

*Zestawienie tabelaryczne sprzętu informatycznego i oprogramowania dla części 2 - załącznik nr 8b*

Gmina Rawicz  
ul. Marszałka Józefa Piłsudskiego 21  
63-900 Rawicz  
Tel. 65 616 49 80  
e-mail: [umg@rawicz.eu](mailto:umg@rawicz.eu)

## Opis Przedmiotu Zamówienia

**Dostawa sprzętu informatycznego i oprogramowania  
w ramach projektu „Cyberbezpieczny Samorząd”  
na potrzeby Gminy Rawicz  
Część 2 – Dostawa serwerów z oprogramowaniem**



## SPIS TREŚCI

1. SERWER TYP 1 DLA DLA JEDNOSTKI PODLEGŁEJ (OŚRODEK SPORTU I REKREACJI W RAWICZU) – WYMAGANIA MINIMALNE 3
2. SERWER TYP 2 DLA DLA JEDNOSTKI PODLEGŁEJ (ZAKŁAD USŁUG KOMUNALNYCH W RAWICZU) – WYMAGANIA MINIMALNE 9
3. OPROGRAMOWANIE SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) TYP 2 DLA DLA JEDNOSTEK PODLEGŁYCH (OŚRODEK SPORTU I REKREACJI W RAWICZU ORAZ ZAKŁAD USŁUG KOMUNALNYCH W RAWICZU) – WYMAGANIA MINIMALNE .... 13



## 1. Serwer typ 1 dla dla Jednostki Podległej (Ośrodek Sportu i Rekreacji w Rawiczu) – wymagania minimalne

Nazwa	Minimalne wymagania dla sprzętu
<b>Typ</b>	Serwer typ 1 dla Ośrodka Sportu i Rekreacji w Rawiczu
<b>Obudowa</b>	<ul style="list-style-type: none"> <li>Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.</li> <li>Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.</li> <li>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.</li> </ul>
<b>Płyta główna</b>	<ul style="list-style-type: none"> <li>Płyta główna z możliwością zainstalowania do dwóch procesorów.</li> <li>Na płycie głównej musi znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci</li> <li>Płyta główna musi obsługiwać do 1TB pamięci RAM.</li> </ul>
<b>Chipset</b>	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
<b>Procesor</b>	Zainstalowany jeden procesor minimum 16-rdzeniowy, min. 2.4 GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 237 w teście SPECrate2017_int_base dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla dwóch procesorów.
<b>RAM</b>	minimum 128GB
<b>Funkcjonalność pamięci RAM</b>	<ul style="list-style-type: none"> <li>Advanced ECC,</li> <li>Memory Page Retire,</li> <li>Fault Resilient Memory,</li> <li>Memory Self-Healing lub PPR,</li> <li>Partial Cache Line Sparing</li> </ul>
<b>Gniazda PCI</b>	minimum dwa sloty PCIe
<b>Interfejsy sieciowe/SAS</b>	Wbudowane minimum 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
<b>Dyski twarde</b>	<ul style="list-style-type: none"> <li>Zainstalowane: <ul style="list-style-type: none"> <li>Minimum 2x dysk SSD SATA o pojemności minimum 480GB, Hot-Plug.</li> <li>Minimum 4x dysk SATA o pojemności minimum 8TB, Hot-Plug.</li> </ul> </li> <li>Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności minimum 240GB Hot-Plug z możliwością konfiguracji RAID 1.</li> <li>Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności minimum 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.</li> </ul>
<b>Kontroler RAID</b>	<p>Sprzętowy kontroler dyskowy, posiadający</p> <ul style="list-style-type: none"> <li>Minimum 8GB nieulotnej pamięci cache,</li> <li>Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.</li> <li>Wsparcie dla dysków samoszyfrujących.</li> </ul>

