**ZAMAWIAJĄCY:**
PRZEDSIĘBIORSTWO WODOCIĄGOWO-KANALIZACYJNE "PŁONIA" SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Na potrzeby postępowania zakupowego pn.: *„Wzmocnienie systemu cyberbezpieczeństwa w Przedsiębiorstwie Wodociągowo-Kanalizacyjnym "PŁONIA" Sp. z o. o.””* w ramach projektu “Cyberbezpieczne Wodociągi” Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo: “Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi”. Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności.

---

## Spis treści

**Wymagania ogólne**

W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”. Dostarczany sprzęt musi być nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w 01.01.2026 r., wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez "wadę fizyczną" należy rozumieć również jakąkolwiek niezgodność ze szczegółowym opisem przedmiotu zamówienia. Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności Sprzętu standardowe rozwiązania softwarowe wraz z prawem do bezterminowego korzystania przez Zamawiającego z tych rozwiązań w takiej funkcji, jednakże w każdym przypadku nie krócej, niż przez czas, w jakim będzie technicznie możliwe używanie Sprzętu. O ile inaczej nie zaznaczono, wszelkie zapisy SOPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.

## 1. Serwer z oprogramowaniem – 4 szt.

| Parametr | Charakterystyka (wymagania minimalne) |
|---|---|
| **Obudowa** | • Obudowa Rack o wysokości max 1U<br>• 8 slotów na dyski 2.5”<br>• Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |
| **Płyta główna** | • Płyta główna z możliwością zainstalowania jednego procesora.<br>• Obsługa procesorów 144 rdzeniowych.<br>• Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.<br>• Na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.<br>• Płyta główna powinna obsługiwać do 4TB pamięci RAM. |
| **Procesor** | • Zainstalowany jeden procesor min. 12-rdzeniowy, min. 2.2GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 155 w teście SPECspeed®2017_fp_base, dostępnym na stronie www.spec.org dla konfiguracji jednoprocesorowej oferowanego serwera. |
| **RAM** | • 128GB DDR5 RDIMM 6400MT/s, |
| **Kontroler RAID** | • Sprzętowy kontroler dyskowy, posiadający<br>  ○ Min. 8GB nieulotnej pamięci cache,<br>  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.<br>  ○ Wsparcie dla dysków samoszyfrujących<br>  ○ Obsługa dysków 22.5 Gbps SAS, 12 Gbps SAS, i 6 Gbps SATA/SAS |
| **Dyski twarde** | • Zainstalowane:<br>  ○ 6x dysk SAS o pojemności min. 1.2TB, Hot-Plug<br>• Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1. |
| **Gniazda PCI** | • Dwa sloty PCIe |
| **Interfejsy sieciowe/FC/SAS** | • 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |
| **Wbudowane porty** | • 4 porty USB w tym min:<br>  ○ 1 port USB 2.0 Type-C<br>  ○ 2 porty USB 3.1<br>  ○ 1 port USB 3.0 wewnątrz obudowy<br>• Port VGA z tyłu obudowy |
| **Video** | • Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| **Zasilacze** | • Redundantne, Hot-Plug min. 1500W klasy Titanium |
| **Elementy montażowe** | • Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |
| **System operacyjny/dodatkowe oprogramowanie** | • Windows Server 2025 Standard – 2 szt. na jeden serwer |
| **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.<br>• Możliwość wyłączenia w BIOS funkcji przycisku zasilania.<br>• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła<br>• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.<br>• Moduł TPM 2.0<br>• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera<br>• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem<br>• Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń. |
| **Karta Zarządzania** | • Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:<br>o zdalny dostęp do graficznego interfejsu Web karty zarządzającej<br>o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika<br>o możliwość podmontowania zdalnych wirtualnych napędów<br>o wirtualną konsolę z dostępem do myszy, klawiatury<br>o wsparcie dla IPv6<br>o wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH<br>o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer<br>o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer<br>o integracja z Active Directory<br>o możliwość obsługi przez sześciu administratorów jednocześnie<br>o Wsparcie dla automatycznej rejestracji DNS<br>o wsparcie dla LLDP<br>o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej<br>o możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy.<br>o Monitorowanie zużycia dysków SSD<br>o Automatyczne zgłaszanie alertów do centrum serwisowego producenta<br>o Automatyczne update firmware dla wszystkich komponentów serwera<br>o Możliwość przywrócenia poprzednich wersji firmware<br>o Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON<br>o Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych<br>o Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram.<br>o Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera<br>o kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania<br>o możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień |

| | |
|---|---|
| | ○ możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera<br>○ możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer<br>○ możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe<br>możliwość rozszerzenia funkcjonalności o:<br>○ 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<br>○ możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej<br>○ Automatyczne odświeżanie certyfikatów SSL<br>○ monitorowanie przepływu powietrza na bieżąco (w CFM) |
| **Oprogramowanie do zarządzania** | • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:<br>○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych<br>○ integracja z Active Directory<br>○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta<br>○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish<br>○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram<br>○ Szczegółowy opis wykrytych systemów oraz ich komponentów<br>○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF<br>○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.<br>○ Grupowanie urządzeń w oparciu o kryteria użytkownika<br>○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji<br>○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach<br>○ Szybki podgląd stanu środowiska<br>○ Podsumowanie stanu dla każdego urządzenia<br>○ Szczegółowy status urządzenia/elementu/komponentu<br>○ Generowanie alertów przy zmianie stanu urządzenia.<br>○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń<br>○ Integracja z service desk producenta dostarczonej platformy sprzętowej<br>○ Możliwość przejęcia zdalnego pulpitu<br>○ Możliwość podmontowania wirtualnego napędu<br>○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów<br>○ Możliwość importu plików MIB<br>○ Przesyłanie alertów „as-is” do innych konsol firm trzecich<br>○ Możliwość definiowania ról administratorów<br>○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów<br>○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)<br>○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta<br>○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów<br>○ 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.<br>o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.<br>o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile<br>o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.<br>o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.<br>o Zdalne uruchamianie diagnostyki serwera.<br>o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.<br>o 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. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:<br>• Monitoring:<br>o ilość podłączonych oraz rozłączonych systemów<br>o stan podłączonych urządzeń<br>o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów<br>o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia<br>o informacje o statusie gwarancji dla poszczególnych urządzeń<br>o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń<br>o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych.<br>o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych<br>o 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.<br>o Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych.<br>o Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC.<br>o Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej.<br>o Monitoring parametrów serwerów z informacją o minimum:<br>▪ Obciążeniu procesora<br>▪ Zużyciu pamięci RAM<br>▪ Temperaturze procesorów<br>▪ Temperaturze powietrza wlotowego<br>▪ Zużyciu prądu<br>▪ Zmianach w fizycznej konfiguracji serwera<br>▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.<br>o Monitoring parametrów pamięci masowych z informacją o minimum:<br>▪ Opóźnieniach<br>▪ IOPS |

| | |
|---|---|
| | ▪ Przepustowości<br>▪ Utylizacji kontrolerów<br>▪ Pojemność całkowita i dostępna<br>▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.<br>▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.<br>▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata<br>▪ Informacje o poziomie redukcji danych<br>▪ Informacje o statusie replikacji oraz snapshotów<br>o Monitoring parametrów przełączników sieciowych z informacją o minimum:<br>▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny<br>▪ Stanie komponentów: zasilacze, wentylatory<br>▪ Podłączonych hostach<br>▪ Ilości i statusu portów<br>▪ Utylizacji procesora<br>▪ Utylizacji poszczególnych portów<br>▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.<br>• Aktualizacja firmware<br>o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania<br>o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania<br>o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania<br>o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania<br>• Raporty<br>o Możliwość generowania raportów dla serwerów zawierających informację o:<br>▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej<br>▪ Średnim obciążeniu: procesorów, pamięci RAM, IO,<br>o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o:<br>▪ 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<br>o Generowanie raportów do plików CSV i PDF<br>• Cyberbezpieczeństwo<br>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.<br>o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.<br>o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych.<br>o Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.<br>• Wspierane urządzenia |

| | |
|---|---|
| | ○ Urządzenie Producenta dostarczane w ramach postępowania<br>○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe.<br>• Wirtualny asystent<br>○ 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;<br>• Możliwość rozszerzenia funkcjonalności<br>○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.<br>• Inne<br>○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |
| **Certyfikaty** | • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001<br>• Serwer musi posiadać deklaracja CE.<br>• Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.**<br>• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025. |
| **Dokumentacja użytkownika** | • Zamawiający wymaga dokumentacji w języku polskim lub angielskim.<br>• Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Warunki gwarancji** | • Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat.<br>• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.<br>• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.<br>• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.<br>• Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.<br>• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.<br>• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki |

| | |
|---|---|
| | dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.<br>• 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.<br>• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:<br>o Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.<br>o Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.<br>o Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.<br>o Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.<br>o Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.<br>• Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |

## 2. Platforma backup z deduplikacją i oprogramowaniem – 2 szt.

**Minimalne wymagania techniczne:**

Przedmiotem niniejszej pozycji jest kompletne rozwiązanie do tworzenia, przechowywania i odtwarzania kopii zapasowych hostów eksploatowanych w środowisku Zamawiającego, dostarczane przez Wykonawcę jako jedna pozycja asortymentowa obejmujące łącznie:

1) warstwę sprzętową — urządzenie serwerowe pełniące funkcję magazynu kopii zapasowych wraz z kompletem dysków danych i dysków pamięci podręcznej (część A);
2) warstwę programową — oprogramowanie serwera kopii zapasowych w wersji z licencją bezterminową (część B);
3) zestaw mechanizmów ochrony repozytorium kopii zapasowych przed atakami typu ransomware, realizowany łącznie w obu warstwach

Wszystkie wskazane w niniejszym OPZ nazwy własne algorytmów, protokołów, standardów i interfejsów stanowią wskazanie poziomu funkcjonalnego wymagań — dopuszcza się rozwiązania równoważne o parametrach nie gorszych od opisanych.

| A - WARSTWA SPRZĘTOWA | | |
|---|---|---|
| 1 | **Obudowa** | Obudowa typu Rack 19", wysokość maksymalnie 2U, minimum 8 gniazd dyskowych obsługujących dyski 3,5" w trybie hot-plug. Konstrukcja dedykowana do montażu w szafie serwerowej, w zestawie z urządzeniem należy dostarczyć komplet szyn montażowych. |

| | | |
|---|---|---|
| 2 | **Procesor** | Procesor wielordzeniowy klasy serwerowej, minimum 4 rdzenie fizyczne i 8 wątków, taktowanie bazowe minimum 2,0 GHz, architektura x86-64, dedykowany do pracy w urządzeniach klasy NAS. |
| 3 | **Pamięć RAM** | Minimum 16 GB pamięci RAM typu DDR4 w formacie SO-DIMM. Urządzenie musi posiadać minimum 2 sloty pamięci RAM. |
| 4 | **Dyski danych** | Urządzenie wyposażone w minimum 8 wnęk dyskowych obsługujących dyski 3,5" z interfejsem SATA 6 Gb/s, w trybie hot-plug. W zestawie z urządzeniem należy dostarczyć minimum 2 sztuki dysków HDD klasy serwerowej (enterprise/NAS) o pojemności minimum 20 TB każdy, format 3,5", interfejs SATA, hot-plug. |
| 5 | **Cache SSD NVMe** | Urządzenie musi posiadać minimum 2 dedykowane gniazda na dyski SSD NVMe w formacie M.2 (interfejs PCIe Gen3 lub szybszy) umożliwiające wykorzystanie ich jako pamięci podręcznej (cache) dla operacji odczytu/zapisu. W zestawie z urządzeniem należy dostarczyć minimum 2 sztuki dysków SSD NVMe M.2 o pojemności minimum 256 GB każdy, dedykowanych do pracy w trybie cache. |
| 6 | **Interfejsy sieciowe** | Minimum 2 wbudowane porty sieciowe klasy 2,5GbE RJ-45, kompatybilne wstecznie ze standardami 1GbE/100Mbps. |
| 7 | **Interfejsy dodatkowe** | Minimum 2 porty USB 3.2 Gen 2 (10 Gbps) typu A oraz minimum 1 port USB typu C, umożliwiające podłączenie zewnętrznych nośników danych. |
| 8 | **Możliwość rozbudowy** | Urządzenie musi posiadać minimum 1 slot rozszerzeń typu PCIe Gen3 x8 (lub szybszy), umożliwiający w przyszłości instalację kart sieciowych 10/25GbE lub kart M.2 SSD. |
| 9 | **Protokoły dostępu** | Wsparcie co najmniej dla protokołów: SMB/CIFS, NFS, iSCSI, AFP, FTP, SFTP, WebDAV. |
| 10 | **Poziomy RAID** | Obsługa konfiguracji RAID co najmniej w trybach: 0, 1, 5, 6, 10, JBOD. Obsługa funkcji rozbudowy macierzy online oraz migracji pomiędzy poziomami RAID. |
| 11 | **Zarządzanie** | Wbudowany webowy interfejs administracyjny dostępny przez przeglądarkę z wykorzystaniem protokołu HTTPS. Wbudowany monitoring stanu urządzenia, zasobów oraz dysków. Powiadomienia o zdarzeniach realizowane co najmniej drogą e-mail oraz SNMP. |
| 12 | **Funkcjonalności** | Wsparcie dla funkcji wykonywania migawek (snapshots) wolumenów danych. Wsparcie dla replikacji danych pomiędzy jednostkami NAS oraz do lokalizacji zdalnej, w tym replikacji opartej o migawki. Wsparcie dla mechanizmów ochrony danych przed modyfikacją (immutable snapshots) lub równoważnych. |
| 13 | **System operacyjny** | Urządzenie musi być dostarczone z preinstalowanym, dedykowanym systemem operacyjnym producenta, obejmującym co najmniej: zarządzanie wolumenami i konfiguracją RAID, obsługę protokołów dostępu, mechanizm snapshotów i replikacji, narzędzia do tworzenia kopii zapasowych oraz integracji z chmurą. Wszystkie funkcjonalności wymagane w niniejszej specyfikacji muszą być dostępne bez konieczności wykupienia dodatkowych licencji. |
| 14 | **Zasilanie** | Zasilacz zgodny z wymaganiami producenta urządzenia; preferowane zasilanie redundantne. |
| 15 | **Chłodzenie** | Aktywny system chłodzenia urządzenia oparty o wentylatory zapewniające prawidłową pracę w warunkach pełnego obciążenia. |

