Załącznik nr 3a do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

PAKIET NR 1 – Dostawa licencji i oprogramowania wraz z wdrożeniem

Przedmiotem zamówienia jest zakup licencji oprogramowania zwiększającego bezpieczeństwo i wdrożenie na potrzeby i na podstawie „ZARZĄDZENIE NR 117/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 20 września 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców".

I. Przedmiot zamówienia:

1. **Zakup licencji oraz wdrożenie centralnego systemu ochrony Endpoint z modułem rozszerzonego wykrywania i reagowania - XDR.**
2. **Zakup i wdrożenie oprogramowania kontroli dostępu i zarządzania tożsamościami użytkowników oraz dostępu komputerów do sieci lokalnej.**

II. Wymagane funkcjonalności

ZAKUP LICENCJI ORAZ WDROŻENIE CENTRALNEGO SYSTEMU OCHRONY ENDPOINT Z MODUŁEM ROZSZERZONEGO WYKRYWANIA I REAGOWANIA – XDR:

Zamawiający wykorzystuje obecnie UTM firmy Sophos XG ze wsparciem do 11 listopada 2025r. Zamawiający wymaga, aby dostarczone oprogramowanie posiadało licencje wieczyste ze wsparciem technicznym min. 36 miesięcy oraz żeby było w pełni kompatybilne z posiadanym zarządzanym urządzeniem UTM Sophos XG.

1. Rozwiązanie musi mieć możliwość ochrony komputerów z systemem Windows (8 i nowsze) oraz serwerów z systemem Windows Server (Windows Server 2012 i nowsze).
2. Rozwiązanie musi umożliwiać stosowanie wielu polityk bezpieczeństwa.
3. Rozwiązanie musi posiadać zarządzalny mechanizm aktualizacji.
4. Rozwiązanie musi zapewniać kategoryzowanie i blokowanie stron.
5. Rozwiązanie musi zapewniać ochronę urządzeń przenośnych (np., USB).
6. Rozwiązanie musi posiadać skaner antymalware oraz kontrolę aplikacji.
7. Rozwiązanie musi posiadać ochronę przed włamaniami (IPS) oraz ochronę przed włamaniami opartą na hostach (HIPS).
8. Rozwiązanie musi oferować ochronę w czasie rzeczywistym.
9. Rozwiązanie musi być rozbudowane o opcję PUA – Blokowanie potencjalnie niechcianych aplikacji.
10. Rozwiązanie musi chronić Zamawiającego przed utratą danych (DLP).
11. Rozwiązanie musi zapewniać zgodność z interfejsem skanowania antymalware AMSI.
12. Rozwiązanie musi wykrywać złośliwy ruch [MTD].
13. Rozwiązanie musi posiadać ochronę przed eksploitami, zmianami w kodzie aplikacji oraz przez ransomware.
14. Rozwiązanie musi posiadać ochronę sektora rozruchowego dysku oraz ochronę przed atakami Man-in-the-Browser.
15. Rozwiązanie musi oferować wykrywanie zagrożeń powiązanych ze sobą procesami.

16. Rozwiązanie musi oferować wykrywanie podejrzanych zdarzeń i priorytetyzację, a także analizę zagrożeń w modelu drzewa.
17. Rozwiązanie musi oferować automatyczne usuwanie malware i izolację zarażonego hosta na żądanie.
18. Rozwiązanie musi gwarantować przechowywanie danych w chmurze do dalszej analizy, a także zdalny dostęp do centralnej konsoli zarządzającej w celu przeprowadzenia śledztwa i usunięcia problemu
19. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
20. Rozwiązanie musi zapewniać korzystanie z szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
21. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do systemu graylog (syslog).
22. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

Ochrona stacji roboczych
1. Rozwiązanie musi wspierać systemy operacyjne Windows dla systemów Windows 8 i nowszych: (Windows 8/Windows 10/Windows 11).
2. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
3. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
5. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
6. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
7. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
8. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
9. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
10. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
11. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
• tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,

• tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,

• tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,

• tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

• tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

• tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,

• tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,

• tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

• tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.

14. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

15. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.

16. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

17. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

18. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.

19. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

20. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.

21.Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
22. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
23. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
24. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
25. Rozwiązanie musi zapewniać ochronę przed zagrożeniami zero-day.
26. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera
1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowsze.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.

5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:
9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Szyfrowanie
1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Extended Detection and Response
1. Rozwiązanie musi posiadać moduł XDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta.
2. Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica”.
6. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
7. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.

8. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
9. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
10. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania poleceń powershell.

ZAKUP I WDROŻENIE OPROGRAMOWANIA KONTROLI DOSTĘPU I ZARZĄDZANIA TOŻSAMOŚCIAMI UŻYTKOWNIKÓW ORAZ DOSTĘPU KOMPUTERÓW DO SIECI LOKALNEJ.

