Załącznik nr 4 do Formularza ofertowego

**OPIS WYMAGAŃ SYSTEMU ANALIZY RUCHU SIECIOWEGO I WYKRYWANIA ANOMALII**

Przedmiotem postępowania jest **zakup i dostawę sprzętu i osprzętu IT oraz systemu analizy ruchu sieciowego i wykrywania anomalii**

**Oferowany model \* ……………………..**

**Producent \* ……………………………...**

|  |  |  |
| --- | --- | --- |
| **WYMAGANIA** | | |
| **Opis wymagań minimalnych** | **Parametry techniczne**  **oferowanego sprzętu**  **(tj. wskazanie konkretnego parametru lub konfiguracji i/albo potwierdzenie opisu minimalnych wymagań)** | |
| System analizuje dane statystyczne (czyli próbki ruchu, flow-y, sample) generowane przez urządzenia sieciowe różnych producentów. System musi obsługiwać co najmniej następujące formaty próbek ruchu: Netflow (wersje 5, 7, oraz 9), Netflow, IPFIX, J-Flow, sFlow, Netstream. | TAK | NIE |
| System analizuje kopię ruchu sieciowego udostępnianą przez sesje port mirroringu zdefiniowane na przełącznikach Ethernet, lub przy pomocy dedykowanych sprzętowych tapów sieciowych. | TAK | NIE |
| System udostępnia funkcję aktywnego tworzenia próbek ruchu z analizowanej kopii ruchu sieciowego. Musi istnieć możliwość aktywnego tworzenia próbek ruchu w formatach co najmniej Netflow, J-Flow, sFlow. System musi posiadać funkcję wysyłania aktywnie tworzonych próbek ruchu do systemu NBAD tego samego producenta oraz do kolektorów innych producentów. | TAK | NIE |
| System wykrywa nowe hosty pojawiające się w sieci teleinformatycznej. System musi zbierać i przechowywać informacje o MAC adresach komputerów oraz o przypisanych do nich adresów IPv4 i IPv6. | TAK | NIE |
| System posiada funkcję pobierania informacji o działających w sieci aktywnych urządzeniach przez protokół SNMP – co najmniej nazw urządzeń, listy interfejsów sieciowych z ich nazwami, opisami i prędkościami. | TAK | NIE |
| System utrzymuje centralne repozytorium informacji o analizowanym ruchu sieciowym otrzymywanych z innych urządzeń sieciowych lub własnych komponentów. Dane muszą być przechowywane w bazie danych SQL. Musi istnieć możliwość wydawania zapytań bezpośrednio do bazy danych. | TAK | NIE |
| System udostępnia graficzny interfejs użytkownika do przetwarzania zebranych danych, w tym wyliczania statystyk i generowania raportów. Statystyki i raporty muszą być dostępne na bieżąco w czasie rzeczywistym. | TAK | NIE |
| Systemu kolekcjonowania danych musi przechowywać informacje o czasie rozpoczęcia i zakończenia strumienia analizowanych danych z dokładnością do 1 milisekundy. | TAK | NIE |
| System posiada funkcje tworzenia profili i widoków analizowanych danych, aktualizowanych na bieżąco, na podstawie kryteriów zdefiniowanych przez administratora. | TAK | NIE |
| System generuje raporty pokazujące dane w formie graficznej (wykresy) jak i tabelarycznej, w oparciu o kryteria wprowadzane przez użytkowników w formie filtrów. Raporty muszą obejmować również informacje o wszystkich konwersacjach pomiędzy monitorowanymi hostami. | TAK | NIE |
| System udostępnia statystyki obciążenia sieci przez adresy i sieci IP (źródłowe i docelowe) | TAK | NIE |
| System udostępnia statystyki obciążenia sieci przez: aplikacje (protokoły, porty źródłowe, docelowe) | TAK | NIE |
| System udostępnia statystyki obciążenia sieci przez: klasy ruchu QoS (ToS/DSCP), | TAK | NIE |
| System udostępnia statystyki obciążenia sieci przez: systemy autonomiczne BGP (AS) | TAK | NIE |
| System udostępnia statystyki obciążenia sieci przez: kraje rozpoznawane na podstawie sieci IP (dla adresów źródłowych i docelowych) | TAK | NIE |