| | | |
|---|---|---|
| 16 | **Dokumentacja** | Dokumentacja techniczna oraz instrukcja obsługi w języku polskim lub angielskim, dostępna w formie elektronicznej. |
| 17 | **Wymagania dodatkowe** | Wszystkie dostarczone komponenty (urządzenie, dyski HDD, dyski SSD NVMe, pamięć RAM, akcesoria montażowe) muszą być ze sobą w pełni kompatybilne i pochodzić z oficjalnego kanału dystrybucji na terenie Unii Europejskiej. |
| **B - WARSTWA PROGRAMOWA** | | |
| 18 | Oprogramowanie dostarczone w modelu licencji bezterminowej (wieczystej / perpetual), z prawem do pobierania aktualizacji i poprawek w okresie obowiązującego wsparcia technicznego.<br>A.2 Licencjonowanie w modelu uniwersalnym, opartym na liczbie chronionych instancji (obciążeń) – **min. 10 urządzeń**, umożliwiające wymienną ochronę maszyn wirtualnych, serwerów fizycznych, stacji roboczych oraz obciążeń chmurowych w ramach tej samej puli licencji.<br>A.3 Brak ograniczeń licencyjnych co do liczby repozytoriów kopii zapasowych oraz ich komponentów (extentów).<br>A.4 Możliwość wdrożenia w postaci gotowego, prekonfigurowanego obrazu zawierającego zahartowany, minimalny system operacyjny klasy Linux wraz z oprogramowaniem backupu.<br>A.5 Obsługa wdrożenia także w postaci instalatora dla systemów Microsoft Windows (instalacja graficzna oraz nienadzorowana z linii poleceń).<br>A.6 Dostępność minimalnego, dedykowanego obrazu systemu dla komponentów infrastruktury: serwerów proxy, repozytoriów, serwerów montujących i bram.<br>A.7 Wbudowany mechanizm automatycznej aktualizacji komponentów (systemu operacyjnego appliance oraz aplikacji) przez interfejs webowy lub linię poleceń.<br><br>B.1 Backup i odtwarzanie maszyn wirtualnych VMware vSphere oraz Microsoft Hyper-V, w tym natychmiastowe odtworzenie całej maszyny oraz odtwarzanie granularne elementów aplikacji.<br>B.2 Backup bezagentowy (agentless) z wykorzystaniem mechanizmu śledzenia zmienionych bloków (CBT) oraz przetwarzania spójnego z aplikacją.<br>B.3 Natychmiastowe odtworzenie (Instant Recovery) maszyny uruchamianej bezpośrednio z pliku kopii do środowiska VMware, Hyper-V.<br>B.4 Backup z migawek macierzy produkcyjnych (storage snapshots) wiodących producentów, z minimalnym wpływem na środowisko produkcyjne.<br>B.5 Wbudowana akceleracja WAN przyspieszająca transfer kopii i replik do lokalizacji zdalnej oraz oszczędzająca pasmo.<br>B.6 Kontrola maksymalnego opóźnienia pamięci masowej (storage latency control), aby zadania backupu i replikacji nie wpływały na dostępność produkcji.<br>B.7 Przechowywanie każdej maszyny wirtualnej w osobnym pliku kopii (per-VM) z równoległym przetwarzaniem oraz powinowactwem proxy i repozytorium.<br><br>C.1 Backup agentowy serwerów i stacji roboczych Windows, Linux oraz macOS, z automatycznym wdrażaniem i zarządzaniem agentami z poziomu centralnej konsoli.<br>C.2 Agenci zoptymalizowani pod chmurę (cloud-integrated) zapisujący kopie bezpośrednio do pamięci obiektowej i działający bez bezpośredniego połączenia sieciowego.<br>C.3 Organizacja i automatyzacja wdrożeń agentów w oparciu o kontenery Active Directory, pliki CSV lub tagi chmurowe (grupy ochrony) z harmonogramami aktualizacji. | |

| | |
|---|---|
| | D.1 Tworzenie kopii spójnych z aplikacją (application-aware) z obsługą backupu logów transakcyjnych dla Microsoft SQL Server.<br>D.2 Dedykowane wtyczki do backupu baz/aplikacji Microsoft SQL, z centralnym zarządzaniem politykami backupu.<br>D.3 Granularne odtwarzanie elementów aplikacji za pomocą dedykowanych narzędzi dla: Microsoft SQL Server, Microsoft Active Directory.<br>D.4 Natychmiastowe odtworzenie bazy danych (Microsoft SQL Server) do stanu bieżącego lub do wskazanego punktu w czasie.<br>D.5 Backup i odtwarzanie Microsoft Entra ID wraz z profilami konfiguracji oraz politykami zgodności urządzeń Intune.s<br><br>E.1 Natywny backup i odtwarzanie zasobów AWS z odtwarzaniem pełnym i granularnym do tego samego lub innego konta/regionu.<br>E.2 Natywny backup i odtwarzanie zasobów Microsoft Azure<br>E.3 Natywny backup i odtwarzanie zasobów Google Cloud<br>E.4 Natywne wykonywanie migawek oraz backup obrazowy i agentowy obciążeń IaaS/PaaS u wiodących dostawców chmury.<br>E.5 Backup pamięci obiektowej z możliwością odtworzenia do innego typu pamięci.<br>E.6 Mechanizmy kontroli kosztów chmury (kompresja, przenoszenie do archiwalnych klas pamięci, prognozowanie kosztów i planowanie pojemności).<br>E.7 Natychmiastowe odtworzenie obciążeń do Microsoft Azure<br>E.8 Migracja kopii i obciążeń pomiędzy chmurami oraz pomiędzy chmurą a środowiskiem lokalnym (AWS, Azure, Google Cloud, on-premises).<br><br>F.1 Obsługa repozytorium zahartowanego opartego na systemie Linux z niezmiennością (immutability) kopii, uniemożliwiającą ich zaszyfrowanie lub usunięcie przez ransomware i nieuprawnionych użytkowników.<br>F.2 Składowanie kopii w pamięci obiektowej (object storage) lokalnej oraz w chmurze publicznej z niezmiennością opartą o blokadę obiektów (S3 Object Lock).<br>F.3 Repozytorium typu scale-out z automatycznym zarządzaniem cyklem życia kopii w warstwach: wydajnościowej, pojemnościowej i archiwalnej.<br>F.4 Warstwa archiwalna z natywną obsługą Amazon S3 Glacier (w tym Glacier Deep Archive) oraz Microsoft Azure Archive Storage.<br>F.5 Backup na napędy taśmowe zgodne ze standardem LTO oraz obsługa protokołu NDMP dla urządzeń NAS; obsługa taśm IBM Jaguar.<br>F.6 Szyfrowanie typu end-to-end algorytmem AES-256 dla danych w źródle, w trakcie transmisji oraz w spoczynku.<br>F.7 Integracja z urządzeniami deduplikującymi (m.in. Dell Data Domain Boost, HPE StoreOnce Catalyst, Quantum DXi, ExaGrid).<br>F.8 Natywna niezmienność migawek/kopii na macierzach i deduplikatorach: HPE 3PAR/Primera/Alletra (Virtual Lock), HPE StoreOnce Catalyst Copy, Dell Data Domain Retention Lock oraz IBM FlashSystem.<br>F.9 Obsługa NetApp ONTAP FlexGroups oraz inteligentne równoważenie obciążenia dla klastrów Isilon i NetApp.<br>F.10 Przenoszenie i kopiowanie plików kopii pomiędzy zadaniami i repozytoriami oraz proaktywna weryfikacja stanu warstwy pojemnościowej (health-check). |

| | |
|---|---|
| | F.11 Realizacja reguły 3-2-1 poprzez zadania kopiowania kopii (backup copy) z walidacją i naprawą; zewnętrzne repozytorium do odtwarzania z kopii chmurowych.<br>F.12 Backup udziałów plikowych NAS (SMB i NFS) z archiwizacją wersji plików oraz backup danych w pamięci obiektowej.<br>F.13 Backup środowiska VMware Cloud Director (vApp, metadane i atrybuty) z odtwarzaniem bezpośrednio do vCloud.<br>F.14 Integracja z gotowym, chmurowym magazynem obiektowym dostawcy oraz backup off-site za pośrednictwem usługodawcy (Cloud Connect).<br>G.1 Wbudowany silnik wykrywania złośliwego oprogramowania działający w trakcie backupu (analiza indeksu plików, wykrywanie szyfrowania i podejrzanych rozszerzeń) z oznaczaniem punktów przywracania jako podejrzane/zainfekowane/czyste.<br>G.2 Wbudowane, niskoobciążeniowe skanowanie sygnaturowe zagrożeń z aktualizowaną w czasie rzeczywistym bazą sygnatur.<br>G.3 Skanowanie zawartości kopii regułami YARA (m.in. w ramach testów odtwarzalności, bezpiecznego odtwarzania oraz skanowania na żądanie).<br>G.4 Skaner wskaźników kompromitacji (IoC) wykrywający narzędzia atakujących oraz narzędzia służące do eksfiltracji danych.<br>G.5 Analiza taktyk, technik i procedur atakujących (TTP) chroniąca serwery backupu przed cyberatakiem.<br>G.6 Bezpieczne odtwarzanie (Secure Restore) z opcjonalnym skanem antywirusowym/YARA pliku kopii przed przywróceniem do produkcji.<br>G.7 Centralne zarządzanie kluczami kryptograficznymi poprzez integrację z systemem zarządzania kluczami (KMS).<br>G.8 Integracja z systemami klasy SIEM/SOAR oraz ITSM (m.in. Splunk, Microsoft Sentinel, Palo Alto XSIAM/XSOAR, ServiceNow, CrowdStrike) oraz przekazywanie zdarzeń do serwerów syslog.<br>G.9 Otwarte API incydentów umożliwiające narzędziom cyberbezpieczeństwa oznaczanie punktów przywracania jako zainfekowane lub wyzwalanie backupu.<br>G.10 Autoryzacja dwuosobowa (zasada czterech oczu) dla operacji destrukcyjnych: usuwania kopii i repozytoriów, dodawania administratorów, zmian uprawnień i MFA.<br>G.11 Uwierzytelnianie wieloskładnikowe (MFA) konsoli oraz obsługa federacyjnego logowania jednokrotnego (SSO).<br>G.12 Granularna kontrola dostępu oparta na rolach oraz audyt działań użytkowników i operacji odtwarzania plików.<br>G.13 Komponenty kryptograficzne zgodne ze standardem FIPS.<br>H.1 Agent głębokiej analizy złośliwego oprogramowania z wizualizacją zagrożeń, oceną ich wpływu oraz prowadzonymi krokami odtwarzania.<br>H.2 Agent analizy danych umożliwiający odpytywanie złożonych danych językiem naturalnym oraz generowanie streszczeń i rekomendacji.<br>H.3 Wprowadzanie głosowe usprawniające pracę operatora.<br>H.4 Codzienne podsumowanie odporności danych korelujące wykryte problemy z bazą wiedzy producenta oraz listą rekomendowanych działań.<br>H.5 Interaktywne, inteligentne raportowanie ułatwiające analizę i podejmowanie decyzji.<br>H.6 Asystent czatu wspierający rozwiązywanie problemów i optymalizację. |

| | |
|---|---|
| | I.1 Odtwarzanie całych maszyn wirtualnych do lokalizacji oryginalnej lub nowej oraz odtwarzanie pojedynczych dysków i plików maszyn.<br>I.2 Natychmiastowe odtwarzanie pojedynczych dysków, baz danych oraz udziałów plikowych bezpośrednio z pliku kopii.<br>I.3 Odtwarzanie plikowe z systemów Windows, Linux, macOS w tym porównanie z produkcją, odtwarzanie uprawnień oraz indeksowanie systemu plików gościa.<br>I.4 Ciągła ochrona danych (CDP) dla obciążeń krytycznych z odtwarzaniem do stanu bieżącego lub wybranego punktu w czasie, w tym CDP dla dowolnych maszyn Windows (fizycznych, wirtualnych i chmurowych).<br>I.5 Odtwarzanie plików i aplikacji z repliki CDP z dowolnego punktu przywracania, bez przerywania replikacji.<br>I.6 Replikacja obrazowa maszyn wirtualnych lokalnie oraz do lokalizacji zapasowej, z asystowanym przełączaniem awaryjnym i powrotem (failover/failback) oraz replikacją tworzoną z plików kopii.<br>I.7 Orkiestracja przełączania awaryjnego jednym kliknięciem (plany failover) oraz replikacja do chmury usługodawcy (DRaaS).<br>I.8 Automatyczna weryfikacja odtwarzalności replik poprzez próbny failover w odizolowanym środowisku, z obsługą własnych skryptów.<br>I.9 Odtwarzanie oraz migracja maszyn lokalnych bezpośrednio do chmur AWS, Microsoft Azure i Google Cloud.<br>I.10 Udostępnianie zawartości kopii aplikacjom i skryptom firm trzecich poprzez API integracji danych (do analiz bezpieczeństwa, kontroli zgodności i ponownego wykorzystania danych).<br><br>J.1 Automatyczne testowanie i weryfikacja odtwarzalności każdej kopii poprzez uruchomienie maszyny z pliku kopii w odizolowanym (fenced-off) środowisku, wraz z obsługą własnych skryptów testowych.<br>J.2 Piaskownica na żądanie (on-demand sandbox) umożliwiająca testowanie aktualizacji, rozwiązywanie problemów i szkolenia bez wpływu na produkcję.<br>J.3 Tworzenie środowisk testowych bezpośrednio z migawek macierzy (on-demand sandbox from storage snapshots) działających z pełną wydajnością I/O.<br>J.4 Odtwarzanie etapowe (staged restore) umożliwiające usunięcie danych wrażliwych z punktu przywracania przed przywróceniem do produkcji.<br><br>K.1 Tworzenie i wykonywanie zautomatyzowanych planów odtwarzania po awarii (planów DR) z konfiguracją bez utraty danych (zero data loss).<br>K.2 Zautomatyzowane, nieinwazyjne testowanie planów DR w odizolowanej sieci, bez wpływu na środowisko produkcyjne, wraz ze szczegółowym raportowaniem.<br>K.3 Orkiestracja międzyplatformowa i planowana migracja obciążeń pomiędzy VMware, Microsoft Hyper-V / Azure Local oraz Microsoft Azure.<br>K.4 Orkiestracja odtwarzania kopii agentowych Windows i Linux do środowisk VMware lub Microsoft Azure.<br>K.5 Monitorowanie zgodności osiąganych parametrów RTO i RPO względem celów zdefiniowanych dla każdego planu DR.<br>K.6 Automatyczne generowanie dokumentacji planów DR (definicje, testy, wykonania) w wersji szczegółowej oraz w formie streszczenia dla kierownictwa.<br>K.7 Audyt planów odtwarzania ze śledzeniem zmian oraz cyklicznym raportem aktywności planów; zaplanowane kontrole gotowości (readiness checks). |

| | | |
|---|---|---|
| | | K.8 Uwierzytelnianie wieloskładnikowe (MFA) zabezpieczające wykonanie i zatwierdzanie planów odtwarzania.<br>K.9 Skanowanie kopii pod kątem złośliwego oprogramowania na potrzeby planów odtwarzania i odtwarzanie wyłącznie z czystych punktów przywracania.<br>K.10 Odtwarzanie jednym kliknięciem w skali masowej (pojedyncza aplikacja lub cała lokalizacja) oraz odtwarzanie do chmury.<br><br>L.1 Centralny pulpit prezentujący zagrożenia, ryzyka oraz ocenę poziomu bezpieczeństwa środowiska.<br>L.2 Monitoring wydajności i alarmowanie dla zadań backupu bez ograniczenia liczby monitorowanych serwerów backupu.<br>L.3 Konfigurowalne raportowanie z możliwością eksportu, raporty interaktywne oraz raportowanie chronionych baz danych.<br>L.4 Monitoring i raportowanie infrastruktury wirtualnej (VMware vSphere oraz Microsoft Hyper-V), w tym ocena infrastruktury wg najlepszych praktyk.<br>L.5 Monitoring i raportowanie ochrony obciążeń w chmurach publicznych (AWS, Microsoft Azure, Google Cloud).<br>L.6 Monitoring na poziomie aplikacji (m.in. wykrycie wyłączenia oprogramowania antywirusowego lub przekroczenia zasobów).<br>L.7 Planowanie pojemności z modelowaniem scenariuszy typu what-if oraz mapy cieplne (heatmaps) wykorzystania repozytoriów i serwerów proxy.<br>L.8 Widok biznesowy (business view) — kategoryzacja zasobów wg jednostki, działu, przeznaczenia i SLA, wspierająca kontrolę dostępu i zgodność.<br>L.9 Inteligentna diagnostyka znanych problemów oraz automatyczne działania naprawcze (self-healing remediation).<br>L.10 Konfigurowalne powiadomienia e-mail o alarmach oraz dwukierunkowa integracja zgłoszeń z ServiceNow.<br>L.11 Monitorowanie stanu wysokiej dostępności (HA) z opcjami naprawczymi oraz alarmami.<br><br>M.1 Zarządzanie przez interfejs webowy (Web UI) z zaawansowanym filtrowaniem i wyszukiwaniem.<br>M.2 Wysoka dostępność (HA) komponentu zarządzającego z wbudowaną redundancją i przełączaniem awaryjnym (klaster HA na appliance).<br>M.3 Centralna, webowa konsola zarządzania rozproszonym wdrożeniem (pojedynczy panel) z możliwością uruchamiania/zatrzymywania zadań oraz wykonywania odtworzeń.<br>M.4 Automatyzacja zadań poprzez RESTful API oraz moduł PowerShell.<br>M.5 Centralne zarządzanie agentami oraz wtyczkami baz danych z poziomu konsoli.<br>M.6 Samoobsługowe portale odtwarzania (plików, maszyn wirtualnych, baz danych, skrzynek pocztowych) z delegacją uprawnień. |
| 19 | **Wsparcie techniczne, gwarancja i utrzymanie całości rozwiązania** | Wykonawca w ramach niniejszej pozycji asortymentowej zapewnia łącznie dla warstwy sprzętowej (część A) i warstwy programowej (część B):<br>a) gwarancję na całość warstwy sprzętowej (urządzenie wraz z dostarczonymi dyskami HDD, dyskami SSD NVMe, pamięcią RAM oraz akcesoriami montażowymi) na okres natywnie nadawany przez producenta bez dodatkowych opłat, świadczoną przez autoryzowany serwis producenta na terenie Rzeczypospolitej Polskiej, liczoną od dnia podpisania protokołu odbioru końcowego; |

| | | |
|---|---|---|
| | | b) wsparcie pierwszej linii świadczone przez Wykonawcę w języku polskim w trybie 8x5 (dni robocze, godziny 8:00–16:00), z czasem reakcji nie dłuższym niż 1 dzień roboczy od chwili zgłoszenia, przez cały okres trwania gwarancji warstwy sprzętowej;<br>c) dostęp do oficjalnej dokumentacji producenta obu warstw w wersji online, w języku polskim lub angielskim. Przedłużenie subskrypcji wsparcia technicznego warstwy programowej po dniu 31 grudnia 2026 r. nie wchodzi w zakres niniejszego zamówienia i nie obciąża budżetu projektu. |

