*Załącznik nr 2 – formularz ofertowy techniczny (część nr 1)*

*Zakup specjalistycznego oprogramowania oraz sprzętu w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych wykorzystywanych w Szpitalu (sygnatura: ZP/2501/104/22)*

*Uwaga: Wykonawca zostaje zobowiązany do uzupełnienia kolumny „Oferowane parametry” o opis spełnienia wymaganych minimalnych parametrów technicznych. Zamawiający wymaga ponadto, aby* ***przedmiotowe środki dowodowe, złożone wraz z ofertą,*** *potwierdziły sporządzony przez wykonawcę opis.*

1. **Analyser**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry**  **(wymagany opis)** |
| 1. | Wymagania Ogólne | 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.  Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP). |  |
| 2. | Interfejsy, Dysk: | System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB. |  |
| 3. | Parametry wydajnościowe: | 1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.  2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów. |  |
| 4. | 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:  a. Listę najczęściej wykrywanych ataków.  b. Listę najbardziej aktywnych użytkowników.  c. Listę najczęściej wykorzystywanych aplikacji.  d. Listę najczęściej odwiedzanych stron www.  e. Listę krajów , do których nawiązywane są połączenia.  f. Listę najczęściej wykorzystywanych polityk Firewall.  g. Informacje o realizowanych połączeniach IPSec.  4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.  5. 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.  6. 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. |  |
| 5. | Raportowanie | W zakresie raportowania system musi zapewniać:  1. Generowanie raportów co najmniej w formatach: 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. |  |
| 6. | 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. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie. |  |
| 7. | 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.  a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.  2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |  |
| 8. | Serwisy i licencje | Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24 godz. przez 7 dni w tygodniu.  W ramach usług wynikających z udzielonej gwarancji jakości oraz technicznego Wykonawca zapewnia:   1. udostępnienie poprawek do Oprogramowania Aplikacyjnego, w przypadku stwierdzenia przez Zamawiającego błędu Oprogramowania Aplikacyjnego: 2. w przypadku tzw. błędu krytycznego, tj. takiego, który uniemożliwia użytkowanie Oprogramowania Aplikacyjnego (w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika) i prowadzi do zatrzymania jego eksploatacji, utraty danych lub naruszenia ich spójności, w wyniku których niemożliwe jest prowadzenie działalności z użyciem Oprogramowania Aplikacyjnego:    * + 1. reakcja Wykonawcy na zgłoszenie Zamawiającego (tj. czas od otrzymania zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego „błędu krytycznego”) 1 dzień roboczy;        2. czas dokonania i udostępnienia Zamawiającemu odpowiednich korekt Oprogramowania Aplikacyjnego wyniesie do 3 dni roboczych od chwili rozpoczęcia czynności serwisowych;        3. w przypadku wystąpienia „błędu krytycznego”, Wykonawca, po uzyskaniu od Zamawiającego zgody, może wprowadzić tzw. rozwiązanie tymczasowe, doraźnie rozwiązujące problem błędu krytycznego; w takim przypadku dalsza obsługa usunięcia dotychczasowego błędu krytycznego będzie traktowana jako błąd zwykły; 3. w pozostałych przypadkach, określanych jako „błędy zwykłe” - błędy Oprogramowania Aplikacyjnego inne niż błędy krytyczne:    * + 1. czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od otrzymania zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego błędu zwykłego) wynosi do 15 dni roboczych;        2. czas dokonania i udostępnienia Zamawiającemu odpowiednich korekt Oprogramowania Aplikacyjnego wyniesie do 60 dni roboczych od chwili rozpoczęcia czynności serwisowych; |  |

|  |  |
| --- | --- |
| miejscowość: |  |
| data: |  |

(podpis pieczątka imienna osoby upoważnionej

do składania oświadczeń woli w imieniu Wykonawcy)