**Opis przedmiotu zamówienia**

**część 3: System do gromadzenia, monitorowania i analizy logów z urządzeń w Urzędzie Miejskim w Nowym Tomyślu**

# Szczegółowe wymagania techniczne dla systemu do gromadzenia, monitorowania i analizy logów z urządzeń w Urzędzie Miejskim w Nowym Tomyślu. W ramach postępowania wymaganym jest dostarczenie centralnego systemu gromadzenia i analizy logów o poniższych parametrach.

Wymagana dostawa systemu wraz z wdrożeniem i implementacją w środowisku zamawiającego zgodnie z wymaganiami zamawiającego. Sprawdzenie poprawności działania przedmiotu zamówienia w środowisku zamawiającego oraz szkoleniem z obsługi systemu.

Miejsce dostawy: Urząd Miejski w Nowym Tomyślu, ul. Poznańska 33, 64-300 Nowy Tomyśl

|  |  |
| --- | --- |
| **L.p.** | **Wymagania minimalne** |
| **1.** | Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń: |
| 1.1. | System operacyjny powinien być na licencji Open Source. |
| 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 |
| 1.4. | Zamawiający na wyżej wymieniony cel planuje przeznaczyć maszynę wirtualną  o parametrach procesor (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 1,76 TB. Dodatkowo zamawiający dopuszcza wykorzystanie posiadanego przez zamawiającego NAS o pojemności 10 TB do przechowywania danych. |
| 1.5. | 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. |
| 1.6. | 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. |
| 1.7. | 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. |
| 1.8. | 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. |
| 1.9. | 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. |
| 1.10. | 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). |
| **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: • (2x) UTM - Stormshiled, Fortigate • (8x) Przełączników zarządzalnych - DCN, TP-LINK, FORTIGATE • (2x) Serwery LINUX • (8x) Serwery WINDOWS • (90x) Stacji roboczych WINDOWS 10 i 11 • (1x) Aplikacje centralnego zarządzania oprogramowania antywirusowego Z możliwością rozszerzenia o: UTM - CISCO SWITCH - CISCO, FORTIGATE, HPE ARUBA Serwer wirtualizacje VMware ESX Serwer Zarządzania wirtualizacją VMware vCenter |
| 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 lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami. |
| **3.** | **Gwarancja i asysta techniczne:** |
| 3.1. | Zamawiający wymaga aby Wykonawca w czasie 24 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu. |
| Zamawiający wymaga aby Wykonawca w okresie do 30.06.2026 r. świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów. |
| 3.2. | Zamawiający wymaga aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 15.30. |
| 3.3. | 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. |