I. Zamawiający wykorzystuje obecnie:
- przełączniki dostępowe (4szt. Aruba 2930F 48G POE+ 4SFP+ JL256A);

- przełącznik zarządzalne przy urządzeniach końcowych (61szt. TP-LINK SG-105E oraz TP-LINK SG-108E).

- kompletny punkt sieci bezprzewodowej (15 szt. Aruba AP-515 (RW) Unified AP Q9H62A) wraz z punktem centralnego zarządzania Aruba AirWave.

Zamawiający wymaga, aby dostarczone oprogramowanie było w pełni kompatybilne z wymienionymi urządzeniami.

II. Minimalne wymagania sprzętowe

1. System musi bazować na standardach RADIUS oraz TACACS+.
1.1 System powinien oferować różne możliwości zastosować, szczególnie:
- autoryzację bezprzewodową i przewodową w sieciach korporacyjnych,
- realizację dostępu dla gości,
- realizację dostępu BYOD (Bring Your Own Device),
- wymuszanie polityk bezpieczeństwa dla użytkowników lokalnych i mobilnych.
2. System musi umożliwiać instalację w środowisku Vmware (ESXi 7).
3. System musi posiadać licencje dostępową pozwalającą równoczesną obsługę co najmniej 250 urządzeń końcowych oraz licencje Onboard pozwalającą na realizację usługi BYOD w sieciach korporacyjnych dla co najmniej 150 urządzeń.

III. Funkcjonalności

1. System musi posiadać element funkcjonalny zarządzania, umożliwiający administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji sytemu oraz jego monitorowanie
1.1. System musi posiadać element funkcjonalny logowania i rozwiązywania problemów, umożliwiający gromadzenie wiadomości logowania z:
- infrastruktury sieciowej, w tym przełączników dostępowych
- sesji uwierzytelniania 802.1X
- zdarzeń kontroli dostępu (autoryzacji)
- zdarzeń głębokiej analizy stacji (posture assessment)
- zdarzeń związanych z błędami
- zdarzeń związanych z alarmami systemowymi
1.2. System musi posiadać element funkcjonalny usługowy (Policy Service), realizujący funkcje:
- serwera RADIUS dla infrastruktury sieciowej
- serwera polityk uwierzytelniania i kontroli dostępu 802.1X
- elementu decyzyjnego dla głębokiej analizy stacji (posture assessment)
- serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego (Guest Auth) i uwierzytelniania webowego (WebAuth)
- usług do profilowania stacji końcowych (Profiler)

2. System musi wspierać protokół Windows Active Directory

3. System musi umożliwiać zarządzanie za pomocą interfejsu graficznego przez przeglądarkę internetową.
4. System musi co najmniej wspierać następujące protokoły uwierzytelniania:
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
- EAP-MS-CHAPv2
- EAP-GTC
- EAP-TLS
5. System musi umożliwiać konfigurację mechanizmów EAP-TLS Session Resume i PEAP Session Timeout.
6. System musi umożliwiać konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect.
7.System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego.
8.System musi umożliwiać tworzenie kopii zapasowej systemu.
9.System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
10.System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów.
11.System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
- dostęp do interfejsu konfiguracji usług tożsamości 802.1X
- dostęp do interfejsu konfiguracji urządzeń sieciowych
- dostęp do interfejsu konfiguracji polityk
- dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
- dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
12.System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.
13.System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
- wiadomości e-mail
- syslog/graylog
14.System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
- nazwy użytkownika
- adresu MAC
- Audit Session ID
- adresu IP NAS
- numeru portu NAS
- statusu uwierzytelnienia (udana lub nieudana)
- powodu, jeżeli uwierzytelnienie nieudane
- zakresu czasowego co do dnia, godziny i minuty
15.System musi umożliwiać uwierzytelnienie i kontrolę dostępu:
- kablowego w sieci LAN
- bezprzewodowego w sieci WLAN
- zdalnego VPN
16.System musi wspierać implementację 802.1X przynajmniej z wbudowanym klientem 802.1X dla Windows 8/10
17.System musi umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based).
18.System musi umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.
19.System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV.

20.System musi posiadać lokalną bazę stacji końcowych. Lokalną bazę stacji końcowych można tworzyć per stacja końcowa na podstawie unikalnego adresu MAC.
21.System musi umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym co najmniej Google Chrome, Mozilla Firefox.
22.System musi umożliwiać dodawanie kont gościnnych przez wybrane osoby.
23System musi umożliwiać konfigurację wyglądu portalu dostępu dla gościa, w tym:
- zmianę logo strony logowania;
- zmianę obrazu tła strony logowania;
- zmianę logo bannera;
- zmianę obrazu tła bannera;
- zmianę koloru tła strony logowania;
- zmianę koloru tła strony bannera;
- zmianę koloru tła strony z treścią;
- zresetowanie ustawień do konfiguracji fabrycznej producenta.