## 3. Platforma SIEM

| | |
|---|---|
| **LICENCJA** | W ramach postępowania Wykonawca jest zobowiązany dostarczyć Oprogramowanie wraz z licencją. Wykonawca musi dostarczyć licencje na czas nieograniczony.<br><br>Oprogramowanie musi posiadać od dnia podpisania protokołu odbioru do 31.12.2026 r.wsparcie techniczne producenta lub dystrybutora. Oprogramowania dla licencji (tj. licencji dostarczonych w ramach niniejszego postępowania).<br>Oprogramowanie musi posiadać możliwość aktualizacji do najnowszej dostępnej wersji w okresie gwarancji. W ramach gwarancji Zamawiający ma prawo zgłaszać błędy w Oprogramowaniu do serwisu producenta.<br>Licencje na Oprogramowanie dostarczone będą do siedziby Zamawiającego w formie papierowej lub elektronicznej.<br>Dostarczona licencja na Oprogramowanie Systemu nie może limitować wielkości przechowywanych danych oraz możliwości wyszukiwania informacji z zgromadzonych danych.<br>Ilość licencji dla hostów (IP address): **min 100 szt.**<br><br>Wykonawca wraz z systemem SIEM może dostarczyć system do aktywnego monitoringu kluczowych systemów Zamawiającego. Wykonawca przeprowadzi instalację, konfigurację oraz podłączenie wszystkich wymaganych systemów będących celem monitorowania. System musi spełniać poniższe wymagania minimalne: |
| **WYMAGANIA DOT. SYSTEMU BEZPIECZEŃSTWA** | Użytkownicy<br>▪ Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat.<br>▪ Zapewnienia równoległego dostępu do systemu dla wielu użytkowników.<br>▪ Ograniczania użytkownikom dostępu do wybranych grup hostów.<br>Monitorowanie<br>▪ Monitorowania serwerów fizycznych.<br>▪ Monitorowania urządzeń sieciowych.<br>▪ Monitorowania stanu połączeń.<br>▪ Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów<br>▪ Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów Windows i Linux.<br>▪ Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych.<br>▪ Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.<br>▪ Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług. |

| | |
|---|---|
| | ▪ Grupowanie hostów.<br>▪ Definiowanie planowanych przerw serwisowych dla hostów i usług.<br>▪ Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).<br>▪ Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych).<br>▪ Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).<br>▪ Monitorowanie serwerów za pomocą agentów<br>▪ Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server.<br>▪ Monitorowanie Active Directory.<br>▪ Monitorowanie serwerów plików, udziałów sieciowych.<br>▪ Monitorowanie statusu serwerów Apache.<br>▪ Monitorowanie baz danych:<br>ORACLE, MySQL, Postgress, MSSQL Server, DB2<br>▪ Monitorowanie urządzeń przez następujące protokoły:<br>SNMP, WMI, IPMI.<br>▪ Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.<br>▪ Monitorowanie poprawności działania DNS.<br>▪ Monitorowanie środowiska VMware.<br>▪ Monitorowanie środowiska Hyper-V.<br>▪ Monitorowanie środowisk Proxmox<br>▪ Monitorowanie działania serwera czasu NTP.<br>▪ Monitorowanie offsetu czasu na serwerach.<br>▪ Monitorowanie ping - czasy odpowiedzi, straty pakietów.<br>▪ Monitorowanie zajętości miejsca na poszczególnych partycjach.<br>▪ Monitorowanie obciążenia dysków.<br>▪ Monitorowanie wykorzystania pamięci RAM.<br>▪ Monitorowanie obciążenia CPU.<br>▪ Monitorowanie logów systemowych Windows.<br>▪ Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.<br>▪ Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane.<br>▪ Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix.<br>▪ Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence)<br>▪ Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe<br>▪ Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów).<br>▪ Wykrywanie niestabilnie działających usług.<br>▪ Monitorowanie dostępności stron internetowych. |

| | |
|---|---|
| | ▪ Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).<br><br>Prezentacja<br>▪ Prezentację stanu urządzeń na mapie.<br>▪ Prezentację danych na dashboardach.<br>▪ Elastyczną konfigurację dashboardów, wybór elementów.<br>▪ Wizualizację stanu działania całej infrastruktury na jednym dashboardzie.<br>▪ Tworzenie indywidualnych dashboardów przez użytkowników<br><br>Powiadomienia<br>▪ Globalne wyłączanie powiadomień.<br>▪ Powiadamianie użytkownika o problemach przez e-mail.<br>▪ Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie.<br>▪ Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników.<br>▪ Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług<br><br>Konfiguracja<br>▪ Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW<br>▪ Automatyczna konfiguracja i działanie z REST-API<br>▪ Centralne zarządzanie agentami<br>▪ Integracja danych z różnych źródeł danych (JSON, XML, SNMP)<br><br>Kolektor logów<br>System monitoruje urządzenia klasy UTM minimum w zakresie:<br>• wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika<br>• monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany” jest uważany za OK, a status „niezsynchronizowany” CRIT.<br>• monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz” (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda” (1).<br>• monitoruje aktualną liczbę sesji na urządzeniu<br>• monitoruje liczbę dostępnych tuneli IPSec VPN<br>• monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika.<br>• Monitoruje poziom wykorzystania procesora<br>• Możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog<br>System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog. |

| | |
|---|---|
| | Cyberbezpieczeństwo<br>System monitoruje urządzenia klasy UTM minimum w zakresie:<br>- wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika<br>- monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany" jest uważany za OK, a status „niezsynchronizowany" CRIT.<br>- monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz" (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda" (1).<br>- monitoruje aktualną liczbę sesji na urządzeniu<br>- monitoruje liczbę dostępnych tuneli IPSec VPN<br>- monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika.<br>- monitoruje poziom wykorzystania procesora<br>- Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne.<br>▪ Możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog<br>▪ System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog. |
| **Rozszerzone wsparcie serwisowe** | System jest objęty rozszerzonym wsparciem technicznym gwarantującym czas reakcji wsparcia technicznego do 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub dystrybutora przez okres do 31.12.2026 r.<br>System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Dystrybutora w języku polskim w zakresie:<br>• Wsparcie telefoniczne zespołu certyfikowanych inżynierów.<br>• Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.<br>• Doradztwo w zakresie konfiguracji.<br>• Zdalne wsparcie techniczne.<br>• Pomoc w zakładaniu zgłoszeń serwisowych u producenta.<br>• Przygotowanie do zdalnej konfiguracji.<br>• Zdalna konfiguracja (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.<br>• Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.<br>• Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.<br>• Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.<br><br>**Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w szczególności w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.** |

| | |
|---|---|
| | Oferent winien przedłożyć dokumenty:<br>• Oświadczanie Producenta lub Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).<br>• Certyfikat ISO 9001 oraz 27001 autoryzowanego podmiotu serwisującego. |

## 4. Switch zarządzalny klasy enterprise z akcesoriami – 4 zest.

### WYMAGANIA MINIMALNE

**1. Architektura, porty i wydajność**

1. Przełącznik zarządzalny, przeznaczony do montażu w szafie 19", wysokość maks. 1U.
2. Min. 48 portów Gigabit Ethernet 10/100/1000 Mb/s w standardzie RJ-45, wszystkie z obsługą PoE/PoE+.
3. Min. 4 porty 10 Gb/s w slotach SFP+ (uplink).
4. Architektura nieblokująca, przełączanie z prędkością łącza (wire-speed) na wszystkich portach.
5. Wydajność przełączania min. 176 Gb/s oraz przepustowość min. 130 Mpps dla pakietów 64-bajtowych.
6. Tablica adresów MAC min. 16 000 wpisów.
7. Bufor pakietów min. 1,5 MB; pamięć Flash min. 512 MB; pamięć operacyjna min. 1 GB.
8. Obsługa ramek jumbo o rozmiarze min. 9000 bajtów.
9. Port konsoli (RJ-45 i/lub USB-C) oraz port USB do zarządzania plikami i obrazami oprogramowania.

**2. Power over Ethernet (PoE)**

10. Obsługa zasilania PoE zgodnie z IEEE 802.3af oraz 802.3at (PoE+).
11. Łączny budżet mocy PoE min. 700 W, z możliwością zasilania PoE na wszystkich 48 portach RJ-45.

**3. Funkcje warstwy 2**

12. Obsługa min. 4093 sieci VLAN (IEEE 802.1Q), w tym VLAN głosowy, VLAN gościnny oraz private VLAN.
13. Protokoły drzewa rozpinającego: 802.1d (STP), 802.1w (RSTP), 802.1s (MSTP) oraz PVST+/RPVST+.
14. Agregacja łączy zgodnie z IEEE 802.3ad (LACP), min. 8 grup agregacji.
15. Mirroring portów oraz RSPAN i sFlow do analizy ruchu.
16. Łączenie przełączników w stos zarządzany jako pojedyncze urządzenie z jednym adresem IP (min. 4 jednostki).

**4. Funkcje warstwy 3**

17. Routing IPv4 oraz IPv6 z prędkością łącza (wire-speed).
18. Obsługa min. 900 tras statycznych oraz min. 120 interfejsów IP.
19. Routing dynamiczny RIP v2, obsługa CIDR oraz Policy-Based Routing (PBR).
20. Wbudowany serwer DHCP oraz DHCP relay w warstwie 2 i 3.

**5. Bezpieczeństwo**

21. Uwierzytelnianie IEEE 802.1X z dynamicznym przypisaniem VLAN, uwierzytelnianiem MAC oraz VLAN gościnnym; uwierzytelnianie przez przeglądarkę (web-based).
22. Mechanizmy DHCP snooping, IP Source Guard oraz Dynamic ARP Inspection (powiązanie IP/MAC/port).
23. IPv6 First Hop Security (RA guard, ND inspection, DHCPv6 guard).
24. Port security, kontrola sztormów (storm control), ochrona przed atakami DoS, BPDU Guard, Root Guard, Loopback Guard.
25. Obsługa serwerów RADIUS oraz TACACS+; bezpieczny dostęp przez SSH oraz SSL/HTTPS.
26. Listy kontroli dostępu (ACL) min. 1000 reguł, w oparciu o adresy MAC/IPv4/IPv6, porty i znaczniki, w tym ACL czasowe.

**6. Jakość usług (QoS)**

27. Min. 8 sprzętowych kolejek na port; obsługa kolejkowania strict priority oraz WRR.
28. Klasyfikacja i oznaczanie ruchu na podstawie 802.1p, DSCP, ToS; ograniczanie pasma (rate limiting / policing).

**7. Zarządzanie**

29. Zarządzanie przez interfejs webowy (HTTP/HTTPS), pełne CLI oraz SNMP v1/v2c/v3.
30. Obsługa RMON, syslog, LLDP/LLDP-MED oraz protokołu wykrywania urządzeń sąsiednich.
31. Aktualizacja oprogramowania przez HTTP/HTTPS, TFTP oraz SCP; obsługa dwóch obrazów systemu (dual image) dla bezpiecznej aktualizacji.
32. Obsługa wdrożeń typu zero-touch / Plug and Play oraz scentralizowanego pulpitu zarządzania.

**8. Zasilanie, środowisko, normy i gwarancja**

33. Wbudowany zasilacz 100-240 V AC, 50/60 Hz.
34. Zakres temperatury pracy obejmujący co najmniej od -5°C do +50°C.
35. Zgodność ze standardami IEEE: 802.3, 802.3u, 802.3ab, 802.3z, 802.3ae, 802.3an, 802.3ad, 802.3af, 802.3at, 802.3az, 802.1D, 802.1Q/p, 802.1w, 802.1s, 802.1X, 802.1AB.
36. Certyfikaty bezpieczeństwa i kompatybilności elektromagnetycznej: CE, UL/CSA oraz FCC Part 15 (klasa A) lub równoważny.
37. Natywna gwarancja nadawana przez producenta.

**Akcesoria niezbędne do uruchomienia projektowanego systemu:**

**WKŁĄDKI ŚWIATŁOWODOWE (Wkładki optyczne 10 Gb/s) – 2 szt.**

1. Wraz z dostarczanymi przełącznikami Wykonawca dostarczy łna jeden switch 2 szt. wkładek SFP+ 10 Gb/s, fabrycznie nowych, w pełni kompatybilnych z oferowanym przełącznikiem i wspieranych przez jego producenta. Typ należy dobrać do oferowanego urządzenia; wymagana pełna interoperacyjność z portami SFP+ oferowanego przełącznika.

**PUNKT DOSTĘPOWY (Access Point sufitowy, Wi-Fi 6 / 802.11ax, PoE) – 1 szt.**

**1. Konstrukcja i interfejsy**

1. Punkt dostępowy w obudowie sufitowej (do dyskretnego montażu na suficie lub ścianie); komplet montażowy (uchwyt sufitowy, wspornik, zestaw mocujący) w zestawie.
2. Min. 2 porty Ethernet 1 Gb/s.
3. Wymiary obudowy okrągłej ok. 228 × 48 mm; fizyczny przycisk funkcyjny/reset.

**2. Parametry radiowe**

4. Zgodność ze standardem Wi-Fi 6 (IEEE 802.11ax), praca dwuzakresowa 2,4 GHz oraz 5 GHz jednocześnie (dwa niezależne moduły radiowe).
5. Obsługa standardów: w paśmie 2,4 GHz 802.11b/g/n/ax, w paśmie 5 GHz 802.11a/n/ac/ax.
6. Konfiguracja radiowa min. dwustrumieniowa (dual-chain, 2×2 MIMO).
7. Zysk anteny min. 5,5 dBi (anteny wewnętrzne).

**3. Wydajność i oprogramowanie**

8. Procesor min. 4-rdzeniowy o taktowaniu min. 1,8 GHz; pamięć RAM min. 1 GB; pamięć masowa min. 128 MB.
9. System operacyjny urządzenia z obsługą zaawansowanego firewalla, szyfrowania IPsec (z akceleracją sprzętową), tuneli VPN (np. IPsec / WireGuard) oraz routingu.
10. Możliwość scentralizowanego zarządzania wieloma punktami dostępowymi z jednego kontrolera (zarządzanie min. setkami urządzeń).

**4. Bezpieczeństwo sieci bezprzewodowej**

11. Obsługa metod uwierzytelniania WPA3-PSK, WPA3-EAP oraz OWE.
12. Obsługa szybkiego roamingu klientów zgodnie z IEEE 802.11r.

**5. Zasilanie i środowisko**

13. Zasilanie PoE-in zgodne z IEEE 802.3af/at oraz funkcja PoE-out (zasilanie kolejnych urządzeń, np. kamer IP lub kolejnego punktu dostępowego).

