**Załącznik nr 1d do SWZ**

**Opis Przedmiotu Zamówienia**

1. Przedmiotem zamówienia jest dostawa wraz z instalacją i uruchomieniem na wskazanym przez Zamawiającego serwerze fizycznym lub wirtualnym oprogramowania centralnego systemu logów, integracja tego systemu z posiadanym UTM oraz instalacja systemu do wizualizacji i korelacji alertów IDS z systemem logów.
2. Usługa zostanie wykonana w siedzibie zamawiającego w terminie 30 dni od daty podpisania umowy. Skrócenie terminu stanowi kryterium oceny ofert.
3. Zakres zadań obejmuje instalację i pierwszą konfigurację systemu logów, instalację systemu do wizualizacji i analizy logów i konfigurację początkową w sieci LAN Zamawiającego oraz pierwsze uruchomienie.
4. Ponadto w zakres usługi wchodzi przeszkolenie 2 wskazanych pracowników zamawiającego z administrowania systemem oraz wsparcie techniczne w zakresie użytkowania systemów przez okres do 12.03.2026 r., w godzinach pracy zamawiającego.
5. Zamawiający zapewni serwer fizyczny lub wirtualny niezbędny do instalacji systemu serwera logów zgodnie z wymaganiami i ustaleniami z Wykonawcą, które zostaną ustalone po podpisaniu umowy.

Wymagania w odniesieniu do rozwiązania serwera logów:

1. rozwiązanie jest przeznaczone do spełnienia wymagań KRI w odniesieniu do zbieranych logów oraz czasu ich przechowywania, w założeniu dla max. 150 źródeł (urządzenia, programy, stacje użytkowników);
2. rozwiązanie jest przeznaczone do centralnego zbierania logów z urządzeń i wskazanych programów oraz przechowywania ich przez okres szacunkowo 2 lat, z możliwością efektywnego przeszukiwania oraz automatyczną retencją starszych wpisów,
3. rozwiązanie musi polegać na instalacji centralnego serwera logów na serwerze (np. rozwiązania zbliżone do Graylog) fizycznym lub wirtualnym Zamawiającego, Zamawiający samodzielnie skonfiguruje wszystkie urządzenia podłączone do sieci, w celu zbierania z nich logów systemowych, po uzyskaniu wskazań od Wykonawcy (np. nr portów, protokołów itp.),
4. rozwiązanie musi polegać na zapisie logów do dedykowanej bazy danych, umieszczonej na tym samym serwerze, o takich zdolnościach, aby była wydolna przy przeszukiwaniu i retencji danych, przy założeniu zapisu z ok. 150 urządzeń przez okres 2 lat (np. rozwiązania zbliżone do OpenSearch/ElasticSearch – dedykowane przez producenta rozwiązania programowego logu do wskazanego rozwiązania zbierania logów),
5. rozwiązanie musi zapewniać agentowe i bezagentowe zbieranie logów,
6. rozwiązanie musi zapewniać wizualizacje danych, dla pulpitów tworzonych przez administratorów z wybranymi założeniami, musi umożliwiać intuicyjne/ustandaryzowane tworzenie zapytań i szybki dostęp do rezultatów;
7. rozwiązanie musi zapewniać powiadamianie (np. e-mail) o generowanych alertach;
8. rozwiązanie musi być bezobsługowe tzn. nie wymagać ingerencji operatora do zbierania logów, ich retencji, musi samodzielnie startować w przypadku zaniku i pojawienia się zasilania;