**Serwer logów:**

**1 sztuka**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

# Przedmiot zamówienia

# Dostawa i montaż centralnego serwera logów - z analizą logów sieciowych, serwerowych i stacji końcowych

Zamawiający wymaga dostawy i montażu urządzenia typu serwer o specyfikacji:

* Obudowa: Rack z szynami, o wysokości max. 2U
* Procesor: zainstalowany procesor osiągający w teście CPU Benchmark publikowanym na stronie: https://www.cpubenchmark.net/ wynik CPU Mark co najmniej 20.000 punktów na dzień publikacji ogłoszenia
* Pamięć RAM: minimum 64GB typu DDR4/DDR5
* Ilość slotów pamięci: min. 16
* Kontrolery I/O: RAID SAS/SATA dla dysków SSD lub NVMe
* poziomy RAID: 0, 1, 10, 5
* Zarządzanie: kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0
* Interfejsy sieciowe: min. 1x Ethernet 10GbE SFP+, 1x RJ45 1GbE
* Pamięć masowa: min. 3 dyski SSD lub NVMe o pojemności min. 4TB
* Pamięć masowa dodatkowa: 1 dysk SSD lub NVMe o pojemności min. 4TB (poza pulą)
* Zasilacz: 2 redundantne zasilacze HotPlug o sprawności min. 94%
* Bezpieczeństwo: Zintegrowany z płytą główną moduł TPM 2.0

**Wraz z instalacją serwera wymagane jest wdrożenie oprogramowania do zbierania i analizy logów sieciowych, serwerowych i stacji końcowych obejmujących wymagania:**

* Centralny serwer logów uruchomiony w środowisku wirtualnym klasy Linux z dostępem do zarządzania za pomocą przeglądarki internetowej z aktywnym certyfikatem SSL.
* Wymagana instalacja agentów na stanowiskach roboczych, pracujących pod kontrolą systemów operacyjnych: Windows 10/11, Windows Server 2019/2022/2025, Linux Debian/Ubuntu (łącznie 45 sztuk)
* System powinien umożliwiać zbieranie logów w zakresie co najmniej:
* Logów zdarzeń systemu, w tym m.in.:
  + informacje, ostrzeżenia i błędy generowane przez aplikacje.
  + zdarzenia związane z komponentami systemu operacyjnego.
  + zdarzenia dotyczące bezpieczeństwa, takie jak logowania, zmiany uprawnień, próby dostępu nieautoryzowanego.
  + informacje o instalacjach i aktualizacjach systemu.
* Monitorowania integralności, w tym, m.in.:
  + Wykrywanie zmian w krytycznych plikach systemowych, katalogach i plikach konfiguracyjnych.
  + Śledzenie modyfikacji, tworzenia i usuwania plików, co może wskazywać na aktywność złośliwego oprogramowania lub nieautoryzowane działania.
* Monitorowanie rejestru systemu, w tym m.in. (dotyczy OS z rodziny Microsoft):
  + Śledzenie zmian w kluczach i wartościach rejestru.
  + Wykrywanie prób modyfikacji ustawień systemowych lub aplikacji.
* Informacje o procesach i usługach, w tym m.in.:
  + Monitorowanie uruchomionych procesów i usług.
  + Wykrywanie uruchomienia nieznanych lub podejrzanych aplikacji.
  + Wykrywanie nieautoryzowanych instalacji lub zmian w konfiguracji sprzętowej.
  + Analiza systemu pod kątem obecności ukrytych procesów, modułów kernelowych i innych oznak infekcji.
* Logi z zapory ogniowej i programów antywirusowych, w tym m.in.:
  + Zbieranie zdarzeń z Windows Defender, zapory ogniowej Windows i innych narzędzi zabezpieczających.
  + Monitorowanie prób włamań, blokowanych połączeń i wykrytych zagrożeń.
* Monitorowanie sieci, w tym m.in.:
  + Zbieranie informacji o aktywnych połączeniach sieciowych.
  + Śledzenie otwartych portów i aktywności sieciowej.
* System powinien umożliwiać wizualizację i analizę danych, wyszukiwanie, archiwizację oraz monitorowanie i raportowanie w formie graficznej.
* Na serwerze powinny być przechowywane logi z urządzeń UTM
* Czas przechowywania wszystkich logów: min. 2 lata

# Opis zasad warunków równoważności:

1. Za równoważne do wyspecyfikowanego rozwiązania Zamawiający uzna rozwiązanie o tym samym przeznaczeniu, cechach technicznych, jakościowych i funkcjonalnych odpowiadających cechom technicznym, jakościowym i funkcjonalnym wskazanych w opisie przedmiotu zamówienia, lub lepszych, oznaczonych innym znakiem towarowym, patentem lub pochodzeniem.
2. Rozwiązanie równoważne musi pozwalać na zrealizowanie zakładanego przez Zamawiającego celu poprzez parametry wydajnościowe i funkcjonalne, mające wpływ na skuteczność działania, takie same lub lepsze od wskazanych wymagań minimalnych.
3. Użycie w opisie przedmiotu zamówienia nazw rozwiązań, materiałów i urządzeń służy ustaleniu minimalnego standardu wykonania i określenia właściwości i wymogów technicznych założonych w dokumentacji technicznej dla projektowanych rozwiązań.
4. Wykonawca zobligowany jest do wykazania, że oferowane rozwiązania równoważne spełnią zakładane wymagania minimalne.
5. Brak określenia „minimum” oznacza wymaganie na poziomie minimalnym, a Wykonawca może zaoferować rozwiązanie o lepszych parametrach.
6. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega lub jest lepsze od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym.
7. Nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób.
8. Przez bardzo zbliżoną (podobną) wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego.