Załącznik nr 1 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Wstęp

Przedmiotem zamówienia jest system typu Next Generation NAC (zwany dalej platforma NG-NAC), który dynamicznie identyfikuje i analizuje systemu podłączone do sieci oraz aplikacje natychmiast po podłączeniu ich do sieci korporacyjnej. Rozwiązanie powinno działać bez potrzeby instalowania agenta na systemach podłączonych do sieci. System powinien natychmiast dostarczać informację o użytkowniku, właścicielu, systemie operacyjnym, ale również o konfiguracji urządzenia, oprogramowaniu, usługach systemowych, zainstalowanych uaktualnieniach i obecności innych rozwiązań odpowiedzialnych za bezpieczeństwo. Jednocześnie rozwiązanie powinno dawać możliwość reagowania, kontroli oraz stałego monitorowania stanu tych urządzeń.

Platforma NG-NAC powinna realizować powyższe funkcjonalności w stosunku do urządzeń będących własnością przedsiębiorstwa, ale i również urządzeń BYOD oraz innych urządzeń typu IoT bez konieczności instalowania agenta. Rozwiązanie powinno umożliwiać szybką instalację w środowisku firmy.

Wymagania ogólne

- **Monitorowanie stanu stacji końcowych w czasie rzeczywistym.** Platforma NG-NAC powinna posiadać aktualny katalog oraz monitorować stan wszystkich urządzeń, które zażądały i uzyskały dostęp do sieci korporacyjnej w ramach sieci kampusowej, WAN, VPN czy DC. Informacje powinny obejmować między innymi użytkownika, parametry urządzenia, systemu operacyjnego, listę aplikacji czy usług – wszystko, aby wspomóc zamawiającego w zarządzaniu ryzykiem przypisanym do każdego urządzenia w sieci.

- **Możliwość wymuszania precyzyjnych polityk dotyczących kontroli dostępu oraz zgodności z wymaganiami (ang. compliance).** Platforma NG-NAC powinna wspierać gromadzenia wszystkich dostępnych danych ze stacji roboczych, aby umożliwić ich prezentację zespołom operacyjnym by z kolei pomóc im lepiej rozumieć ryzyko, podejmować lepsze decyzje oraz wymuszać akcje bazując na szerokim katalogu atrybutów, takich jak: typ urządzenia, użytkownik, lokalizacja, stan uwierzytelniania, stan zabezpieczeń, podatności czy inne w zależności od sytuacji. System dodatkowo powinien wspierać proces zarządzania gośćmi oraz automatycznie identyfikować i usuwać obce/szkodliwe urządzenia czy aplikacje.

- **Umożliwienie zespołom operacyjnym automatyczne reagowanie na incydenty.** Platforma NG-NAC powinna dawać możliwość automatycznego reagowania na naruszenia polityki bezpieczeństwa i zagrożenia poprzez realizację zautomatyzowanych akcji. Do najbardziej podstawowych akcji powinny należeć: alertowanie, notyfikacja zespołów IT czy powiadomienie dla użytkownika. Bardziej zdecydowane akcji powinny co najmniej zawierać reakcje na poziomie sieci w postaci ograniczania dostępu do zasobów sieciowych. Dodatkowo system powinien umożliwiać podjęcie prób naprawy systemu w postaci instalowania patcha, zmiany ustawień

bezpieczeństwa czy wyłączenia/deinstalacji aplikacji lub usługi. Wszystkie te funkcjonalności mają na celu zmianę modelu zachowania użytkowników, redukcję czasu pomiędzy atakiem a jego wykryciem i reakcją oraz minimalizację wpływu ataków na działanie firmy.

- **Realizację funkcji platformy integracyjnej rozwiązań bezpieczeństwa.** Platforma NG-NAC powinna posiadać możliwość integracji z innymi systemami poprzez otwarte standardy integracji. Celem integracji jest wymiana danych o systemach sieciowych aby zwiększyć możliwości analizy innych systemów jak SIEM, Threat Intelligence, MDM, firewalli czy skanerów podatności.