14. Obsługa zasilania w zakresie 18-57 V (PoE-in lub gniazdo DC); w zestawie zasilacz oraz zastrzykiwacz PoE (injector).
15. Zakres temperatury pracy obejmujący co najmniej od -40°C do +70°C.

## 5. Zasilanie awaryjne UPS – 2 szt.

| Opis wymagań techniczno-funkcjonalnych | Konfiguracja minimalna Zamawiającego |
|---|---|
| Technologia | VFI (true on-line, podwójne przetwarzanie energii) |
| Budowa | Rack 19'' 2U |
| Moc znamionowa | 3 kVA / 3 kW |
| Wyjściowy współczynnik mocy (PF) | 1 |
| Napięcie wejściowe | 230 Vac |
| Sposób zasilania | Plug&Play Gniazdo w standardzie IEC 320<br>W komplecie powinien znajdować się przewód zasilający. |
| Tolerancja napięcia wejściowego przy obciążeniu 100%; bez przechodzenia na baterie | 161 – 299 Vac |
| Regulowany zakres napięcia wejściowego zależnie od poziomu obciążenia UPS bez przechodzenia na baterie | 110 – 299 Vac |
| Częstotliwość wejściowa | 40-70 Hz |
| Sprawność AC-AC w trybie pracy on-line z obciążeniem 100% | nie mniejsza niż 92% |
| Sprawność AC-AC w trybie pracy Oszczędzania energii Eco Mode | nie mniejsza niż 99% |
| Tryb pracy z konwersją częstotliwości | Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie. |
| Napięcie wyjściowe | 230 Vac<br>W komplecie powinny znajdować się przynajmniej 2 przewody odbiorcze. |
| Częstotliwość wyjściowa | 50/60Hz (programowalna) z funkcją autosensing |
| Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass) | Statyczny przełącznik (SCR) z możliwością ręcznego przełączenia UPSa do trybu Bypass elektroniczny – wymuszanie opcji Bypass z poziomu panelu LCD |
| Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem | Wymagane |
| Regulowany charger wewnętrzny | Prąd ładowania 1-8A |
| Baterie zewnętrzne | Minimum 6 x 9Ah/12V |
| Baterie | Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 10-12 lat. |
| Stabilizacja napięcia wyjściowego w stanie ustalonym | ± 1% |

| | |
|---|---|
| Stabilizacja napięcia wyjściowego w stanie nieustalonym | ± 3% |
| Stabilność częstotliwości wyjściowej: | bez synchronizacji: ± 0,05 Hz |
| Współczynnik szczytu | 3:1 |
| Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD oraz sygnalizacją akustyczną | Wymagane ze wskazaniem parametrów napięcia wejściowego i wyjściowego, częstotliwości a także napięcia i pozostałej autonomii pracy z baterii podczas gdy UPS pracuje w trybie bateryjnym. |
| Złącze interfejsów | RS232, USB, programowane złącze REPO do zdalnego wyłącznika pożarowego NO lub NC. Port zabezpieczający transmisję danych TVSS, slot karty SNMP. |
| Gniazda wyjściowe IEC320 na zasilaczu UPS z możliwością zarządzania | Wymagane minimum gniazd – 2 grupy gniazd, w każdej przynajmniej 4 gniazda w standardzie IEC 320-C13. Możliwość programowania czasu obecności napięcia na gniazdach w pracy z baterii w zakresie 0-999 minut. |
| Karta sieciowa SNMP | Wymagana SNMP z protokołem IP v. 4 i 6, obsługą virmware oraz ModBus TCP. |
| Interfejs EPO (do wyłącznika ppoż.) | Wymagane – styk programowany NO lub NC |
| Diagnostyka parametrów urządzenia UPS i baterii | Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS |
| Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego | Wymagane. Oprogramowanie powinno jednocześnie współpracować z przełącznikiem ATS. |
| Poziom hałasu w odległości 1m, | < 48 dBA<br>Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury |
| Możliwość regulacji z poziomu LCD tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu | Wymagane |
| Zasilacz musi posiadać możliwość upgrade'u wersji oprogramowania sterującego pracą zasilacza. | Wymagane |
| Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE | Wymagane |
| Producent zasilacza UPS posiadający biuro dystrybucji i serwisu na terenie kraju. | Wymagane |
| Wymiary zasilacza UPS w szafie rack z bateriami | Maks 2U. Dopuszczalna głębokość UPS 63cm |
| Komplet szyn montażowych Rack | Wymagane |
| Instrukcja w języku polskim | Wymagane |
| Gwarancja | 24 miesiące |

## 6. NGFW z pełna licencją – 2 szt.

**Wymagania Ogólne**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.

Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 128 GB.
5. System jest wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1.3 Gbps.
6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps.

**Funkcje Systemu Bezpieczeństwa:**

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

**Polityki, Firewall**

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application-Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

**Połączenia VPN**

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.

- Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

**Routing i obsługa łączy WAN**

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

**Funkcje SD-WAN**

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

**Zarządzanie pasmem**

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

**Ochrona przed malware**

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

**Ochrona przed atakami**

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

**Kontrola WWW**

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

**Logowanie**

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

**Testy wydajnościowe oraz funkcjonalne**

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.

**Gwarancja oraz wsparcie**

System jest objęty serwisem gwarancyjnym producenta przez okres do 31.12.2026 r., polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.

Dodatkowo wymagana: subskrypcja chmurowej usługi zarządzania i analityki dla oferowanego urządzenia NGFW, zapewniająca centralne zarządzanie konfiguracją, monitorowanie oraz analizę ruchu i zdarzeń bezpieczeństwa wraz z raportowaniem, świadczona przez producenta urządzenia. Usługa musi obejmować przechowywanie logów (retencję) przez okres co najmniej 12 miesięcy, na okres ważności subskrypcji nie krótszy niż 12 miesięcy.

---

## 7. Oprogramowanie typu EDR – 1 kpl.

**Przedmiotem niniejszej pozycji jest rozbudowa oraz aktualizacja posiadanej przez Zamawiającego infrastruktury bezpieczeństwa IT opartej na rozwiązaniu ESET. Zamawiający aktualnie posiada aktywną licencję wymagającą rozszerzenia w celu dostosowania do rosnących potrzeb organizacji w zakresie ochrony stacji roboczych oraz centralnego zarządzania bezpieczeństwem. Oczekiwana licencja docelowa: ESET PROTECT ENTERPRISE – 25 szt.**

**Rozszerzenie licencji musi być w pełni kompatybilne z istniejącym środowiskiem oraz zapewniać zachowanie ciągłości działania systemu, w tym centralnego zarządzania w ramach platformy ESET. Zamawiający oczekuje, że dostarczone rozwiązanie będzie zgodne z wymaganiami producenta oraz zapewni wsparcie techniczne w wymaganym okresie obowiązywania licencji.**

**Poniżej przedstawiamy opis równoważności w razie oferowania rozwiązania innego niż ww.:**

### Centralne zarządzanie

1. Rozwiązanie musi udostępniać konsolę centralnego zarządzania w wersji lokalnej (on-prem) oraz w wersji chmurowej, hostowanej bezpośrednio przez producenta rozwiązania. (SaaS).
2. Rozwiązanie musi udostępniać konsolę centralnego zarządzania przynajmniej w języku polskim i angielskim.
3. Rozwiązanie musi udostępniać możliwość zmiany języka bez przeinstalowania ani ponownego uruchamiania usług centralnego zarządzania.
4. Rozwiązanie musi udostępniać konsolę centralnego zarządzania zabezpieczoną za pośrednictwem protokołu szyfrowanego SSL/TLS.
5. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft ENTRA ID.

6. Rozwiązanie musi udostępniać możliwość integracji użytkowników z Microsoft Active Directory.
7. Rozwiązanie musi udostępniać mechanizm wykrywający sklonowane maszyny na podstawie unikalnego identyfikatora sprzętowego stacji.
8. Rozwiązanie musi udostępniać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiająca co najmniej:
   - Pośredniczenie w komunikacji pomiędzy zarządzanym urządzeniem a serwerem centralnego zarządzania.
   - Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacji producenta.
   - Buforowanie ruchu HTTPS.
9. Rozwiązanie musi udostępniać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
10. Rozwiązanie musi udostępniać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli centralnego zarządzania.
11. Rozwiązanie musi udostępniać uwierzytelnianie dwuskładnikowe co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
    - Google Authenticator,
    - Microsoft Authenticator,
    - Authy,
    - Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
12. Rozwiązanie musi udostępniać minimum 80 szablonów raportów, przygotowanych przez producenta, które mogą być dowolnie modyfikowane przez administratora.
13. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
14. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej:
    - Adresy sieciowe IP.
    - Aktywne zagrożenia.
    - Stan funkcjonowania oraz ochrony.
    - Wersja systemu operacyjnego.
    - Podzespoły komputera.
15. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
    - Wyrażenie CRON.
    - Codziennie.
    - Cotygodniowo.
    - Co miesiąc.
    - Co rok.
    - Po wystąpieniu nowego zdarzenia.
    - Po automatycznym umieszczeniu hosta w grupie dynamicznej.
16. Rozwiązanie musi udostępniać możliwość tagowania obiektów.
17. Rozwiązanie musi udostępniać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
18. Rozwiązanie musi udostępniać eksport danych w co najmniej następujących formatach:
    - JSON.
    - LEEF.
    - CEF.

Ochrona stacji roboczych - Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi udostępniać możliwość instalacji co najmniej w języku polskim oraz angielskim.

3. Rozwiązanie musi udostępniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   - Wirus.
   - Trojan.
   - Robak.
   - Adware.
   - Spyware.
   - Dialer.
   - Phishing.
   - Backdoor.
4. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi udostępniać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
6. Rozwiązanie musi udostępniać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi udostępniać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.

- Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
- Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).
- Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.

8. Rozwiązanie musi udostępniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi udostępniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi udostępniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
    - Całego dysku.
    - Wybranych katalogów.
    - Pojedynczych plików.
    - Plików spakowanych oraz skompresowanych.
    - Dysków sieciowych.
    - Dysków przenośnych.
11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    - Wybranych plików.
    - Wybranych procesów.
    - Wybranych lokalizacji.
    - Wybranych rozszerzeń.
    - Nazwy wykrycia.
    - Sumy kontrolnej (SHA1).
12. Rozwiązanie musi udostępniać integrację z Intel Threat Detection Technology.
13. Rozwiązanie musi udostępniać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    - Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
    - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
    - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

14. Rozwiązanie musi udostępniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Rozwiązanie musi udostępniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. Rozwiązanie musi udostępniać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
17. Rozwiązanie musi udostępniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

A. Typ urządzenia:

- Pamięci masowe.
- Optyczne pamięci masowe.
- Pamięci masowe Firewire.
- Urządzenia do tworzenia obrazów.
- Drukarki USB.
- Urządzenia Bluetooth.
- Czytniki kart inteligentnych.
- Modemy.
- Porty LPT/COM.
- Urządzenia przenośne.

B. parametry urządzenia:

- Numer seryjny.
- Producent.
- Model.

C. typ dostępu:

- Brak możliwości zapisu.
- Pełen dostęp.
- Ostrzeżenie użytkownika.
- Brak dostępu.

18. Rozwiązanie musi udostępniać moduł HIPS, który musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
    A. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
    B. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy

dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

C. Raport musi posiadać co najmniej:
   - Listę zainstalowanych aplikacji.
   - Listę usług systemowych.
   - Informacje o systemie operacyjnym i sprzęcie.
   - Listę aktywnych procesów i połączeń sieciowych.
   - Harmonogram systemu operacyjnego.
   - Szczegóły pliku hosts.
   - Informacje o sterownikach.

20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
- Antywirus.
- Zapora osobista.
- Sandbox.
- Antyspyware.
- Metody heurystyczne.

21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
    A. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
    B. Ochrona musi być realizowana w oparciu o co najmniej:
       - globalna czarna lista RBL,
       - czarna lista użytkownika,
       - biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
    A. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
       - Skanowanie portów TCP oraz UDP,
       - Wykrywanie duplikacji adresu IP,
       - Atak zatruwania ARP,
       - Nieprawidłowa długość pakietu TCP oraz UDP.
    B. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
       - RDP,
       - SMB,
       - My SQL,
       - MS SQL.
    C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
    A. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
    B. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
       - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

- tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

- tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.
    - Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
    - Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
    - W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.
    A. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
    B. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej:
        - Treść komunikatu.
        - Obraz.

### Ochrona stacji roboczych – MacOS

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
    - Wirus.
    - Trojan.
    - Robak.
    - Adware.
    - Spyware.
    - Dialer.
    - Phishing.
    - Backdoor.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość
   wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi chronić pliki co najmniej za pomocą:
    - Sygnatur wirusów.
    - Reputacji chmurowej.
7. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
    - Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.
    - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.

- Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.

9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   - całego dysku,
   - wybranych katalogów,
   - pojedynczych plików,
   - plików spakowanych oraz skompresowanych,
   - Dysków sieciowych,
   - dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    - wybranych plików,
    - wybranych procesów,
    - wybranych lokalizacji,
    - wybranych rozszerzeń,
    - nazwy wykrycia,
    - sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
    A. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.
    B. Zapora osobista musi posiadać co najmniej dwa tryby pracy:
       - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
       - tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

### Ochrona stacji roboczych – Linux

1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:
   - Ubuntu Desktop,
   - Red Hat Enterprise Linux
   - Linux Mint.

2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:
   - Cinnamon.
   - GNOME.
   - KDE.
   - MATE.
   - XFCE.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   - Wirus.
   - Trojan.
   - Robak.
   - Adware.
   - Spyware.
   - Dialer.
   - Phishing.
   - Backdoor.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący

pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość

wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   - Całego dysku.
   - Wybranych katalogów.
   - Pojedynczych plików.
   - Plików spakowanych oraz skompresowanych.
   - Dysków sieciowych.
   - Dysków przenośnych.
8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   - Wybranych plików.
   - Wybranych procesów.
   - Wybranych lokalizacji.
   - Wybranych rozszerzeń.
9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
   A. typ urządzenia:
      - pamięci masowe,
      - optyczne pamięci masowe,

   B. parametry urządzenia:
      - numer seryjny,
      - producent,
      - model.

   C. typ dostępu:
      - brak możliwości zapisu,
      - pełen dostęp,
      - brak dostępu.

Ochrona serwera – Windows Server

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
   - Microsoft Windows Server 2012 R2,
   - Microsoft Windows Server 2016,
   - Microsoft Windows Server 2019,
   - Microsoft Windows Server 2022,
   - Microsoft Windows Server 2025.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
   - Wirus.
   - Trojan.
   - Robak.

- Adware.
- Spyware.
- Dialer.
- Phishing.
- Backdoor.

4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   - Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
   - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   - całego dysku,
   - wybranych katalogów,
   - pojedynczych plików,
   - plików spakowanych oraz skompresowanych,
   - dysków sieciowych,
   - dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
    - wybranych plików,
    - wybranych procesów,
    - wybranych lokalizacji,
    - wybranych rozszerzeń,
    - nazwy wykrycia,
    - sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
    A. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania

wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

B. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

C. Raport musi posiadać co najmniej:
   - Listę zainstalowanych aplikacji,
   - Listę usług systemowych,
   - informacje o systemie operacyjnym i sprzęcie,
   - Listę aktywnych procesów i połączeń sieciowych,
   - harmonogram systemu operacyjnego,
   - Szczegóły pliku hosts,
   - Informacje o sterowników.

14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
   - antywirus,
   - zapora osobista
   - sandbox,
   - antyspyware,
   - metody heurystyczne.
15. Rozwiązanie musi skanować system wirtualny w trybie online oraz ofline w środowisku Hyper-V.
16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
   A. typ urządzenia:
      - Pamięci masowe.
      - Optyczne pamięci masowe.
      - Pamięci masowe Firewire.
      - Urządzenia do tworzenia obrazów.
      - Drukarki USB.
      - Urządzenia Bluetooth.
      - Czytniki kart inteligentnych.
      - Modemy.
      - Porty LPT/COM.
      - Urządzenia przenośne.
   B. parametry urządzenia:
      - Numer seryjny,
      - Producent,
      - Model.
   C. typ dostępu:
      - Brak możliwości zapisu,
      - Pełen dostęp,
      - Ostrzeżenie użytkownika,
      - Brak dostępu.
18. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:

- MS SQL.
- Active Directory.
- IIS.
- Sysvol.
- DNS.
- DHCP.
- Hyper-V.
- Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.