<b>Wbudowane porty</b>	<ul style="list-style-type: none"> <li>• Przednie: minimum 1x VGA, minimum 1x USB 2.0, minimum 1x USB dedykowane dla karty zarządzającej,</li> <li>• Tylne: minimum 1x VGA, minimum 2x USB w tym 1x USB 3.0,</li> </ul>
<b>Video</b>	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości minimum 1920x1200
<b>Zasilacze</b>	Redundantne, Hot-Plug maksymalnie 1100W klasy Titanium
<b>System operacyjny</b>	<p>Zakres Przedmiotu Zamówienia obejmuje dostarczenie Oprogramowania Systemowego zwanego dalej SSO. Zamawiający wymaga dostarczenia min. 15 sztuk licencji dostępowych do zakupionego serwera.</p> <p>Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.</p> <p>SSO musi posiadać następujące, wbudowane cechy:</p> <ul style="list-style-type: none"> <li>a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,</li> <li>b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,</li> <li>c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,</li> <li>d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,</li> <li>e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,</li> <li>f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,</li> <li>g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.</li> <li>h) wbudowane wsparcie instalacji i pracy na wolumenach, które:             <ul style="list-style-type: none"> <li>I. pozwalają na zmianę rozmiaru w czasie pracy systemu,</li> <li>II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</li> <li>III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</li> <li>IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL),</li> </ul> </li> <li>i) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,</li> <li>j) wbudowane szyfrowanie dysków</li> <li>k) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,</li> <li>l) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,</li> <li>m) wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,</li> <li>n) graficzny interfejs użytkownika,</li> </ul>

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

	<p>nn) 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,</p> <p>oo) 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,</p> <p>pp) 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),</p> <p>qq) v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,</p> <p>rr) w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),</p> <p>ss) x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,</p> <p>tt) y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,</p> <p>uu) z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p>
<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>• Zatrzaszk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.</li> <li>• Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li> <li>• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</li> <li>• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>• Moduł TPM 2.0</li> <li>• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</li> <li>• Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).</li> </ul>
<b>Karta Zarządzania</b>	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:</p> <ul style="list-style-type: none"> <li>• zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> <li>• zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li> <li>• szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li> <li>• możliwość podmontowania zdalnych wirtualnych napędów;</li> <li>• wirtualną konsolę z dostępem do myszy, klawiatury;</li> <li>• wsparcie dla IPv6;</li> <li>• wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li> <li>• możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li> <li>• możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;</li> <li>• integracja z usługą katalogową;</li> <li>• możliwość obsługi przez dwóch administratorów jednocześnie;</li> <li>• wsparcie dla dynamic DNS;</li> </ul>



	<ul style="list-style-type: none"> <li>wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li> <li>możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</li> <li>możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</li> </ul> <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"> <li>Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej</li> <li>Przesyłanie danych telemetrycznych w czasie rzeczywistym</li> <li>Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze</li> <li>Automatyczna rejestracja certyfikatów (ACE)</li> </ul>
Oprogramowanie do zarządzania	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none"> <li>Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</li> <li>integracja z usługą katalogową</li> <li>Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li> <li>Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish</li> <li>Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li> <li>Szczegółowy opis wykrytych systemów oraz ich komponentów</li> <li>Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li> <li>Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li> <li>Grupowanie urządzeń w oparciu o kryteria użytkownika</li> <li>Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji</li> <li>Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li> <li>Szybki podgląd stanu środowiska</li> <li>Podsumowanie stanu dla każdego urządzenia</li> <li>Szczegółowy status urządzenia/elementu/komponentu</li> <li>Generowanie alertów przy zmianie stanu urządzenia.</li> <li>Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li> <li>Integracja z service desk producenta dostarczonej platformy sprzętowej</li> <li>Możliwość przejęcia zdalnego pulpitu</li> <li>Możliwość podmontowania wirtualnego napędu</li> <li>Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li> <li>Możliwość importu plików MIB</li> <li>Przesyłanie alertów „as-is” do innych konsol firm trzecich</li> <li>Możliwość definiowania ról administratorów</li> <li>Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li> <li>Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li> <li>Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li> <li>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</li> </ul>

