Opis Przedmiotu Zamówienia

Usługa wsparcia producenta dla oprogramowania systemu zarządzania dostępem do sieci - NAC

1. Przedmiot zamówienia:

1.1. Zakup usługi wsparcia producenta dla posiadanego przez Zamawiającego oprogramowania systemu zarządzania dostępem do sieci – NAC (Network Access Control), określonego przez producenta jako Sup-NV-2500 NACVIEW Support service for NACVIEW 2500 License for 2 year.

1.2. Zamawiający posiada dożywotnią licencję na system określoną przez producenta jako NV-2500-VM.

2. Termin realizacji zamówienia:

2.1. Usługa będzie świadczona przez okres 12,24 lub 60 miesięcy od dnia zakończenia wsparcia producenta **12-03-2026** lub od daty podpisania protokołu odbioru, jeżeli umowa będzie zawarta po wskazanym terminie.

2.2. Wykonawca w ciągu 14 dni roboczych dostarczy Zmawiającemu dokument od producenta oprogramowania potwierdzający możliwość korzystania z Usługi przez Zamawiającego. W przypadku formy elektronicznej dokumentu Wykonawca przekaże Zamawiającemu dokument na adres administrator@cez.gov.pl.

3. Zakres usługi:

W ramach usługi wsparcia producenta dostarczonego przez Wykonawcę wymagany jest:

3.1. Kontakt z działem wsparcia technicznego producenta w celu uzyskania pomocy technicznej dotyczącej oprogramowania NACVIEW za pośrednictwem poczty elektronicznej w dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego, w godzinach od 8:00 do 16:00.

3.2. Pomoc techniczna mająca na celu rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem. Udzielane wsparcia przy identyfikacji problemów trudnych do powtórzenia. Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów. Pomoc techniczna będzie udzielana zdalnie za pośrednictwem poczty elektronicznej.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

3.3. Dostęp do dokumentacji technicznej oprogramowania NACVIEW, najnowszych wersji dokumentów i instrukcji nowych wersji oprogramowania. Dostęp do dokumentacji będzie udzielany poprzez stronę internetową (portal producenta).

3.4. Dostęp do aktualizacji oraz poprawek oprogramowania NACVIEW. Dostęp do aktualizacji będzie udzielany poprzez stronę internetową (portal producenta).

4. **Opis równoważności:**

4.1. Zamawiający dopuszcza rozwiązanie równoważne, przy następujących założeniach:

4.1.1. Zamawiający przez „rozwiązanie równoważne" rozumie oprogramowanie zapewniające bez dodatkowych nakładów finansowych bezkonfliktowe działanie posiadanego środowiska zbudowanego w oparciu o licencje wymienione w pkt. 1.1 – 1.2.

4.1.2. Zamawiający wymaga, żeby dostarczone rozwiązanie równoważne integrowało się z posiadanymi urządzaniami takimi jak: FortiGate (logowanie VPN w oparciu o konta z NAC), Active Directory (pobieranie bazy użytkowników, komputerów), przełączniki CISCO, HP (autoryzacja 802.1.x).

4.1.3. Dodatkowo w przypadku błędnego działania środowiska po instalacji oprogramowania równoważnego Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania w przeciągu 24h od stwierdzenia przez Zamawiającego niepoprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ w terminie do 3 dni kalendarzowych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

Załącznik nr 1 do OPZ

Opis wymagań dla oprogramowania równoważnego systemu zarządzania dostępem do sieci NAC

Zamawiający posiada licencje na oprogramowanie NAC oraz zintegrowane systemy informatyczne, które korzystają z rozwiązania firmy NACVIEW.

Zamawiający wymaga, żeby dostarczone oprogramowanie integrowało się z posiadanymi urządzaniami takimi jak: FortiGate (logowanie VPN w oparciu o konta z NAC), Active Directory (pobieranie bazy użytkowników, komputerów), przełączniki CISCO, HP (autoryzacja 802.1.x).

Jeżeli Zamawiający określił w Opisie przedmiotu zamówienia wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.

I. Zamawiający dopuszcza zaoferowanie produktów równoważnych do oprogramowania NACVIEW

1. W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie Przedmiotu Zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w Istotnych Warunkach Zamówienia, w szczególności w zakresie:
   a) warunków licencji / sublicencji w każdym aspekcie licencjonowania / sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla oprogramowania NACVIEW.
   b) funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w pkt III - „Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego”.
   c) oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego.
   d) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie.
   e) oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem.
2. W przypadku zaoferowania przez Wykonawcę oprogramowania Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.
3. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.

4. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.