19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
    A. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
        - Skanowanie portów TCP oraz UDP,
        - Wykrywanie duplikacji adresu IP,
        - Atak zatruwania ARP,
        - Nieprawidłowa długość pakietu TCP oraz UDP.
    B. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
        - RDP,
        - SMB,
        - My SQL,
        - MS SQL.
    C. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
21. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
    A. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
        - tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
        - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
        - tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
        - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

### Ochrona serwera – Linux

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
    - RedHat Enterprise Linux (RHEL),
    - Rocky Linux,
    - Ubuntu,
    - Debian,
    - SUSE Linux Enterprise Server (SLES),
    - Oracle Linux,
    - Amazon Linux.
2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
    - Wirus.
    - Trojan.
    - Robak.

2.1. Adware.
2.2. Spyware.
2.3. Dialer.
2.4. Phishing.
2.5. Backdoor.

3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
4. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
   - Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
   - Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
   - całego dysku,
   - wybranych katalogów,
   - pojedynczych plików,
   - plików spakowanych oraz skompresowanych,
   - dysków sieciowych,
   - dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
   - wybranych plików,
   - wybranych procesów,
   - wybranych lokalizacji,
   - wybranych rozszerzeń,
10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
    - Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
12. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:
    - proces budowania obrazu kontenera,
    - wdrażanie obrazu kontenera.

Mobile Device Management

1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
   A. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:
      - Android,

- iOS,
- iPadOS.

B. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
- Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),
- Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
- VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
- Apple Business Manager (ABM),
- Android Enterprise (co najmniej w zakresie Device Owner).

3. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
- usunięcie zawartości urządzenia,
- przywrócenie urządzenia do ustawień fabrycznych,
- zablokowanie urządzenia,
- uruchomienie sygnału dźwiękowego,
- lokalizację GPS,
- Resetowanie hasła blokady ekranu.

4. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
5. MDM musi umożliwiać co najmniej:

A. Dla systemów iOS oraz iPadOS
- konfigurację kont e-mail,
- konfigurację połączeń VPN,
- Konfigurację połączeń Wi-Fi,
- Konfigurację listy certyfikatów,
- możliwość uruchomienia trybu jednej aplikacji.

B. Dla systemu Android:
- blokadę wykonywania połączeń,
- blokadę konfiguracji sieci Wi-Fi,
- blokadę konfiguracji tuneli VPN,
- zarządzenie aktualizacjami sytemu operacyjnego,
- blokadę zmiany tapety urządzenia.

### Mobile Threat Defense (MTD) dla systemu Android

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
- Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
- Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.

3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:

A. Złożoność kodu blokady ekranu:
- Wzór.
- PIN.
- Hasło.

B. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,

C. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.

5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   - nazwę aplikacji,
   - nazwę pakietu,
   - kategorię sklepu Google Play,
   - uprawnienia aplikacji,
   - pochodzenie aplikacji z nieznanego źródła.
6. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

Sandbox w chmurze

1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi wspierać systemy w tym co najmniej:
   - Microsoft Windows 10 oraz 11,
   - Microsoft Windows Server,
   - macOS 11 (Big Sur) oraz nowszych
   - RedHat Enterprise Linux (RHEL),
   - Rocky Linux,
   - Ubuntu,
   - Debian,
   - SUSE Linux Enterprise Server (SLES),
   - Oracle Linux,
   - Amazon Linux.
4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
5. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
6. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
   - archiwa,
   - skrypty,
   - pliki wykonywalne,
   - pliki rejestru systemowego (.reg),
   - możliwy spam,
   - dokumenty.
7. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
   - natychmiast po ich przeanalizowaniu,
   - po upływie 30 dni,
   - nigdy.
8. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
10. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
11. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
12. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego

produktu.

- Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.

13. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
    - czysty,
    - podejrzany,
    - bardzo podejrzany,
    - szkodliwy.
14. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:
    A. wstrzymania uruchamiania pobieranych plików z następujących źródeł:
        - przeglądarki internetowe,
        - programy poczty e-mail,
        - nośniki wymienne,
        - pliki wyodrębnione z archiwum.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzenia oraz z poziomu klienta antywirusowego.

### Szyfrowanie

1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
3. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
4. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
5. Rozwiązanie musi posiadać autentykacje typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
    - Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
    - Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
    - Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
    - Hasło odzyskiwania nie może być krótsze niż 8 znaków.
    - Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
10. Rozwiązanie musi wspierać dyski wykorzystującego funkcji OPAL w wersji co najmniej 2.0.
11. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.
12. Rozwiązanie musi umożliwiać automatyczne wstrzymanie uwierzytelnienia w przypadku aktualizacji systemu operacyjnego.

### Endpoint Detection and Response / eXtended Detection and Response

1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:
    - Tworzenie procesów.

- Uruchamianie, zatrzymanie i modyfikacja usług.
- Utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym.
- Usuwanie oraz zmiana nazw plików.
- Tworzenie i usuwanie kluczy rejestru systemowego.
- Ładowanie bibliotek DLL.
- Zalogowanie użytkowników.

A. elementy sieciowe, w tym co najmniej:

- Pobranie plików wykonywalnych.
- Zestawienie połączeń TCP/IP.
- Zapytania http.
- Zapytania DNS.

4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.
   A. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:
      - Blokowanie pliku wykonywalnego.
      - Blokowanie pliku wykonywalnego i poddanie go kwarantannie.
      - Blokowanie podejrzanej biblioteki DLL.
      - Zakończenie procesu.
      - Skanowanie komputera w poszukiwaniu zagrożeń.
      - Wyłączenie komputera.
      - Izolacja sieciowa hosta dla systemów Windows oraz Linux.
      - Wylogowanie użytkownika.
   B. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.
5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
   A. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.
   B. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:
      - Proces.
      - Proces nadrzędny (proces rodzica).
      - Nazwę procesu.
      - Ścieżkę procesu.
      - Wiersz polecenia.
      - Wydawcę.
      - Typ podpisu cyfrowego.
      - SHA-1.
      - SHA-2.
      - Użytkownika.
   C. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.
6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.
   A. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
   B. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):
      - SHA-1.

- SHA-256.

7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:
   - Hash pliku SHA-1.
   - Hash pliku SHA-256.
   - Hash pliku MD5.
   - Typ sygnatury podpisu cyfrowego.
   - Wydawcę certyfikatu.
   - Wersję pliku.
   - Oryginalną nazwę pliku.
   - Rozmiar pliku.
   - Reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego.
   - Pierwsze uruchomienie pliku w środowisku.
   - Ostatnie uruchomienie pliku w środowisku.
8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
   - Oznaczania ich jako bezpieczne lub niebezpieczne.
   - Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
   - Zablokowania wykonywania i wykorzystania pliku.
   - Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
   - Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
   - Pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
   - Wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.Administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
   - Administrator musi posiadać możliwość odczytania informacji o języku skryptu.
10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.
    - Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.
11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.
12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.
13. Rozwiązanie musi umożliwiać moduł zaawansowanego wyszukiwania, które umożliwia badanie wskaźników danych zawartych w XDR, przynajmniej w oparciu o:
    - Wyszukiwanie dowolnego tekstu.
    - Wyszukiwanie, pozwalające łączyć ze sobą różne słowa, oddalone od siebie nie więcej niż 3 innymi słowami.
    - Wyszukiwanie po nazwie procesów.
    - Wyszukiwanie po ocenie ryzyka.
    - Filtrowanie według daty.

Ochrona serwerów w chmurze AWS, Microsoft Azure i Google Cloud Platform

1. Rozwiązanie musi być dostępne z tej samej konsoli chmurowej co rozwiązanie antywirusowe.
2. Rozwiązanie musi udostępniać możliwość integracji przynajmniej z rozwiązaniami:
   - Microsoft Azure.
   - Google Cloud Platform.
   - Amazon Web Services.

3. Rozwiązanie powinno zapewniać możliwość zarówno automatycznego uruchamiania ochrony dla nowych i już istniejących maszyn wirtualnych, jak i ręcznego wskazania wybranych zasobów do objęcia ochroną.

Wsparcie techniczne.

1. Rozwiązanie musi udostępniać wsparcie techniczne w języku polskim przez cały okres trwania licencji.

---

## 8. SZAFA RACK – 2 szt.

| Parametr | Wymaganie minimalne |
|---|---|
| **Typ i przeznaczenie** | Szafa serwerowa/sieciowa stojąca (wolnostojąca) w standardzie 19", przeznaczona do montażu serwerów, zasilaczy UPS oraz osprzętu sieciowego. |
| **Wysokość użytkowa** | Min. 42U. |
| **Wymiary zewnętrzne** | Szerokość 800 mm, głębokość 1000 mm, wysokość maks. ok. 2100 mm. |
| **Nośność** | Nośność statyczna min. 800 kg; udźwig pionowych szyn nośnych 19" min. 1200 kg. |
| **Szyny montażowe 19"** | Cztery szyny profilowe 19" (483 mm) montowane z przodu i z tyłu, bezstopniowo regulowane na głębokość, ocynkowane i numerowane (oznaczenia U), usztywnione rozpórkami. Zakres regulacji głębokości montażu komponentów obejmujący co najmniej 688-943 mm. |
| **Drzwi przednie** | Drzwi przednie zamykane na zamek, blokada min. 1-punktowa (dopuszczalne wspomaganie ryglowania góra/dół). Dopuszczalne wykonanie: szyba ze szkła bezpiecznego (certyfikowanego) w ramie stalowej albo stalowe perforowane. |
| **Drzwi tylne** | Drzwi tylne stalowe, zamykane na zamek, blokada min. 1-punktowa. Dopuszczalne wykonanie dwuczęściowe. |
| **Ściany boczne** | Zdejmowane panele/ściany boczne w komplecie, zamykane na zamek (zamek skrzydłowy oraz zatrzask). |
| **Zabezpieczenie dostępu** | Drzwi przednie, drzwi tylne oraz panele boczne wyposażone w zamki. Z uwagi na lokalizację ogólnodostępną wymagana możliwość zamknięcia wszystkich osłon (przód, tył, boki) na klucz. |

| Parametr | Wymaganie minimalne |
|---|---|
| **Stopień ochrony IP** | Min. IP20. |
| **Odporność na uderzenia** | Min. IK07. |
| **Konstrukcja** | Konstrukcja modułowa z blachy stalowej malowanej proszkowo; otwierana/zdejmowana obudowa bazowa ze zdejmowanymi panelami zaślepiającymi 19". |
| **Wprowadzenia kablowe** | Przepusty kablowe w podstawie (od dołu/tyłu i boku) oraz w dachu, umożliwiające doprowadzenie okablowania od góry i od dołu. |
| **Wentylacja** | Dach przygotowany do montażu wentylatorów, ze zdejmowaną pokrywą. |
| **Organizacja okablowania** | Pionowe kanały kablowe (organizery) z panelem maskującym. |
| **Uziemienie** | Punkty uziemienia w obudowie oraz na zdejmowanych drzwiach i ścianach bocznych. |
| **Poziomowanie / stabilność** | Min. 4 nóżki poziomujące w zestawie (gwint min. M10). |
| **Kolor** | Szary lub czarny (RAL do uzgodnienia z Zamawiającym). |
| **Dostawa i montaż** | Dostawa w stanie zmontowanym, gotowym do użycia; konstrukcja umożliwiająca pełny demontaż w razie potrzeby. |

# 9. Usługa SOC

**Usługa monitorowania bezpieczeństwa (SOC) w trybie 24/7 — monitorowanie, analiza i informowanie**

Niniejszy opis określa wymagania dla usługi nadzoru nad bezpieczeństwem infrastruktury IT Zamawiającego, ograniczonej do monitorowania, analizy oraz informowania o zdarzeniach i incydentach bezpieczeństwa (charakter zewnętrznego stróża). Usługa nie obejmuje aktywnego reagowania ani ingerencji w infrastrukturę Zamawiającego.

*Usługa jest realizowana zdalnie, w oparciu o narzędzia będące w posiadaniu Zamawiającego (SIEM oraz XDR/EDR), z minimalnym, koniecznym wkładem rozwiązań własnych Wykonawcy. Wymagania mają charakter obligatoryjny, a wskazane wartości liczbowe stanowią minimum lub propozycję do decyzji Zamawiającego.*

**1. Przedmiot i charakter usługi**

1. Przedmiotem zamówienia jest świadczenie zdalnej usługi monitorowania bezpieczeństwa teleinformatycznego (Security Operations Center, dalej: SOC) dla infrastruktury IT Zamawiającego, obejmującej ciągłe monitorowanie, wykrywanie, korelację, analizę oraz informowanie o zdarzeniach i incydentach bezpieczeństwa.
2. Usługa ma charakter nadzorczo-informacyjny. Wykonawca nie wykonuje żadnych aktywnych działań ani zmian w infrastrukturze Zamawiającego — w szczególności nie dokonuje rekonfiguracji urządzeń, blokowania ruchu sieciowego, izolacji hostów, usuwania plików ani innych ingerencji. Reagowanie i działania naprawcze realizuje Zamawiający, a Wykonawca dostarcza ostrzeżenia, analizę oraz rekomendacje.
3. Celem usługi jest zwiększenie wykrywalności zagrożeń, skrócenie czasu wykrycia incydentu oraz zapewnienie Zamawiającemu rzetelnej i terminowej informacji umożliwiającej podjęcie własnych działań.
4. Usługa świadczona jest dla zakładu wodociągowego, z uwzględnieniem wymogów właściwych dla podmiotu świadczącego usługę kluczową (krajowy system cyberbezpieczeństwa / NIS2).

**2. Definicje i pojęcia**

1. Zdarzenie bezpieczeństwa — pojedyncza, zaobserwowana sytuacja w systemie lub sieci, mogąca mieć znaczenie dla bezpieczeństwa informacji.
2. Alert — zdarzenie lub korelacja zdarzeń spełniające regułę detekcji i wymagające weryfikacji przez analityka.
3. Incydent — zdarzenie lub seria zdarzeń naruszających albo zagrażających bezpieczeństwu informacji, wymagające obsługi i poinformowania Zamawiającego.
4. Wynik fałszywie dodatni (false positive) — alert błędnie wskazujący na incydent.
5. Scenariusz detekcji (use case) — reguła lub zestaw reguł wykrywających określoną technikę lub wzorzec ataku.
6. Informacja o zagrożeniach (threat intelligence) — zewnętrzne i wewnętrzne dane o zagrożeniach wykorzystywane do podnoszenia skuteczności wykrywania.
7. Czas wykrycia oraz czas powiadomienia — mierniki poziomu usług (SLA) zdefiniowane w rozdziale 7.

**3. Tryb i dostępność usługi**

1. Monitorowanie zdarzeń bezpieczeństwa oraz powiadamianie w trybie 24/7/365 (całodobowo, przez wszystkie dni w roku), bez przerw w monitorowaniu.
2. Całodobowy, jednolity punkt kontaktu (Service Desk / SPOC) do przyjmowania i przekazywania informacji o incydentach oraz przyjmowania zgłoszeń od Zamawiającego.
3. Gwarantowana dostępność usługi monitorowania min. 99% w miesięcznym okresie.
4. Obsługa, powiadomienia, raporty oraz komunikacja z Zamawiającym prowadzone w języku polskim.
5. Zapewnienie ciągłości obsady analityków (praca zmianowa) oraz zastępowalności personelu, gwarantujące nieprzerwane świadczenie usługi.

