ZAŁĄCZNIK NR 1.1 do PFU

Analizator logów dla brzegowego urządzenia UTM

L.p.	Parametr	Wymagania techniczne
1	Architektura systemu ochrony	System logowania i raportowania powinien stanowić centralne repozytorium danych gromadzonych przez wiele urządzeń oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców.
2	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.
3	Parametry fizyczne systemu	System może zostać uruchomiony na dedykowanej przez producenta platformie sprzętowej lub na niezależnym serwerze, którego parametry będą co najmniej wystarczające do realizacji wszystkich funkcji analizatora - przy założeniu że nominalne obciążenie procesora (wszystkie rdzenie) przy obsłudze wszystkich urządzeń sieciowych użytych do realizacji projektu nie przekroczy 25%, a zajętość pamięci nie przekroczy 30%.
4	Funkcjonalności podstawowe i uzupełniające	System musi zapewniać: • Odbieranie danych z urządzeń zewnętrznych przez protokół syslog (TCP i UDP). • Składowanie oraz archiwizację logów z możliwością ich grupowania w oparciu o urządzenia, użytkowników. • Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. • Wyświetlanie nowych logów w czasie rzeczywistym. • Wizualizację danych w postaci wykresów.

		• Export zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych) w postaci otwartych formatów (CSV, JSON). • Dostęp do wyszukiwania danych przez HTTP API.
5	Parametry wydajnościowe	Urządzenie musi obsługiwać: – minimum 250 urządzeń sieciowych jednocześnie.
6	Zarządzanie	System udostępnia: – Lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS