SIEM w infrastrukturze Zamawiającego. W ramach wdrożenia Wykonawca:

- przeprowadzi analizę infrastruktury IT oraz OT i określi źródła logów przeznaczone do integracji z systemem,
- zainstaluje i skonfiguruje serwer systemu SIEM wraz z komponentami zarządzającymi,
- skonfiguruje bezpieczną komunikację pomiędzy agentami oraz serwerem centralnym,
- wdroży monitorowanie serwerów, stacji roboczych, urządzeń sieciowych, systemów operacyjnych oraz wybranych urządzeń OT,
- skonfiguruje zbieranie logów z wykorzystaniem agentów oraz mechanizmów bezagentowych (m.in. Syslog),
- wdroży monitorowanie integralności plików (FIM), kontrolę konfiguracji, wykrywanie podatności, inwentaryzację sprzętu i oprogramowania oraz mechanizmy Rootcheck,
- skonfiguruje reguły korelacji zdarzeń, mechanizmy wykrywania zagrożeń oraz mapowanie zdarzeń do macierzy MITRE ATT&CK,
- skonfiguruje polityki zgodności z wymaganiami bezpieczeństwa oraz mechanizmy monitorowania zmian konfiguracji,
- przygotuje dashboardy administracyjne, raporty oraz mechanizmy powiadamiania o incydentach,
- przeprowadzi strojenie (tuning) reguł detekcji w celu ograniczenia liczby fałszywych alarmów i zwiększenia skuteczności wykrywania zagrożeń,
- wykona testy poprawności działania systemu obejmujące zbieranie logów, korelację zdarzeń, generowanie alarmów oraz mechanizmy aktywnej odpowiedzi,
- przekaże system do eksploatacji wraz z dokumentacją powdrożeniową obejmującą konfigurację systemu, źródła logów, zastosowane reguły oraz procedury administracyjne.

27 Sondy/sensory do pasywnego monitorowania ruchu i protokołów przemysłowych w sieciach OT – 3 szt

Ogólne	Rozwiązanie przeznaczone do pasywnego monitorowania ruchu sieciowego w środowiskach OT/ICS, umożliwiające identyfikację urządzeń, analizę komunikacji oraz wykrywanie anomalii bez ingerencji w pracę sieci przemysłowej.
Monitorowanie ruchu	Sondy muszą obsługiwać monitorowanie ruchu z wykorzystaniem portów SPAN, TAP lub równoważnych mechanizmów, zapewniając analizę komunikacji pomiędzy urządzeniami pracującymi w sieci OT.
Obsługa protokołów przemysłowych	Rozwiązanie musi umożliwiać analizę ruchu charakterystycznego dla środowisk przemysłowych oraz identyfikację urządzeń i usług wykorzystujących protokoły przemysłowe.
Integracja	Sondy muszą zapewniać pełną integrację z Systemem monitorowania infrastruktury OT do analizy logów, zdarzeń i anomalii w środowisku przemysłowym opisanym w poz. 25, przekazując dane telemetryczne, informacje o wykrytych urządzeniach, zdarzeniach oraz wykrytych anomaliach.
Nazwa	**Minimalne wymagania dla sprzętu**
Typ urządzenia	Urządzenie wykonane w kompaktowej obudowie umożliwiającej pracę ciągłą 24/7.
Procesor	Minimum czterordzeniowy procesor x86-64 o taktowaniu do 3,4 GHz, TDP nie większym niż 10 W.
Pamięć operacyjna	Minimum 8 GB DDR5 z możliwością rozbudowy do co najmniej 32 GB.
Pamięć masowa	Minimum 1 × gniazdo M.2 NVMe 2280 umożliwiające instalację dysku SSD.
Interfejsy sieciowe	Minimum 2 × port Ethernet 10 Gb/s SFP+ lub RJ45 oraz minimum 4 × port Ethernet 2.5 Gb/s RJ45.
Interfejsy I/O	Minimum 1 × USB 3.0, minimum 4 × USB 2.0, minimum 1 × USB-C, gniazdo kart pamięci microSD/TF oraz port konsolowy lub równoważny interfejs administracyjny.

