Załącznik nr 1

Opis Przedmiotu Zamówienia
do postępowania na realizację zamówienia pn.:

Dostawa, wdrożenie i uruchomienie sprzętu i oprogramowania dla potrzeb cyberbezpieczeństwa – Część 3

Część 3:

1. Serwer wysokiej dostępności (HA) niezbędny do wdrożenia rozwiązań z zakresu bezpieczeństwa – 1 szt.

Zakup serwera fizycznego do zainstalowania i wdrożenia rozwiązań z zakresu bezpieczeństwa, w tym wirtualnych usług HA, na którym uruchomione zostaną serwery wirtualne - systemy wirtualne dla systemów bezpieczeństwa IT i OT/ICS/IIoT, zakup systemu operacyjnego Windows Server wraz z licencjami dostępowymi (User/Device CAL) umożliwiającymi korzystanie z systemów wdrażanych w ramach projektu oraz wdrożenie serwera fizycznego, oraz systemów operacyjnych wraz wirtualnymi serwerami oraz systemem wirtualizacji.

Lp.	Parametry techniczne - wymagania minimalne
1	Obudowa typu Rack o wysokości maksymalnie 2U w konfiguracji pozwalającej zainstalować 8 dysków twardych. Komplet wysuwanych szyn i organizer okablowania, umożliwiający montaż w szafie rack i wysuwanie do celów serwisowych.
2	Płyta główna – zaprojektowana do pracy w systemie jednoprocesorowym przez producenta węzła i oznaczona jego znakiem firmowym.
3	Chipset - dedykowany przez producenta procesora do pracy w systemie jednoprocesorowym.
4	Procesory - zainstalowany jeden procesor maksimum 16-rdzeniowy klasy x86 uzyskujące w teście „SPECrate2017_fp_base" dostępnym na stronie www.spec.org wynik min. 346 punktów, dla oferowanego procesora. Do oferty należy załączyć wydruk ze strony potwierdzający osiągnięty wynik dla oferowanego procesora w oferowanym modelu serwera. Maksymalna liczba rdzeni procesora ograniczona przez licencjonowanie zastosowanego w projekcie oprogramowania.
5	Pamięć RAM – minimum 256 GB DDR5. Płyta główna powinna obsługiwać do minimum 6TB pamięci RAM Pojemność zastosowanych kości pamięci RAM min. 32 GB.
6	Zabezpieczenia pamięci RAM - ECC
7	Gniazda PCI – minimum dwa sloty PCIe
8	Interfejsy sieciowe: - minimum 4 porty typu Ethernet 1Gbps Base-T - minimum 4 porty typu Ethernet 25Gbps SFP28 (zorganizowane minimum na dwóch fizycznych karach sieciowych)
9	Przestrzeń dyskowa: - dysk twardy typu SSD o pojemności minimum 480GB, każdy – 2szt.

10	Wbudowane porty: - minimum 2 port USB 2.0 - minimum 2 porty USB 3.1, - 1 port RJ45 dedykowany do zarządzania, - 1 porty VGA
11	Video - zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
12	Wentylatory - redundantne
13	Zasilacze - redundantne, Hot-Plug minimum 1100W.
14	Karta Zarządzania - niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płyta główną, posiadająca minimalną funkcjonalność : - komunikacja poprzez interfejs RJ45, - podstawowe zarzadzanie poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging, - wbudowana diagnostyka, - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń, - monitorowanie temperatury oraz zużycia energii w czasie rzeczywistym, - lokalna oraz zdalna konfiguracja serwera, - wsparcie dla IPv4 i IPv6, - obsługa komunikacji szyfrowanej tls 1.2 oraz tls 1.3 - możliwość zdalnego dostępu do konsoli graficznej z przejęciem kontroli nad klawiaturą i myszką, zainstalowanego systemu operacyjnego serwera.
15	Urządzenie musi być wyprodukowane zgodnie z normą ISO-9001:2008 oraz ISO-14001. Urządzenie musi być zgodne z normami UE i przeznaczone na rynek UE, musi posiadać certyfikat CE.
16	Oprogramowanie systemu operacyjnego Microsoft Windows Server 2025 Standard. Licencja wieczysta zgodna z liczbą fizycznych rdzeni procesorów. Opis równoważności znajduje się pod tabelą.
17	Dostarczone urządzenia muszą być fabrycznie nowe, nieregenerowane i wyprodukowane najwcześniej w ciągu ostatnich 6 miesięcy przed dostawą, muszą pochodzić z oficjalnego kanału sprzedaży producenta.
18	Oferowane urządzenie musi być objęte co najmniej 3-letnim wsparciem producenta sprzętu w dni robocze, czas reakcji w miejscu instalacji sprzętu Następny Dzień Roboczy. Musi istnieć możliwość sprawdzenia na stronie WWW producenta serwera, prowadzonej w języku polskim, po podaniu numeru seryjnego urządzenia minimum: - okresu oraz poziomu gwarancji, - zainstalowanych komponentów (w tym m.in. procesorów, pamięci RAM, dysków, zasilaczy i kart komunikacyjnych). Adres strony WWW producenta na której można sprawdzić powyższe dane musi być podany w złożonej ofercie.

