Warszawa, 15 stycznia 2026 r.

Zapytanie o wycenę w celu ustalenia szacunkowej wartości zamówienia na dostawę urządzenia do logowana i analizy ruchu sieciowego z urządzeń Fortigate

Urząd Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych w Warszawie (02-222), Al. Jerozolimskie 181C, przekazuje zapytanie w celu ustalenia szacunkowej wartości zamówienia.

Proszę o wycenę przedmiotu zamówienia uwzględniając niżej przedstawione informacje.

1. Przedmiot zamówienia

Przedmiotem zamówienia będzie dostawa urządzenia do logowana i analizy ruchu sieciowego z urządzeń Fortigate wg poniższej specyfikacji:

Oferowane rozwiązanie musi mieć możliwość pobrania lub migracji danych z posiadanego urządzenia Fortinet FortiAnalyzer 300F i być kompatybilne z posiadanymi przez zamawiającego urządzeniami/systemami producenta FortiNet: Fortigate, FortiMail, FortiClient EMS, umożliwiając odbiór, analizę oraz przechowywanie zbieranych zdarzeń oraz posiadać minimalne parametry:

Parametry fizyczne:

- wyposażony w minimum 4 porty Gigabit Ethernet RJ-45,
- zasoby dyskowe co najmniej 8 TB,
- zasilacz AC.

Parametry wydajnościowe:

- zdolność odbioru - minimum 80 GB zdarzeń dziennie,
- zdolność analizy ruchu - minimum 2000 logów na sekundę,
- zdolność kolekcjonowania logów z co najmniej 20 systemów,
- możliwość zastosowania mechanizmu zabezpieczającego przed utratą danych w przypadku awarii nośnika: minimalnie RAID 0,1.

Logowanie

- podgląd zdarzeń w czasie rzeczywistym,
- możliwość przeglądania i filtrowania logów historycznych,
- wbudowane lub edytowalne raporty graficzne lub tekstowe wizualizujące stan pracy urządzenia oraz informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej listy oraz informacje:
    - najczęściej wykrywanych ataków,
    - najczęściej wykorzystywanych aplikacji,
    - najczęściej odwiedzanych stron www,
    - najbardziej aktywnych użytkowników,
    - krajów, do których nawiązywane są połączenia,
    - najczęściej wykorzystywanych polityk Firewall,
    - o realizowanych połączeniach IPSec.
- możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych danych,
- komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.

System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie:

- generowanie raportów co najmniej w formatach: PDF, CSV,

- predefiniowane lub edytowalne zestawy raportów, dla których można modyfikować parametry prezentowania wyników,
- funkcję definiowania własnych raportów,
- możliwość spolszczenia raportów, jeżeli zaoferowane rozwiązanie nie jest polskojęzyczne,
- generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

- korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany,
- konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa,
- wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne w tym co najmniej:
    - malware,
    - aplikacje sieciowe,
    - email,
    - IPS,
    - ruch sieciowy,
    - systemowe tj. utracone połączenie VPN, sieciowe.

Zarządzanie:

- System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów:
    - HTTPS,
    - SSH,
    - lub producent rozwiązania musi dostarczać dedykowaną konsoli zarządzania, która komunikuje się z rozwiązaniem wykorzystując szyfrowane protokoły.
- Proces uwierzytelniania administratorów musi być realizowany w oparciu o:
    - lokalną bazę,
    - Radius,
    - LDAP,
    - PKI.
- System musi umożliwiać utworzenie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których dostarczane są zdarzenia.

Obecnie posiadane urządzenie: FortiAnalyzer 300F pozostaje w dyspozycji zamawiającego.

Rozwiązanie musi być posiadać wsparcie techniczne umożliwiającym dostarczenie sprzętu zastępczego na czas naprawy przez okres 12 miesięcy.

2. Termin realizacji zamówienia

Wykonawca zobowiązany będzie do dostarczenia w terminie do **30 dni** od dnia podpisania umowy, urządzeń zgodnych ze powyższą specyfikacją oraz wymaganych dokumentów.

3. Wycena

Przesłana wycena powinna zawierać wszystkie koszty, związane z realizacją zamówienia z uwzględnieniem warunków wskazanych w Zapytaniu.

4. Składanie ofert szacunkowych

Odpowiedzi na niniejsze Zapytanie należy udzielić, nie później niż do dnia **26.01.2026 r**., pocztą elektroniczną na adres email: **jacek.piliszczuk@urpl.gov.pl**.

5. Inne

Informujemy, że przedmiotowe zaproszenie nie stanowi ofert w rozumieniu art. 66 KC ani też nie jest ogłoszeniem o zamówieniu w rozumieniu ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych (Dz. U. z 2024 r,

poz. 1320 ze zm.) i ma ono wyłącznie na celu rozeznanie cenowe rynku wśród wykonawców mogących zrealizować powyższe zamówienie oraz uzyskanie wiedzy na temat szacunkowych kosztów związanych z planowanym zamówieniem publicznym.

Klauzula informacyjna o zasadach przetwarzania Państwa/Pani/Pana danych osobowych dostępna jest pod adresem: https://www.urpl.gov.pl/pl/daneosobowe