Grafika	Wyjście HDMI oraz DisplayPort lub USB-C DisplayPort Alternate Mode umożliwiające lokalną administrację urządzeniem.
Obudowa	Aluminiowa obudowa przystosowana do ciągłej pracy, wyposażona w aktywny układ chłodzenia.
Zasilanie	Zasilacz zewnętrzny 12 V DC.
Funkcjonalność	Obsługa automatycznego uruchamiania po przywróceniu zasilania (Auto Power On).
Warunki pracy	Temperatura pracy minimum od -20°C do +60°C
Gwarancja	12 miesięcy

28 Wdrożenie sond/sensorów do pasywnego monitorowania ruchu i protokołów przemysłowych w sieciach OT

Usługa obejmuje instalację, konfigurację oraz uruchomienie sond monitorujących ruch sieciowy w środowisku OT, ich podłączenie do punktów monitorowania ruchu (SPAN, TAP lub równoważnych), integrację z **Systemem monitorowania infrastruktury OT do analizy logów, zdarzeń i anomalii w środowisku przemysłowym** opisanym w **poz. 25**, konfigurację przekazywania danych, zdarzeń i wykrytych anomalii do tego systemu oraz przeprowadzenie testów poprawności działania całego rozwiązania.
W ramach wdrożenia Wykonawca:

- skonfiguruje monitorowanie ruchu sieciowego w środowisku OT,
- skonfiguruje analizę wykorzystywanych protokołów przemysłowych,
- zintegruje rozwiązanie z systemem monitorowania OT opisanym w poz. 25,
- skonfiguruje przekazywanie danych telemetrycznych, zdarzeń oraz wykrytych anomalii,
- przeprowadzi testy poprawności działania monitorowania oraz integracji z systemem centralnym.

29 Instalacja, konfiguracja i wsparcie techniczne systemu uwierzytelniania i autoryzacji dostępu do sieci RADIUS

1. Wymagania funkcjonalne i techniczne

L.p.	Wymaganie / Opis wymagania
1	**Cel systemu** Centralny system AAA zapewniający uwierzytelnianie użytkowników i urządzeń próbujących uzyskać dostęp do zasobów sieciowych, kontrolujący polityki dostępu oraz rejestrujący zdarzenia dostępowe na potrzeby audytów bezpieczeństwa.
2	**Uwierzytelnianie użytkowników** System musi obsługiwać uwierzytelnianie użytkowników metodami EAP: co najmniej EAP-TLS (certyfikaty X.509), PEAP/MSCHAPv2 oraz EAP-TTLS/MSCHAPv2 lub EAP-TTLS/PAP.
3	**Obsługa 802.1X** System musi obsługiwać uwierzytelnianie portów sieciowych zgodnie z normą IEEE 802.1X dla sieci bezprzewodowej (WPA2-Enterprise lub WPA3-Enterprise) oraz sieci przewodowej.

L.p.	Wymaganie / Opis wymagania
4	**Autoryzacja i dynamiczne VLAN** System musi umożliwiać definiowanie polityk autoryzacji z dynamicznym przypisywaniem identyfikatora VLAN (Tunnel-Private-Group-ID) do sesji sieciowej.
5	**Rozliczanie dostępu (accounting)** System musi rejestrować zdarzenia rozliczeniowe (accounting start, stop, interim-update) zgodnie z RFC 2866. Logi muszą zawierać: tożsamość użytkownika, adres MAC urządzenia, adres IP, czas trwania sesji oraz wynik uwierzytelnienia. Wymagany eksport logów do zewnętrznego systemu zarządzania logami (Syslog lub równoważny).
6	**Obsługa wielu klientów RADIUS** System musi obsługiwać równoczesną pracę z wieloma klientami RADIUS (NAS): punktami dostępowymi Wi-Fi, przełącznikami sieciowymi. Każdy klient konfigurowany z indywidualnym kluczem współdzielonym (shared secret).
7	**Wymagania techniczne** Oprogramowanie musi działać jako usługa systemowa na serwerze GNU/Linux (Ubuntu Server, Debian lub równoważny). Dopuszczalna instalacja na maszynie wirtualnej w infrastrukturze Zamawiającego. Minimalne wymagania sprzętowe: 2 vCPU, 4 GB RAM, 40 GB przestrzeni dyskowej. Porty: UDP 1812 (uwierzytelnianie/autoryzacja) i UDP 1813 (accounting). Wymagane szyfrowanie TLS 1.2 lub wyższe dla metod EAP.
8	**Kompatybilność z infrastrukturą** System musi współpracować z urządzeniami sieciowymi wdrożonymi u Zamawiającego. Szczegółowy wykaz urządzeń zostanie przekazany Wykonawcy przed rozpoczęciem prac wdrożeniowych.