19	W zakresie wsparcia i gwarancji Zamawiający wymaga przestawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą.
20	Instalacja serwera w szafie rack Podłączenie serw serwera do zasilania i podsieci wskazanych przez Zamawiającego Instalacja i konfiguracja Windows Server z rolą Hyper-V lub równoważną, z infrastrukturą Zamawiającego. Podłączenie macierzy dyskowej wymienionej w pkt.2 do serwera wysokiej dostępności Integracja z usługą katalogową Microsoft Active Directory wykorzystywaną przez Zamawiającego.

Opis równoważności dla Oprogramowanie systemu operacyjnego

Współpraca z procesorami o architekturze x86-64.

Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.

Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu.

Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie minimum Microsoft Windows Server 2019.

Licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

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.

Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.

Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).

Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.

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.

Zdalna dystrybucja oprogramowania na stacje robocze.

Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.

PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

Dystrybucję certyfikatów poprzez http,

Konsolidację CA dla wielu lasów domeny,

Automatyczne rejestrowania certyfikatów pomiędzy rożnymi lasami domen.

Szyfrowanie plików i folderów.

Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

Serwis udostępniania stron WWW.

Wsparcie dla protokołu IP w wersji 6 (IPv6).

Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

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.

Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).

Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF; W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania.

2. Macierz dyskowa - 1 szt.

Zakup i wdrożenie macierzy dyskowej wraz z dyskami.

Lp.	Parametry techniczne - wymagania minimalne
1	Do instalacji w standardowej szafie RACK 19" rozwiązanie może zajmować maksymalnie 2U i pozwalać na instalacje co najmniej 12 dysków 3.5".
2	Zarządzanie rozwiązaniem poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN'ów oraz 1024 kopii migawkowych na całą macierz.
3	Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów Ethernet 25Gbps SFP28. Zamawiający wymaga dostarczenia co najmniej 2 kabli DAC SFP28 to SFP28 25Gbps o długości 3 metrów.
4	Minimum 16GB pamięci na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii.
5	Przestrzeń surowa macierzy (ang. RAW) nie mniejsza niż 120TB zrealizowana na co najmniej 10 dyskach twardych wyposażonych w interfejsy 12 Gbps SAS oraz 3,84TB zrealizowane na co najmniej 2 dyskach SSD.
6	Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych maksymalnie do 264 dysków, która posiada: • możliwości rozbudowy przez dodawanie kolejnych półek dyskowych; • możliwości mieszania obsługiwanych typów dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.

7	Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków.
8	Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji.
9	Wymagane wsparcie dla systemów operacyjnych: Windows Server 2022, Windows Server 2019, Windows Server 2016, Red Hat Enterprise Linux (RHEL), SLES, VMware ESXi 7 lub VMware vSphere/ESXi 8.0 lub nowszego.
10	Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.
11	Rozwiązanie musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym.
12	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
13	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
14	Rozwiązanie musi być wyprodukowany zgodnie z normą ISO 9001:2008.
15	Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy
16	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 9x5 poprzez ogólnopolską linię telefoniczną producenta. Serwis musi zawierać usługę pozostawiania bez opłat u Zamawiającego uszkodzonych dysków w okresie obowiązywania gwarancji.
17	W zakresie wsparcia i gwarancji Zamawiający wymaga przestawienia oświadczenia producenta oferowanego urządzenia, wskazującego, że oferowane urządzenie będzie objęte serwisem producenta i/lub serwisem autoryzowanego serwisu producenta oraz, że uszkodzone dyski w przypadku wymiany z powodu awarii w okresie obowiązywania gwarancji, pozostaną własnością Zamawiającego. Niniejsze oświadczenie ma zostać dostarczone wraz z ofertą.
18	Instalacja macierzy szafie rack Podłączenie macierzy do zasilania i podsieci wskazanej przez Zamawiającego Konfiguracja macierzy, w tym: stworzenie RAID, stworzenie LUN'ów Konfiguracja przestrzeni dyskowe i wystawienie jej do serwera z pkt 1.

