1. **DIS System analizy ruchu w sieci Netflow**

Opis Przedmiotu Zamówienia dla zamówienia

DIS System analizy ruchu w sieci Netflow

Technologia Bluecat/LiveNX

1. Wymagania ogólne system monitoringu
2. Kompleksowy system umożliwiający monitorowanie ruchu sieciowego i aplikacji.
3. System monitorujący musi składać się z 2 elementów logicznych:
   1. System zarządzający – centralny panel do wyświetlania statusu ruchu sieciowego oraz raportowania o alarmach.
   2. System monitoringu ruchu sieciowego (dla urządzeń sieciowych, z wykorzystaniem telemetrii sieciowej – minimum protokołu NetFlow/IPFIX oraz SNMP).
4. Wszystkie elementy muszą być zainstalowane w dedykowanym miejscu umożliwiającym korelację danych.
5. Architektura systemów oparta o rozwiązanie zwirtualizowane VM.
6. Oferta musi zawierać wszystkie niezbędne licencje wymagane przez cały system
   1. Monitorowanie minimum 100 urządzeń brzegowych generujących eksporty netflow z możliwością rozszerzenia do 1000 monitorowanych urządzeń poprzez zwiększenie klucza licencyjnego (bez konieczności instalacji dodatkowego kolektora netflow).
   2. Monitorowanie minimum 100 urządzeń brzegowych za pomocą odpytań SNMP z możliwością rozszerzenia do 1000 monitorowanych urządzeń poprzez zwiększenie klucza licencyjnego (bez konieczności instalacji dodatkowego kolektora netflow).
   3. Wszystkie niezbędne licencje potrzebne do obsługi systemów operacyjnych, baz danych, brak ograniczeń funkcjonalnych tych licencji.
7. Analiza wydajności aplikacji i ruchu sieciowego musi odbywać się pasywnie (z wyjątkiem zapytań SNMP).
8. Wszystkie elementy systemu muszą pochodzić od tego samego dostawcy, aby zagwarantować wymaganą wydajność i interoperacyjność.
9. Oferowany system powinien zapewnić możliwość opcjonalnego rozszerzenia (dodania) nowych elementów,
   1. moduł monitoringu ruchu sieciowego i aplikacyjnego (kolektor pakietów, zbierający i analizujący ruch sieciowy pod kątem zdefiniowanych metryk)
   2. moduł do zbierania statystyk działania urządzeń w monitorowanej infrastrukturze z wykorzystaniem protokołu SNMP
   3. moduł monitoringu ruchu sieciowego i aplikacyjnego na końcówkach użytkowników polegający na zainstalowaniu agentów na laptopach klientów i zbierania lokalnie ruchu w postaci plików \*.pcap z możliwością ich przesłania do dalszej analizy w oferowanym systemie
   4. moduł wspomagający pracę użytkowników systemu działający w oparciu o możliwość za-dawania pytań w dowolnym języku (minimum język polski i angielski) do analityki opartej na algorytmach AI
10. Wymagania dotyczące Systemu Zarządzającego
11. Sprzęt
    1. Serwer w postaci maszyny VM
    2. Zamawiający udostępni zasoby w ramach posiadanych zasobów mocy obliczeniowej opartej o technologię VMware.
12. Działanie
    1. Zbieranie i korelacja danych ze wszystkich komponentów systemu.
    2. Dla każdej lokalizacji widoki kompleksowo obejmujące parametry aplikacyjne, sieciowe i wydajnościowe.
    3. Konieczność logowania się przez użytkowników
    4. Logowanie w oparciu o uwierzytelniania w oparciu o dane z Active Directory.
    5. Definiowanie lokalizacji poprzez przypisanie podsieci klienckich oraz przyporządkowanie interfejsów opisywanych przez protokół NetFlow.
    6. Definiowanie różnych zestawów godzin roboczych i przyporządkowania im alarmowania i/lub monitorowania.
    7. Powiadamianie poprzez wiadomość email wysłaną z posiadanego przez klienta serwera SMTP.
    8. Definiowanie grup dla monitorowania statusu opartego o alarmy, grupy powinny pozwolić na równoczesne umieszczenie elementów monitorowanych:
       1. Aplikacji.
       2. Serwerów.
       3. Lokalizacji klienckich.
    9. Filtrowanie danych według różnych kryteriów dostępnych z raportu NetFlow.
    10. Automatyczne generowanie, zapisywanie i wysyłanie raportów pocztą email.
    11. Udostępnianie raportów za pośrednictwem adresu URL bez dostępu administracyjnego.
    12. System automatycznego alarmowania opartego o numeryczne progi.
    13. System automatycznego alarmowania wykorzystujący progi dynamiczne lub dynamiczne i statyczne, oparty na automatycznym ustalaniu wartości bazowej z co najmniej ostatnich 30 dni.
