

Załącznik nr 1 do SWZ

Numer postępowania: **B.271.1.3.2026**

OPIS PRZEDMIOTU ZAMÓWIENIA

DO ZADANIA PT.:

Dostawa sprzętu informatycznego oraz oprogramowania wraz instalacją, konfiguracją i uruchomieniem na potrzeby Urzędu Gminy Blizanów i 2 jednostek

CZĘŚĆ nr I – Dostawa i wdrożenie kolektorów logów systemowych w 3 jednostkach

I. Dostawa macierzy dyskowej na potrzeby kolektora logów w UG – 1 szt.

NAZWA PARAMETRU:	MINIMALNA WARTOŚĆ PARAMETRU:
Obudowa i komponenty	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5".
Przestrzeń dyskowa	Zainstalowane: min. 8 dysków SAS o pojemności min. 2.4TB, Hot-Plug min. 3 dyski SSD SAS o pojemności min. 1.92TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.

	Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania baterijnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów 25Gb iSCSI (4 porty na kontroler)
Kable/wkładki	2x kabel DAC 25GbE SFP28/SFP28 min. 2m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International). Wymagane dołączenie do oferty dokumentu potwierdzające spełnienie powyższych wymagań.

Inne	<p>Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.</p> <p>Deklaracja zgodności CE.</p>
Warunki gwarancji	<p>Zamawiający wymaga zapewnienia dodatkową gwarancji producenta z zakresu wdrażanej technologii na okres min. 36 miesięcy.</p> <p>Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.</p> <p>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.</p> <p>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>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.</p> <p>Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</p> <p>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.</p> <p>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.</p> <p>Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:</p> <ul style="list-style-type: none"> • Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. • 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. • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. • 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.

	<ul style="list-style-type: none"> 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 przekaze 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. <p>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.</p>
--	---

II. Dostawa serwera wraz z systemem operacyjnym na potrzeby kolektora logów w UG – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 1U z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. 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/iOS) przy użyciu jednego z protokołów BLE/WIFI
Płyta główna	<ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 144 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 3 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Chipset	<ul style="list-style-type: none"> Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	<ul style="list-style-type: none"> Zainstalowane min. dwa procesory min. 16-rdzeniowe (każdy) klasy x86, taktowane częstotliwością min. 2.3GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 245 pkt. w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	<ul style="list-style-type: none"> Minimum 256GB DDR5 RDIMM
Gniazda PCI	<ul style="list-style-type: none"> Min. 2 sloty PCIe LP
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane: <ul style="list-style-type: none"> 2 x dysk M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Wbudowane porty	<ul style="list-style-type: none"> 4 porty USB w tym min: <ul style="list-style-type: none"> 1 port USB 2.0 Type-C 2 porty USB 3.1 1 port USB 3.0 wewnątrz obudowy Port VGA z tyłu obudowy
Video	<ul style="list-style-type: none"> Zintegrowana karta graficzna
Zasilacze	<ul style="list-style-type: none"> Redundantne, Hot-Plug min. 1100W klasy Titanium

System operacyjny/dodatkowe oprogramowanie	<ul style="list-style-type: none"> Ze względu na potrzebę zachowania kompatybilności ze stosowanym obecnie przez Zamawiającego oprogramowaniem wymagane jest dostarczenie wraz z serwerem bezterminowej, nowej (nieaktywowanej wcześniej) licencji na oprogramowanie MS Windows Server 2025 Standard licencjonowanej na wszystkie rdzenie procesorów w zaoferowanym serwerze oraz 40 licencji dostępowych MS Windows Server User CAL Do serwera należy dołączyć nośnik fizyczny umożliwiający instalację systemu operacyjnego w wyspecyfikowanej wersji.
Bezpieczeństwo	<ul style="list-style-type: none"> Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem 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).
Karta Zarządzania	<ul style="list-style-type: none"> Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> zdalny dostęp do graficznego interfejsu Web karty zarządzającej szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika możliwość podmontowania zdalnych wirtualnych napędów wirtualną konsolę z dostępem do myszy, klawiatury wsparcie dla IPv6 wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer integracja z Active Directory możliwość obsługi przez sześciu administratorów jednocześnie Wsparcie dla automatycznej rejestracji DNS wsparcie dla LLDP wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. Monitorowanie zużycia dysków SSD

	<ul style="list-style-type: none"> ○ Automatyczne zgłaszanie alertów do centrum serwisowego producenta ○ Automatyczne update firmware dla wszystkich komponentów serwera ○ Możliwość przywrócenia poprzednich wersji firmware ○ Możliwość eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON ○ Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych ○ Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram. ○ Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera ○ kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania ○ możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień ○ możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera ○ możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer ○ możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe możliwość rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> ○ możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, Elasticsearch ○ możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielokrotnego przy logowaniu do karty zarządzającej ○ Automatyczne odświeżanie certyfikatów SSL ○ monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach

	<ul style="list-style-type: none"> ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przetłaczników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. ○ Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: <ul style="list-style-type: none"> ▪ wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów ▪ wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji ▪ z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
--	--

	<ul style="list-style-type: none"> ▪ inwentaryzacja komponentów w serwerze i ich mikrokodów ▪ historia poboru mocy i temperatury serwera ▪ zbieranie danych diagnostycznych serwera do paczki serwisowej
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> • Monitoring: <ul style="list-style-type: none"> ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: <ul style="list-style-type: none"> ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: <ul style="list-style-type: none"> ▪ Opóźnień ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów

	<ul style="list-style-type: none"> ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: <ul style="list-style-type: none"> ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware <ul style="list-style-type: none"> ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty <ul style="list-style-type: none"> ○ Możliwość generowania raportów dla serwerów zawierających informację o: <ul style="list-style-type: none"> ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: <ul style="list-style-type: none"> ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomowi redukcji danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo <ul style="list-style-type: none"> ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa.
--	--

	<p>System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia.</p> <ul style="list-style-type: none"> ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. <ul style="list-style-type: none"> • Wspierane urządzenia <ul style="list-style-type: none"> ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent <ul style="list-style-type: none"> ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; • Możliwość rozszerzenia funkcjonalności <ul style="list-style-type: none"> ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. • Inne <ul style="list-style-type: none"> ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty	<ul style="list-style-type: none"> • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • 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.
Dokumentacja użytkownika	<ul style="list-style-type: none"> • Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	<ul style="list-style-type: none"> • Zamawiający wymaga zapewnienia dodatkowej gwarancji Producenta z zakresu wdrażanej technologii na okres min. 36 miesięcy. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.

	<ul style="list-style-type: none"> • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • 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. • Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • 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. • Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: <ul style="list-style-type: none"> ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. ○ 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. ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ 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. ○ 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 przekaze 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. • 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.
--	---

III. Dostawa UPS na potrzeby kolektorów logów w UG, ZUK i GOPS – 3 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz przeprowadzenie instruktażu stanowiskowego zasilacza bezprzerwowego.

