**CZĘŚĆ 1:**

**Urządzenie do analizy logów ruchu sieciowego**

|  |
| --- |
| **Oferowane urządzenie:** |
| Model urządzenia / oznaczenie producenta: | podać |
| **Parametry techniczne:** |
| lp. | Parametr | Minimalna wartość wymagana: | Parametr oferowany: |
| 1 | **Typ urządzenia** | Centralny system logowania, raportowania i korelacji, umożliwiający centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń opartej o produkty posiadane przez zamawiającego tj. * FortiGate,
* FortiWeb,
* FortiAP,
* Fortimail.

Rozwiązanie musi być dostarczone w postaci komercyjnej platformy sprzętowej. |  |
| 2 | **Gniazda i porty** | System musi dysponować co najmniej:* 4 porty Gigabit Ethernet RJ45
* 2 gniazda SFP 1 Gbps
 |  |
| 3 | **Powierzchnia dyskowa** | Powierzchnia dyskowa min. 16 TB z rozbudową o mechanizm zabezpieczający przed utratą danych w przypadku awarii nośnika – minimum RAID 0,1,5,10 |  |
| 5 | **Zasilanie** | Redundantne zasilanie AC |  |
|  | **Obsługa logów** | * System musi być w stanie przyjmować min 200GB logów na dzień
* System musi być w stanie przeanalizować min. 4000 logów na sekundę
* Rozwiązanie musi umożliwić kolekcjonowanie logów z co najmniej 800 systemów
* Podgląd logowań w czasie rzeczywistym
* **Możliwość przeglądanie logów historycznych z funkcją filtrowania**
	+ ***NIE – 0 pkt.***
	+ ***TAK – 40 pkt.***
 | podać element punktowany |
|  | **Raportowanie** | System musi oferować predefiniowane podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą zawierać co najmniej:* Liczbę najczęściej wykrywanych ataków
* Liczbę najbardziej aktywnych użytkowników
* Liczbę najczęściej wykorzystywanych aplikacji
* Listę najczęściej odwiedzanych stron www
* Listę krajów, do których nawiązywane są połączenia
* Listę najczęściej wykorzystywanych polityk firewall
* Informacja o realizowanych połączeniach VPN IPsec
* Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie posiadać mechanizmy filtrowania dla wysyłanych logów
* 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 co najmniej w formatach PDF, CSV
* Funkcje definiowania własnych raportów
* Możliwość spolszczenia raportów
* Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesyłania wyników na określony adres lub adresy email
 |  |
|  | **Korelacja logów** | W zakresie korelacji zdarzeń system musi zapewnić:* Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany
* Konfiguracje powiadomień przez: email, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych i bezpieczeństwa
* Wybór kategorii zdarzeń dla których tworzone będą reguły korelacyjne. System ma korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: Malware, aplikacje sieciowe, email, IPS, Traffic, Systemowe: utracone połączenie VPN, utracone połączenia sieciowe
 |  |
|  | **Zarządzanie** | System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH |  |
|  | **Administratorzy** | * Proces uwierzytelnienia administratorów musi być realizowany w oparciu o: lokalną bazę danych, Radius, LDAP,PKI
* System musi umożliwić definiowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
 |  |
|  | **Serwisy i licencje** | Gwarancja:* System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi również zapewnić dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7
 |  |
|  | **Opis do wymagań ogólnych** | Dostawca winien wraz z dostawą przedłożyć dokument pochodzący od importera stwierdzający ze przy wprowadzeniu urządzenia na terytorium Polski zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004, Nr 229, poz. 2315 z późniejszymi zmianami) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. |  |
|  | **Gwarancja i wsparcie** | Gwarancja:System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi również zapewnić dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 |  |