3. Klucz sprzętowy U2F - 200 szt.

Zakup i wdrożenie kluczy sprzętowych U2F w celu uwierzytelnienia dostępu. Zakup 200 kluczy U2F/FIDO2 jest uzasadniony liczbą użytkowników wymagających silnego uwierzytelnienia w środowiskach IT i OT/ICS/IIoT oraz koniecznością zapewnienia zapasowych kluczy rezerwowych dla kont uprzywilejowanych i administracyjnych.

Lp.	**Parametry techniczne - wymagania minimalne**
1	Sprzętowy klucz uwierzytelniający, zapewniający silne uwierzytelnianie dwuskładnikowe (2FA/MFA) oraz bezhasłowe logowanie. Interfejs: USB-A oraz obsługa NFC
2	Protokoły uwierzytelniania: FIDO2 / WebAuthn FIDO U2F,

3	Kompatybilność: Systemy operacyjne: Microsoft Windows, Apple macOS, Linux, ChromeOS, Android, iOS Usługi: minimum Microsoft Entra ID,
4	Odporność: spełniający standard IP68
5	Certyfikaty: CE, RoHS, FCC, UKCA, FIDO Certified.
6	Oferowany produkt musi być nowy, oryginalny, fabrycznie zapakowany, z pełną gwarancją producenta (minimum 12 miesięcy). Dostarczany z oryginalnym opakowaniem i instrukcją.

4. Wdrożenie oprogramowania z zakresu bezpieczeństwa z wykorzystaniem oprogramowania typu open source i/lub oprogramowania używanego obecnie przez Zamawiającego

4.1. Wdrożenie rozwiązania open-source do badania i zarządzania podatnościami.

Wdrożenie rozwiązania open source, oprogramowanie do badania podatności oraz zarządzania podatnościami.

Lp.	Parametry techniczne - wymagania minimalne
1	Przedmiotem zamówienia jest świadczenie usługi polegającej na wdrożeniu spójnego rozwiązania open-source do badania podatności oraz zarządzania podatnościami, działającego w infrastrukturze Zamawiającego. Rozwiązanie ma zapewniać: - identyfikację podatności w systemach i sieci, - centralne zarządzanie podatnościami, - obsługę procesu ich usuwania (remediacji), - możliwość integracji z innymi systemami bezpieczeństwa.
2	W ramach usługi Wykonawca: - zainstaluje i skonfiguruje narzędzie do skanowania podatności, - skonfiguruje: - skany sieciowe, - skany systemów, - skany usług, - przygotuje polityki skanowania, - skonfiguruje harmonogram skanów, - przeprowadzi pierwsze skany testowe.
3	Wykonawca dostarczy: - dokumentację techniczną wdrożenia, - opis architektury rozwiązania.
4	Wykonawca przeszkoli Zamawiającego z obsługi dostarczanego rozwiązania – min. 2h
5	Rozwiązanie musi: - umożliwiać automatyczne skanowanie podatności, - identyfikować podatności w: systemach operacyjnych, usługach sieciowych.

6	Okres realizacji: Maksymalnie do 10.12.2026r.
7	Informacja o ilości stanowisk Zamawiającego: Serwer: 54 Host: 180 Urządzeń sieciowych: 325
8	Konfiguracja kopii zapasowej wdrożonego rozwiązania w systemie backupowym Zamawiającego.

4.2. Wdrożenie rozwiązania open-source do badania podatności stron WWW.

Wdrożenie rozwiązania open source, oprogramowanie do badania podatności stron www umożliwiających skanowanie i badanie podatności.