II. **W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:**

1. Przeprowadzić Instruktaż dla 2 administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania oprogramowaniem równoważnym, umożliwiającym pełne poznanie produktu równoważnego. Wykonawca w terminie 3 Dnia Roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogram Instruktażu.
2. Przeprowadzić Instruktaż dla 2 operatorów Zamawiającego z zakresu użytkowania oprogramowania równoważnego, umożliwiającego pełne poznanie produktu równoważnego.
3. Wykonawca w terminie 3 Dnia Roboczego od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogramy Instruktaży.
4. Instruktaże będą realizowane w Dni Robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub w formie zdalnej o ile zostaną spełnione wszystkie wymagania dotyczące Instruktażu. Instruktaże będzie trwał minimum 2 Dni Robocze każdy (łącznie minimum 14 godzin zegarowych każdy).
5. Zainstalować oprogramowanie równoważne w środowisku Zamawiającego oraz dokonać poprawnej integracji z systemami/urządzeniami wykorzystywanymi w ramach działalności systemu NAC Zamawiającego w terminie do **10 dni roboczych** od dnia podpisania Umowy.
6. Dostarczyć wszelkich dodatkowych licencji - niezbędnych do prawidłowego funkcjonowania oprogramowania równoważnego.

III. Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego w stosunku do oprogramowania NACVIEW

1. Architektura Systemu.

a) System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor).

b) W przypadku dostarczenia Systemu jako maszyny wirtualnej muszą być wspierane środowiska Hyper-V oraz Vmware.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

c) System musi wspierać możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive w celu zwiększenia niezawodności.

d) System musi oferować pracę w trybie out-of-band, tj. realizować wszystkie wymagane funkcje bez konieczności analizy ruchu sieciowego (na porcie SPAN, inline).

e) Jeżeli System będzie instalowany jako oprogramowanie na systemie operacyjnym należy dostarczyć produkt, który będzie mógł być zainstalowany na jednym z systemów operacyjnych: Windows Server 2022+ lub Red Hat Enterprise Linux 9.

f) System musi być w pełni zarządzalny z jednej konsoli przez graficzny interfejs www, należy dostarczyć rozwiązanie obsługiwane za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w aktualnych wersji na dzień składania oferty.

g) Konsola zarządzania musi umożliwiać dostęp szyfrowany z pomoc protokołu SSL.

h) Wszystkie komponenty Systemu na stacji monitorowanej powinny mieć możliwość automatycznego wdrażania i konfiguracji w oparciu o predefiniowane reguły zarządzania.

i) Elementy zarządzające i analityczne Systemu muszą być skalowane w celu obsługi co najmniej 2500 jednoczesnych unikatowych autoryzacji do sieci w ciągu doby.

j) Praca Systemu musi pozwalać na działanie bez dostępu do Internetu.

k) Wymagana jest możliwość wykorzystania mechanizmy proxy do komunikacji z Internetem.

l) W przypadku braku dostępu do Internetu System zarządzający ma mieć możliwość aktualizacji za pomocą ręcznej aktualizacji.

m) System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych urządzeń w sieci.

n) Licencja na jednoczesne unikatowe uwierzytelniania ma być zwalniana po rozłączeniu urządzenia końcowego.

2. Zarządzanie Systemem.

a) System musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora Systemu.

b) System musi pozwalać na ustalenie silnej polityki haseł.

c) System musi umożliwiać konfigurowanie zakresu uprawnień w Systemie z wykorzystaniem predefiniowanych ról wewnętrznych – zarządzanie RBA (Role based Access) - np. dostęp tylko do raportów, administrator systemu, analityk itp.).

d) System powinien się integrować z zewnętrznym repozytorium użytkowników (LDAP i RADIUS) w zakresie uwierzytelnienia do Systemu oraz kontroli dostępu na bazie zdefiniowanych ról. Dopuszcza się rozwiązanie używające wewnętrznego mechanizmu uwierzytelniania do Systemu.

e) System musi mieć możliwość definiowania raportów i alertów z wykorzystaniem danych zbieranych przez system.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

f) System musi mieć wbudowany panel sterowania (Dashboard) z predefiniowaną zawartością dostosowaną do potrzeb określonej roli co najmniej analityka, kierownika zespołu, dyrektora bezpieczeństwa. Dashboard powinien umożliwiać schodzenie do szczegółu poszczególnych elementów od poziomu informacji podstawowych.

g) System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć urządzeń końcowych.

h) Konsola zarządzania systemu musi być dostępna co najmniej w angielskiej wersji językowej.

