

Opis przedmiotu zamówienia dla części 2

Zaproponowany sprzęt musi być kompletny, posiadać niezbędne instrukcje umożliwiające spełnianie swoich funkcji. Sprzęt musi być wolny od obciążeń prawami osób trzecich; posiadać dołączone niezbędne materiały dotyczące użytkowania w języku polskim (preferowany) lub angielskim. Sprzęt powinien być kompletny posiadający wszelkie kable, podzespoły, oprogramowanie, nośniki itp., niezbędne do jego prawidłowego użytkowania, gotowy do uruchomienia i użytkowania bez dodatkowych zakupów. Wszystkie dostarczone urządzenia powinny być fabrycznie nowe, posiadać wszelkie certyfikaty zezwalające na sprzedaż na terenie Unii Europejskiej oraz pochodzić z oficjalnych kanałów sprzedaży producenta.

Wykonawca powinien przedstawić oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

WYMAGANIA

1. Termin dostawy przedmiotu do 30 dni kalendarzowych od daty zawarcia umowy. Termin realizacji zamówienia stanowi poza cenowe kryterium oceny ofert i uzależniony jest od oferty Wykonawcy, nie może być jednak dłuższy niż 30 dni kalendarzowych.
2. Przedmiot umowy dostawca dostarczy do miejsca wskazanego przez Zamawiającego.
3. Na minimum 3 dni przed dostawą Wykonawca przedstawi zamawiającemu numery seryjne sprzętu w celu ewentualnej weryfikacji.
4. Odbiór przedmiotu zamówienia nastąpi u Zamawiającego po wykonaniu dostawy i sporządzeniu protokołu zdawczo-odbiorczego przez Wykonawcę i podpisaniu przez obie strony.

5. Wykonawca udziela gwarancji na przedmiot umowy –potwierdzony w karcie gwarancyjnej:

System centralnego logowania, raportowania i korelacji z licencją na okres 60 miesięcy

6. Wykonawca zapewni bezpłatny serwis w okresie gwarancyjnym.

7. Serwis gwarancyjny świadczony będzie w miejscu użytkowania sprzętu (siedziba Zamawiającego). Wykonawca zapewni bezpłatny dojazd serwisanta do siedziby Zamawiającego. Jednakże w przypadku kiedy serwisant stwierdzi konieczność wykonania naprawy w serwisie Wykonawcy, Wykonawca zapewni na własny koszt odbiór sprzętu do naprawy i jego dostawę po dokonaniu naprawy oraz dostarczenie sprzętu zastępczego na czas naprawy o nie gorszych parametrach w Następnym Dniu Roboczym po zgłoszeniu awarii.

8. Dedykowany adres email lub portal techniczny (dołączyć adres portalu) producenta lub autoryzowanego partnera ma umożliwiać Zamawiającemu zgłaszanie awarii komputera. Obsługa zgłoszeń ma odbywać się w języku polskim.

9. W przypadku wystąpienia awarii w okresie gwarancyjnym Wykonawca przystąpi do jej usunięcia w czasie nie dłuższym niż 48 godzin od daty zgłoszenia awarii. W wyniku awarii komputera, dyski twarde zostają u Zamawiającego chyba, że Zamawiający zdecyduje inaczej.

10. W przypadku awarii wynikłych z niewłaściwej eksploatacji sprzętu przez Zamawiającego (co powinno być potwierdzone sporządzonym przez producenta sprzętu protokołem), Wykonawca ma prawo do żądania zapłaty za działania serwisowe w oparciu o aktualne właściwe cenniki po wcześniejszym uzgodnieniu i zaakceptowaniu kosztów naprawy przez Zamawiającego.

11. Wszystkie dostarczone urządzenia powinny być fabrycznie nowe, posiadać wszelkie certyfikaty zezwalające na sprzedaż na terenie Unii Europejskiej oraz pochodzić z oficjalnych kanałów sprzedaży producenta.

1. System centralnego logowania, raportowania i korelacji z licencją na okres 60 miesięcy

Wymagania Ogólne

W ramach postępowania wymagany 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 sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Interfejsy, Dysk, Zasilanie:

1. System musi dysponować co najmniej:
 - 2 portami Gigabit Ethernet RJ-45.
2. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 terabajty (TB).
3. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 25 GB logów na dzień.
2. System musi być w stanie przeanalizować minimum 500 logów na sekundę.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 50 systemów.

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:

- 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 z 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.

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.

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.

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. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
2. System musi umożliwiać 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 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 lub równoważny w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim. Wykonawca winien przedłożyć dokumenty:
 - Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
 - Certyfikat ISO 9001 podmiotu serwisującego lub równoważny.