Wymagania funkcjonalne:

1. Rozwiązanie powinno wspierać wielu producentów urządzeń sieciowych – w tym minimum Cisco, Brocade, Extreme, 3COM, HPE oraz Huawei. Dodawanie urządzeń do systemu powinno odbywać się ręcznie lub automatycznie poprzez użycie protokołów automatyzujących: CDP, FDP oraz LLDP.
2. Rozwiązanie powinno wspierać wielu producentów urządzeń WLAN – w tym minimum: Aerohive, Cisco, Meru Networks, Aruba Networks oraz Xirrus.
3. System powinien wspierać użycie protokołu 802.1x, jednakże, aby uzyskać pełną funkcjonalność użycie tego protokołu nie może być wymagane.
4. Rozwiązanie powinno wspierać uwierzytelniania pre-admission oraz post-admission. Pre-admission oznacza, że urządzenie będzie uwierzytelniane i sprawdzane pod względem zgodności przed dostępem do sieci. Post-admission oznacza, że dostęp do sieci jest zapewniony od razu po podłączeniu jednak w tym samym czasie realizowane jest sprawdzanie pod względem zgodności z politykami.
5. Rozwiązanie powinno wspierać centralne zarządzanie politykami bezpieczeństwa w ramach całej organizacji w ramach *systemu zarządzającego*.
6. Rozwiązanie zapewnia widoczność wszystkich urządzeń widocznych w sieci, które posiadają co najmniej jeden z adresów: MAC, IP. Baza urządzeń jest aktualizowana w czasie rzeczywistym. Wśród monitorowanych urządzeń powinny być: stacje robocze, laptopy, smartfony, tablety, urządzenia IoT (projektory, kamery IP, systemy HVAC, systemy OT, itp.).
7. System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego.
8. System musi umożliwić aktualizację definicji oraz aktualizacje modułów zależnych przez Internet bezpośrednio z serwerów producenta.
9. System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
10. Kopie zapasowe powinny być możliwe do zapisania bezpośrednio na serwerach FTP, SFTP oraz SCP. Uwierzytelnianie do zasobu SCP powinno być możliwe poprzez użycie klucza publicznego.
11. Powinna istnieć też możliwość zapisania kopii zapasowej na dysku lokalnym komputera administratora, jednak taka kopia powinna być zaszyfrowana z użyciem hasła.
12. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.

Klasyfikacja:

13. System powinien umożliwiać klasyfikację urządzeń bazując na definicjach dostarczonych przez producenta rozwiązania w ramach *silnika klasyfikacji*.

14. System powinien dostarczyć minimum 80 kategorii klasyfikacji w tym podział na urządzenia IT oraz OT. Wśród dostępnych klasyfikacji powinny być dostępne co najmniej:
    a. Komputer
    b. Smartfon
    c. Smartwatch
    d. Tablet
    e. Drukarka
    f. Telefon IP
    g. Zestaw wideokonferencji
    h. Projektor
    i. Smart TV
    j. Urządzenia sprzedające (tzw vending machine)
    k. Kontrolery klimatyzacji
    l. Kamery IP
    m. Systemy kontroli dostępu

15. Producent NG-NAC powinien stale aktualizować bazę klasyfikacji używaną przez *silnik klasyfikacji* oraz umożliwić pobieranie informacji zwrotnej od klientów, która to ma na celu udoskonalanie klasyfikacji w kolejnych aktualizacjach *silnika klasyfikacji*.
16. W sytuacji, gdzie *silnik klasyfikacji* jest aktualizowany oraz niektóre systemy mają w konsekwencji zmienioną klasyfikację to system powinien wskazać, których systemów dotyczy zmiana i umożliwić akceptację przed podjęciem zmiany klasyfikacji.
17. Klasyfikacja powinna dotyczyć systemów zarządzanych i niezarządzanych bazując na wielu technikach pasywnych i aktywnych. Do technik pasywnych powinny należeć co najmniej DHCP fingerprinting, HTTP User-Agent, TCP Fingerprinting. Do technik aktywnych powinno należeć co najmniej użycie skanów NMAP, RPC, SSH, SMB, WMI oraz SNMP.
18. Silnik klasyfikacji obok wspomnianej wcześniej kategorii klasyfikacji powinien również umożliwić identyfikację systemu operacyjnego.

