Załącznik nr 1 do szacowania OR.272.2.2023

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest wdrożenie rozwiązania do centralnego składowania dzienników zdarzeń w Starostwie Powiatowym w Gołdapi w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotyczący realizacji projektu grantowego „Cyfrowy Powiat” o numerze POPC.05.01.00-00-0001/21-00.

**I.** **Nazwa i adres Zamawiającego:**

**Powiat Gołdapski**

**ul. Krótka 1**

**19-500 Gołdap**

Osoba do kontaktu:

Łukasz Dębowski, tel. 87 615 44 05

email: lukasz.debowski@powiatgoldap.pl

**II. Tryb udzielania zamówienia:**

Do niniejszego postępowania nie ma zastosowania ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.) – wyłączenie zgodnie z brzmieniem art. 2 ust. 1 pkt 1 ustawy. Postępowanie prowadzone jest zgodnie z procedurami określonymi w Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020 zgodnie z zasadą konkurencyjności oraz Zarządzeniem nr 1/2021 Starosty Gołdapskiego z dnia 04 stycznia 2021 w sprawie regulaminu udzielania zamówień publicznych, których wartość szacunkowa jest mniejsza niż 130 000 złotych netto.

**III. Szczegółowy opis przedmiotów zamówienia:**

1. Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:

1.1. System operacyjny powinien być na licencji Open Source (przykładowo Ubuntu 18.04 lub 20.04, Debian Linux 10, CentOS 8 lub nowsze).

1.2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego wirtualna maszyna w środowisku Hyper-V.

1.3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source, przykładowo:

* MongoDB oraz Elasticsearch.

1.4. Zamawiający na wyżej wymieniony cel planuje przeznaczyć maszynę wirtualną o parametrach minimalnych: procesor (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 4TB.

1.5. Tworzenie użytkowników w systemie centralnego składowania logów powinno odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.

1.6. Konta użytkowników w systemie powinny podlegać regulacją pozwalającym na przypisanie ról dla poszczególnych pracowników departamentu IT. Wymagane jest minimalnie, aby system pozwalał na kreowanie ról dostępowych do systemu, które pozwalają na przyznawanie m.in. pełnych uprawnień do systemu, roli menadżera alarmów, operatora widoków nawigacyjnych (dashboardów), dostępu tylko do odczytu do wybranych zestawów danych.

1.7. 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.

1.8. 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.

1.9. System centralnego składowania dzienników zdarzeń powinna 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.

1.10. 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.

1.11. 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).

1.12. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia lub importowania listy z pliku do użycia w źródłach wejściowych.

2. W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:

2.1. Instalacja systemu operacyjnego na wybranych przez Zamawiającego maszynie wirtualnej.

2.2. 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.

2.3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.

2.4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.

2.5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:

• (1x) Urządzenie klasy UTM firmy Fortinet

• (4x) Przełączniki zarządzalne firmy HPE

• (11x) Serwery Windows (3 serwery fizyczne 8 maszyn wirtualnych)

• (1x) Serwery Linux

• (58x) stacji roboczych Windows 10 i 11

• (1x) Aplikację centralnego zarządzania ESET Endpoint Security

• (2x) Serwery NAS

• (1x) Macierz dyskowa

• (1x) Jednostka kontrolna monitoringu środowiskowego serwerowni Vutlan

2.6. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.

2.7. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.

2.8. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.

2.9. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.

2.10. Konfiguracja wysyłania powiadomień poprzez maila w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.

2.11. Szkolenie pracowników z obsługi wdrożonego systemu.

3. Gwarancja i asysta techniczne:

3.1. Zamawiający wymaga aby Wykonawca w czasie do 12 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.

3.2. Zamawiający wymaga aby Wykonawca w okresie do 12 miesięcy od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.

3.3. Zamawiający wymaga aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 15.30.

3.4. 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.

**IV. Warunki realizacji zamówienia**

Zamawiający nie dopuszcza możliwości składania ofert częściowych.

Miejsce wdrożenia rozwiązania: Starostwo Powiatowe w Gołdapi, ul. Krótka 1, 19-500 Gołdap

**IV. Termin wykonania zamówienia**

Termin wykonania zamówienia: do 14 dni od podpisania umowy.

**V. Zastrzeżenia:**

1. Zamawiający zastrzega sobie prawo:

a) do nie wyłonienia żadnego z oferentów bez podawania uzasadnienia.

b) do przeprowadzenia dodatkowych negocjacji w przypadku wpływu identycznych ofert.

**VI. Opis kryteriów oceny oferty**

Przy wyborze oferty zamawiający będzie się kierował następującymi kryteriami**: kryterium cena 80% oraz długość wsparcia technicznego 20% .**

**VII. Warunki płatności:**

1. Podstawą do rozliczenia pomiędzy Zamawiającym, a Wykonawcą jest faktura – płatna w terminie do 21 dni licząc od dnia jej otrzymania przez Zamawiającego. Płatność nastąpi przelewem na konto Wykonawcy wskazane na fakturze.

2. Za datę zapłaty uważa się dzień uznania rachunku Wykonawcy.

3. Podstawą wystawienia faktury jest protokół odbioru ilościowego i jakościowego, podpisany przez upoważnionych przedstawicieli Zamawiającego i Wykonawcy.