| System udostępnia statystyki obciążenia sieci przez: ruch z określonymi flagami TCP | TAK | NIE |
| System musi udostępniać statystyki obciążenia sieci przez: protokoły IPv4 oraz IPv6. | TAK | NIE |
| System generuje raporty zgodnie z kryteriami ustalanymi przez administratorów oraz na podstawie predefiniowanych wzorców. Raport musza być tworzone w różnych formatach – minimum PDF i CSV. Użytkownik musi posiadać wpływ na układ raportu poprzez dobór ilości i rodzaju informacji, z których raport będzie się składał. | TAK | NIE |
| Formaty raportów:  ………………………………….. | |
| System posiada funkcję automatycznego rozwiązywania adresów IP do nazw domenowych. | TAK | NIE |
| System posiada funkcję nadawania nazw własnych następującym zaobserwowanym obiektom: podsieciom, aplikacjom (adresom IP i portom), systemom autonomicznym BGP (AS). | TAK | NIE |
| System musi udostępniać zbiorcze dane statystyczne zawierające sumaryczną liczbę otrzymanych eksportów próbek ruchu określonego typu wysłanych przez każde z urządzeń, wraz z informacjami na temat średniej oraz szczytowej liczby otrzymywanych eksportów od każdego z urządzeń. | TAK | NIE |
| System pozwala na definiowanie alarmów, które będą powiadamiać administratora o ruchu sieciowym (globalnym oraz z wybranych sieci, protokołów i aplikacji) przekraczającym zdefiniowane wartości progowe wyrażone w jednostkach ilości danych (pakietach oraz bajtach), a także w jednostkach prędkości transmisji (bitach/sekundę, pakietach/sekundę). | TAK | NIE |
| Alarmy są wysyłane przy wykorzystaniu co najmniej następujących metod: syslog, e-mail, SNMP trap, komunikaty SMS (w typ przypadku dopuszcza się możliwość integracji z zewnętrzną bramką SMS). | TAK | NIE |
| System musi posiadać możliwość uruchomienia funkcji NBAD (Network Behavior Anomaly Detection). | TAK | NIE |
| System musi posiadać możliwość analizy stanu i efektywności działania sieci teleinformatycznej, w tym również wykrywania sytuacji nieprawidłowych (tj. anomalii) związanych z kondycją sieci oraz stanem jej bezpieczeństwa. | TAK | NIE |
| System posiada możliwość wykrywania anomalii w działaniu sieci teleinformatycznej za pomocą analizy statystycznej i behawioralnej. W tym celu system na bieżąco buduje profile normalnego stanu i zachowania sieci oraz identyfikuje odchylenia od stanu normalnego – poprzez zaobserwowanie zwiększenia lub zmniejszenie natężenia ruchu sieciowego oraz przekraczanie zdefiniowanych wartości progowych. | TAK | NIE |
| System posiada możliwość wykrywania ataków Denial of Service i Distributed Denial of Service. | TAK | NIE |
| System działa w architekturze standalone – kluczowe funkcje, czyli zbieranie danych, analiza zdarzeń oraz wykrywanie anomalii muszą być wykonywane na tym samym urządzeniu. | TAK | NIE |
| W celu zwiększenia skalowalności systemu musi istnieć możliwość uruchomienia systemu w architekturze rozproszonej, poprzez uruchomienie funkcji zbierania danych, a także ich wstępnej analizy na dedykowanych kolektorach. | TAK | NIE |
| System działa pod kontrolą dostrojonego przez producenta systemu operacyjnego klasy Unix. Nie jest dopuszczalne zastosowanie systemu operacyjnego klasy Microsoft Windows. | TAK | NIE |
| System będzie dostarczony jako wirtualny appliance przeznaczony do pracy w środowisku VMWare ESX , wymagający co najmniej 16 GB pamięci RAM, oraz obsługujący nie mniej niż 1 TB pojemności dyskowej. | Ilość pamięci RAM: ……...  Pojemność dysku: ……….. | |