Wymagania techniczne:

1. Urządzenie dedykowane do zastosowań serwerowych,
2. Moc wyjściowa pozorna: 2000 VA,
3. Moc wyjściowa czynna: 2000 W,
4. Współczynnik mocy PF min.: 0,9

5. Topologia:

- Podwójna konwersja online (VFI-SS-111)
 - Sprawność min. 90% w trybie online
 - Sinusoidalny kształt fali wyjściowej
 - Zniekształcenia napięcia wyjściowego max. 2% przy obciążeniu liniowym
6. Liczba faz (wejście/wyjście): 1/1 (230V),
 7. Czas podtrzymania przy 100% obciążenia: min. 5,0 min,
 8. Typ obudowy: Rack 19" (2U),
 9. Stopień ochrony: IP20 lub IP21,
 10. Zabezpieczenia: przeciwzwarciove, EPO (Emergency Power Off), ochrona przed przepięciami,
 11. Możliwość wydłużenia czasu podtrzymania przez podłączenie zewnętrznych modułów bateryjnych (min. 4 sztuk),
 12. Możliwość wymiany akumulatorów w trakcie pracy,
 13. Predykcja czasu podtrzymania – wyświetlanie na panelu oraz w dedykowanym oprogramowaniu,
 14. Zimny start,
 15. Interfejsy: slot na kartę SNMP/Web + min. USB/RS232,
 16. Dostępne bezpłatne/dostawa w ramach zadania - oprogramowania monitorująco-zarządzającego
 17. Gwarancja: 24 miesiące na urządzenie i baterię

Zakres zamówienia:

1. Dostawa fabrycznie nowego zasilacza UPS wraz z akcesoriami (kable, szyny montażowe rack, instrukcja, karta gwarancyjna),
2. Instalacja urządzenia w miejscu wskazanym przez Zamawiającego, w konfiguracji Rack
3. Podłączenie do istniejącej infrastruktury elektrycznej zgodnie z instrukcją producenta,
4. Konfiguracja podstawowa UPS, uruchomienie oraz test działania (w tym test czasu podtrzymania),
5. Przeprowadzenie instruktażu stanowiskowego dla wskazanych pracowników Zamawiającego w zakresie obsługi, eksploatacji, podstawowej diagnostyki oraz zasad bezpieczeństwa użytkowania UPS,
6. Przekazanie kompletnej dokumentacji: instrukcja obsługi w języku polskim, karta gwarancyjna, protokół z instruktażu.

Wymagania dotyczące instalacji

1. Instalacja musi być wykonana przez osobę posiadającą aktualne uprawnienia SEP do 1 kV,
2. Instalacja budynku, do której podłączony będzie UPS, musi być wyposażona w ochronę przed przeciążeniem oraz zwarcie
3. Po stronie wejściowej dopuszczalne są tylko konfiguracje sieci typu TN-S lub TN-C-S
4. Po zakończeniu instalacji należy wykonać test poprawności działania oraz przekazać potwierdzenie Zamawiającemu

Wymagania dotyczące instruktażu stanowiskowego

1. Omówienie budowy i zasad działania UPS
2. Zasady bezpiecznego użytkowania i obsługi
3. Procedury uruchamiania, wyłączania, testowania oraz postępowania w sytuacjach awaryjnych
4. Omówienie funkcji oprogramowania monitorująco-zarządzającego
5. Przekazanie materiałów szkoleniowych (instrukcja obsługi)

6. Potwierdzenie przeprowadzenia instruktażu – podpisany protokół

Wymagania dodatkowe

1. Wykonawca zobowiązany jest do zapewnienia serwisu gwarancyjnego,
2. Wykonawca zobowiązany jest do zapewnienia wsparcia technicznego w okresie gwarancji,
3. Wszystkie elementy muszą być fabrycznie nowe, wolne od wad i uszkodzeń
4. Wszystkie prace muszą być wykonane zgodnie z obowiązującymi przepisami BHP, Prawem budowlanym oraz ustawą Prawo zamówień publicznych.

IV. Dostawa urządzenia klasy NAS na potrzeby kolektorów logów systemowych w ZUK i GOPS – 2 szt.

NAZWA PARAMETRU:	MINIMALNA WARTOŚĆ PARAMETRU:
Procesor	Procesor 64-bitowy x86 osiągający w teście PassMark Performance Test, co najmniej 8 600 punktów w kategorii Average CPU Mark, o taktowaniu nie mniejszym niż 2.2 GHz
Zainstalowana pamięć RAM	Min. 8 GB ECC, możliwość rozbudowy do 64 GB
Liczba zatok na dyski	Min. 16 w tym min. 12 x 3,5-calowych SATA oraz min. 4 x E1.S/M.2 PCIe Gen 3 x2
Obsługiwane dyski twarde	3.5" SATA, 2.5" SATA, 2,5" SSD SATA, E1.S SSD oraz M.2 NVMe SSD, wszystkie Hot Plugin
Zainstalowane dyski twarde	Min. 6 szt. o pojemności min. 12TB 7200. Dysk dedykowany do pracy w urządzeniach typu NAS. Dyski musi znajdować się na oficjalnej liście kompatybilności dla danego urządzenia
Porty LAN 2,5 GbE	Min. 2 szt.
Porty LAN 10 GbE	Min. 1 szt.
Porty USB 3.2 Gen1	Min. 2 szt.
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 3U
Zasilanie	230V
Specyfikacja oprogramowania	
Agregacja łączy	Tak
Obsługiwane systemy plików	EXT4, ZFS lub BTRFS
Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Poziomy RAID: Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Pula pamięci masowej Obsługa migawek
Obsługiwane protokoły	CIFS, SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, Fibre Channel, HTTP, HTTPs, FTP, SNMP, LDAP,
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer

Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer Monitoringu
VPN	VPN client / VPN server
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Monitor zasobów Kosz sieciowy dla CIFS/SMB Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Tak
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Warunki gwarancji	Wymagane min. 3 lata gwarancji producenta urządzenia. W przypadku awarii dysków uszkodzone nośniki danych pozostają u Zamawiającego.

V. Dostawa przełącznika sieciowego na potrzeby kolektorów logów w ZUK i GOPS – 2 szt.

Dostawa zarządzalnego przełącznika sieciowego spełniającego wymagania techniczne określone poniżej, wraz z licencjami i wsparciem technicznym.

1. Minimalne wymagania techniczne urządzenia

1) Ogólne

- Przełącznik zarządzalny L2+ z routingiem statycznym IPv4/IPv6,
- Obudowa typu RACK 1U z możliwością montażu w standardowej szafie serwerowej.

2) Porty i łączność

- Minimum 48 portów RJ-45 10/100/1000 Mbps.
- Minimum 4 sloty SFP 1000Base-X (1 Gbps).
- Obsługa agregacji łącza (Link Aggregation Control Protocol, LACP) do 26 grup x8 portów.