Inspekcja systemów zarządzalnych:

19. System musi umożliwiać bezagentową inspekcję zarządzanych stacji, która jest w stanie określić wersję systemu operacyjnego, obecnie zalogowanego użytkownika, uruchomione procesy i usługi, zainstalowane aplikacje oraz weryfikację stanu oprogramowania zabezpieczającego.
20. System musi wspierać następujące systemy klienckie w ramach bezagentowej inspekcji: Windows, MAC, Linux.
21. Producent NG-NAC musi umożliwić w ramach licencji podstawowej instalację agenta, który może realizować funkcje inspekcji podobnej do inspekcji bezagentowej. Musi istnieć wersja agenta dla systemów Windows, MAC oraz Linux. Instalacja agenta powinna być realizowana przez rozwiązanie NG-NAC oraz powinna być możliwość instalacji przez system Microsoft SCCM.
22. System powinien umożliwić wskazanie konta dostępowego, które ma być użycie w ramach inspekcji bezagentowej. Musi być możliwość podania konta domenowego w przypadku środowisk Microsoft ActiveDirectory.
23. System musi wspierać następujące mechanizmy uwierzytelniania w stosunku do komputerów pracujących pod kontrolą systemu Microsoft Windows: NTLMv1, NTLMv2 oraz Kerberos.

24. W przypadku inspekcji bezagentowej systemów Linux oraz Mac musi być możliwość uwierzytelniania zarówno z użyciem pary użytkownik i hasło oraz z użyciem klucza publicznego.
25. System powinien wskazać otwarte porty TCP oraz UDP na wykrytych systemach w ramach inspekcji bezagentowej.
26. System powinien mieć możliwość wykrywania, czy dana stacja robocza jest ukryta za mechanizmem Network Address Translation.

Obsługa gości:

27. System powinien umożliwiać obsługę procesu zarządzania gośćmi w ramach bazowej licencji. Jako gościa zamawiający rozumie osobę, która nie jest zatrudniona w firmie ale potrzebuje wykorzystać jej infrastrukturę za zgodną pracownika firmy (zwanego dalej sponsora).
28. Użytkownik po podłączeniu się do sieci powinien być przekierowany na stronę obsługi gości, gdzie może się zalogować lub utworzyć nowe konto. W ramach tworzenia nowego konta użytkownik powinien wskazać osobę w organizacji, która może zaakceptować jego żądanie dostępu do sieci – *sponsora*.
29. System powinien umożliwić wskazanie, którzy użytkownicy mogą pełnić rolę sponsora i akceptować prośby dostępu do sieci.
30. Email użytkownika powinien być weryfikowany w czasie rejestracji poprzez wysłanie linku aktywacyjnego.
31. Sponsorzy powinni otrzymywać powiadomienie emailem każdorazowo, jak ktokolwiek zażąda dostępu do sieci wskazując ich jako sponsora.
32. Hasło do konta użytkownika-gościa powinno spełniać możliwe do skonfigurowania wymagania dotyczące długości hasła, ilości małych i wielkich liter, obecności cyfr czy znaków specjalnych.

Remediacja i reakcja:

33. W ramach zadanej polityki system powinien umożliwić wysyłanie informacji w następujący sposób:
    a. Wyświetlenie strony użytkownikowi bez użycia agenta
    b. Wyświetlenie strony użytkownikowi z użyciem agenta (Windows i Mac)
    c. Wysłanie email do użytkownika
    d. Wysłanie email do administratora systemu
    e. Wysłanie logu w formacie CEF oraz syslog do innego systemu. Log powinien być w pełni konfigurowalny.
    f. Wygenerowania powiadomienia tzw. baloon notification dla systemu Windows.
34. W ramach zadanej polityki system powinien umożliwić zrealizowanie następujących czynności na zarządzanych stacjach roboczych:
    a. wykonanie predefiniowanego skryptu (Windows, Linux, MAC). Skrypt powinien być wgrywany na system w momencie wykonania. Nie dopuszczalne jest wymaganie, by wymagane było wgranie skryptu ręcznie przed jego wykonaniem.
    b. zabicie wskazanego procesu
    c. uruchomienie wskazanego systemu antywirusowego
    d. wpisanie do rejestru konkretnej wartości (Windows)
    e. dezaktywacja aplikacji typu peer-to-peer.
    f. dezaktywacja oprogramowania typu cloud storage

g. wszczęcie procesu aktualizacji systemu (Windows, MAC)
h. wyłączenie interfejsów dual-home.
i. wyłącznie wskazanych urządzeń zewnętrznych jak dyski, drukarki czy modemy.