Lp.	Parametry techniczne - wymagania minimalne
1	Przedmiotem zamówienia jest wdrożenie rozwiązania open-source służącego do skanowania i analizy podatności aplikacji oraz stron WWW, obejmujące instalację, konfigurację, uruchomienie oraz przygotowanie do eksploatacji w środowisku Zamawiającego.
2	Zakres zamówienia obejmuje: - dostawę i wdrożenie rozwiązania open-source do skanowania podatności WWW, - instalację w infrastrukturze Zamawiającego (środowisko fizyczne lub wirtualne), - konfigurację mechanizmów skanowania (pasywnego i aktywnego), - konfigurację skanowania aplikacji publicznych i wewnętrznych, - przygotowanie profili i polityk skanowania, - uruchomienie testów bezpieczeństwa, - przygotowanie mechanizmów raportowania.
3	Funkcjonalności rozwiązania: - skanowanie pasywne i aktywne aplikacji WWW, - identyfikację podatności zgodnych z OWASP Top 10, - możliwość generowania raportów, - możliwość konfiguracji zakresu testów, - możliwość pracy w środowisku lokalnym Zamawiającego.
4	Wykonawca dostarczy: - dokumentację techniczną wdrożenia, - opis architektury rozwiązania.
5	Wykonawca przeszkoli Zamawiającego z obsługi dostarczanego rozwiązania – min 2h
6	Rozwiązanie musi: - umożliwiać automatyczne skanowanie podatności, - identyfikować podatności w: systemach operacyjnych, usługach sieciowych.
7	Okres realizacji: Maksymalnie do 10.12.2026r.

8	Konfiguracja kopii zapasowej wdrożonego rozwiązania w systemie backupowym Zamawiającego .

4.3. Wdrożenie rozwiązania open-source typu NAC.

Wdrożenie rozwiązania open-source systemu typu NAC jako usługę obejmuje wdrożenie i integrację systemu służącego do kontroli dostępu urządzeń i użytkowników do sieci informatycznej. Zakres obejmuje instalację, opracowanie reguł autoryzacji, testy funkcjonalne dla IT i OT/ICS/IIoT.

Lp.	Parametry techniczne - wymagania minimalne
1	Przedmiotem zamówienia jest wdrożenie rozwiązania open-source służącego do skanowania i analizy podatności aplikacji oraz stron WWW, obejmujące instalację, konfigurację, uruchomienie oraz przygotowanie do eksploatacji w środowisku Zamawiającego.
2	Zakres zamówienia obejmuje: - dostawę i wdrożenie rozwiązania open-source do skanowania podatności WWW, - instalację w infrastrukturze Zamawiającego (środowisko fizyczne lub wirtualne), - konfigurację mechanizmów skanowania (pasywnego i aktywnego), - konfigurację skanowania aplikacji publicznych i wewnętrznych, - przygotowanie profili i polityk skanowania, - uruchomienie testów bezpieczeństwa, - przygotowanie mechanizmów raportowania.
3	Funkcjonalności rozwiązania: - skanowanie pasywne i aktywne aplikacji WWW, - identyfikację podatności zgodnych z OWASP Top 10, - możliwość generowania raportów, - możliwość konfiguracji zakresu testów, - możliwość pracy w środowisku lokalnym Zamawiającego.
4	Wykonawca dostarczy: - dokumentację techniczną wdrożenia, - opis architektury rozwiązania.
5	Wykonawca przeszkoli Zamawiającego z obsługi dostarczanego rozwiązania – min. 2h
6	Rozwiązanie musi: - umożliwiać automatyczne skanowanie podatności, - identyfikować podatności w: systemach operacyjnych, usługach sieciowych.
7	Okres realizacji: Maksymalnie do 10.12.2026r.
8	Konfiguracja kopii zapasowej wdrożonego rozwiązania w systemie backupowym Zamawiającego .

4.4. Wdrożenie rozwiązania open-source typu NDR.

Wdrożenie i integracja systemu open-source typu NDR, przeznaczonego do monitorowania i analizy ruchu sieciowego w sieci IT. Zakres obejmuje konfigurację punktów zbierania danych, reguł detekcji, integrację z systemem SIEM, testy działania, opracowanie raportów dla IT i OT/ICS/IIoT.