	<p>sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</p> <ul style="list-style-type: none"> <li>• Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li> <li>• Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile</li> <li>• Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li> <li>• Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li> <li>• Zdalne uruchamianie diagnostyki serwera.</li> <li>• Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</li> <li>• Oprogramowanie dostarczane jako wirtualny appliance</li> </ul>
<b>Certyfikaty</b>	<ul style="list-style-type: none"> <li>• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub z normami równoważnymi</li> <li>• Serwer musi posiadać deklaracja CE lub z normami równoważnymi</li> </ul>
<b>Dokumentacja użytkownika</b>	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
<b>Wdrożenie</b>	<p>W ramach dostawy sprzętu Wykonawca zobowiązany jest do wykonania następujących usług:</p> <ul style="list-style-type: none"> <li>• Konfiguracja serwera: <ul style="list-style-type: none"> <li>○ stworzenie planu wdrożenia polegający na wykonaniu schematów wdrażanej infrastruktury uwzględniający położenie serwera wirtualizacyjnego w wskazanej przez Zamawiającego szafie rack.</li> <li>○ montażu w/w sprzętu w szafie rack w sposób zgodny z zaleceniami producenta dostarczanych serwerów.</li> </ul> <p>Prowadzenie kabli nie może powodować zaburzeń w cyrkulacji gorącego powietrza wydmuchiwanego z serwerów. uruchomienie systemu operacyjnego wraz z aktualizacją do najnowszych wersji systemu operacyjnego oraz oprogramowania układowego serwera.</p> <ul style="list-style-type: none"> <li>○ podłączenia serwera do wskazanej przez Zamawiającego infrastruktury sieciowej za pomocą właściwych kabli zapewniający bezawaryjną i ciągłą pracę w przypadku awarii jednej z kart sieciowych serwera</li> <li>○ wykonać testy niezawodności środowiska serwerowego poprzez odłączanie jednej ze ścieżki/wyłączanie urządzenia oraz test redundancji zasilania.</li> </ul> </li> <li>• Wykonawca musi przygotować niezbędną dokumentację w zakresie dokumentacji powdrożeniowej zawierającej opis konfigurowanych opcji wdrożonego środowiska serwerowego.</li> <li>• Wymaga się aby wdrożenie było przeprowadzone przez inżynierów (minimum 1 osoba) posiadających wiedzę na temat dostarczanego modelu serii serwerów danego producenta.</li> </ul>



**Warunki gwarancji**

- Gwarancja producenta na minimum 36 miesięcy, świadczona przez podmiot posiadający ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych. Na potwierdzenie wymogu wymagane jest dołączenie oświadczenia producenta na etapie podpisania umowy z Zamawiającym, potwierdzającego, że serwis oferowanego serwera będzie:
  - realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta;
  - firma serwisująca posiada autoryzację producenta oferowanego serwera;
  - firma serwisująca posiada ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych.
- Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.
- Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
- Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych.
- Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.
- Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
- Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
- Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.
- Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.
- Zamawiający w ramach gwarancji wymaga dodatkowo usługi, w ramach której, w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Na potwierdzenie, że oferowany serwer będzie posiadał odpowiednią gwarancję, wymagane jest dołączenie oświadczenia producenta oferowanego sprzętu na etapie podpisania umowy z Zamawiającym,

Ilość

1 szt.

**2. Serwer typ 2 dla Jednostki Podległej (Zakład Usług Komunalnych w Rawiczu) – wymagania minimalne**

Nazwa	Minimalne wymagania dla sprzętu
Typ	Serwer typ 2 dla Zakładu Usług Komunalnych w Rawiczu

<b>Obudowa</b>	<ul style="list-style-type: none"> <li>Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiającym montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.</li> <li>Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.</li> <li>Obudowa z możliwością wyposażenia 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.</li> </ul>
<b>Płyta główna</b>	<ul style="list-style-type: none"> <li>Płyta główna z możliwością zainstalowania do dwóch procesorów.</li> <li>Na płycie głównej musi znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci</li> <li>Płyta główna musi obsługiwać do 1TB pamięci RAM.</li> </ul>
<b>Chipset</b>	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
<b>Procesor</b>	Zainstalowany jeden procesor 16-rdzeniowy, min. 2.4 GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 231 w teście SPECrate2017_int_base dostępnym na stronie <a href="http://www.spec.org">www.spec.org</a> dla dwóch procesorów.
<b>RAM</b>	minimum 64GB
<b>Funkcjonalność pamięci RAM</b>	<ul style="list-style-type: none"> <li>Advanced ECC,</li> <li>Memory Page Retire,</li> <li>Fault Resilient Memory,</li> <li>Memory Self-Healing lub PPR,</li> <li>Partial Cache Line Sparing</li> </ul>
<b>Gniazda PCI</b>	minimum jeden slot PCIe x16
<b>Interfejsy sieciowe/SAS</b>	Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
<b>Dyski twarde</b>	<ul style="list-style-type: none"> <li>Zainstalowane min.: <ul style="list-style-type: none"> <li>2x dysk SSD SATA MU o pojemności min. 480GB, 6Gb, 2,5" Hot-Plug.</li> <li>2x dysk SAS o pojemności min. 2.4TB, 12Gb, 2,5" Hot-Plug.</li> </ul> </li> <li>Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.</li> <li>Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde</li> </ul>
<b>Kontroler RAID</b>	Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
<b>Wbudowane porty</b>	<ul style="list-style-type: none"> <li>Przednie: minimum 1x VGA, minimum 1x USB 2.0, minimum, 1x USB dedykowane dla karty zarządzającej,</li> <li>Tylne: minimum 1x VGA, minimum 2x USB w tym 1x USB 3.0,</li> </ul>
<b>Video</b>	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości minimum 1600x900
<b>Wentylatory</b>	Redundantne
<b>Zasilacze</b>	Redundantne, Hot-Plug maksymalnie 700W klasy Titanium
<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>Zatrzaśk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.</li> <li>Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</li> </ul>