35. W ramach zadanej polityki system powinien umożliwić realizację następujących reakcji na poziomie sieci przewodowej:
    a. przypisanie portu do zdefiniowanego VLANu
    b. przypisanie IP ACL do portu. System powinien sam konfigurować ACL na urządzeniu. Nie jest dopuszczone wymaganie ręcznej konfiguracji ACL przed jej użyciem w rozwiązaniu.
    c. przypisanie MAC ACL do portu. System powinien sam konfigurować ACL na urządzeniu. Nie jest dopuszczone wymaganie ręcznej konfiguracji ACL przed jej użyciem w rozwiązaniu.
    d. wyłącznie portu
    e. Przypisanie tagu SGT dla sieci opartych na Cisco TrustSec.
36. W ramach zadanej polityki system powinien umożliwić realizację następujących reakcji na poziomie sieci bezprzewodowej WLAN:
    a. Blokowanie
    b. Przypisanie roli WLAN na poziomie kontrolera
37. W ramach zadanej polityki system powinien umożliwić realizację następujących reakcji na poziomie private cloud.
    a. Zmianę portgrupy przypisanej do maszyny wirtualnej
    b. Wyłączenie maszyny wirtualnej
    c. Uśpienie maszyny wirtualnej
    d. Restart maszyny wirtualnej
    e. Włączenie maszyny wirtualnej

Architektura:

38. Rozwiązanie powinno być dostarczone jako rozwiązanie sprzętowe przez producenta systemu NG-NAC.
39. W ramach licencji podstawowej powinna istnieć możliwość instalacji nieograniczonej ilości maszyn wirtualnych co najmniej na środowisku VMware oraz Hyper-V.
40. Rozwiązanie powinno umożliwiać centralne zarządzanie z jednego punktu (urządzenia centralnego).
41. Rozwiązanie NG-NAC powinno wspierać obsługę architektury centralnej i rozproszonej, gdzie niektóre urządzenia mogą być zainstalowane poza centralną lokalizacją firmy.

Wysoka dostępność:

42. Rozwiązanie powinno oferować funkcje wysokiej dostępności na poziomie systemu zarządzania. W przypadku awarii urządzenia podstawowego – urządzenie zapasowe powinno przełączyć się w tryb aktywny automatycznie.
43. Rozwiązanie powinno być w pełni redundantne. Awaria jednego urządzenia nie powinna wpływać na funkcjonalność rozwiązania. W szczególności powinna być zapewniona redundancja:
    a. na poziomie 1:1 w ramach systemu zarządzania i podsystemu monitoringu.
    b. na poziomie N+1 w ramach podsystemu monitoringu.

44. Redundancja rozwiązania powinna przywidywać scenariusz Disaster Recovery, gdzie jedno lub więcej urządzeń centralnych jest zainstalowanych w zdalnej lokalizacji.

Środowisko Wirtualne

45. Rozwiązanie powinno umożliwiać monitorowanie i zarządzanie maszynami wirtualnymi uruchomionym w środowisku wirtualizacyjnym, przynajmniej VMware vSphere oraz NSX.
46. System powinien umożliwiać integracje z rozwiązaniami chmury publicznej, przynajmniej Amazon AWS oraz Microsoft Azure.