**4. Zakres monitorowanych źródeł (infrastruktura IT)**

1. Monitorowaniem objęte są źródła infrastruktury IT Zamawiającego, w szczególności: serwery (Windows/Linux), usługi katalogowe (Active Directory), zapory sieciowe / NGFW, urządzenia sieciowe (przełączniki, punkty dostępowe), systemy bezpieczeństwa oraz dane z systemu XDR/EDR i pozostałych źródeł zintegrowanych w systemie SIEM Zamawiającego.
2. Na etapie wdrożenia Wykonawca przeprowadzi inwentaryzację dostępnych źródeł logów i telemetrii oraz uzgodni z Zamawiającym ostateczną listę źródeł objętych monitoringiem.
3. Usługa zapewnia możliwość dołączania nowych źródeł logów w trakcie trwania umowy, w ramach uzgodnionego zakresu, bez konieczności zmiany modelu usługi.
4. Usługa nie obejmuje środowiska OT/SCADA, o ile Zamawiający nie rozszerzy zakresu odrębnym uzgodnieniem.

**5. Narzędzia realizacji usługi oraz wykorzystanie systemów własnych Wykonawcy**

1. Usługa jest realizowana w oparciu o narzędzia będące w posiadaniu Zamawiającego (system klasy SIEM oraz XDR/EDR). Wykonawca wykorzystuje rozwiązania własne wyłącznie w minimalnym, koniecznym zakresie (np. konektory, bezpieczny dostęp zdalny, pulpit/raportowanie), bez konieczności zakupu przez Zamawiającego dodatkowych licencji platformowych.
2. Wykonawca może wykorzystać do realizacji usługi własne systemy lub narzędzia monitorowania, analizy bądź zbierania danych wyłącznie po uprzednim uzyskaniu pisemnej zgody Zamawiającego, na warunkach przez niego zaakceptowanych. Uruchomienie lub instalacja takiego narzędzia bez zgody Zamawiającego stanowi nienależyte wykonanie umowy.
3. Wniosek Wykonawcy o zgodę na użycie systemu własnego musi wskazywać co najmniej: nazwę i funkcję narzędzia, zakres oraz rodzaj przetwarzanych danych, lokalizację przetwarzania i przechowywania danych (wymagany obszar Europejskiego Obszaru Gospodarczego), sposób zabezpieczenia danych, model i zakres dostępu oraz wpływ narzędzia na systemy i sieć Zamawiającego.
4. Wykorzystanie systemów własnych Wykonawcy nie może powodować dodatkowych kosztów licencyjnych po stronie Zamawiającego, ograniczać jego praw do danych ani prowadzić do uzależnienia od jednego dostawcy (vendor lock-in). Dane i logi Zamawiającego pozostają jego wyłączną własnością.
5. Zamawiający może w każdym czasie cofnąć zgodę na wykorzystanie danego narzędzia własnego Wykonawcy; w takim przypadku Wykonawca niezwłocznie zaprzestanie jego używania i zaproponuje rozwiązanie zastempcze w ramach umowy.
6. Po zakończeniu umowy Wykonawca usunie własne narzędzia z infrastruktury Zamawiającego, wycofa wszystkie udzielone dostępy, przekaże Zamawiającemu zgromadzone dane oraz trwale usunie je ze swoich systemów, potwierdzając ten fakt pisemnie.

**6. Wykrywanie i analiza**

1. Bieżąca korelacja i analiza zdarzeń w oparciu o reguły i scenariusze detekcji (use case) w systemie SIEM Zamawiającego oraz alerty z systemu XDR/EDR.
2. Mapowanie wykrywanych technik ataku na uznaną, publiczną bazę wiedzy o taktykach i technikach przeciwnika (np. MITRE ATT&CK).
3. Triage alertów: weryfikacja, eliminacja wyników fałszywie dodatnich oraz wstępna klasyfikacja zdarzeń jako incydentów wraz z określeniem ich krytyczności.
4. Bieżące tworzenie, rozwój i dostrajanie reguł detekcji (tuning) wraz z prowadzeniem ich dokumentacji oraz okresowym przeglądem skuteczności.
5. Wykorzystanie informacji o zagrożeniach (threat intelligence) w celu wzbogacania i podnoszenia skuteczności detekcji.
6. Analiza prowadzona przez wykwalifikowanych analityków bezpieczeństwa (poziomy L1/L2), z możliwością zaangażowania kompetencji L3 w przypadku incydentów złożonych.
7. Cykliczne, proaktywne poszukiwanie zagrożeń (threat hunting) w danych zgromadzonych w SIEM, w zakresie i częstotliwości uzgodnionych z Zamawiającym.

**7. Klasyfikacja incydentów i poziomy usług (SLA)**

1. Wykonawca klasyfikuje incydenty według krytyczności co najmniej w kategoriach: krytyczny, wysoki, średni, niski, stosując jednolitą i uzgodnioną z Zamawiającym metodykę oceny.
2. Czas powiadomienia Zamawiającego liczony od momentu potwierdzenia incydentu: incydent krytyczny do 1 godziny, wysoki do 2 godzin, średni do 4 godzin, niski — w najbliższym raporcie okresowym.

3. Wykonawca prowadzi pomiar realizacji wskaźników SLA i raportuje ich dotrzymanie w raportach okresowych; szczegółowe zasady rozliczania poziomów usług oraz ewentualne kary umowne określa umowa.
4. Powiadamianie odbywa się wieloma kanałami (telefon oraz e-mail/portal zgłoszeniowy), zgodnie z uzgodnioną listą kontaktów i procedurą eskalacji.

**8. Informowanie, rekomendacje i obsługa zgłoszeń**

1. Dla każdego incydentu Wykonawca przekazuje co najmniej: opis zdarzenia, wstępną ocenę wpływu i krytyczności oraz rekomendowane działania zaradcze do samodzielnego wykonania przez Zamawiającego.
2. Wszystkie zdarzenia, alerty, incydenty i zgłoszenia są rejestrowane w systemie ewidencji zgłoszeń (ticketowym), z zachowaniem historii obsługi i możliwością bieżącego wglądu przez Zamawiającego.
3. Wykonawca przyjmuje i rejestruje zgłoszenia kierowane przez Zamawiającego (np. obserwacje, podejrzane zdarzenia) oraz informuje o wynikach ich weryfikacji.
4. Wykonawca zapewnia wsparcie konsultacyjne (zdalne/telefoniczne) przy analizie incydentu i interpretacji rekomendacji, bez ingerencji w systemy Zamawiającego.

**9. Eskalacja i komunikacja**

1. Wykonawca opracuje i uzgodni z Zamawiającym macierz eskalacji oraz listę osób kontaktowych po obu stronach, wraz z trybem kontaktu poza godzinami pracy.
2. Komunikacja prowadzona uzgodnionymi kanałami (telefon, poczta elektroniczna, portal/system zgłoszeniowy), w języku polskim.
3. Wykonawca zapewnia okresowe spotkania statusowe oraz kontakt operacyjny w sprawach bieżących.

**10. Raportowanie i przeglądy**

1. Raporty miesięczne obejmujące co najmniej: statystyki zdarzeń, alertów i incydentów, opis incydentów istotnych, najważniejsze zagrożenia, dotrzymanie wskaźników SLA, trendy oraz rekomendacje.
2. Raport indywidualny po każdym incydencie o krytyczności wysokiej i krytycznej, zawierający przebieg zdarzenia, ustalenia analizy i rekomendacje.
3. Cykliczne przeglądy stanu bezpieczeństwa z Zamawiającym (co najmniej kwartalne), obejmujące ocenę skuteczności detekcji i propozycje usprawnień.
4. Bieżący dostęp Zamawiającego do statusu usługi oraz pulpitu prezentującego kluczowe informacje, a także możliwość uzyskania raportów doraźnych (ad-hoc) na żądanie.

**11. Wdrożenie, integracja i okres przejściowy**

1. Uruchomienie usługi obejmuje: inwentaryzację źródeł, integrację z posiadanym przez Zamawiającego systemem SIEM oraz XDR/EDR, konfigurację i dostrojenie reguł detekcji oraz uzgodniony okres dostrajania (tuning).
2. Wykonawca opracuje plan wdrożenia i uzgodni je z Zamawiającym przed rozpoczęciem świadczenia usługi.
3. Wykonawca minimalizuje wkład rozwiązań własnych, dostarczając wyłącznie elementy niezbędne do integracji i bezpiecznego dostępu, z poszanowaniem zasad z rozdziału 5.

**12. Wymagania wobec zespołu i kompetencji**

1. Usługę realizuje zespół analityków bezpieczeństwa posiadających udokumentowane doświadczenie w monitorowaniu i analizie incydentów; mile widziane uznane certyfikaty branżowe.
2. Wykonawca zapewnia obsadę w trybie zmianowym gwarantującą ciągłość usługi 24/7 oraz zastępowalność personelu kluczowego.
3. Personel realizujący usługę porozumiewa się z Zamawiającym w języku polskim.

**13. Bezpieczeństwo informacji, poufność i ochrona danych**

1. Usługa realizowana jest na danych i logach Zamawiającego; Wykonawca zapewnia ich poufność na podstawie umowy o zachowaniu poufności oraz, jeżeli dotyczy, umowy powierzenia przetwarzania danych osobowych.

2. Dostęp zdalny Wykonawcy zabezpieczony jest co najmniej uwierzytelnianiem wieloskładnikowym (MFA) oraz szyfrowanym połączeniem, z zachowaniem zasady minimalnych niezbędnych uprawnień i z rejestrowaniem dostępu.
3. Dane i logi Zamawiającego są przetwarzane i przechowywane wyłącznie na obszarze Europejskiego Obszaru Gospodarczego.
4. Wykonawca działa zgodnie z politykami bezpieczeństwa Zamawiającego oraz uzgodnionymi zasadami retencji danych i logów.

**14. Zgodność z krajowym systemem cyberbezpieczeństwa / NIS2**

1. Wykonawca wspiera Zamawiającego w realizacji obowiązków wynikających z krajowego systemu cyberbezpieczeństwa / NIS2, w tym przygotowuje informacje i analizy niezbędne do zgłoszenia incydentu poważnego.
2. Zgłoszenie incydentu poważnego do właściwego zespołu CSIRT pozostaje obowiązkiem Zamawiającego jako podmiotu świadczącego usługę kluczową; Wykonawca zapewnia współpracę i dane na potrzeby tego zgłoszenia w wymaganych terminach.
3. Wykonawca wspiera Zamawiającego w obsłudze incydentu od strony analitycznej, bez przejmowania działań naprawczych w infrastrukturze Zamawiającego.

**15. Konsultacyjne wsparcie bezpieczeństwa (helpdesk cyberbezpieczeństwa).**

W ramach usługi Wykonawca zapewnia bieżące wsparcie konsultacyjne (helpdesk) w zakresie cyberbezpieczeństwa, dostępne w dni robocze w godzinach pracy Zamawiającego, realizowane zdalnie (telefonicznie, pocztą elektroniczną oraz przez system zgłoszeniowy) w języku polskim, obejmujące w szczególności:

a) doradztwo i odpowiedzi na bieżące pytania dotyczące bezpieczeństwa teleinformatycznego, w tym oceny ryzyka, dobrych praktyk konfiguracyjnych, uwierzytelniania, bezpieczeństwa poczty i pracy zdalnej oraz reagowania na podejrzane sytuacje (np. wiadomości phishingowe);

b) doradztwo w zakresie zgodności z wymaganiami regulacyjnymi mającymi zastosowanie do Zamawiającego (m.in. krajowy system cyberbezpieczeństwa / NIS2, ochrona danych osobowych, wewnętrzne polityki bezpieczeństwa), w tym pomoc w interpretacji wymagań oraz wskazywanie luk i rekomendowanych działań dostosowawczych;

c) konsultacje rozwojowe dotyczące podnoszenia poziomu bezpieczeństwa, w tym opiniowanie planowanych zmian w infrastrukturze IT, rekomendowanie usprawnień i kierunków rozwoju zabezpieczeń oraz wsparcie w priorytetyzacji działań naprawczych;

d) pomoc merytoryczną (doradczą i analityczną) przy reagowaniu na incydenty oraz przy przygotowaniu informacji niezbędnych do realizacji obowiązków sprawozdawczych, z zachowaniem zasady, że Wykonawca nie wykonuje aktywnych działań ani zmian w infrastrukturze Zamawiającego;

Zgłoszenia w ramach helpdesku są rejestrowane i obsługiwane w systemie ewidencji zgłoszeń, z uzgodnionym czasem reakcji na zapytania (max. 48h)

**16. Okres świadczenia usługi**

1. Usługa świadczona jest od dnia jej uruchomienia (po zakończeniu wdrożenia i akceptacji przez Zamawiającego) do dnia 31.12.2026 r. z możliwością przedłużenia usługi po 31.12.2026 r. bez dublowania kosztów wdrożenia. Docelowo usługa musi być zaprojektowana na wieloletnie świadczenie u Zamawiającego.

# 10. Kompleksowy system IDS dla OT wraz monitorowaniem i zarządzaniem infrastrukturą.

**1. Wymagania platformowe i licencyjne**

1.1. Oprogramowanie musi być licencjonowane w modelu nieograniczającym liczby obsługiwanych zmiennych (tagów), monitorowanych zasobów oraz podłączonych urządzeń. Niedopuszczalny jest model licencyjny rozliczany za liczbę zmiennych, punktów wejścia/wyjścia lub liczbę podłączonych urządzeń.

1.2. Oprogramowanie musi umożliwiać rejestrację danych historycznych bez ograniczeń licencyjnych co do liczby rejestrowanych zmiennych. Jedynym ograniczeniem wolumenu i okresu przechowywania danych może być dostępna przestrzeń dyskowa infrastruktury Zamawiającego.

1.3. Oprogramowanie musi umożliwiać jednoczesną pracę co najmniej 5 użytkowników (sesji klienckich). Dostęp do aplikacji musi być realizowany zarówno:

1.3.1. przez przeglądarkę internetową zgodną ze standardem HTML5,

1.3.2. przez dedykowaną (natywną) aplikację kliencką dostępną dla komputerów z systemem Windows i Linux oraz dla urządzeń mobilnych z systemem Android.

1.4. Oprogramowanie musi być instalowane i eksploatowane w całości w infrastrukturze teleinformatycznej Zamawiającego. Niedopuszczalne jest rozwiązanie wymagające do działania chmury dostawcy lub przetwarzania danych poza infrastrukturą Zamawiającego.

1.5. Oprogramowanie musi być dostarczone na podstawie licencji wieczystej (bezterminowej). Działanie oprogramowania nie może być uzależnione od wnoszenia obowiązkowych, cyklicznych opłat subskrypcyjnych; ewentualne wsparcie i aktualizacje mogą być świadczone w ramach odrębnej, dobrowolnej usługi.

1.6. Oprogramowanie musi zapewniać bezpośrednią komunikację ze sterownikami w sieci OT zainstalowanymi na ujęciach wody Zamawiającego z wykorzystaniem wbudowanego, natywnego sterownika protokołu komunikacyjnego. Niedopuszczalne jest pośredniczenie zewnętrznego serwera OPC innego producenta.

1.7. Oprogramowanie musi stanowić otwartą platformę umożliwiającą Zamawiającemu samodzielne tworzenie, modyfikację i rozbudowę - w tym widoków wizualizacji, logiki działania, skryptów i raportów bez udziału producenta

1.8. Część serwerowa oprogramowania musi być instalowalna i w pełni funkcjonalna zarówno w środowisku Microsoft Windows, jak i Linux.

1.9. Oprogramowanie musi posiadać natywną, wbudowaną funkcję pracy redundantnej z automatycznym przełączeniem (failover) między serwerem podstawowym a zapasowym, bez utraty danych. Mechanizm redundancji musi być realizowany wyłącznie środkami samej platformy, bez konieczności stosowania dodatkowego, zewnętrznego oprogramowania klastrującego lub HA innego producenta. Konfiguracja redundantna musi zapewniać synchronizację danych historycznych, stanów alarmów oraz bieżących wartości procesowych.

1.10. Wsparcie producenta. Producent oprogramowania musi zapewniać możliwość wykupienia komercyjnego wsparcia technicznego obejmującego co najmniej:

1.10.1. gwarantowany czas reakcji (SLA),

1.10.2. dostęp do aktualizacji oprogramowania oraz poprawek bezpieczeństwa. Wsparcie musi być świadczone przez producenta oprogramowania, a nie wyłącznie przez integratora realizującego wdrożenie.