2. Instalacja i konfiguracja

Wykonawca zainstaluje i skonfiguruje oprogramowanie w siedzibie Zamawiającego. Zakres prac obejmuje:

a) Instalację oprogramowania i wszystkich niezbędnych komponentów na serwerze wskazanym przez Zamawiającego.

b) Konfigurację metod EAP wraz z certyfikatami TLS dla serwera.

c) Konfigurację klientów RADIUS: punktów dostępowych Wi-Fi, przełączników.

d) Konfigurację polityk autoryzacji z dynamicznym przypisywaniem VLAN.

r) Testy funkcjonalne potwierdzone protokołem odbioru.

f) Dokumentację powdrożeniową w języku polskim (opis architektury, konfiguracja, instrukcja obsługi).

Wszystkie prace muszą być realizowane stacjonarnie w siedzibie Zamawiającego. Nie dopuszcza się formy zdalnej.

3. Szkolenie administratorów

Wykonawca przeprowadzi szkolenie stacjonarne administratorów IT Zamawiającego z obsługi wdrożonego systemu. Szkolenie musi trwać minimum 8 godzin dydaktycznych i obejmować co najmniej:

a) Architekturę protokołu RADIUS i zasadę działania systemu AAA.

b) Zarządzanie klientami RADIUS – dodawanie, modyfikacja, usuwanie.

c) Modyfikację polityk autoryzacji i reguł dostępu.

d) Zarządzanie certyfikatami TLS – odnawianie i wymiana certyfikatu serwera.

e) Analizę logów i diagnozowanie błędów uwierzytelniania.

f) Procedury awaryjne: restart usługi, odtwarzanie po awarii.

Szkolenie odbywa się stacjonarnie w siedzibie Zamawiającego. Nie dopuszcza się formy zdalnej. Wykonawca dostarcza materiały szkoleniowe i wystawia potwierdzenie odbycia szkolenia dla każdego uczestnika.

4. Wsparcie techniczne

Wykonawca zapewni wsparcie techniczne przez okres 36 miesięcy od daty odbioru końcowego, obejmujące:

a) Pomoc w rozwiązywaniu problemów z uwierzytelnianiem użytkowników i urządzeń.

b) Konsultacje w zakresie modyfikacji konfiguracji, aktualizacji oprogramowania i zarządzania certyfikatami.

c) Ogólną asystę w utrzymaniu systemu.

Wsparcie świadczone jest stacjonarnie w siedzibie Zamawiającego w godzinach roboczych (pon.–pt. 6:00–15:00). Nie dopuszcza się formy zdalnej. Zakres i czas reakcji na zgłoszenia będzie zgodny z umową.

5. Warunki odbioru

Odbiór nastąpi po pozytywnym przejściu testów akceptacyjnych obejmujących co najmniej: pomyślne uwierzytelnienie użytkownika AD do sieci Wi-Fi metodą EAP, pomyślne uwierzytelnienie urządzenia OT/ICS metodą MAB z przypisaniem do właściwego VLAN, pomyślne uwierzytelnienie połączenia VPN, odrzucenie próby uwierzytelnienia dla użytkownika spoza uprawnionych grup AD, poprawną rejestrację zdarzeń accounting w logach, przeprowadzenie szkolenia oraz przekazanie dokumentacji powdrożeniowej.

Zamawiający ma prawo do zgłoszenia uwag i usterek w terminie 14 dni od odbioru. Wykonawca usuwa usterki w terminie uzgodnionym z Zamawiającym.