    14. Automatyczne rozwiązywanie adresów IP na nazwy domenowe dla lokalnego DNS
    15. Tworzenie raportów długoterminowych obejmujących dowolny okres czasu (zależnie od udostępnionej dla systemu przestrzeni plikowej) z rozdzielczością 5 minutową.
    16. Identyfikacja aplikacji w oparciu o technologie DPI (Cisco NBAR i AVC lub równoważne).
    17. Przesyłanie powiadomień do innych systemów o alarmach za pomocą mechanizmu SNMP trap, Syslog oraz API
    18. Tworzenia spersonalizowanych widoków zawierających niestandardowe zestawienia danych, w tym z różnych źródeł (np. dane NetFlow z różnych urządzeń).
13. Konfiguracja
    1. Konfiguracja dostępu i zarządzania zarówno lokalnie jak i zdalnie
    2. Zdefiniowanie wielu użytkowników z różnymi uprawnieniami, w tym możliwość różnicowania uprawnień odczytu oraz różnicowania uprawnień administracyjnych
    3. Stworzenie personalizowanych widoków, zawierających niestandardowe zestawienia danych, w tym pochodzące z różnych źródeł (np. dane NetFlow oraz dane wydajnościowe aplikacji) dla każdego użytkownika i grupy niezależnie
    4. Uwierzytelnienie użytkowników za pomocą LDAP.
    5. Logowanie jednokrotnego (SSO) przy użyciu ADFS
    6. Konfiguracja integracji z Cisco ISE
       1. Informacje o użytkowniku (mapowanie użytkownika na adres IP).
    7. Dane o przepływach powinny pozostać lokalnie w kolektorach netflow, tylko informacje statystyczne powinny być przesyłane do systemu zarządzania
    8. Licencjonowanie oparte na liczbie monitorowanych urządzeń i musi obejmować pełną funkcjonalność.
    9. Brak ograniczeń odnośnie pojemności (ilości Flowów/sek) oferowanego systemu, zwiększenie pojemności systemu wymaga jedynie dodania nowego kolektora bez konieczności dokupienia dodatkowych licencji lub sprzętu od dostawcy rozwiązania.
    10. System musi zawierać lokalną instancję Grafany do zaawansowanej analizy danych i personalizacji
14. Wymagania dotyczące systemu monitorowania sieci (Kolektor NetFlow)
15. Moc obliczeniowa - wirtualizacja
    1. Jeden kolektor danych netflow
    2. Kolektor wykonuje realizację zarówno zbierania danych jak i ich obróbki oraz raportowania do elementu zarządzającego
    3. Zebrane dane Netflow i SNMP muszą pozostać lokalne w systemie monitorowania sieci (kolektorze netflow) i nie mogą być kopiowane/przesyłane na serwer zarządzania.
    4. Wirtualny serwer VM
       1. Zamawiający udostępni zasoby mocy obliczeniowym we własnym środowisku VMware.
       2. Zbieranie i zapisywanie pełnych niezagregowanych danych (wszystkie pola rekordu NetFlow v5 oraz v9) z wydajnością minimum 150 000 strumieni na sekundę przez dedykowany kolektor VM
16. Działanie
17. Zbieranie danych z urządzeń generujących NetFlow
18. Routery
19. Przełączniki L3 umożliwiające generowanie eksportów NetFlow
20. Bezprzewodowe punkty dostępowe/kontrolery generujące NetFlow
21. Zbieranie danych z urządzeń sieciowych za pomocą protokołu SNMP
22. Routery
23. Przełączniki warstwy L3
24. Bezprzewodowe punkty dostępowe/kontrolery
25. Możliwość przechowywania pełnych, dokładnych (wszystkie pola rekordu NetFlow v5 oraz v9) i niezagregowanych danych przez dowolny okres czasu (ograniczenie jedynie dostępną przestrzenią plikową).
26. Możliwość przechowywania niezagregowanych danych SNMP przez dowolny okres czasu (ograniczenie jedynie dostępną przestrzenią plikową).
27. Możliwość zbierania danych niezależnie od stacji zarządzającej (zbieranie danych jest kontynuowane w przypadku utraty połączenia ze stacją zarządzania)
28. Konfiguracja
29. Uruchomione wsparcie co najmniej dla protokołów:
30. NetFlow (wersje 1, 5, 7, 9 oraz FNF)
31. Sampled NetFlow
32. IPFIX
33. J-Flow
34. cflowd
35. sFlow
36. HSL
37. NSEL
38. Automatyczne odczytywanie nazw urządzeń, listy interfejsów wraz z nazwami, opisami i prędkościami poprzez protokół SNMP w wersjach 1,2(2c),3. Możliwość automatycznego ponawiania odczytu SNMP o ustalonej godzinie każdego dnia. Wyświetlanie informacji o protokole i wersji otrzymywanych danych dla każdego urządzenia.
39. Monitorowanie obciążenia urządzeń sieciowych poprzez protokół SNMP (minimalnie: CPU, pamięć).
40. Możliwość wykonania kopii zapasowej systemu uwzględniającej pełną konfigurację.