**2. Wymagania bezpieczeństwa i kontroli dostępu**

2.1. Oprogramowanie musi obsługiwać uwierzytelnianie wieloskładnikowe (MFA) jako dodatkowy poziom weryfikacji tożsamości użytkownika. Mechanizm MFA musi być konfigurowalny - z możliwością włączenia/wyłączenia per użytkownik lub per grupa użytkowników.

2.2. Oprogramowanie musi umożliwiać integrację z usługą katalogową Active Directory lub LDAP w celu centralnego zarządzania tożsamościami użytkowników, grupami i przynależnościami. Uwierzytelnianie domenowe musi eliminować konieczność tworzenia osobnych kont w platformie.

2.3. Oprogramowanie musi posiadać wbudowany mechanizm kontroli dostępu oparty na rolach (Role-Based Access Control). Administrator musi mieć możliwość:
- definiowania dowolnych ról użytkownika,
- nadawania uprawnień granularnych (odczyt, zapis, administracja) z podziałem per obiekt, per widok wizualizacji oraz per obszar funkcjonalny,
- przypisywania użytkownikom jednej lub wielu ról,

2.4. Szyfrowanie komunikacji.

2.4.1. Komunikacja klient–serwer musi być szyfrowana z wykorzystaniem protokołu TLS w wersji 1.2 lub nowszej. W tym zakresie oprogramowanie musi umożliwiać wymuszenie połączeń szyfrowanych oraz blokowanie połączeń nieszyfrowanych.

2.4.2. Oprogramowanie musi umożliwiać zarządzanie certyfikatami: import, wymianę oraz kontrolę terminów wygasania.

**3. Wymagania funkcjonalne**

3.1. Monitorowanie infrastruktury OT.

3.1.1. Oprogramowanie musi monitorować stan i dostępność urządzeń podłączonych do przełączników (switchy) sieci OT - w tym sterowników PLC, paneli HMI, analizatorów, przetwornic częstotliwości, serwerów, urządzeń sieciowych oraz pozostałych urządzeń w obiektach - co najmniej w zakresie statusu (online/offline) i dostępności komunikacyjnej.

3.1.2. Oprogramowanie musi pozyskiwać dane o stanie infrastruktury z wykorzystaniem standardowych, otwartych protokołów, co najmniej: SNMP, OPC UA, Modbus TCP - bez konieczności stosowania zamkniętych, dedykowanych sond jednego producenta. Dane pozyskiwane ze sterowników PLC ujęć wody muszą być odczytywane z wykorzystaniem natywnego protokołu sterownika.

3.1.3. Oprogramowanie musi prowadzić i przechowywać wzorcową (bazową) mapę połączeń (topologię) pomiędzy urządzeniami.

3.1.4. Oprogramowanie musi monitorować zmiany w konfiguracji połączeń względem stanu wzorcowego (m.in. pojawienie się nowego urządzenia, odłączenie urządzenia, zmianę przypisania portu).

3.1.5. W przypadku wykrycia zmiany nieautoryzowanej oprogramowanie musi automatycznie generować alarm oraz powiadomienie, z dystrybucją co najmniej kanałami e-mail i SMS oraz z możliwością definiowania reguł eskalacji i grup odbiorców.

3.1.6. Oprogramowanie musi umożliwiać wizualizację stanu infrastruktury i topologii połączeń w dedykowanych, konfigurowalnych przez Zamawiającego widokach.

3.1.7. Oprogramowanie musi prowadzić dziennik zdarzeń (audit log) obejmujący wykryte zmiany oraz wygenerowane alarmy.

3.2. Inwentaryzacja zasobów OT.

3.2.1. Oprogramowanie musi umożliwiać inwentaryzację zainstalowanych urządzeń, gromadząc dla każdego urządzenia co najmniej: producenta, model, numer seryjny, wersję oprogramowania układowego (firmware), adres sieciowy (IP/MAC), lokalizację (obiekt) oraz funkcję.

3.2.2. Dane inwentaryzacyjne muszą być przechowywane w sposób umożliwiający Zamawiającemu samodzielne tworzenie zapytań, filtrowanie, raportowanie oraz eksport (co najmniej do formatów CSV/XLSX).

3.2.3. Oprogramowanie musi umożliwiać aktualizację danych inwentaryzacyjnych - automatyczną z dostępnych źródeł (protokoły komunikacyjne) oraz ręczne uzupełnianie i korektę rekordów.

3.2.4. Korelacja inwentaryzacji z bazą podatności NVD (NIST).

3.2.4.1. Oprogramowanie musi pobierać informacje o podatnościach z bazy National Vulnerability Database (NVD) prowadzonej przez NIST, z wykorzystaniem jej publicznego interfejsu REST API (wersja 2.0), i zestawiać je z rekordami inwentaryzacyjnymi na podstawie identyfikatora urządzenia (słowa kluczowego lub identyfikatora CPE) oraz wersji firmware.

3.2.4.2. Korelacja musi uwzględniać wersję firmware urządzenia, tak aby wskazywane były podatności dotyczące zainstalowanej wersji, z uwzględnieniem zakresów wersji publikowanych w rekordach CVE.

3.2.4.3. Oprogramowanie musi umożliwiać cykliczną, zaplanowaną aktualizację danych o podatnościach z bazy NVD oraz powiadamianie użytkownika o nowo wykrytych podatnościach dotyczących posiadanych urządzeń - co najmniej kanałami e-mail i SMS. Wysyłanie wiadomości SMS musi być realizowane przez dedykowany moduł, kartę SIM dostarczy zamawiający.

3.2.4.4. Oprogramowanie musi prezentować wykryte podatności w powiązaniu z urządzeniem w rejestrze inwentaryzacyjnym, co najmniej: identyfikator CVE, ocenę istotności (CVSS) - na podstawie danych udostępnianych przez NVD.

3.2.4.5. Oprogramowanie musi umożliwiać budowę konfigurowalnych raportów i pulpitów inwentaryzacyjnych.

3.3. Monitorowanie bezpieczeństwa OT.

3.3.1. Oprogramowanie musi agregować dane i zdarzenia z systemów bezpieczeństwa eksploatowanych przez Zamawiającego, z wykorzystaniem standardowych mechanizmów wymiany danych (co najmniej API/REST, OPC UA, MQTT).

3.3.2. Oprogramowanie musi udostępniać centralny pulpit prezentujący zagregowany stan bezpieczeństwa w dedykowanych, konfigurowalnych widokach.

3.3.3. Oprogramowanie musi umożliwiać definiowanie reguł korelacji i progów, na podstawie których generowane są alarmy.

3.3.4. Wygenerowane alarmy muszą być przekazywane do użytkownika co najmniej kanałami e-mail i SMS, z możliwością definiowania priorytetów, grup odbiorców i reguł eskalacji.

3.3.5. Oprogramowanie musi przechowywać historię zdarzeń i alarmów z możliwością przeglądania, filtrowania i raportowania.

3.4. Bezpieczeństwo fizyczne, techniczne i wizyjne obiektów.

3.4.1. Oprogramowanie musi umożliwiać integrację zdarzeń z systemów bezpieczeństwa fizycznego, technicznego i wizyjnego (CCTV, SSWiN, sterowników PLC) obiektów Zamawiającego

3.4.2. Oprogramowanie musi pozyskiwać zdarzenia z tych systemów z wykorzystaniem standardowych interfejsów.

3.4.3. Oprogramowanie musi umożliwiać korelację zdarzeń bezpieczeństwa fizycznego/wizyjnego ze zdarzeniami z infrastruktury OT.

3.4.4. Oprogramowanie musi prezentować stan bezpieczeństwa poszczególnych obiektów w dedykowanych, konfigurowalnych widokach, z kontrolą dostępu opartą na rolach.

3.4.5. Oprogramowanie musi generować alarmy i powiadomienia dla zdarzeń bezpieczeństwa fizycznego, technicznego i wizyjnego

3.5. Konfigurowalna częstotliwość odczytu (polling). Oprogramowanie musi umożliwiać niezależną konfigurację częstotliwości odczytu danych dla poszczególnych grup zmiennych z rozdzielczością co najmniej 1 sekundy dla zmiennych krytycznych oraz możliwością ustawienia dłuższych interwałów dla zmiennych o niższym priorytecie.

3.6. Eksport logów systemowych. Oprogramowanie musi umożliwiać eksport dzienników zdarzeń do pliku (co najmniej w formacie tekstowym/CSV) oraz przekazywanie zdarzeń do systemów zewnętrznych, w celu dalszej analizy lub archiwizacji. Mechanizm musi być dostępny dla administratora bez konieczności stosowania dodatkowego oprogramowania.

**4. Wdrożenie, szkolenia i wsparcie**

4.1. Wykonawca zobowiązany jest przeprowadzić po zakończeniu wdrożenia minimum dwie sesje szkoleniowe:

4.1.1. szkolenie administracyjne - dla osób odpowiedzialnych za konfigurację, zarządzanie użytkownikami, kopie zapasowe i utrzymanie platformy

4.1.2. szkolenie operatorskie — dla osób odpowiedzialnych za bieżący monitoring, reakcję na alarmy i obsługę widoków wizualizacji. Łączny wymiar szkoleń musi wynosić minimum 24 godziny zegarowe. Materiały szkoleniowe muszą zostać przekazane Zamawiającemu w formie elektronicznej.

4.2. Wykonawca (lub producent oprogramowania) zobowiązany jest zapewnić minimum 12 miesięcy wsparcia technicznego po odbiorze końcowym wdrożenia, obejmującego co najmniej:

4.2.1. Konsultacje techniczne w zakresie konfiguracji i eksploatacji

4.2.2. W przypadku zmian na istniejących obiektach bezpłatne wprowadzenia zmian w celu dostosowania oprogramowania

## 11. UPS dla urządzeń bezpieczeństwa OT – 2 szt.

| Lp. | Opis wymagań techniczno-funkcjonalnych | Konfiguracja minimalna Zamawiającego |
|---|---|---|
| 1. | Technologia | VFI (true on-line, podwójne przetwarzanie energii) |
| 2. | Budowa | Rack 19'' 2U |
| 3. | Moc znamionowa | 1 kVA / 1 kW |
| 4. | Wyjściowy współczynnik mocy (PF) | 1 |
| 5. | Napięcie wejściowe | 230 Vac |
| 6. | Sposób zasilania | Plug&Play Gniazdo w standardzie IEC 320<br>W komplecie powinien znajdować się przewód zasilający. |
| 7. | Tolerancja napięcia wejściowego przy obciążeniu 100%; bez przechodzenia na baterie | 161 – 299 Vac |
| 8. | Regulowany zakres napięcia wejściowego zależnie od poziomu obciążenia UPS bez przechodzenia na baterie | 110 – 299 Vac |
| 9. | Częstotliwość wejściowa | 40-70 Hz |
| 10. | Sprawność AC-AC w trybie pracy on-line z obciążeniem 100% | nie mniejsza niż 93% |
| 11. | Sprawność AC-AC w trybie pracy Oszczędzania energii Eco Mode | nie mniejsza niż 99% |
| 12. | Przeciążalność falownika | 110% - bez limitu, 130% - 5 min, 140% - 30 sek., >140% - 1,5 sek. |
| 13. | Tryb pracy z konwersją częstotliwości | Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie. |
| 14. | Napięcie wyjściowe | 230 Vac<br>W komplecie powinny znajdować się przynajmniej 2 przewody odbiorcze. |
| 15. | Częstotliwość wyjściowa | 50/60Hz (programowalna) z funkcją autosensing |
| 16. | Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass) | Statyczny przełącznik (SCR) z możliwością ręcznego przełączenia UPSa do trybu Bypass elektroniczny – wymuszanie opcji Bypass z poziomu panelu LCD |
| 17. | Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem | Wymagane |
| 18. | Wbudowany charger o regulowanym prądzie ładowania | Wymagana regulacja ładowania w zakresie 1A – 12A, pozwalająca na szybkie ładowanie baterii o dużej pojemności. |
| 19. | Regulacja prądu chargera | Regulacja powinna być możliwa z poziomu użytkownika na panelu LCD |

| | | |
|---|---|---|
| 20. | Baterie wewnętrzne | Minimum 3 x 9Ah/12V |
| 21. | Autonomia | Minimum 7minut dla obciążenia 1000W |
| 22. | Gniazdo baterii zewnętrznych | Wymagane, umożliwia podłączenie dodatkowych pakietów baterii w celu wydłużenia czasu autonomii. |
| 23. | Baterie | Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 10-12 lat, umieszczone wewnątrz zasilacza UPS |
| 24. | Możliwość rozbudowy pojemności baterii do min. 120Ah | Tak |
| 25. | Stabilizacja napięcia wyjściowego w stanie ustalonym | ± 1% |
| 26. | Stabilizacja napięcia wyjściowego w stanie nieustalonym | ± 3% |
| 27. | Stabilność częstotliwości wyjściowej: | bez synchronizacji: ± 0,05 Hz |
| 28. | Współczynnik szczytu | 3:1 |
| 29. | Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD oraz sygnalizacją akustyczną | Wymagane ze wskazaniem parametrów napięcia wejściowego i wyjściowego, częstotliwości a także napięcia i pozostałej autonomii pracy z baterii podczas gdy UPS pracuje w trybie bateryjnym. |
| 30. | Złącze interfejsów | RS232, USB, programowane złącze REPO do zdalnego wyłącznika pożarowego NO lub NC. Port zabezpieczający transmisję danych TVSS, slot karty SNMP. |
| 31. | Gniazda wyjściowe IEC320 na zasilaczu UPS z możliwością zarządzania | Wymagane minimum gniazd – 2 grupy gniazd, w każdej przynajmniej 4 gniazda w standardzie IEC 320-C13. Możliwość programowania czasu obecności napięcia na gniazdach w pracy z baterii w zakresie 0-999 minut. |
| 32. | Karta sieciowa SNMP | Wymagana SNMP z protokołem IP v. 4 i 6, obsługą VM oraz ModBus TCP. |
| 33. | Zdalny panel LCD | UPS powinien posiadać możliwość podłączenia wyniesionego panelu LCD ze wskazaniem parametrów pracy i czasu autonomii. |
| 34. | Interfejs EPO (do wyłącznika ppoż.) | Wymagane – styk programowany NO lub NC z poziomu wyświetlacza LCD. |
| 35. | Diagnostyka parametrów urządzenia UPS i baterii | Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS |
| 36. | Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego | Wymagane |
| 37. | Poziom hałasu w odległości 1m, | < 48 dBA<br>Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury |
| 38. | Funkcja oszczędzania energii | UPS powinien automatycznie wyłączyć się podczas pracy bateryjnej, gdy obciążenie UPS spadnie <5% wartości mocy nominalnej. |

| | | |
|---|---|---|
| 39. | Możliwość regulacji z poziomu LCD tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu | Wymagane |
| 40. | Zasilacz musi posiadać możliwość upgrade'u wersji oprogramowania sterującego pracą zasilacza. | Wymagane |
| 41. | Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa, kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE | Wymagane |
| 42. | Producent zasilacza UPS posiadający biuro dystrybucji i serwisu na terenie kraju. | Wymagane |
| 43. | Wymiary zasilacza UPS w szafie rack | Maks 2U |
| 44. | Maksymalne wymiary urządzenia | Szerokość: 440 mm<br>Głębokość: 410 mm<br>Wysokość: 2U (88mm) |
| 45. | Komplet szyn montażowych Rack | Wymagane |
| 46. | Instrukcja w języku polskim | Wymagane |