3. Obligatoryjne funkcjonalności Systemu.

a) System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników oraz urządzeń końcowych.

b) System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN z wykorzystaniem: standardu 802.1X, adresu MAC urządzenia, formularza webowego (captive portal) z wykorzystaniem LDAP lub przy pomocy loginu i hasła z lokalnej bazy danych użytkowników w Systemie.

c) System musi obsługiwać uwierzytelnianie w oparciu o: wbudowany serwer RADIUS, zewnętrzny serwer Radius, protokół LDAP, jak również w oparciu o wewnętrzną bazę użytkowników i urządzeń.

d) System musi obsługiwać autoryzację w oparciu o adresy MAC definiowane w wewnętrznej bazie z wykorzystaniem protokołu RADIUS.

e) System musi zapewniać automatyczne wykrywanie urządzeń końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, LDAP) lub żądania RADIUS pochodzących z przełączników dostępowych. W ramach postępowania muszą zostać dostarczone wszystkie niezbędne elementy, które umożliwią realizację powyższej funkcji we wszystkich lokalizacjach i segmentach sieci.

f) System musi aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych urządzeń końcowych i innych niechronionych urządzeń. Dla tak zdefiniowanych urządzeń końcowych muszą być zapewnione mechanizmy automatycznej kwarantanny.

g) System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z minimum systemów zewnętrznych: Microsoft Active Directory, Radius, LDAP.

h) System musi umożliwiać dodawania rozpoznanych urządzeń do grup systemowych.

i) System na podstawie rodzaju rozpoznanego urządzenia musi umożliwiać różnicowanie poziomu dostępu.

j) System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, adres MAC, nazwa urządzenia

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

końcowego HOSTNAME, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony VLAN z przydzielonym adresem IP.

k) System musi zapewniać scentralizowane zarządzanie z pomocą panelu zarządzania urządzeniami sieciowymi. Zarządzanie musi dopuszczać możliwość zarządzania agentowo jak i bez-agentowo.

l) System musi umożliwiać monitorowanie urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.

m) Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu oraz konfiguracji ustawień portu z zakresu: VLAN, Autoryzacja, Status, Opis.

n) System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.

o) System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.

p) System musi posiadać mechanizm automatyzacji wg harmonogramu z możliwością symulacji działania, min: włączenie wskazanych portów urządzeń sieciowych, wyłączenie wskazanych portów urządzeń sieciowych, wykonania komend na wskazanych urządzeń sieciowych, dodanie znalezionych urządzeń sieciowych w skazanych podsieciach z możliwością sklonowania konfiguracji z podanego urządzenia sieciowego wg podanych parametrów jak: parametry dostępowe SNMP w wersji 1, 2c, 3, producenta, modelu urządzenia.

q) System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).

r) Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor lub inne konta z delegowanymi uprawnieniami.

s) Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.

t) Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.

u) System musi oferować wsparcie dla linków akceptacyjnych generowanych z portalu sponsorskiego.

v) System musi oferować możliwość powiązania z bramką SMS celem wysyłania PIN-ów weryfikacyjnych. Wymagana jest obsługa PIN-ów składających się ze znaków alfanumerycznych i znaków specjalnych.

w) System musi umożliwiać przyznanie dostępu czasowego dla gości.

x) System musi umożliwiać dopasowanie wyglądu portalu logowania gościnnego, w tym co najmniej zmianę logo strony logowania, zmianę koloru tła i czcionek, treści, grafiki.

y) System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

z) System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.

aa) System musi posiadać funkcję automatycznego profilowania urządzeń nieposiadających agenta 802.1x (suplikanta) na podstawie: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI, Location, Agent, IP Range, Network Traffic i przyznawania dostępu do sieci na podstawie zdefiniowanych polityk dostępu do sieci.

bb) System musi posiadać obsługę realizowaną przez dedykowanego agenta przełączanie VLANów na określonych portach urządzeń sieciowych.

cc) System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:

a) MAC
b) PAP/ASCII
c) CHAP
d) 802.1X wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), itp.

dd) System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:

a) Tożsamość/Urządzenie końcowe,
b) Grupa tożsamości/urządzeń końcowych,
c) Parametry urządzeń końcowych, min: system operacyjny, wersja,
d) Atrybuty Active Directory,
e) Jednostka organizacyjna tożsamości/urządzeń końcowych,
f) Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
g) Grupy urządzeń sieciowych,
h) Porty urządzeń sieciowych,
i) Grupy portów urządzeń sieciowych,
j) Jednostka organizacyjna portów,
k) Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
l) Metoda autoryzacji.

ee) System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów:

a) Cisco Networks
b) Aruba Networks
c) Hewlett Packard Enterprise
d) Juniper Networks

ff) System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.

gg) System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

hh) System musi posiadać wewnętrzną bazę urządzeń. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych z poziomu Systemu lub z wykorzystaniem API.