3) Wydajność i pamięć

- Przepustowość przełączania (switching capacity) min. 104 Gbps.
- Przekierowywanie pakietów (forwarding rate) min. 77 Mpps.
- MAC Table min. 16.000
- Jumbo Frames: min. 9 kB
- Bufor na pakiety co najmniej 12 Mbit.
- Pamięć DRAM co najmniej 512 MB.
- Pamięć Flash minimum 32 MB.

4) Funkcje sieciowe i bezpieczeństwo

- Obsługa VLAN do 4094 sieci.
- Protokoły Spanning Tree: STP, RSTP, MSTP.
- Lista kontroli dostępu (ACL) do minimum 512 zasad.
- Ochrona przed atakami DoS, zabezpieczenia portów (port security), filtrowanie MAC.
- Obsługa Energy Efficient Ethernet (IEEE 802.3az).

- f) Możliwość stosowania zaawansowanych funkcji QoS (802.1p),
 - g) Obsługa protokołów uwierzytelniania 802.1X, funkcje DHCP Snooping oraz Dynamic ARP Inspection (DAI),
 - h) Dostęp do zarządzania przez interfejs web GUI, CLI (Command Line Interface) oraz protokoły SNMP v1/v2c/v3, SSH v2, Telnet
- 5) Zasilanie
- a) Wbudowany zasilacz o napięciu wejściowym 100-240 V AC, 50-60 Hz.
 - b) Wentylator zapewniający chłodzenie urządzenia.
2. Zarządzanie
- 1) Dostęp zarządzania przez interfejs web GUI.
 - a) Porty konsoli: RJ-45.
 - b) Omada SDN lub równoważne:
 - Zero-Touch Provisioning (ZTP)
 - Cloud Management przez Omada Controller
 - Dual Firmware Images (aktualizacja bez przestoju)
3. Gwarancja i wsparcie
- 1) Producent udziela dożywotniej gwarancji serwisowej.
 - 2) Zapewnienie wsparcia technicznego dostępnego w języku polskim.
- VI. Wdrożenie kolektorów logów systemowych:
- VII. W ramach wdrożenia Wykonawca musi dostarczyć sprzęt spełniający wymagania opisane w punktach I. Dostawa macierzy dyskowej na potrzeby kolektora logów w UG, II. Dostawa serwera wraz z systemem operacyjnym na potrzeby kolektora logów w UG, III. Dostawa UPS na potrzeby kolektorów logów w UG, ZUK i GOPS, IV. Dostawa urządzenia klasy NAS na potrzeby kolektorów logów systemowych w ZUK i GOPS oraz V. Dostawa przełącznika sieciowego na potrzeby kolektorów logów w ZUK i GOPS, a także wdrożyć rozwiązanie oparte na oprogramowaniu ze sklepu z aplikacjami w zakresie zbierania logów systemowych we wskazanych przez Zamawiającego dwóch lokalizacjach (ZUK i GOPS).
- 1. Dostarczone rozwiązania muszą być fabrycznie nowe oraz pochodzić z oficjalnego kanału dystrybucji w UE.
 - 2. Dostarczone rozwiązania należy odpowiednio skonfigurować i dokonać ich integracji z posiadanym przez Zamawiającego oraz nowowdrażanym oprogramowaniem i sprzętem.
 - 3. Dostarczone rozwiązania muszą zostać zainstalowane w infrastrukturze Zamawiającego z uwzględnieniem najlepszych praktyk w zakresie cyberbezpieczeństwa. Wdrożenie musi obejmować konfigurację wszystkich dostępnych funkcjonalności zgodnie z zaleceniami Zamawiającego.
 - 4. Wykonawca musi również wykonać aktualizacje firmware wszystkich urządzeń do najnowszej wersji.
 - 5. Zamawiający oczekuje świadczenia przez Wykonawcę opieki serwisowej w zakresie wykonanych prac oraz wdrożonych rozwiązań z uwzględnieniem następujących warunków:
 - 1) Opieka serwisowa winna być świadczona przez okres min. jednego miesiąca od dnia zakończenia wdrożenia.
 - 2) Opieka serwisowa winna być świadczona w wymiarze nie mniejszym niż 10 osobogodzin.
 - 3) Czas reakcji na zgłoszenie nie powinien przekroczyć 4 godzin roboczych.
 - 4) Zakres opieki serwisowej winien obejmować:

- a) konsultacje,
 - b) pomoc w rozwiązywaniu problemów,
 - c) usuwanie błędów.
- 5) Zgłaszanie i obsługa zdarzeń musi być realizowana za pomocą systemu helpdesk z rozliczeniem zadań. Wykonawca musi posiadać wdrożony tego typu system wsparcia serwisowego.
6. Zamawiający wymaga również przeprowadzenia instruktażu stanowiskowego z obsługi dostarczonej platformy dla min. 3 osób. Instruktaż musi zostać przeprowadzony stacjonarnie lub w formie zdalnej, w języku polskim. Zamawiający dopuszcza realizację tego obowiązku przez dostarczenie vouchera na realizację takiego instruktażu przez centrum szkoleniowe, pod warunkiem, że wskazane centrum szkoleniowe gwarantuje realizację takiego instruktażu w terminie max. do 31 maja br.
7. Instruktaż stanowiskowy musi pozwolić na uzyskanie wiedzy teoretycznej oraz praktycznych umiejętności niezbędnych w administrowaniu dostarczonym oprogramowaniem w zakresie zbierania logów systemowych.
8. Zamawiający wymaga, aby instruktaż trwał min. 1 dzień roboczych (7 godz.)
9. Na zakończenie uczestnik winien otrzymać certyfikat potwierdzający ukończenie instruktażu