## 12. Urządzenie backup OT – 2 szt.

| Parametr | Wymagania minimalne |
|---|---|
| Procesor | Procesor osiągający wynik min. 4,5 tysiąca punktów w teście PassMark. |
| Obudowa | Typu tower (wolnostojąca) |
| Pamięć RAM | Minimum 8GB typu DDR4 lub DDR5 |
| Ilość obsługiwanych dysków | Minimum 4 dyski o rozmiarze 3.5" i maksymalnej pojemności nie mniejszej niż 22TB każdy. |
| Zainstalowane dyski | 2 dyski o pojemności 8TB każdy zgodne z listą kompatybilności oferowanego serwera oraz charakteryzujące się następującymi parametrami:<br>- prędkość obrotowa: minimum 7200 RPM,<br>- pamięć cache: minimum 256MB,<br>- gwarancja: minimum 60 miesięcy,<br>- MTBF: minimum 1 milion |
| Interfejsy sieciowe | Minimum 2 porty 2.5GbE RJ-45.<br><br>Możliwość zamontowania minimum dwóch dodatkowych karty sieciowych z portami 10GbE SFP+ lub 10GbE RJ-45.<br><br>Obsługa VLAN i Jumbo Frame. |
| Wskaźniki LED | Minimum status, USB, LAN, dyski 1–4 |

| | |
|---|---|
| Obsługa RAID | RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity, RAID 5, 6, 10 + dysk zapasowy. |
| Funkcje RAID | Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD. |
| Szyfrowanie | 256-bitowe szyfrowanie AES folderów oraz szyfrowanie dysków zewnętrznych. |
| System Operacyjny | Apple Mac OS 10.10 lub nowszy<br>Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 lub nowszy Linux<br>IBM AIX 7, Solaris 10 lub nowszy UNIX<br>Microsoft Windows 7, 8, 10, 11<br>Microsoft Windows Server 2008 R2, 2012, 2012 R2 oraz 2016, 2019, 2022 |
| Protokoły | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer WWW, Serwer plików, Manager plików przez WWW, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog. |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. |
| Język GUI | Polski |
| Gwarancja i serwis | Minimum 36 miesięcy gwarancji Next Business Day zapewniającej dostawę serwera zastępczego na następny dzień roboczy po wystąpieniu awarii sprzętowej. |
| System plików | Dyski wewnętrzne ZFS lub EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ |
| Funkcje ZFS | Liniowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL |
| iSCSI | Obsługa MPIO, MC/S i SPC-3 Persistent Reservation |
| Zasilanie | Zewnętrzny (adapter) lub wewnętrzny o mocy minimum 90W. |
| UPS | Obsługa sieciowych awaryjnych zasilaczy UPS. |

## 13. Switche Zarządzalne OT – 2 szt.

Poniższa specyfikacja określa minimalne wymagania techniczne dla przemysłowego, zarządzalnego przełącznika sieciowego przeznaczonego do pracy w sieciach automatyki przemysłowej (OT). Wszystkie wymagania mają charakter obligatoryjny, a podane wartości stanowią wymagane minimum (parametry równoważne lub lepsze), o ile nie wskazano inaczej. Wymagania sformułowano w sposób neutralny technologicznie, umożliwiający zaoferowanie urządzeń różnych producentów.

| Lp. | Parametr | Wymaganie minimalne (parametry równoważne lub lepsze) |
|---|---|---|
| 1 | **Typ i przeznaczenie** | Przemysłowy, zarządzalny przełącznik sieciowy warstwy 2 (L2), przeznaczony do budowy sieci komunikacyjnych w środowisku automatyki przemysłowej (OT) — |

| Lp. | Parametr | Wymaganie minimalne (parametry równoważne lub lepsze) |
|---|---|---|
| | | łączenia sterowników PLC, paneli HMI, urządzeń pomiarowych oraz systemów nadrzędnych SCADA. |
| 2 | **Porty Fast Ethernet** | Min. 8 portów Fast Ethernet 10/100 Mb/s w standardzie RJ-45. |
| 3 | **Porty Gigabit / uplink** | Min. 2 porty Gigabit typu combo (RJ-45 10/100/1000 Mb/s lub gniazdo SFP do wyboru), z obsługą wkładek światłowodowych SFP 1 Gb/s. |
| 4 | **Obudowa i montaż** | Metalowa obudowa przemysłowa, stopień ochrony min. IP30, montaż na szynie DIN. Chłodzenie pasywne (bez wentylatorów). |
| 5 | **Zasilanie** | Podwójne, redundantne wejście zasilania DC. Zakres napięcia pracy obejmujący co najmniej 24 VDC (dopuszczalny szeroki zakres, np. 12–48 VDC). |
| 6 | **Zakres temperatury pracy** | Co najmniej od -40°C do +70°C. |
| 7 | **Zarządzanie warstwą 2** | Pełna zarządzalność L2; konfiguracja i monitorowanie urządzenia. |
| 8 | **Sieci VLAN** | Obsługa VLAN zgodnie z IEEE 802.1Q — min. 256 sieci VLAN. |
| 9 | **Redundancja sieci** | Obsługa STP / RSTP / MSTP (IEEE 802.1D / 802.1w / 802.1s) oraz mechanizmu szybkiej redundancji pierścieniowej o czasie rekonwergencji ≤ 50 ms (np. MRP, ERPS lub równoważny mechanizm pierścieniowy producenta). |

| Lp. | Parametr | Wymaganie minimalne (parametry równoważne lub lepsze) |
|---|---|---|
| 10 | **Optymalizacja ruchu multicast** | Obsługa IGMP Snooping co najmniej v1/v2. |
| 11 | **QoS** | Obsługa priorytetyzacji ruchu (QoS) co najmniej wg IEEE 802.1p oraz DSCP. |
| 12 | **Agregacja łączy** | Obsługa agregacji łączy zgodnie z IEEE 802.3ad (LACP) oraz trunkingu statycznego. |
| 13 | **Funkcje bezpieczeństwa** | Co najmniej: Port Security (kontrola adresów MAC na porcie), uwierzytelnianie IEEE 802.1X, listy kontroli dostępu (ACL), Storm Control oraz mirroring portów (port mirroring). |
| 14 | **Protokoły przemysłowe** | Natywna obsługa co najmniej jednego z przemysłowych protokołów komunikacyjnych: PROFINET, EtherNet/IP lub Modbus/TCP. |
| 15 | **Zarządzanie i dostęp** | Zarządzanie przez interfejs WWW oraz SNMP v1/v2c/v3. Obsługa szyfrowanego dostępu administracyjnego (HTTPS i/lub SSH) oraz możliwość wyłączenia nieszyfrowanych usług zarządzania. Obsługa wysyłania logów do serwera Syslog. |
| 16 | **Pozostałe funkcje** | Obsługa ramek Jumbo Frames (min. 9000 bajtów). |
| 17 | **Gwarancja** | Gwarancja producenta min. 24 miesiące. |

# 14.Kompleksowe wdrożenie technologii z zakresu bezpieczeństwa

Wszystkie elementy dostarczane w ramach niniejszego postępowania — sprzęt, oprogramowanie oraz usługi opisane w poszczególnych pozycjach OPZ — tworzą jeden, wzajemnie powiązany system bezpieczeństwa obejmujący środowisko IT oraz środowisko OT. W poszczególnych pozycjach OPZ przewidziano integracje i wymianę danych pomiędzy komponentami, w szczególności: przekazywanie i korelację zdarzeń w systemie SIEM (integrację danych z różnych źródeł oraz monitorowanie rozproszone wielu lokalizacji/oddziałów), integrację systemu IDS dla OT z systemami zabezpieczeń z platformami centralnego zarządzania oraz łączność pomiędzy lokalizacjami z wykorzystaniem tuneli IPSec VPN, a także oparcie usługi SOC o system SIEM oraz EDR.

Z uwagi na powyższe wzajemne zależności oraz na rozproszenie środowiska (część IT w siedzibie głównej, część OT w lokalizacjach zdalnych) przedmiot zamówienia jest wdrażany jako jedno, kompleksowe wdrożenie realizowane przez jednego Wykonawcę — tak, aby zapewnić poprawną i kompletną współpracę wszystkich komponentów oraz spójność systemu bezpieczeństwa wymaganą dla osiągnięcia celu projektu.

**Architektura wdrożenia — lokalizacje (IT w siedzibie głównej, OT w lokalizacjach zdalnych)**

1. Część IT przedmiotu zamówienia (serwery z oprogramowaniem, platforma backup z deduplikacją, platforma SIEM, switche zarządzalne klasy enterprise wraz z wkładkami światłowodowymi 10 Gb/s oraz punktem dostępowym Wi-Fi, zasilanie awaryjne UPS, NGFW, oprogramowanie EDR oraz szafy RACK) zostanie wdrożona w siedzibie głównej Zamawiającego. Usługa SOC realizowana jest zdalnie w oparciu o systemy SIEM oraz EDR eksploatowane w siedzibie głównej.
2. Część OT przedmiotu zamówienia (kompleksowy system IDS dla OT wraz ze sprzętowymi sondami monitorującymi, UPS dla urządzeń bezpieczeństwa OT, urządzenia backup OT oraz switche zarządzalne OT) zostanie wdrożona w rozproszonych lokalizacjach zdalnych Zamawiającego. Sondy oraz urządzenia OT instalowane są w miejscach wskazanych przez Zamawiającego, bez powodowania przerw i zakłóceń w pracy sieci przemysłowej; serwer systemu IDS instalowany jest w środowisku serwerowym wskazanym przez Zamawiającego.
3. Komunikacja pomiędzy lokalizacjami zdalnymi OT a systemami centralnymi w siedzibie głównej: Transmisja danych pomiędzy lokalizacjami jest zabezpieczona.

**Zakres kompleksowego wdrożenia**

1. Wykonawca dostarczy, zainstaluje, skonfiguruje, zintegruje i uruchomi wszystkie elementy objęte OPZ (sprzęt, oprogramowanie oraz usługi z poszczególnych pozycji), zapewniając ich wzajemną współpracę zgodnie z wymaganiami właściwych pozycji OPZ.
2. W siedzibie głównej Wykonawca dokona zabudowy urządzeń IT w szafach RACK oraz podłączenia zasilania gwarantowanego (UPS), a także instalacji i konfiguracji serwerów, platformy backup, systemu SIEM, switchy enterprise (wraz z wkładkami światłowodowymi i punktem dostępowym), NGFW oraz oprogramowania EDR.
3. W lokalizacjach zdalnych OT Wykonawca zainstaluje i skonfiguruje sprzętowe sondy systemu IDS, switche zarządzalne OT, urządzenia backup OT oraz UPS dla urządzeń OT, wykonując wszystkie niezbędne połączenia i okablowanie pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą, bez przerw i zakłóceń w pracy sieci przemysłowej.
4. Wykonawca zapewni przekazywanie danych ze środowiska OT (z lokalizacji zdalnych) do systemu IDS oraz dalej do systemu SIEM w siedzibie głównej (poprzez Syslog), z zachowaniem zabezpieczenia transmisji między lokalizacjami.
5. Wykonawca zintegruje źródła zdarzeń z systemem SIEM (m.in. NGFW, oprogramowanie EDR, system IDS, urządzenia sieciowe oraz serwery), zapewniając centralny odbiór i korelację zdarzeń.
6. Wykonawca uruchomi usługę SOC w oparciu o wdrożony system SIEM oraz oprogramowanie EDR — zgodnie z pozycją OPZ dotyczącą usługi SOC.
7. Dla całości zakresu objętego kompleksowym wdrożeniem Wykonawca przeprowadzi testy sprawdzające prawidłowość instalacji, konfiguracji oraz współpracy komponentów; przekaże Zamawiającemu hasła użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień — zgodnie z zasadami wdrożenia przyjętymi w OPZ (opisanymi w pozycji dotyczącej systemu IDS).

**Komunikacja i integracja pomiędzy komponentami**

Wdrożenie zapewnia współpracę komponentów zgodnie z integracjami wymaganymi w poszczególnych pozycjach OPZ. Poniższe zestawienie podsumowuje powiązania wynikające z OPZ:

| Komponent | Integracja / komunikacja w ramach systemu (wynikająca z OPZ) |
|---|---|
| **System SIEM (siedziba główna)** | Centralny odbiór i korelacja zdarzeń z różnych źródeł, w tym z rozproszonych lokalizacji/oddziałów; stanowi podstawę działania usługi SOC. |
| **NGFW (siedziba główna)** | Przekazywanie zdarzeń/logów do SIEM; współpraca z platformą centralnego zarządzania; tunele IPSec VPN łączące lokalizacje. |
| **Oprogramowanie EDR** | źródło danych dla usługi SOC; przekazywanie zdarzeń do SIEM; bieżąca ochrona i prewencja |
| **System IDS dla OT** | Pasywny monitoring sieci przemysłowej w lokalizacjach OT; odbiór ruchu ze sprzętowych sond; integracja z systemem SIEM |
| **Sprzętowe sondy OT (lokalizacje zdalne)** | Instalowane w lokalizacjach zdalnych; pasywne zbieranie ruchu (SPAN/mirror lub pass-through); szyfrowana komunikacja z systemem IDS. |
| **Switche enterprise + wkładki 10G + punkt dostępowy** | Źródło zdarzeń (syslog); uwierzytelnianie dostępu; połączenia uplink 10 Gb/s (wkładki SFP+); zarządzanie centralne. |
| **Switche zarządzalne OT (lokalizacje zdalne)** | Element sieci OT w lokalizacjach zdalnych; udostępnianie kopii ruchu (SPAN/mirror) dla sond systemu IDS. |
| **Serwery / platforma backup / backup OT** | Źródła zdarzeń; kopie zapasowe środowiska IT (siedziba główna) oraz OT (lokalizacje zdalne). |
| **UPS / UPS OT / szafa RACK** | Zasilanie gwarantowane oraz zabudowa urządzeń: część IT w siedzibie głównej, część OT w lokalizacjach zdalnych. |
| **Usługa SOC** | Zdalne monitorowanie, analiza i informowanie w oparciu o system SIEM oraz EDR. |

**Elementy wdrożenia opisane w innych pozycjach OPZ (odniesienie)**

1. Zakres wdrożenia systemu IDS dla OT (monitorowania sieci przemysłowej) został szczegółowo opisany w pozycji dotyczącej tego systemu i obowiązuje bez zmian. W skrócie obejmuje on: dostawę i instalację sprzętowych sond w lokalizacjach wskazanych przez Zamawiającego oraz wykonanie niezbędnych połączeń i okablowania bez przerw w pracy sieci, instalację, licencjonowanie i pełną konfigurację systemu IDS w środowisku serwerowym wskazanym przez Zamawiającego, testy poprawności, przekazanie haseł, szkolenie administratorów Zamawiającego oraz dokumentację powykonawczą warunkującą odbiór.
2. Zakres wdrożenia usługi SOC został opisany w pozycji dotyczącej tej i obowiązuje bez zmian. W skrócie obejmuje on: inwentaryzację źródeł, integrację z posiadanym przez Zamawiającego systemem SIEM oraz EDR, konfigurację i dostrojenie reguł detekcji wraz z uzgodnionym okresem dostrajania, a także opracowanie i uzgodnienie planu wdrożenia.

**Klauzula ogólna**

1. Celem wdrożenia jest zapewnienie pełnej, poprawnej i efektywnej adaptacji wszystkich dostarczonych rozwiązań z zakresu infrastruktury IT i cyberbezpieczeństwa w środowisku Zamawiającego, w sposób umożliwiający ich rzeczywiste wykorzystanie operacyjne.
2. Wykonawca zobowiązany jest do realizacji wdrożenia w sposób kompleksowy, obejmujący wszystkie czynności niezbędne do osiągnięcia zakładanego efektu funkcjonalnego i bezpieczeństwa, nawet jeżeli nie zostały one wprost wskazane w niniejszym OPZ, o ile są standardowo wymagane dla prawidłowego uruchomienia i eksploatacji danego typu rozwiązań.
3. Zamawiający wskazuje, iż nie posiada specjalistycznej wiedzy technicznej w zakresie wdrażanych technologii na poziomie szczegółowym, w związku z czym Wykonawca zobowiązany jest do: zaproponowania optymalnych rozwiązań

konfiguracyjnych, dostosowania wdrożenia do rzeczywistego środowiska Zamawiającego, uwzględnienia dobrych praktyk oraz zaleceń producentów, a także zapewnienia kompletności i spójności wdrożenia.

4. Odpowiedzialność za prawidłową konfigurację, integrację oraz osiągnięcie zakładanych funkcjonalności systemów spoczywa na Wykonawcy.