Wykonawca zobowiązany jest do zachowania poufności wszelkich danych uzyskanych w trakcie realizacji zamówienia, w tym logów i danych dostępowych.

30 instalacja, konfiguracja, wdrożenie i uruchomienie systemu log manager do scentralizowanego gromadzenia, przechowywania, wyszukiwania, analizy i alarmowania zdarzeń logowych z infrastruktury IT/OT

System ma być oparty na oprogramowaniu open-source (self-managed, bez opłat licencyjnych), zapewniającym bezpieczeństwo, nadzór operacyjny oraz szybką reakcję na incydenty, z wsparciem dla wielu źródeł danych i mechanizmów raportowania.

System powinien spełniać minimum wymagania opisane poniżej i być realizowany na infrastrukturze Zamawiającego (fizycznej lub wirtualnej). Licencja oprogramowania musi być bezpłatna dla Zamawiającego, z prawem do nieograniczonego korzystania w ramach własnej infrastruktury.

1. **Wymagania minimalne**

I. Wymagania funkcjonalne

- Zbieranie dzienników z wielu źródeł jednocześnie: serwery Windows i Linux, urządzenia sieciowe (firewalle, routery, przełączniki przemysłowe), systemy katalogowe, aplikacje biznesowe i środowisko OT; obsługiwane protokoły i formaty: Syslog UDP/TCP, GELF, CEF, JSON, Beats/NXLog lub równoważne, z możliwością zdefiniowania dowolnego numeru portu nasłuchu dla każdego wejścia.
- Klasyfikacja i filtrowanie dzienników na niezależne strumienie danych z możliwością przypisywania uprawnień dostępu per strumień; zaawansowane wyszukiwanie pełnotekstowe po dowolnych polach, zakresach czasu i słowach kluczowych; zapisywanie często używanych zapytań oraz eksport wyników.
- Tworzenie interaktywnych dashboardów zawierających wykresy, tabele i wskaźniki KPI prezentujące dane w czasie rzeczywistym lub zbiorczym; możliwość udostępniania dashboardów w trybie tylko do odczytu (read-only) lub dowolnej przeglądarce bez konieczności logowania.
- Definiowanie reguł alarmowania wyzwalanych przez zdarzenia w napływających danych (m.in. nieudane próby logowania, błędy krytyczne, anomalie w ruchu sieciowym, zmiany konfiguracji urządzeń OT); automatyczne powiadomienia e-mail po wyzwoleniu alarmu; możliwość integracji z zewnętrznymi systemami przez REST API.
- Zarządzanie retencją i rotacją indeksów z możliwością konfiguracji okresu przechowywania i zasad rotacji; eksport wybranych zbiorów dzienników do archiwizacji zewnętrznej; rozszerzalność przez REST API i importowalne pakiety konfiguracyjne (content packs).

II. Wymagania techniczne i architektura

- Architektura trójskładowa oparta na komponentach open-source: warstwa aplikacyjna systemu log manager + baza metadanych i konfiguracji (np. MongoDB lub równoważna) + silnik wyszukiwania i indeksowania danych (np. OpenSearch/Elasticsearch lub równoważny).
- Minimalne wymagania sprzętowe dla wolumenu 1–10 GB dzienników dziennie: węzeł aplikacyjny z bazą metadanych – min. 8 vCPU, 16 GB RAM, 130 GB SSD; węzeł silnika wyszukiwania – min. 8 vCPU, 24 GB RAM, 100 GB SSD o wysokim IOPS. Możliwość skalowania pionowego i poziomego przez dodawanie węzłów. Zamawiający dysponuje serwerem lub maszyną wirtualną – Wykonawca jest zobowiązany wskazać w ofercie czy dostępna infrastruktura spełnia powyższe wymagania, a w przypadku niezgodności zaproponować rozwiązanie alternatywne.
- System operacyjny: Linux (dystrybucja LTS wspierana przez producenta oprogramowania, np. Ubuntu Server, Debian lub RHEL/równoważna).
- Bezpieczeństwo: dostęp do interfejsu webowego wyłącznie przez HTTPS; uwierzytelnianie przez lokalne konta użytkowników oraz opcjonalnie przez LDAP/Active Directory; polityka kontroli dostępu per strumień danych i dashboard; możliwość szyfrowania transmisji dzienników od źródeł do systemu (TLS).