Lp.	Parametry techniczne - wymagania minimalne
1	Przedmiotem zamówienia jest wdrożenie, konfiguracja oraz uruchomienie systemu typu NDR (Network Detection and Response) do monitorowania i analizy ruchu sieciowego w środowisku IT.
2	Zakres zamówienia obejmuje: - analizę środowiska Zamawiającego, - wdrożenie i konfigurację rozwiązania, - konfigurację punktów monitorowania (SPAN/mirror/TAP).
3	Funkcjonalności rozwiązania: - analizę ruchu sieciowego w czasie rzeczywistym, - wykrywanie anomalii i incydentów bezpieczeństwa, - identyfikację nieautoryzowanych działań w sieci, - korelację zdarzeń z różnych źródeł, - wizualizację i analizę danych, - generowanie alertów, - możliwość integracji z systemami zewnętrznymi, - monitoring środowisk IT oraz OT/ICS, - działanie pasywne (bez ingerencji w ruch sieciowy), - analizę ruchu wewnętrznego (east-west), w tym identyfikację komunikacji pomiędzy segmentami i strefami bezpieczeństwa.
4	Wykonawca dostarczy: - dokumentację techniczną wdrożenia, - opis architektury rozwiązania.
5	Wykonawca przeszkoli Zamawiającego z obsługi dostarczanego rozwiązania – min. 2h
6	Okres realizacji: Maksymalnie do 10.12.2026r.
7	Konfiguracja kopii zapasowej wdrożonego rozwiązania w systemie backupowym Zamawiającego.

4.5. Wdrożenie rozwiązania open-source typu RADIUS.

Usługa obejmuje wdrożenie, konfigurację i integrację systemu open-source typu RADIUS oraz rozwiązania w systemach serwerowych w środowisku sieciowym organizacji IT i OT/ICS/IIoT.

Lp.	Parametry techniczne - wymagania minimalne
1	Przedmiotem zamówienia jest usługa polegająca na wdrożeniu, konfiguracji oraz integracji systemu uwierzytelniania i autoryzacji opartego o rozwiązanie typu RADIUS w technologii

	open-source, przeznaczonego do obsługi dostępu do zasobów sieciowych w środowisku IT oraz OT/ICS/IIoT.
2	Zakres zamówienia obejmuje: - instalację i konfigurację systemu RADIUS (np. FreeRADIUS lub równoważnego), - wdrożenie mechanizmów uwierzytelniania: • konfiguracji uwierzytelniania i autoryzacji, • 802.1X, • MAC Authentication Bypass (MAB), • uwierzytelnianie użytkowników (np. LDAP/AD).
3	Funkcjonalności rozwiązania: - centralne uwierzytelnianie użytkowników i urządzeń, - obsługę standardu RADIUS (RFC 2865 i pokrewne), - wsparcie dla: 802.1X, EAP (np. PEAP, TLS), - integrację z katalogiem użytkowników (LDAP/AD), - możliwość definiowania polityk dostępu (np. VLAN, ACL), - logowanie zdarzeń uwierzytelniania, - możliwość integracji z systemami NAC.
4	Wykonawca dostarczy: - dokumentację techniczną wdrożenia, - opis architektury rozwiązania.
5	Wykonawca przeszkoli Zamawiającego z obsługi dostarczanego rozwiązania – min. 2h
6	Okres realizacji: Maksymalnie do 10.12.2026r.
7	Konfiguracja kopii zapasowej wdrożonego rozwiązania w systemie backupowym Zamawiającego.

4.6. Wdrożenie rozwiązania open-source do monitorowania infrastruktury.

Wdrożenie i integracja oprogramowania open-source przeznaczonego do monitorowania infrastruktury informatycznej IT i OT/ICS/IIoT.

Lp.	**Parametry techniczne - wymagania minimalne**
1	Przedmiotem zamówienia jest wdrożenie, konfiguracja, integracja oraz uruchomienie systemu monitorowania infrastruktury informatycznej i technicznej Zamawiającego, obejmującej środowiska IT oraz – w zakresie uzasadnionym technicznie – OT/ICS/IIoT. Zamówienie obejmuje usługę wdrożeniową systemu opartego o rozwiązanie typu open-source lub równoważne, umożliwiające monitorowanie dostępności, wydajności oraz stanu infrastruktury, wraz z konfiguracją alertów, wizualizacji, raportowania oraz integracji z istniejącymi systemami Zamawiającego.
2	Zakres zamówienia obejmuje: - instalację i konfigurację systemu, - konfigurację monitoringu infrastruktury: - serwerów, - stacji roboczych, - urządzeń sieciowych,