| System zbiera dane z wydajnością nie mniejszą niż 100 próbek ruchu na sekundę (flow-ów/sekundę). System nie posiada ograniczeń co do liczby obsługiwanych urządzeń będących źródłami informacji. | TAK | NIE |
| System będzie dostarczony jako rozwiązanie gotowe do użytku, pochodzące od tego samego producenta. Nie jest dopuszczalna sytuacja, w której funkcje wymagane dla systemu realizowane są przez zestaw programów pochodzących od różnych producentów, działających na tej samej platformie sprzętowej ogólnego przeznaczenia. | TAK | NIE |
| System jest kompletny tzn. zawiera wszystkie licencje i zezwolenia, niezbędne do poprawnego funkcjonowania zgodnie z niniejszą specyfikacją, bez konieczności wnoszenia dodatkowych\*. | TAK | NIE |
| Dodatkowe licencje i zezwolenia wymagane do poprawnego funkcjonowania systemu: | …………………………. | |
| Pełne zarządzanie systemem, analiza danych oraz raportowanie odbywać się poprzez graficzny interfejs użytkownika dostępny za pomocą standardowych przeglądarek WWW. Nie jest dopuszczalne zarządzanie przy pomocy dodatkowych aplikacji klienckich. | TAK | NIE |
| System pozwala na definiowanie kont administratorów o zróżnicowanym poziomie uprawnień w zakresie co najmniej: pełnej kontroli nad systemem, kontroli na poszczególnymi modułami funkcjonalnymi systemu, kont uprawnionych tylko do odczytu. Ponadto musi istnieć funkcja ograniczania uprawnień kont użytkowników do poszczególnych źródeł informacji (tj. urządzeń sieciowych generujących próbki ruchu) oraz do zbioru danych definiowanych na podstawie kryteriów z warstwy 3 i 4 modelu ISO. | TAK | NIE |
| Tożsamość administratorów jest weryfikowana w lokalnej bazie danych użytkowników, a także przy pomocy zewnętrznych serwerów uwierzytelniania (co najmniej LDAP). | Zewnętrzne serwery uwierzytelnienia: …………………………..  ………………………….. | |
| System posiada funkcję zapisywania i odtwarzania pełnej konfiguracji systemu oraz jedynie wybranych jego komponentów. | TAK | NIE |
| System posiada funkcję wykonania kopii zapasowej systemu uwzględniającej konfigurację i ewentualne licencje. | TAK | NIE |
| System posiada narzędzia do: | | |
| informowania o statusie systemu | TAK | NIE |
| zajętości pamięci | TAK | NIE |
| dostępności przestrzeni dyskowej | TAK | NIE |
| konfiguracji interfejsów sieciowych | TAK | NIE |
| zapisywania pełnego dziennika zdarzeń (logów) związanych z działaniem systemu i uruchomionym na nim usług | TAK | NIE |
| inne: ………………………………………………………………………………………. | TAK | NIE |

**Dodatkowe wymagania:**

1. Wykonawca będzie świadczył usługi serwisu technicznego producenta w okresie 12 miesięcy od zakupu, obejmujące   
   co najmniej:
   1. dostęp do aktualizacji oprogramowania, aktualizacji baz sygnatur wykorzystywanych przez urządzenie, aktualizacji systemu operacyjnego urządzenia;
   2. dostęp do pomocy technicznej za pośrednictwem strony www producenta.
2. Wykonawca zrealizuje usługi wdrożeniowe obejmujące:
   1. uzgodnienia techniczne z Zamawiającym dotyczące trybu pracy urządzenia, miejsca wpięcia w sieć Zamawiającego;
   2. fizyczną instalację urządzeń i podłączenie do sieci Zamawiającego;
   3. konfigurację według zaleceń producenta i wymagań integracji z infrastrukturą Zamawiającego, na podstawie dokonanych uzgodnień technicznych;
   4. dokumentację powykonawczą przedstawiającą szczegóły wdrożenia.

……………………………………………..

*(miejscowość, data)*

……………………………………………..

*(podpis z pieczątką imienną, lub podpis czytelny osoby uprawnionej do reprezentowania Wykonawcy)*