III. Wymagania licencyjne i dokumentacja

- Oprogramowanie open-source bez opłat licencyjnych za samo oprogramowanie; Zamawiający uzyskuje prawo do nieograniczonego czasowo korzystania z oprogramowania w granicach własnej infrastruktury.
- Wykonawca dostarczy dokumentację powdrożeniową w języku polskim lub angielskim zawierającą: opis architektury systemu, konfigurację źródeł dzienników, opis zdefiniowanych reguł alarmowania oraz zasady zarządzania retencją i archiwizacją.

IV. Zakres wdrożenia i usług

Instalacja i konfiguracja

- Instalacja systemu operacyjnego na wskazanym przez Zamawiającego serwerze lub maszynie wirtualnej.
- Instalacja i konfiguracja wszystkich komponentów systemu log manager wraz z testami funkcjonalnymi.
- Weryfikacja synchronizacji czasu (NTP) na wszystkich urządzeniach wysyłających dzienniki; w przypadku braku wspólnego zegara Wykonawca zaproponuje rozwiązanie uwspólniające czas w sieci Zamawiającego.
- Konfiguracja osobnych wejść (inputs) z odrębnymi portami nasłuchu dla poszczególnych kategorii urządzeń, umożliwiająca separację danych napływających z różnych typów źródeł.

Podłączenie źródeł dzienników

W zakresie minimalnym Wykonawca skonfiguruje przesyłanie dzienników z następujących urządzeń i systemów Zamawiającego:

- urządzenie klasy UTM (Fortigate lub równoważne),
- przełączniki zarządzalne (Cisco lub równoważne),
- serwery Windows,
- serwer Linux,
- stacje robocze Windows 10/11 (konfiguracja zbiorcza przez politykę grupową GPO lub agenta).

Konfiguracja analityczna

- Konfiguracja ekstraktorów i reguł przetwarzania dla napływających strumieni danych.
- Konfiguracja polityki retencji i rotacji indeksów zgodnie z wymogami prawnymi i wskazaniami Zamawiającego.
- Konfiguracja co najmniej 3 dashboardów zbiorczych (odrębnie dla urządzeń sieciowych, serwerów i stacji roboczych) prezentujących kluczowe wskaźniki bezpieczeństwa i operacyjne.
- Konfiguracja co najmniej 5 reguł alarmowania e-mail, obejmujących m.in.: nieudane próby logowania, błędy krytyczne urządzeń, zmiany konfiguracji urządzeń sieciowych, wykrycie aktywności poza godzinami pracy.

Szkolenie

Wykonawca przeprowadzi szkolenie dla administratora Zamawiającego w wymiarze co najmniej 8 godzin, obejmujące: zasady działania systemu, zarządzanie źródłami danych, wyszukiwanie i filtrowanie dzienników, tworzenie dashboardów i reguł alarmowania, zarządzanie użytkownikami oraz zarządzanie retencją.

Szkolenie odbędzie się w siedzibie Zamawiającego lub zdalnie, nie później niż 14 dni od odbioru końcowego.

Wsparcie techniczne

Wykonawca świadczyć będzie wsparcie techniczne w formie puli 60 godzin zegarowych do wykorzystania w ciągu 36 miesięcy od daty odbioru końcowego. Wsparcie obejmuje zdalną pomoc techniczną i modyfikacje konfiguracji systemu. Zgłoszenia przyjmowane e-mailem i telefonicznie w godzinach roboczych (8:00–16:00). Czas reakcji: do 4 godzin roboczych dla zgłoszeń krytycznych, do końca następnego dnia roboczego dla zgłoszeń standardowych. Jednostka rozliczeniowa: 0,5 godziny. Dostęp zdalny wyłącznie za jednorazową zgodą Zamawiającego. Godziny niewykorzystane wygasają po 12 miesiącach.