	- usług i aplikacji, - wybranych elementów OT/ICS/IIoT, - konfigurację alertów i progów, - przygotowanie dashboardów i raportów, - integrację z systemami Zamawiającego.
3	Funkcjonalności rozwiązania: - monitorowanie dostępności hostów, urządzeń i usług, - monitorowanie parametrów wydajnościowych (CPU, RAM, dyski, sieć), - monitorowanie usług sieciowych i aplikacyjnych, - obsługę monitoringu: - agentowego, - bezagentowego, - obsługę standardowych protokołów, co najmniej: - SNMP, - ICMP, - zbieranie logów (np. syslog lub równoważne), - możliwość monitorowania systemów Windows i Linux, - możliwość monitorowania środowisk wirtualnych.
4	Wykonawca dostarczy: - dokumentację techniczną wdrożenia, - opis architektury rozwiązania.
5	Wykonawca przeszkoli Zamawiającego z obsługi dostarczanego rozwiązania – min. 2h
6	Okres realizacji: Maksymalnie do 10.12.2026r.
7	Konfiguracja kopii zapasowej wdrożonego rozwiązania w systemie backupowym Zamawiającego.

4.7. Wdrożenie rozwiązania open-source typu ITSM.

Usługa obejmuje wdrożenie, konfigurację i integrację systemu open-source typu ITSM zapewniającego obsługę zgłoszeń, incydentów i zmian w środowiskach IT oraz OT/ICS/IIoT.

Lp.	**Parametry techniczne - wymagania minimalne**
1	Przedmiotem zamówienia jest wdrożenie, konfiguracja, integracja oraz uruchomienie systemu klasy ITSM (IT Service Management), opartego o rozwiązanie open-source lub równoważne.
2	Zakres zamówienia obejmuje: - instalację i konfigurację systemu, - wdrożenie systemu obsługi zgłoszeń i incydentów, - integrację z systemami Zamawiającego.
3	Funkcjonalności rozwiązania: - obsługę zgłoszeń (Service Desk), - obsługę incydentów, zmian i problemów,

	- portal użytkownika (self-service), - obsługę zgłoszeń przez e-mail, - historię i rejestr działań.
4	Wykonawca dostarczy: - dokumentację techniczną wdrożenia, - opis architektury rozwiązania.
5	Wykonawca przeszkoli Zamawiającego z obsługi dostarczanego rozwiązania – min. 2h
6	Okres realizacji: Maksymalnie do 10.12.2026r.
7	Konfiguracja kopii zapasowej wdrożonego rozwiązania w systemie backupowym Zamawiającego.

4.8. Wdrożenie rozwiązania open-source typu SIEM.

Usługa obejmuje wdrożenie, konfigurację i integrację systemu typu SIEM zapewniającego zbieranie, korelację i analizę zdarzeń bezpieczeństwa z różnych źródeł (IT (serwery, urządzenia sieciowe, aplikacje), systemy OT/ICS/IIoT).

Lp.	Parametry techniczne - wymagania minimalne
1	Przedmiotem zamówienia jest usługa obejmująca wdrożenie, konfigurację oraz integrację funkcjonalności klasy SIEM w środowisku Zamawiającego, umożliwiających centralne zbieranie, normalizację, korelację oraz analizę zdarzeń bezpieczeństwa.
2	Zakres zamówienia obejmuje: - instalację i konfigurację systemu, - integracje z serwerami, - integracje z systemami operacyjnymi użytkowników – 100 stacji roboczych, - integrację z systemami Zamawiającego, - wdrożenie komponentów odpowiedzialnych za: - zbieranie danych, - analizę i korelację, - wizualizację, - konfigurację mechanizmów zbierania logów (agentowych lub bezagentowych), - integrację z systemami IT (Windows, Linux, urządzenia sieciowe) - musi być instalacja agent pasywny lub aktywny, konfiguracja SNMP) - integrację z systemami OT/ICS (jeżeli dostępne źródła danych), - konfigurację reguł detekcji i korelacji, - konfigurację dashboardów i raportów, - konfigurację mechanizmów alertowania.
3	Funkcjonalności rozwiązania: - centralne zbieranie zdarzeń i logów (np. syslog, API, agenty), - korelację zdarzeń w czasie zbliżonym do rzeczywistego, - wykrywanie incydentów bezpieczeństwa, - generowanie alertów, - wizualizację danych (dashboardy),

	- możliwość definiowania własnych reguł, - archiwizację i przeszukiwanie danych.
4	Wykonawca dostarczy: - dokumentację techniczną wdrożenia, - opis architektury rozwiązania.
5	Wykonawca przeszkoli Zamawiającego z obsługi dostarczanego rozwiązania – min. 2h
6	Okres realizacji: Maksymalnie do 10.12.2026r.
7	Konfiguracja kopii zapasowej wdrożonego rozwiązania w systemie backupowym Zamawiającego.