ii) System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.

jj) System musi wykorzystywać informacje zawarte w bazie urządzeń końcowych dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania oraz autoryzacji.

kk) System musi pozwalać na weryfikację zalogowanego urządzenia końcowego IoT (Internet of Things) minimum za pomocą mechanizmów SNMP, DHCP, NMAP, Agenta oraz wywołania akcji: powiadomienie administratorów i/lub zablokowanie i rozłączenie sesji.

ll) Raportowanie i monitoring. System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

a) System musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń).
b) System musi mieć możliwość generowania szczegółowego wykazu urządzeń podłączonych do sieci, zorganizowanego według typu urządzenia końcowego.
c) System musi rejestrować dane o atrybutach urządzeń końcowych i raportować zmiany w atrybutach np. przydział do VLAN-u, przyznany adres IP, klasyfikacja urządzenia w Systemie.
d) System musi zapewniać dane historyczne o zmianach stanu konfiguracji portów dostępowych.
e) System musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania i procesem podłączanych urządzeń. Dane muszą być przechowywane i dostępne do analizy przez co najmniej 12 miesięcy.
f) System musi oferować możliwość tworzenia własnych szablonów raportów.
g) System musi umożliwiać logowanie do zewnętrznych serwerów logowania z wykorzystaniem Syslog.
h) System musi umożliwiać konfigurację generowanych alarmów i zautomatyzowanych akcji w oparciu o zdarzenia wewnętrzne np. w przypadku stwierdzenia zagrożenia na stacji, zablokowanie jej i powiadomienie administratora.
i) System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.

mm) System powinien logować i przetrzymywać we własnej bazie danych co najmniej następujące informacje:

a) adresy MAC przełączników, urządzeń końcowych i dostępowych.
b) adresy IP ww. urządzeń.
c) identyfikatory i nazwy portów przełączników określające porty na przełącznikach i urządzeniach dostępowych do których podłączane są urządzenia końcowe.
d) stan skanowania - wyniki skanowania urządzenia końcowego i jego ocena w oparciu skanowanie przeprowadzone przy pomocy dostępnych w rozwiązaniu agentów.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

e) informacje o użytkownikach.
f) nazwa użytkownika, do którego przypisany jest urządzenie końcowe.
g) nazwa zalogowanego użytkownika na urządzeniu końcowym, jeśli wykonywana jest na nim autoryzacja.
h) profil/rola jak została przydzielona urządzeniowi końcowemu przez System.
i) data zarejestrowania urządzenia końcowego w Systemie.
j) data ostatniego logowania urządzenia końcowego w sieci lub/i podłączenia.

nn) System musi umożliwiać wykonywanie na urządzeniach sieciowych skryptów CLI, które są elementem polityk bezpieczeństwa.

2. **Dodatkowe funkcjonalności Systemu.**

a) Wszystkie komponenty Systemu na stacji monitorowanej powinny mieć możliwość automatycznego wdrażania i konfiguracji w oparciu o predefiniowane reguły zarządzania.
b) System powinien obsługiwać automatyczny/zaplanowany transfer logów z agentów w celu archiwizacji.
c) Wymagana jest możliwość wykorzystania mechanizmy proxy do komunikacji z Internetem.
d) System musi umożliwiać personalizację wyglądu interfejsu zarządzania, w tym co najmniej zmianę logo strony logowania, zmianę koloru tła i czcionek, treści, grafiki.
e) Monitoring autoryzacji:
   a) Autoryzacje zaakceptowane w ciągu ostatnich 30 dni.
   b) Autoryzacje odrzucone w ciągu ostatnich 30 dni.
   c) Obciążenie serwera autoryzacji.
   d) Ostatnie 100 zdarzeń autoryzacji.
f) Monitoring dla zdarzeń systemowych:
   a) Ostatnie 100 zdarzeń systemowych.
g) Monitoring dla tożsamości:
   a) Podział tożsamości ze względu na typ konta.
   b) Podział tożsamości ze względu na tożsamości aktywne i nieaktywne.
   c) Podział tożsamości ze względu na konta, które straciły ważność.
   d) Wykorzystanie kont gościnnych z dostępem czasowym.
h) Monitoring dla urządzeń końcowych:
   a) Podział urządzeń ze względu na ich status.
   b) Podział urządzeń ze względu na ich typ.
   c) Podział urządzeń ze względu na urządzenia aktywne i nieaktywne.
i) Monitoring dla urządzeń sieciowych:
   a) Podział urządzeń ze względu na urządzenia aktywne i nieaktywne.
   b) Podział urządzeń ze względu na ich typ.
j) Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706