VIII. Zapisy uzupełniające

1. Zamawiający wymaga skonfigurowania i wdrożenia całego dostarczonego sprzętu oraz oprogramowania we wszystkich wymienionych lokalizacjach wraz z instalacją w istniejących szafach serwerowych.
2. Jeżeli w celu optymalnej instalacji urządzeń konieczna będzie reorganizacja elementów umieszczonych już w szafach, Wykonawca jest zobowiązany, w porozumieniu z Zamawiającym, do realizacji tych prac we własnym zakresie
3. Zamawiający wymaga przygotowania optymalnego projektu prac oraz harmonogramu planowanych prac w zakresie instalacji i wdrożeń, a także przedstawienie obu dokumentów do akceptacji Zamawiającemu na minimum 5 dni roboczych przed rozpoczęciem prac.
4. Wykonawca musi uwzględnić wszelkie koszty związane z prawidłowym demontażem i montażem wszystkich elementów oraz wykonaniem całości wdrożenia zgodnie ze sztuką. Zamawiający zaleca dokonanie oględzin w miejscu, gdzie prowadzone będą prace związane z wykonaniem zamówienia, celem zdobycia kompletnych informacji, służących właściwemu oszacowaniu oferty. Oględzin można dokonać po wcześniejszym umówieniu terminu z przedstawicielem Zamawiającego.
5. Zamawiający udostępni szczegółowe informacje o środowisku teleinformatycznym po podpisaniu umowy projektowej i umowy o poufności.
6. Zamawiający ma prawo do wprowadzania zmian i wytycznych do wskazanych powyżej dokumentów, niezaakceptowanie ich przez Wykonawcę w ciągu 3 dni stanowi przesłankę do rozwiązania umowy.
7. W czasie prac instalacyjnych musi być zapewniona ciągłość działania wszystkich JO Zamawiającego. Przerwy serwisowe ustalone będą na bieżąco z personelem informatycznym Zamawiającego.
8. Wykonawca jest zobowiązany do wykonania dokumentacji powykonawczej zawierającej szczegółowy opis i konfigurację całego systemu, sporządzonej w języku polskim. Wykonawca prześle dokumentację w wersji papierowej oraz na informatycznym nośniku danych w formie plików edytowalnych.

9. W celu legalizacji posiadanych i użytkowanych przez Zamawiającego licencji oprogramowania systemowego w opisie przedmiotu zamówienia wskazano znak towarowy firmy Microsoft jako wzorzec funkcjonalno – jakościowy przedmiotu zamówienia. Oznacza to tym samym, że Zamawiający dopuszcza złożenie oferty na oprogramowanie o parametrach funkcjonalnych i jakościowych tożsamy z parametrami oprogramowania określonego we wzorcu. Wykazanie równoważności złożonej oferty leży po stronie Wykonawcy i powinno zostać udokumentowane w możliwie najbardziej obiektywny sposób. W przypadku zaoferowania przez Wykonawcę oprogramowania innego niż wskazanego w przedmiocie zamówienia, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem istniejącej infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), poziomu serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla administratorów i użytkowników oferowanego rozwiązania.
10. Gwarancja Wykonawcy, o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczony sprzęt oraz wykonane usługi, musi być udzielona na min. 36 miesięcy. Zamawiający oczekuje realizacji uprawnień gwarancyjnych na następujących warunkach:
- a) Gwarancja, w miarę możliwości, winna być realizowana w siedzibie Zamawiającego.
 - b) Czas reakcji na zgłoszony problem (rozumiany, jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego.
 - c) Usunięcie usterki ma zostać wykonane do 21 dni roboczych od momentu zgłoszenia usterki.
 - d) Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego) lub drogą elektroniczną (e-mail, formularz WWW itp.), przez całą dobę.
 - e) Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań.
 - f) Zgłaszanie i obsługa zdarzeń musi być realizowana za pomocą systemu helpdesk z rozliczeniem zadań. Wykonawca musi posiadać wdrożony tego typu system wsparcia serwisowego.
 - g) W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę, Zamawiający dopuszcza podstawienie na czas naprawy sprzętu o nie gorszych parametrach funkcjonalnych.
 - h) Wykonawca ma obowiązek przekazać Zamawiającemu dokumenty sporządzone w języku polskim, poświadczające zakres oraz okres obowiązywania gwarancji.

UWAGA! Powyższe zapisy w zakresie gwarancji Wykonawcy obowiązują jedynie w przypadku braku szczegółowych zapisów w niniejszym opisie przedmiotu zamówienia.

CZĘŚĆ nr II – Aktualizacje UTM

I. Dostawa serwisów aktualizacyjnych do UTM Fortigate 60F

Zamawiający posiada w UG urządzenie UTM firmy Fortinet FG-60F w ramach postępowanie wymagane jest dostarczenie następujących usług i funkcjonalności:

- Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service) – min. 1 rok
- FortiCare Premium – min. 1 rok

II. Dostawa serwisów aktualizacyjnych do UTM Fortigate 40F

Zamawiający posiada w ZUK urządzenie UTM firmy Fortinet FG-40F w ramach postępowanie wymagane jest dostarczenie następujących usług i funkcjonalności:

- Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service) – min. 1 rok
 - FortiCare Premium – min. 1 rok
1. Dostarczone serwisy pochodzić z oficjalnego kanału dystrybucji w UE.
 2. Poza dostarczeniem serwisów Zamawiający oczekuje weryfikacji i odpowiedniej konfiguracji posiadanych urządzeń, a także integracji z posiadanym przez Zamawiającego oraz nowowdrażanym oprogramowaniem i sprzętem.
 3. Konfiguracja musi uwzględniać najlepsze praktyki w zakresie cyberbezpieczeństwa oraz obejmować konfigurację wszystkich dostępnych funkcjonalności zgodnie z zaleceniami Zamawiającego.
 4. Wykonawca musi również wykonać aktualizacje firmware obu urządzeń do najnowszej wersji.
 5. Zamawiający oczekuje świadczenia przez Wykonawcę opieki serwisowej w zakresie wykonanych prac oraz wdrożonych rozwiązań z uwzględnieniem następujących warunków:
 - 1) Opieka serwisowa winna być świadczona przez okres min. jednego miesiąca od dnia zakończenia wdrożenia.
 - 2) Opieka serwisowa winna być świadczona w wymiarze nie mniejszym niż 10 osobogodzin.
 - 3) Czas reakcji na zgłoszenie nie powinien przekroczyć 4 godzin roboczych.
 - 4) Zakres opieki serwisowej winien obejmować:
 - a) konsultacje,
 - b) pomoc w rozwiązywaniu problemów,
 - c) usuwanie błędów.
 - 5) Zgłaszanie i obsługa zdarzeń musi być realizowana za pomocą systemu helpdesk z rozliczeniem zadań. Wykonawca musi posiadać wdrożony tego typu system wsparcia serwisowego.
 6. W czasie prac instalacyjnych musi być zapewniona ciągłość działania wszystkich UG i ZUK. Przerwy serwisowe ustalane będą na bieżąco z personelem informatycznym Zamawiającego.

Część nr III – Dostawa stanowiskowych zasilaczy awaryjnych

Przedmiotem zamówienia jest dostawa stanowiskowych zasilaczy bezprzerwowych – 52 szt.

1. Przedmiotem zamówienia jest dostawa fabrycznie nowego zasilacza awaryjnego UPS o mocy 1200 VA (660 W), wyposażonego w port USB, przeznaczonego do ochrony sprzętu komputerowego i teleinformatycznego przed skutkami przerw oraz zakłóceń w zasilaniu.
2. Wymagania funkcjonalne i techniczne:
 - 1) Zasilacz UPS typu line-interactive.
 - 2) Moc pozorna: minimum 1200 VA.