4.9. Wdrożenie rozwiązania open-source typu SOAR.

Usługa obejmuje wdrożenie, konfigurację i integrację systemu open-source typu SOAR służącego do automatyzacji reakcji na incydenty bezpieczeństwa i orkiestracji działań między systemami bezpieczeństwa IT i OT/ICS/IIoT.

Lp.	Parametry techniczne - wymagania minimalne
1	Przedmiotem zamówienia jest usługa wdrożenia, konfiguracji i integracji systemu open-source klasy SOAR (Security Orchestration, Automation and Response), przeznaczonego do automatyzacji reakcji na incydenty bezpieczeństwa oraz orkiestracji działań pomiędzy systemami bezpieczeństwa.
2	Zakres zamówienia obejmuje: - instalację i konfigurację systemu, - instalację i konfigurację systemu SOAR, - integrację z dostarczanym systemem SIEM.
3	Funkcjonalności rozwiązania: - obsługę incydentów bezpieczeństwa (case management), - rejestrację, klasyfikację i obsługę incydentów, - możliwość tworzenia, modyfikacji i wykonywania scenariuszy reagowania (playbooków), - automatyczne i półautomatyczne wykonywanie działań, - agregację danych z systemu SIEM oraz innych źródeł.
4	Wykonawca dostarczy: - dokumentację techniczną wdrożenia, - opis architektury rozwiązania.
5	Wykonawca przeszkoli Zamawiającego z obsługi dostarczanego rozwiązania – min. 2h
6	Okres realizacji: Maksymalnie do 10.12.2026r.
7	Konfiguracja kopii zapasowej wdrożonego rozwiązania w systemie backupowym Zamawiającego.

4.10. Wdrożenie rozwiązania open-source do zarządzania logami.

Usługa obejmuje wdrożenie i konfigurację systemu open-source do zarządzania logami, zapewniającego centralne gromadzenie, przechowywanie i analizę danych dzienników zdarzeń z systemów IT i OT/ICS/IIoT.

Lp.	Parametry techniczne - wymagania minimalne
1	Przedmiotem zamówienia jest usługa obejmująca wdrożenie, konfigurację oraz integrację systemu open-source do zarządzania logami, umożliwiającego centralne zbieranie, przetwarzanie, przechowywanie, przeszukiwanie oraz analizę danych dzienników zdarzeń.
2	Zakres zamówienia obejmuje: - instalację i konfigurację systemu, - wdrożenie komponentów odpowiedzialnych za: - zbieranie logów, - przetwarzanie i normalizację danych, - indeksowanie i przechowywanie danych, - wyszukiwanie i wizualizację, - konfigurację źródeł logów (agentowych i bezagentowych), - integrację z systemami monitorowania sieci.
3	Funkcjonalności rozwiązania: - centralne zbieranie logów z wielu źródeł, - odbiór logów (np. syslog, API, agenty, inne wspierane mechanizmy), - przetwarzanie, filtrowanie i normalizację danych, - indeksowanie i przechowywanie logów, - konfigurację retencji i rotacji danych, - przeszukiwanie logów w czasie rzeczywistym i historycznie, - wizualizację danych (dashboardy), - możliwość definiowania parserów i reguł przetwarzania (pipeline rules), - generowanie raportów operacyjnych i audytowych.
4	Wykonawca dostarczy: - dokumentację techniczną wdrożenia, - opis architektury rozwiązania.
5	Wykonawca przeszkoli Zamawiającego z obsługi dostarczanego rozwiązania – min. 2h
6	Okres realizacji: Maksymalnie do 10.12.2026r.
7	Konfiguracja kopii zapasowej wdrożonego rozwiązania w systemie backupowym Zamawiającego.