

OPIS PRZEDMIOTU ZAMÓWIENIA	
<p>Przedmiot zamówienia obejmuje niżej wymieniony asortyment.</p> <p>Wykonawca zobowiązany jest do dostawy, instalacji, konfiguracji, uruchomienia, wdrożenia oraz przeprowadzenia szkolenia użytkowników w zakresie prawidłowej obsługi dostarczonego sprzętu i/lub oprogramowania.</p>	
Cecha/Funkcjonalność	Minimalne parametry wymagane przez Zamawiającego
Zakup oprogramowania do gromadzenia logów z serwerów, urządzeń sieciowych – 1 szt.	
Ogólne	<p>Przedmiotem zamówienia jest dostawa, wdrożenie, konfiguracja oraz uruchomienie systemu klasy SIEM (Security Information and Event Management) w wersji open source do centralnego zbierania, analizy i wizualizacji logów z infrastruktury informatycznej Zamawiającego.</p> <p>Oprogramowanie musi zapewniać funkcjonalności umożliwiające skuteczne monitorowanie bezpieczeństwa systemów, detekcję incydentów oraz wsparcie w analizie zdarzeń.</p>
Wymagania funkcjonalne systemu	<p>Oprogramowanie musi umożliwiać co najmniej:</p> <ul style="list-style-type: none"> • Zbieranie i konsolidację logów • Obsługa logów z różnych źródeł: serwery, stacje robocze, urządzenia sieciowe, systemy operacyjne, aplikacje i usługi. • Obsługa standardów: Syslog, GELF, JSON, CSV, REST API. • Możliwość odbierania logów w czasie rzeczywistym. • Przechowywanie i indeksowanie danych • Wydajne gromadzenie i indeksowanie dużych wolumenów danych logów. • Obsługa szybkiego wyszukiwania danych historycznych. • Mechanizmy retencji danych z możliwością definiowania okresów przechowywania. • Analiza i wizualizacja • Interfejs webowy do wyszukiwania, filtrowania oraz analizy logów. • Tworzenie dashboardów z wizualizacjami (wykresy, alerty, statystyki). • Możliwość budowania zapytań warunkowych na podstawie wielu parametrów. • Alertowanie i obsługa incydentów • Konfiguracja reguł alertów na podstawie wykrytych zdarzeń. • Powiadomienia o zdarzeniach przez e-mail, webhooks lub integracje z innymi systemami bezpieczeństwa. • Wysoka dostępność i skalowalność • Możliwość pracy w architekturze klastrowej. • Obsługa rozproszonych węzłów indeksujących i przetwarzających dane. • Obsługa mechanizmów load-balancingu. • Bezpieczeństwo i zarządzanie dostępem • Integracja z mechanizmami LDAP/Active Directory. • Definiowanie ról i uprawnień użytkowników. • Szyfrowanie danych w tranzycie i w spoczynku.
Wymagania techniczne	<ul style="list-style-type: none"> • System musi być dostępny w modelu open source, bez dodatkowych kosztów licencyjnych.

	<ul style="list-style-type: none"> • Musi być kompatybilny z systemami Linux (np. Ubuntu, Debian, CentOS). • Oprogramowanie musi być przystosowane do instalacji na maszynie wirtualnej • Oprogramowanie musi być aktywnie rozwijane i posiadać aktualizacje bezpieczeństwa. • Preferowane rozwiązania oparte na architekturze Elasticsearch / OpenSearch. • System musi umożliwiać integrację poprzez REST API • Oprogramowanie musi być przystosowane do instalacji na maszynie wirtualnej • Oprogramowanie nie powinno wymagać więcej niż 1 instancji serwera wirtualnego
Wymagania dotyczące wdrożenia	<p>W ramach realizacji zamówienia Wykonawca zobowiązany jest do:</p> <ul style="list-style-type: none"> • dostarczenia i instalacji oprogramowania na serwerach Zamawiającego, • przeprowadzenia konfiguracji wstępnej, • utworzenia minimum 2 przykładowych dashboardów i reguł alertów, • przeprowadzenia szkolenia administratorów w zakresie obsługi systemu, • przekazania dokumentacji powdrożeniowej.
Wymagania dotyczące wsparcia	<p>Zamawiający wymaga zapewnienia dostępu do oficjalnej dokumentacji producenta.</p> <p>Wykonawca zapewni wsparcie techniczne w trakcie okresu wdrożenia oraz przez 30 dni po jego zakończeniu.</p>
Dodatkowe wymagania	<p>Oprogramowanie musi być wolne od opłat licencyjnych i dostępne na zasadach licencji open source (np. SSPL).</p> <p>Rozwiązanie musi być zgodne z obowiązującymi przepisami w zakresie ochrony danych osobowych i RODO.</p> <p>Wersja oprogramowania musi być stabilna i wspierana przez producenta.</p>
Gwarancja	30.06.2026 r.