Integracje:

47. System powinien umożliwiać integrację z Microsoft Active Directory w celu odczytania właściwości użytkownika zalogowanego na analizowanej stacji.
48. System powinien umożliwić integrację z systemem Microsoft SCCM w celu wymuszania aktualizacji danej stacji z użyciem serwera Microsoft SCCM. Integracja powinna być łatwa w realizacji. Nie dopuszcza się integracji, która wymaga wpisania kwerend SQL.
49. System powinien umożliwić integrację z systemem SIEM [] posiadanym przez Zamawiającego. W ramach integracji system SIEM powinien mieć dostęp do informacji o urządzeniach zebranych przez rozwiązanie. Dodatkowo w ramach integracji operator SIEM powinien mieć możliwość realizowania akcji kontrolnych na poziomie sieci z użyciem rozwiązania bez konieczności logowania się do konsoli rozwiązania.
50. System powinien integrować się ze środowiskiem Vmware vSphere w celu odczytywania informacji o maszynach wirtualnych (co najmniej czas startu maszyny, nazwa, przypisana portgrupa, stan uruchomienia, przypisany IP oraz stan instalacji Vmware Tools) oraz do wykonywania akcji (co najmniej wyłączenia maszyny, pauza, włączenie maszyny).
51. System powinien integrować się ze środowiskiem Sandbox firmy []. W ramach integracji wymagane jest automatyczne ściąganie IoC (Indicators of Compromise) i zapisywane w katalogu IoC a następnie systemy podłączone do sieci musza być cyklicznie sprawdzane, czy nie są nośnikami infekcji w ramach zdefiniowanych IoC.

Raportowanie:

52. System powinien umożliwiać generowanie raportów w postaci PDF oraz plików XLS.
53. W ramach raportów w postaci PDF powinno być możliwe wygenerowanie co najmniej następujących zestawień:
    a. Dane systemów gości
    b. Wyniki działania konkretnej polityki
    c. Wynik działania konkretnej polityki na przestrzeni czasu
    d. Zestawienie stanu występowania podatności dla wybranych hostów Windows
    e. Dane zgodności z wymaganiami firmy.
54. Raporty powinny być generowane na żądane lub w określonym harmonogramie czasowym. Po wygenerowaniu raportu powinna istnieć możliwość automatycznej wysyłki na wskazany adres email.
55. System powinien również umożliwiać przedstawianie wyników pracy w postaci interaktywnej strony WWW, gdzie możliwe jest drążenie danych.

Wymagania fizyczne:

56. Rozwiązanie powinno być oparte o system operacyjny Linux.
57. Rozwiązanie powinno być dostarczone jako appliance fizyczny lub wirtualny. Nie jest dopuszczalne dostarczenie aplikacji, którą należy samodzielnie zainstalować na własnym systemie operacyjnym.

Licencjonowanie i wsparcie:

58. Licencje w ramach rozwiązania powinny być dostarczone w modelu licencji permanentnych. Zamawiający nie dopuszcza licencji bazujących na subskrypcji.
59. System powinien umożliwiać elastyczną rozbudowę poprzez dodawanie licencji bazowych oraz zaawansowanych w ramach wzrostu liczby obsługiwanych stacji końcowych.
60. Na urządzenia zakupione w ramach systemu NG-NAC powinna być zapewniona minimum 3-letnia gwarancja producenta.
61. Wsparcie powinno być świadczone przez producenta i powinno zawierać:
    a. Telefoniczną obsługę zgłoszeń co najmniej przez co najmniej 8 godzin dziennie, 5 dni w tygodniu.
    b. Obsługę zgłoszeń przez portal klienta.
    c. Dostęp do bazy wiedzy producenta.
    d. Dostęp do dokumentacji technicznej.
    e. Dostęp do najnowszych wersji produktu oraz uaktualnień.

Liczba urządzeń przewidzianych w dostawie

Licencja dla 500 numerów IP,

Licencje ważne 3 lata

Zamówienie dodatkowe

Możliwość rozszerzenia o 100 numerów IP w ciągu 3 lat (20%),

Wymagania dotyczące wykonawcy

Ubezpieczenie OC minimum 1.000.000 zł od każdego zdarzenia (oświadczenie dostarczane wraz z ofertą a polisa wraz z podpisaną umową),

Posiadanie co najmniej dwóch inżynierów wdrożeniowców (oświadczenie z podaniem danych inżynierów),

Czas wykonania instalacji i uruchomienie

W terminie 60 dni od dnia podpisania umowy

Zamawiający udostępni Wykonawcy następujące parametry środowiska do instalacji systemu:

16 GB RAM, 6 do 8 CPU, 250 GB Użytkowej pamięci dyskowej

Jeżeli zadeklarowane parametry środowiska do instalacji systemu musza być większe należy wskazać te parametry.