- 3) Moc czynna: minimum 660 W.
 - 4) Możliwość podtrzymania pracy minimum jednego stanowiska komputerowego przez co najmniej 14 minut przy typowym obciążeniu.
 - 5) Automatyczna regulacja napięcia (AVR).
 - 6) Możliwość zimnego startu.
 - 7) Automatyczny test baterii oraz ochrona przed głębokim rozładowaniem.
 - 8) Sygnalizacja stanu pracy za pomocą wskaźników LED oraz alarmu dźwiękowego.
 - 9) Port komunikacyjny USB (HID compliant)
 - 10) Liczba gniazd wyjściowych min. 4 (Schuko lub IEC C13)
 - 11) Chłodzenie: aktywne
 - 12) Poziom hałasu: ≤ 35 dB(A)
 - 13) Certyfikaty: CE, RoHS, WEEE, IEC/EN 62040-1/2/3
3. Wymagania dotyczące gwarancji i wsparcia
 - 1) Gwarancja producenta minimum 36 miesięcy.
 - 2) Możliwość realizacji gwarancji na terenie UE.
 - 3) Dostępność wsparcia technicznego online i telefonicznie.
 - 4) Możliwość pobierania aktualizacji oprogramowania i firmware z oficjalnej strony producenta.
 4. Wymagania dodatkowe
 - 1) Urządzenie fabrycznie nowe, z oficjalnej dystrybucji na rynek UE.
 - 2) Komplet akcesoriów: przewód zasilający, instrukcja obsługi.
 - 3) Zgodność z normami bezpieczeństwa i kompatybilności elektromagnetycznej obowiązującymi w UE.

Część nr IV – Dostawa licencji, wdrożenie i utrzymanie systemu SIEM wraz z usługami MIDS

1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja systemu bezpieczeństwa IT, składającego się z dwóch współpracujących ze sobą programów dla min. 40 użytkowników:

- 1) System zarządzania bezpieczeństwem IT - odpowiada za centralne zarządzanie bezpieczeństwem zasobów informatycznych, audyty, zgodność z normami, analizę konfiguracji oraz budowę scoringu bezpieczeństwa.
- 2) Platforma analizy podatności i testów bezpieczeństwa - odpowiada za techniczne testy bezpieczeństwa, wykrywanie podatności, analizę anomalii oraz symulację ataków w infrastrukturze IT.

Oba programy muszą tworzyć spójny system bezpieczeństwa, który umożliwia zarządzanie i analizę bezpieczeństwa na poziomie organizacyjnym oraz technicznym.

- 3) Świadczenie usług doradczych klasy MIDS.

2. CELE I PRZEZNACZENIE SYSTEMU

- 1) Celem wdrożenia systemu jest:
 - a) zapewnienie kompleksowego nadzoru nad bezpieczeństwem infrastruktury IT,
 - b) umożliwienie centralnego zarządzania zasobami, audytami i politykami bezpieczeństwa,
 - c) przeprowadzanie automatycznych i manualnych testów podatności,
 - d) wczesne wykrywanie zagrożeń i reagowanie na incydenty,

- e) weryfikacja zgodności z wymogami prawnymi i normami bezpieczeństwa (RODO, NIS2, ISO 27001).
 - 2) System ma wspierać działania zarówno operacyjne (monitoring, analiza, testy), jak i strategiczne (zarządzanie, raportowanie, zgodność).
3. STRUKTURA SYSTEMU
- 1) System składa się z dwóch głównych komponentów: systemu zarządzania bezpieczeństwem IT oraz platformy analizy i testów bezpieczeństwa.
 - 2) System zarządzania bezpieczeństwem IT
 - a) Charakterystyka ogólna
 - Oprogramowanie musi stanowić zcentralizowany system zarządzania bezpieczeństwem, obejmujący:
 - panel webowy pełniący funkcję centrali zarządzania,
 - usługę instalowaną na komputerach klienckich, realizującą funkcje wykonawcze i transmisję danych,
 - moduły z podstawowym zestawem narzędzi bezpieczeństwa instalowane lokalnie.
 - Oprogramowanie musi posiadać architekturę opartą o podział na Centra Bezpieczeństwa:
 - centrum lokalne,
 - centrum chmurowe,
 - centrum tożsamości,
 - centrum zgodności,
 - centrum aplikacji i usług.
 - Oprogramowanie musi prezentować listę obsługiwanych zasobów w ramach każdego centrum.
 - b) Parametry zasobów
 - Oprogramowanie musi przypisywać każdemu zasobowi minimum 10 parametrów.
 - Pozyskiwanie danych do co najmniej połowy zdefiniowanych parametrów musi być zautomatyzowane.
 - W przypadku zasobów (Serwery, stacje robocze) liczba monitorowanych i zautomatyzowanych parametrów nie może być niższa niż 100 kluczowych dla bezpieczeństwa parametrów na każdy zasób.
 - Oprogramowanie musi umożliwiać instalację agentów na stacjach roboczych oraz serwerach opartych o systemy operacyjne z rodziny Windows, Linux oraz macOS, które:
 - zbierają dane do automatyzacji parametrów,
 - monitorują pracę zasobów,
 - wykonują zaplanowane automatyzacje,
 - zarządzają kluczowymi elementami systemów operacyjnych,
 - wprowadzają polityki bezpieczeństwa,
 - umożliwiają uruchamianie skryptów i operacji zdefiniowanych przez użytkownika.
 - c) Funkcje audytowe i kontrolne
 - Oprogramowanie musi zawierać ponad 300 kontrolek audytowych.

- Każdy zasób musi posiadać co najmniej 5 kontrolek audytowych.
- Oprogramowanie musi umożliwiać przeprowadzanie audytów bezpieczeństwa, zgodności z normami i konfiguracji.

d) Obsługa zasobów

- Minimalna lista obsługiwanych zasobów musi umożliwiać zbieranie danych, monitorowanie, wykonywanie predefiniowanych skryptów, realizować audyty bezpieczeństwa dla następujących typów zasobów:
 - Stacja robocza Windows,
 - Stacja robocza macOS,
 - Serwer Windows lokalny,
 - Serwer Windows publiczny,
 - Serwer Linux lokalny,
 - Serwer Linux publiczny,
 - Urządzenie sieciowe LAN/WAN
 - Router FortiGate,
 - Router MicroTik,
 - Serwery plików NAS
 - Drukarka sieciowa / urządzenie wielofunkcyjne
 - System wirtualizacji Proxmox,
 - Proxmox Backup Server,
 - Virtualmin,
 - Serwer WWW,
 - Serwer FTP,
 - Serwer DNS,
 - Serwer pocztowy IMAP,
 - Serwer pocztowy POSTFIX,
 - Serwer VPN OpenVPN,
 - Serwer VPN Wireguard,
 - Platforma e-commerce PrestaShop,
 - Strona internetowa WordPress,
 - Baza danych MSSQL,
 - Baza danych PostgreSQL,
 - Baza danych MySQL/MariaDB,
 - Microsoft 365 konto pocztowe,
 - Microsoft 365 skrzynka współdzielona,
 - Microsoft 365 Tenant,
 - Microsoft 365 Użytkownik,
 - Adres IP,
 - Domena internetowa,
 - Internet rzeczy,
 - Tożsamość Internetowa,
 - Konto pocztowe (imap),
 - Licencja,
 - Dane osobowe,

