# Załącznik nr 2 do zapytania ofertowego

# OPIS PRZEDMIOTU ZAMÓWIENIA - OPROGRAMOWANIE DO ANALIZY LOGÓW

# Wstęp

Niniejszy dokument stanowi szczegółowy opis przedmiotu zamówienia na zakup, dostarczenie i wdrożenie oprogramowania.

# 2. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1. sprzedaż, dostarczenie i konfiguracja oprogramowania;
2. przeszkolenie wyznaczonych pracowników Zamawiającego w zakresie obsługi i konfiguracji oprogramowania
3. udzielenie przez Wykonawcę gwarancji i zapewnienie serwisu gwarancyjnego na dostarczone oprogramowanie na okres 36 m-cy.
4. udzielenie licencji na oprogramowanie;
5. dostarczenie przez Wykonawcę dokumentacji wykonanej konfiguracji;
6. Wykonawca musi przedstawić pełną specyfikację oferowanego programu w odniesieniu do przedstawionej szczegółowej specyfikacji oprogramowania

# 3. Zakres zamówienia i termin realizacji

Zamawiający wymaga, aby dostawa do Zamawiającego nastąpiła w terminach określonych w poniższej tabeli.

|  |  |  |  |
| --- | --- | --- | --- |
| LP | Przedmiot dostawy | Liczba | Termin dostawy –  liczba dni od podpisania umowy  (max) |
| 1 | Dostawa Oprogramowania  i Wykonanie konfiguracji | 1 | 90 |

Sposób wykonania zamówienia:

Wykonawca dostarcza oprogramowanie i w ustalonym terminie dokonuje jego konfiguracji na aktualnej infrastrukturze Zamawiającego.

Instalacja obejmuje także zainstalowanie niezbędnej maszyny wirtualnej.

Wykonawca przeszkoli wskazane osoby Zamawiającego w wymiarze 16 godzin, szkolenie może mieć formę zdalną.

Zestawienie sprzętu objętego wdrożeniem:

Zamawiający posiada:

- 2 serwery fizyczne

- 4 serwery wirtualne

- 3 switche zarządzalne cisco

- 1 switch zarządzalny zyxel

- 1 switch zarządzalny hp

- UTM Stormshield

- ok. 30 stacji roboczych

- 13 drukarek sieciowych

- 2 kontrolery zdalnego dostępu do serwerów

|  |  |
| --- | --- |
| **Charakterystyka (wymagania minimalne)** | **Oferowane parametry techniczne** |
| Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:   * 1. System operacyjny powinien być na licencji Open Source. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source   2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego z wirtualizatorem Hyper-V   3. Zamawiający na wyżej wymieniony cel planuje przeznaczyć maszynę wirtualną o parametrach: 8 vCPU, 8 GB RAM oraz dysk twardy HDD min. 2TB.   4. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.   5. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się 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.   6. System centralnego składowania dzienników zdarzeń powinien 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.   7. System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.   8. System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.   9. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów). |  |
| 1. W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego zbierania i analizy logów:    1. Instalacja systemu operacyjnego na wybranej przez Zamawiającego maszynie wirtualnej.    2. 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 uspójnienie zegarów czasów sieci Zamawiającego.    3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.    4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów obowiązujących aktów prawnych i dobrych praktyk występujących w środowisku Zamawiającego.    5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:    6. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.    7. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.    8. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.    9. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.    10. Konfiguracja wysyłania powiadomień poprzez maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.    11. Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu. |  |
| Gwarancja i asysta techniczne:   * 1. Zamawiający wymaga aby Wykonawca w czasie od wdrożenia do okresu realizacji projektu tj. 19.06.2026 r. zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.   2. Zamawiający wymaga aby Wykonawca w czasie od wdrożenia do okresu realizacji projektu tj. 19.06.2026 r. świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.   3. Zamawiający wymaga aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 7.30 a 15.30.   4. Zamawiający akceptuje fakt, ze 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.  1. Zamawiający wymaga aby Wykonawca zorganizował i przeprowadził w swojej siedzibie lub innym miejscu nie zależnym od Zmawiającego konsultacje z zarządzenia i administracji wdrożonego systemu. 2. Zamawiający wymaga aby usługa konsultacji została zrealizowana w terminie do 3 miesięcy od wdrożenia usługi. 3. Konsultacje udzielone zostaną dwóm osobom wskazanym przez Zamawiającego. 4. Zamawiający wymaga aby w trakcie konsultacji realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym systemem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych. 5. Wymagana zagadnienia konsultacyjne:    1. Wstęp do zarządzania logami    2. System centralnego składowania logów – wymagania, architektura oraz różnice w wersjach    3. Instalacja i konfiguracja ogólnych ustawień systemu centralnego składowania logów    4. Zbieranie logów, czyli konfiguracja metod pozyskiwania dzienników zdarzeń.    5. Przetwarzanie dzienników zdarzeń, czyli tworzenie strumieni logów, ich parsowanie oraz filtrowanie    6. Wizualizacja logów czyli tworzenie czytelnych zestawień tabelarycznych i graficznych    7. Konfiguracja alertów i powiadomień.    8. Administracja i utrzymanie systemu centralnego składowania logów    9. Case Study czyli praktyczne przykłady użycia systemu centralnego składowania logów |  |
| Zamawiający wymaga aby konsultacje zamykały się w ramach czasowych 2 dni roboczych (2 x 7 godz.) |  |