	<ul style="list-style-type: none"> <li>• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</li> <li>• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>• Moduł TPM 2.0</li> <li>• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</li> <li>• Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania.</li> </ul>
<b>Karta Zarządzania</b>	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:</p> <ul style="list-style-type: none"> <li>• zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> <li>• zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li> <li>• szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li> <li>• możliwość podmontowania zdalnych wirtualnych napędów;</li> <li>• wirtualną konsolę z dostępem do myszy, klawiatury;</li> <li>• wsparcie dla IPv6;</li> <li>• wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li> <li>• możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li> <li>• możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;</li> <li>• integracja z Active Directory;</li> <li>• możliwość obsługi przez dwóch administratorów jednocześnie;</li> <li>• wsparcie dla dynamic DNS;</li> <li>• wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li> <li>• możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</li> <li>• możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</li> </ul> <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"> <li>• Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej</li> <li>• Przesyłanie danych telemetrycznych w czasie rzeczywistym</li> <li>• Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze</li> <li>• Automatyczna rejestracja certyfikatów (ACE)</li> </ul>
<b>Oprogramowanie do zarządzania</b>	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none"> <li>• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych</li> <li>• integracja z usługą katalogową</li> <li>• Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta</li> <li>• Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish</li> <li>• Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram</li> <li>• Szczegółowy opis wykrytych systemów oraz ich komponentów</li> <li>• Możliwość eksportu raportu do CSV, HTML, XLS, PDF</li> <li>• Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.</li> <li>• Grupowanie urządzeń w oparciu o kryteria użytkownika</li> </ul>

	<ul style="list-style-type: none"> <li>• Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji</li> <li>• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach</li> <li>• Szybki podgląd stanu środowiska</li> <li>• Podsumowanie stanu dla każdego urządzenia</li> <li>• Szczegółowy status urządzenia/elementu/komponentu</li> <li>• Generowanie alertów przy zmianie stanu urządzenia.</li> <li>• Filtry raportów umożliwiające podgląd najważniejszych zdarzeń</li> <li>• Integracja z service desk producenta dostarczonej platformy sprzętowej</li> <li>• Możliwość przejęcia zdalnego pulpitu</li> <li>• Możliwość podmontowania wirtualnego napędu</li> <li>• Kreator umożliwiający dostosowanie akcji dla wybranych alertów</li> <li>• Możliwość importu plików MIB</li> <li>• Przesyłanie alertów „as-is” do innych konsol firm trzecich</li> <li>• Możliwość definiowania ról administratorów</li> <li>• Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów</li> <li>• Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)</li> <li>• Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta</li> <li>• 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.</li> <li>• Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.</li> <li>• Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile</li> <li>• Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.</li> <li>• Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.</li> <li>• Zdalne uruchamianie diagnostyki serwera.</li> <li>• Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.</li> <li>• Oprogramowanie dostarczane jako wirtualny appliance</li> </ul>
<b>Certyfikaty</b>	<ul style="list-style-type: none"> <li>• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 lub z normami równoważnymi</li> <li>• Serwer musi posiadać deklarację CE lub z normami równoważnymi</li> </ul>
<b>Dokumentacja użytkownika</b>	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>
<b>Warunki gwarancji</b>	<ul style="list-style-type: none"> <li>• Gwarancja producenta na minimum 36 miesięcy, świadczona przez podmiot posiadający ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych. Na potwierdzenie wymogu wymagane jest</li> </ul>

	<p>dołączenie oświadczenia producenta na etapie podpisania umowy z Zamawiającym, potwierdzającego, że serwis oferowanego serwera będzie:</p> <ul style="list-style-type: none"> <li>- realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta;</li> <li>- firma serwisująca posiada autoryzację producenta oferowanego serwera;</li> <li>- firma serwisująca posiada ISO 9001:2015 (lub równoważną) oraz ISO-27001 (lub równoważną) na świadczenie usług serwisowych.</li> </ul> <ul style="list-style-type: none"> <li>• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.</li> <li>• Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>• Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych.</li> <li>• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.</li> <li>• Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</li> <li>• Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.</li> <li>• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.</li> <li>• Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.</li> <li>• Zamawiający w ramach gwarancji wymaga dodatkowo usługi, w ramach której, w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Na potwierdzenie, że oferowany serwer będzie posiadał odpowiednią gwarancję, wymagane jest dołączenie oświadczenia producenta oferowanego sprzętu na etapie podpisania umowy z Zamawiającym</li> </ul>
Ilość	1 szt.

**3. Oprogramowanie SIEM (Security Information and Event Management) typ 2 dla Jednostek Podległych (Ośrodek Sportu i Rekreacji w Rawiczu oraz Zakład Usług Komunalnych w Rawiczu) – wymagania minimalne**

Nazwa	Minimalne wymagania dla oprogramowania
Typ	Oprogramowanie SIEM (Security Information and Event Management) typ 2 dla Ośrodka Sportu i Rekreacji w Rawiczu oraz Zakładu Usług Komunalnych w Rawiczu
Wymagania ogólne	Zamawiający wymaga dostarczenia rozwiązania spełniającego wymagania minimalne:



1. Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:
  - System operacyjny musi być oparty na licencji Open Source.
  - Platformą sprzętową dla rozwiązania centralnego składowania dzienników musi być w sieci Zamawiającego serwer fizyczny.
  - Architektura systemu musi bazować na komponentach o licencjonowaniu Open Source
  - Zamawiający na wyżej wymieniony cel planuje przeznaczyć serwer:
    - serwer typ 1 dla dla jednostki podległej (Ośrodek Sportu i Rekreacji w Rawiczu) - opisanym w punkcie 6 OPZ
    - serwer typ 2 dla dla jednostki podległej (Zakład Usług Komunalnych w Rawiczu) opisanym w punkcie 7 OPZ
  - Tworzenie użytkowników w systemie centralnego składowania logów musi odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (usługą katalogową) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
  - System centralnego składowania dzienników zdarzeń musi mieć możliwość zdefiniowania dowolnej liczby skonfigurowanych źródeł danych, m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.
  - System centralnego składowania dzienników zdarzeń musi mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport.
  - System centralnego składowania dzienników zdarzeń musi udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trybie ReadOnly (tylko do odczytu) na urządzeniach z dowolną przeglądarką WWW.
  - System centralnego składowania dzienników zdarzeń musi pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.
  - System centralnego składowania dzienników zdarzeń musi mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).
2. W zakresie wdrożenia proponowanego rozwiązania wykonawca musi wykonać następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:
  - Instalacja systemu operacyjnego na wybranym przez Zamawiającego serwerze.
  - Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspoźnienie zegarów czasów sieci Zamawiającego.



	<ul style="list-style-type: none"> <li>• Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracją parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.</li> <li>• Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.</li> <li>• Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły: <ul style="list-style-type: none"> <li>• Urządzenie klasy UTM</li> <li>• Przetącniki zarządzalne</li> <li>• Serwery fizyczne</li> <li>• Serwery wirtualizacji</li> <li>• stacje roboczych</li> </ul> </li> <li>• aplikację centralnego zarządzania posiadanego antywirusa łącznie z modulem XDR</li> <li>• aplikację do monitorowania infrastruktury</li> <li>• Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.</li> <li>• Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.</li> <li>• Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.</li> <li>• Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.</li> <li>• Konfiguracja wysyłania powiadomień poprzez maila w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.</li> <li>• Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.</li> </ul>
Gwarancja i asysta techniczna	<ul style="list-style-type: none"> <li>• Zamawiający wymaga, aby Wykonawca w czasie od wdrożenia rozwiązania do 25.04.2026 roku zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.</li> <li>• Zamawiający wymaga, aby Wykonawca w okresie od wdrożenia rozwiązania do 25.04.2026 roku świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.</li> <li>• Zamawiający wymaga, aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.</li> <li>• Zamawiający akceptuje fakt, że każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.</li> </ul>
Ilość	2 szt.