- Konto social media Facebook,
 - Agregat prądotwórczy,
 - UPS.
 - Oprogramowanie musi automatycznie wykrywać i proponować dodanie nowych zasobów na bazie pobranych parametrów i umożliwiać ich wdrożenie jednym kliknięciem.
 - Oprogramowanie musi automatycznie tworzyć relacje między zasobami, automatycznie generując mapę powiązań (minimum 50 typów relacji między zasobami) na bazie zebranych w zasobach parametrów.
- e) Aktualizacje i zarządzanie oprogramowaniem
- Oprogramowanie musi posiadać subskrypcje:
 - na aktualizacje baz podatności,
 - na aktualizacje baz zainstalowanego oprogramowania.
 - Oprogramowanie musi umożliwiać wykrywanie, klasyfikowanie, analizowanie, instalowanie, odinstalowywanie, aktualizowanie minimum 200 popularnych programów Windows.
 - Oprogramowanie musi umożliwiać zarządzanie pakietami systemów Linux (apt, yum), w tym instalację, aktualizację i deinstalację co najmniej 50 pakietów.
- f) Wizualizacja i raportowanie
- Oprogramowanie musi wizualizować poziom bezpieczeństwa w formie zestawień, wykresów i rankingów.
 - Oprogramowanie musi generować raporty bezpieczeństwa na podstawie parametrów i zagrożeń poszczególnych zasobów.
 - Oprogramowanie musi posiadać dashboards umożliwiające przegląd sytuacji bezpieczeństwa organizacji.
- g) Moduły dodatkowe i integracje
- Oprogramowanie musi umożliwiać dokupienie kompatybilnych i w pełni obsługiwanych modułów:
 - skanowania podatności i symulacji ataków,
 - kopii zapasowych,
 - analizy poprawności kopii wykonywanych przez systemy zewnętrzne (na podstawie e-maili).
 - Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa (SOAR, EDR, NDR, XDR).
 - Dostawca oprogramowania musi świadczyć usługę tworzenia nowych modułów i integracji na zamówienie, aby dopasować oprogramowanie do konkretnej infrastruktury.
- h) Analiza i bezpieczeństwo danych
- Oprogramowanie musi analizować zależności między logami i zdarzeniami w celu wykrycia wzorców zagrożeń.
 - Oprogramowanie musi alarmować w przypadku wykrycia anomalii lub naruszeń polityk bezpieczeństwa.
 - Oprogramowanie musi przechowywać logi przez określony czas, umożliwiając analizę historyczną.
- i) Zgodność z normami

- Oprogramowanie musi weryfikować zgodność zasobów z normami RODO, NIS2, ISO 27001.
- Oprogramowanie musi prezentować listę parametrów i stan ich zgodności z ww. normami.
- Oprogramowanie musi automatycznie aktualizować punktację po każdej zmianie konfiguracji, wykryciu podatności lub wdrożeniu rekomendacji.
- Oprogramowanie musi budować scoring bezpieczeństwa dla zasobów, centrów i oddziałów, bazując na analizie audytów, relacji, podatności i trendów.

j) Struktura organizacyjna i dostęp

- Oprogramowanie musi umożliwiać podział organizacji na oddziały z przypisywaniem zasobów.
- Oprogramowanie musi zapewniać co najmniej dwustopniową gradację uprawnień.
- Oprogramowanie musi być dostępne w modelach: SaaS, on-premise, hybrydowym i konteneryzowanym.
- Oprogramowanie musi być dostępne w języku polskim.

k) Aplikacje klienckie dla systemu Windows

- Oprogramowanie musi zawierać aplikację umożliwiającą:
 - wyświetlanie poziomu bezpieczeństwa komputera w postaci punktowej (0–100),
 - prezentację informacji o systemie operacyjnym, dysku, pamięci, CPU, zaporze, antywirusie, aktualizacjach i szybkości Internetu.
- Oprogramowanie musi zawierać aplikację umożliwiającą przegląd parametrów bezpieczeństwa i zagrożeń komputera.
- Oprogramowanie musi zawierać aplikację umożliwiającą:
 - sprawdzenie bezpieczeństwa strony internetowej,
 - generowanie bezpiecznych haseł,
 - weryfikację wycieków plików,
 - skanowanie plików w poszukiwaniu wirusów,
 - sprawdzenie bezpieczeństwa haseł.
- Oprogramowanie musi zawierać aplikację umożliwiającą zgłaszanie i monitorowanie zleceń do działu IT, obsługiwanych w panelu webowym.

l) Architektura i Technologia

- Oprogramowanie musi być dostępne jako aplikacja webowa, w pełni responsywna i przystosowana do pracy na urządzeniach desktopowych i mobilnych.
- Oprogramowanie musi być wdrażane w modelach: SaaS, maszyna wirtualna, kontener lub urządzenie fizyczne on-premises.
- Oprogramowanie musi być kompatybilne z popularnymi przeglądarkami (Chrome, Firefox, Edge) oraz systemami operacyjnymi Windows, Linux i macOS.
- Oprogramowanie musi wspierać szyfrowanie komunikacji (TLS 1.2 lub wyższy).
- Oprogramowanie musi być zdolne do pracy w środowiskach konteneryzowanych i wirtualnych z zachowaniem pełnej wydajności.

