**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – CZĘŚĆ IV**

|  |  |
| --- | --- |
| **L.p.** | **Parametry wymagane** |
| 1. **Urządzenie aktywne do zabezpieczenia sieci teleinformatycznej – 1 szt.**
 |
| 1 | **Wymagania Ogólne:**1. w ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń,
2. rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
 |
| 2 | **Interfejsy, dysk, zasilanie:**1. system musi dysponować co najmniej 2 portami Gigabit Ethernet RJ-45,
2. rozwiązanie musi dysponować powierzchnią dyskową minimum 4 TB.
 |
| 3 | **Parametry wydajnościowe:**1. system musi być w stanie przyjmować minimum 100 GB logów na dzień,
2. system musi być w stanie przeanalizować minimum 3000 logów na sekundę,
3. rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 150 systemów.
4. **W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje**:

logowanie:1. podgląd logowanych zdarzeń w czasie rzeczywistym,
2. możliwość przeglądania logów historycznych z funkcją filtrowania,
3. system musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
* listę najczęściej wykrywanych ataków,
* listę najbardziej aktywnych użytkowników,
* listę najczęściej wykorzystywanych aplikacji,
* listę najczęściej odwiedzanych stron www,
* listę krajów , do których nawiązywane są połączenia,
* listę najczęściej wykorzystywanych polityk Firewall,
* informacje o realizowanych połączeniach IPSec,
1. rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów,
2. 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,
3. 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 **-** w zakresie raportowania system musi zapewniać:1. generowanie raportów co najmniej w formatach: HTML, PDF, CSV,
2. predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników,
3. funkcję definiowania własnych raportów,
4. możliwość spolszczenia raportów,
5. generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email,

korelacja logów **-** w zakresie korelacji zdarzeń system musi zapewniać:1. korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany,
2. konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa,
3. wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
* Malware,
* aplikacje sieciowe,
* email,
* IPS,
* Traffic,
* systemowe: utracone połączenie VPN, utracone połączenie sieciowe.
 |
| 4 | **Zarządzanie:**1. system logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów,
2. proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI,
3. system musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
 |
| 5 | **Gwarancja -** 36 miesięcy. |

|  |  |
| --- | --- |
| **L.p.** | **Parametry wymagane** |
| 1. **Odnowienie na kolejny rok usługi rocznego wsparcia dla urządzenia FortiGate - FG60C UTM – 1 szt.**
 |
| **Odnowienie na kolejny rok usługi rocznego wsparcia technicznego i aktualizacji dla urządzeń FortiGate – FG60C UTM Bundle (8x5 FortiCare plus NGFW, AV, Web Filtering and Antispam Services).** Rozpoczęcie usługi musi być liczone od dnia następującego po ostatnim dniu upływu okresu świadczenia aktualnie obowiązującej usługi. Numer urządzenia zmawiającego: FGT60C3G11028367 |

|  |  |
| --- | --- |
| **L.p.** | **Parametry wymagane** |
| 1. **Odnowienie na kolejny rok usługi rocznego wsparcia dla urządzenia FortiGate – FG30D UTM – 1 szt.**
 |
| **Odnowienie na kolejny rok usługi rocznego wsparcia technicznego i aktualizacji dla urządzeń FortiGate – FG30D UTM Bundle (8x5 FortiCare plus NGFW, AV, Web Filtering and Antispam Services).** Rozpoczęcie usługi musi być liczone od dnia następującego po ostatnim dniu upływu okresu świadczenia aktualnie obowiązującej usługi. Numer urządzenia zmawiającego: FGT30D3X14007168 |