3) Platforma analizy podatności i testów bezpieczeństwa

- a) System stanowi platformę służącą do wykrywania, analizy i testowania podatności w infrastrukturze IT.
- b) Oprogramowanie umożliwia:
 - pasywne i aktywne skanowanie sieci,
 - detekcję anomalii i zagrożeń,
 - monitorowanie podatności zgodnie ze standardem CVSS,
 - symulację ataków i weryfikację skuteczności zabezpieczeń,
 - działanie w różnych trybach pracy (pasywny, aktywny, symulacyjny),
 - raportowanie wyników i wniosków z testów.
- c) Cel i przeznaczenie systemu
 - Oprogramowanie musi stanowić kompleksową prokformę do analizy bezpieczeństwa sieci komputerowych, wykrywania podatności w infrastrukturze informatycznej jednostki samorządowej.
 - Oprogramowanie musi umożliwiać prowadzenie działań w zakresie testów wewnętrznych (intranetowych),
 - Oprogramowanie musi wspierać procesy audytu bezpieczeństwa, detekcji zagrożeń, reagowania na incydenty oraz weryfikacji skuteczności istniejących zabezpieczeń.
 - Oprogramowanie musi być wykorzystywane przez działy informatyczne, zespoły bezpieczeństwa oraz audytorów w celu oceny stanu zabezpieczeń i doskonalenia polityk bezpieczeństwa.
- d) Zakres zastosowania
 - Oprogramowanie musi być przeznaczone do wykorzystania w jednostkach administracji publicznej.
 - Oprogramowanie musi umożliwiać prowadzenie działań kontrolnych i testowych w sposób bezpieczny, zgodny z polityką bezpieczeństwa Zamawiającego.
 - Oprogramowanie musi być możliwe do wykorzystania w środowisku produkcyjnym (po autoryzacji).
- e) Zakres funkcjonalny
 - Odkrywanie i inwentaryzacja (Passive Discovery)
 - Oprogramowanie musi umożliwiać pasywne, szybkie wykrywanie hostów (ang. quick enumeration) bez generowania aktywnego ruchu sieciowego, który mógłby zostać wykryty przez systemy IDS/IPS.
 - Oprogramowanie musi wykrywać aktywne urządzenia w podsieciach na podstawie obserwowanego ruchu, wykorzystując dane z poziomu ramek ARP, DHCP, DNS, NetBIOS lub innych protokołów warstwy sieciowej.
 - Oprogramowanie musi wspierać monitorowanie i inwentaryzację dowolnej liczby podsieci w obrębie infrastruktury objętej nadzorem.
 - Oprogramowanie musi obsługiwać podsieci VPN, umożliwiając pasywne monitorowanie urządzeń oraz połączeń zestawianych w tunelach VPN.
 - Oprogramowanie musi wykrywać konflikty adresów IP oraz zduplikowane urządzenia w sieci, generując odpowiednie wpisy w logach zdarzeń.
 - Wykrywanie anomalii i ataków
 - Oprogramowanie musi wykrywać próby enumeracji sieci wykonywane przez inne urządzenia lub usługi.

- Oprogramowanie musi rejestrować próby skanowania portów.
- Oprogramowanie musi zawierać dedykowany sensor do wykrywania ataków na porty i usługi, rejestrujący anomalie w ruchu sieciowym.
- Oprogramowanie musi rejestrować i raportować zmiany w strukturze sieci, w tym zmiany adresów IP, rekordów ARP, identyfikatorów VLAN, oraz parametrów wydajnościowych.
- Enumeracja i skanowanie
 - Oprogramowanie musi zawierać moduł pasywnej i aktywnej enumeracji usług, oparty na autorskiej bazie danych zawierającej co najmniej 10 000 rekordów z opisami typów usług, wersji i protokołów wraz z opcją wykupienia subskrypcji na aktualizację bazy danych.
 - Oprogramowanie musi umożliwiać pełnoskalowe skanowanie portów TCP, UDP oraz protokołów warstwy aplikacji w celu identyfikacji uruchomionych usług i aplikacji.
 - Oprogramowanie musi umożliwiać konfigurację zakresu i agresywności skanowania.
- Monitorowanie podatności
 - Oprogramowanie musi automatycznie wykrywać i klasyfikować podatności w infrastrukturze sieciowej, przypisując im poziomy ryzyka zgodne ze standardem CVSS (Common Vulnerability Scoring System).
- Zbieranie danych i gateway
 - Oprogramowanie musi umożliwiać integrację z zewnętrznymi dedykowanymi i kompatybilnymi gateway i sensorami, które rozszerzają zasięg monitorowania o lokalizacje niedostępne dla głównego systemu.
 - Oprogramowanie musi wspierać komunikację z sensorami zewnętrznymi poprzez protokoły szyfrowane (TLS, SSH, VPN).
 - Oprogramowanie musi umożliwiać centralne zarządzanie wszystkimi sensorami z poziomu panelu administracyjnego, w tym monitorowanie ich stanu, aktualizacji i synchronizacji danych.
- Architektura, wdrożenie i utrzymanie
 - Oprogramowanie musi być dostarczone w postaci konteneryzowanej, z obsługą orkiestracji (np. Kubernetes, Docker Swarm), umożliwiającej elastyczne wdrażanie i skalowanie.
 - Oprogramowanie musi umożliwiać wdrożenie w modelach: SaaS, maszyny wirtualnej lub urządzenia fizycznego on-premises.
 - Oprogramowanie musi zawierać mechanizmy automatycznej dystrybucji aktualizacji bezpieczeństwa i baz podatności.
 - Oprogramowanie musi wspierać mechanizmy kopii zapasowych konfiguracji i danych analitycznych, z możliwością przywracania systemu po awarii.
 - Oprogramowanie musi zapewniać zgodność z wymogami bezpieczeństwa określonymi w normach ISO/IEC 27001 lub równoważnych.
- Identyfikacja i klasyfikacja urządzeń
 - Oprogramowanie musi automatycznie identyfikować nazwy hostów i adresy MAC wszystkich urządzeń w sieci.

- Oprogramowanie musi umożliwiać tworzenie profili urządzeń zawierających dane o historii połączeń, wykrytych usługach i potencjalnych podatnościach.
- f) Tryby pracy systemu
- Wymagania ogólne
 - Oprogramowanie musi udostępniać cztery odrębne tryby pracy:
 - tryb uśpienia (Sleep / Stealth Passive),
 - tryb pasywnego skanu (Passive Scan),
 - tryb aktywnego skanu (Active Scan),
 - tryb symulacji ataku (Adversary Emulation).
 - Przełączanie pomiędzy trybami musi być możliwe w czasie rzeczywistym poprzez GUI, API (REST).
 - Wszystkie zmiany trybów pracy muszą być rejestrowane w dzienniku audytu z uwzględnieniem użytkownika, roli, czasu oraz powodu zmiany.
 - Dostęp do przełączania trybów musi być ograniczony do użytkowników z odpowiednimi uprawnieniami w ramach mechanizmu RBAC (role-based access control).
 - Oprogramowanie musi umożliwiać zdalne przełączanie trybów z wykorzystaniem szyfrowanych połączeń TLS.
- g) Tryby operacyjne
- Tryb uśpienia (Sleep / Stealth Passive)

Oprogramowanie musi działać w sposób pasywny, bez generowania ruchu sieciowego, w celu pozostania niewykrywalnym dla systemów IDS/IPS i EDR. Musi wykonywać:

 - pasywne mapowanie topologii sieci,
 - wykrywanie anomalii, korelację zdarzeń,
 - identyfikację potencjalnie skompromitowanych urządzeń.

Wszystkie dane muszą być zapisywane w logach audytowych.
 - Tryb pasywnego skanu (Passive Scan)

Oprogramowanie musi wykonywać działania inwentaryzacyjne i analityczne przy minimalnym ryzyku wykrycia. Musi:

 - skanować porty i usługi z ograniczonym natężeniem ruchu,
 - tworzyć mapę sieci i wykrywać podatności,
 - monitorować zmiany w konfiguracji i widoczności WAN.
 - Tryb aktywnego skanu (Active Scan)

Oprogramowanie musi prowadzić aktywne testy bezpieczeństwa, które mogą być wykrywane przez systemy ochrony. Musi:

 - wykonywać pełnoskalowe skanowanie portów i usług,
 - przeprowadzać testy brute-force,
 - symulować ataki i weryfikować reakcje systemów IDS/IPS,
 - generować szczegółowe raporty z przebiegu testu.
 - Tryb symulacji ataku (Adversary Emulation)

Oprogramowanie musi emulować zachowania atakującego, w tym łączenie technik skanowania, eksploatacji i ukrywania śladów.

Uruchomienie tego trybu musi wymagać formalnej autoryzacji.

System musi prowadzić pełną rejestrację wszystkich działań, w tym logi, rzuty PCAP i raporty końcowe.

h) Ograniczenia i gwarancje bezpieczeństwa

- Oprogramowanie musi zawierać mechanizmy zapobiegające przeciążeniu infrastruktury monitorowanej.
- Oprogramowanie nie może wykorzystywać wykrytych podatności w sposób powodujący szkody lub utratę dostępności usług.
- W trybach innych niż symulacja ataku oprogramowanie musi zapewniać minimalny wpływ na działanie sieci poprzez ograniczenia konfigurowalne (limity połączeń, przepustowości, czasu trwania testów).
- W trybie symulacji ataku działania muszą być wykonywane wyłącznie w ramach autoryzowanego scenariusza i z zachowaniem polityk bezpieczeństwa Zamawiającego.
- Oprogramowanie musi prowadzić ciągły monitoring własnego wpływu na infrastrukturę i generować alerty w przypadku przekroczenia progów bezpieczeństwa.

i) Architektura i technologia

- Oprogramowanie musi być dostępne jako aplikacja webowa, w pełni responsywna i przystosowana do pracy na urządzeniach desktopowych i mobilnych.
- Oprogramowanie musi być wdrażane w modelach: SaaS, maszyna wirtualna, kontener lub urządzenie fizyczne on-premises.
- Oprogramowanie musi być kompatybilne z popularnymi przeglądarkami (Chrome, Firefox, Edge) oraz systemami operacyjnymi Windows, Linux i macOS.
- Oprogramowanie musi wspierać szyfrowanie komunikacji (TLS 1.2 lub wyższy).
- Oprogramowanie musi być zdolne do pracy w środowiskach konteneryzowanych i wirtualnych z zachowaniem pełnej wydajności.

4) Integracja i współdziałanie komponentów

System musi zapewniać pełną interoperacyjność pomiędzy obiema aplikacjami.

W szczególności:

- a) Wymiana danych o podatnościach i wynikach testów - platforma analizy podatności i testów bezpieczeństwa przekazuje do systemu zarządzania bezpieczeństwem informacje o wykrytych podatnościach i wynikach testów, które są automatycznie przypisywane do zasobów w systemie zarządzania.
- b) Wspólna baza zasobów - oba systemy korzystają z jednej bazy identyfikatorów zasobów, co umożliwia powiązanie wyników testów technicznych z audytami organizacyjnymi.
- c) Synchronizacja alertów i raportów - alerty i logi z platformy są agregowane w panelu zarządzania, umożliwiając jednolitą analizę bezpieczeństwa.
- d) Centralny interfejs raportowy - raporty z obu komponentów mogą być konsolidowane w jednym widoku (dashboardzie bezpieczeństwa).
- e) Bezpieczna komunikacja - wymiana danych pomiędzy komponentami musi odbywać się z wykorzystaniem szyfrowanych kanałów (TLS 1.2 lub wyższy).

5) Język, subskrypcje i wsparcie

- a) oprogramowanie musi być dostępne w języku polskim.
- b) dostawca musi zapewnić wsparcie techniczne, aktualizacje oraz możliwość rozszerzenia funkcjonalności o dodatkowe moduły.
- c) dostarczone licencje winny być bezterminowe.
- d) w ramach wdrożenia Wykonawca winien zagwarantować subskrypcję min. do 30 czerwca 2026 r.
- e) subskrypcja systemu zarządzania bezpieczeństwem IT musi obejmować przynajmniej:
 - dostęp do aktualizacji oprogramowania
 - dedykowane wsparcie konsultanta technicznego i merytorycznego
 - dostęp do nowych funkcjonalności
 - wdrażanie nowych funkcjonalności
 - priorytet w opracowywaniu dedykowanych funkcjonalności
 - aktualizowanie bazy oprogramowania (Windows, Linux, MacOS)
 - aktualizacje integracji z zewnętrznymi systemami
- f) subskrypcja platformy analizy podatności i testów bezpieczeństwa musi obejmować przynajmniej:
 - aktualizowanie bazy podatności
 - aktualizowanie danych heurystycznych
 - dostęp do nowych funkcjonalności
 - wdrażanie nowych funkcjonalności
 - dedykowane wsparcie konsultanta technicznego i merytorycznego
 - dostęp do aktualizacji oprogramowania
 - priorytet w opracowywaniu dedykowanych funkcjonalności
 - aktualizacje baz sygnatur
 - aktualizacje integracji z zewnętrznymi systemami
- g) wykonawca, w ramach subskrypcji zobowiązany będzie do realizacji usług klasy Managed Intrusion Detection System (MIDS), realizowanych w trybie pomocy zdalnej dotyczącej konsultacji i merytorycznego wsparcia w zakresie takich działań jak:
 - konfiguracja urządzeń, sieci (w tym segmentacji), podpięcie licencji
 - hardening systemów operacyjnych Windows i Linux, w tym:
 - minimalizacja usług
 - minimalizacja pakietów
 - usunięcie fingerprint
 - konfiguracja UTM
 - wdrożenie lokalnych systemów IDS/IPS oraz zasad
 - konfiguracja wystawionych publicznie usług pod kątem zwiększenia bezpieczeństwa
 - wdrożenie kont uprzywilejowanych zgodnie z procedurą least privilege
 - integracja z kolektorami logów
 - hardening sieci:
 - ograniczenie ruchu east-west
 - konfiguracja UTM
 - zmniejszenie widoczności WAN
 - segmentacja sieci (VLAN)

- Konfiguracja NTP
- konfiguracja DNS
- wymuszenie szyfrowanych połączeń
- integracja z kolektorami logów

4. Instruktaż stanowiskowy:

- 1) Zamawiający wymaga przeprowadzenia instruktażu stanowiskowego z obsługi dostarczonego rozwiązania dla min. 2 osób. Instruktaż musi zostać przeprowadzony stacjonarnie w siedzibie Zamawiającego, w języku polskim z wykorzystaniem dostarczonego rozwiązania.
- 2) Instruktaż stanowiskowy musi pozwolić na uzyskanie wiedzy teoretycznej oraz praktycznych umiejętności niezbędnych w administrowaniu dostarczonym oprogramowaniem.