24.System musi umożliwiać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP oraz HTTPS.
25.System musi umożliwiać zmianę adresu URL strony dostępowej dla gościa.
26.System musi umożliwiać automatyczne kasowanie wygasłych kont gościnnych na żądanie oraz okresowo co zadaną liczbę dni i o określonej godzinie.
27.System musi umożliwiać wyświetlenie czasu: ostatniego kasowania wygasłych kont gościnnych oraz następnego kasowania wygasłych kont gościnnych.
28.System musi umożliwiać stworzenie własnego wzorca językowego portalu dostępowego.
29.System musi umożliwiać specyfikację opcjonalną lub obowiązkową danych gościa w trakcie próby logowania.
30.System musi wyświetlać gościom informację o akceptacji polityki akceptowalnego użycia sieci (AUP).
31.System musi umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego w przedziale od 1 do 9.
32.System musi umożliwiać konfigurację czasu ważności hasła.
33.System musi umożliwiać kreację profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego.
34.System musi umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych.
35.System musi umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego.
36.System musi umożliwiać dokonanie profilowania (profiling) stacji końcowej i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.
37.System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł: DHCP, HTTP, RADIUS, Network Scan (NMAP), DNS, SNMP.
38.System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.
39.System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym minimum dla:
- Android;
- Apple: Apple MacBook, Apple iPad, Apple iPhone, Apple iPod;
- Microsoft Workstation: Windows 7, Windows 8, Windows 10, Windows 11;

40.System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Windows 11 pod kątem wpisów w rejestrze, w tym kluczy rejestru z kluczem root: HKLM, HKCC, HKCU, HKU, HKCR z zadanym podkluczem.
41.System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows 7, Windows 8, Windows 10, Windows 11 pod kątem uruchomionych aplikacji (Application Condition).
42.System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows 7, Windows 8, Windows 10, Windows 11 pod kątem zainstalowanych aplikacji Antywirusowych w tym:
- stwierdzenia czy system AV jest obecny na stacji;

- stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni;
- daty ostatniego pliku definicji;
- aktualnego czasu systemowego.

43.System musi umożliwiać głęboką analizę stacji końcowej z systemem Windows 7, Windows 8, Windows 10, Windows 11 pod kątem zainstalowanych aplikacji AntiSpyware w tym:
- stwierdzenia czy system AS jest obecny na stacji;
- stwierdzenia czy definicje sygnatur AS są nie starsze niż zadana ilość dni;
- daty ostatniego pliku definicji;
- aktualnego czasu systemowego.

IV. Raportowanie

System musi umożliwiać generowanie przynajmniej następujących raportów:
- raportów dla protokołów AAA;
- accountingu RADIUS;
- uwierzytelniania RADIUS;
- raportów dozwolonych protokołów;
- sumarycznej informacji o uwierzytelnieniach RADIUS per protokół;
- raportów dla poszczególnych instancji serwerów systemu, w tym:
    a) administratorów systemu i ich uprawnień (administrator entitlements);
    b) logowania administratorów do systemu;
    c) zmian konfiguracji serwera dokonanych przez administratorów;
    d) zdrowia serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS);
    e) zmian operacyjnych serwera dokonanych przez administratorów;
- raportów dla stacji końcowych, w tym:
    a) Top N uwierzytelnień per adres MAC stacji;
    b) Top N uwierzytelnień per użytkownik;
    c) działań podsystemu profilera per adres MAC;
    d) zarejestrowane urządzenia per użytkownik;
- raportów dla błędów, w tym:
    a) błędów uwierzytelniania per szczegółowy kod błędu który wystąpił;
    b) sumarycznych przyczyn nieudanych uwierzytelnień;
    c) Top N uwierzytelnień per rodzaj błędu;
- raportów dla urządzeń sieciowych:
    a) sumarycznych uwierzytelnień dla urządzeń sieciowych;
    b) Top N uwierzytelnień per urządzenie sieciowe;
    c) niedostępności serwera AAA dla urządzenia sieciowego;
    d) wiadomości logowanych przez urządzenia sieciowe;
    e) stanu portów i sesji urządzenia sieciowego z perspektywy SNMP;
    f) top N niedostępności serwera AAA dla urządzeń sieciowych;
- raportów użytkowników;
- raportów katalogu sesji, m.in. aktywnych sesji RADIUS, historii sesji RADIUS, zaterminowanych sesji RADIUS.

V. Organizacja wdrożenia

1.Przeprowadzenie analizy przedwdrożeniowej i uzgodnienie z Zamawiającym harmonogramu wdrożenia.

2.Dostarczeniu licencji Systemu.

3.Instalacja i konfiguracja Systemu (w tym prace konfiguracyjne systemu uwierzytelniania opartego o protokół PEAP z protokołem EAP-TLS w wersji 802.1x oraz konfiguracja Captive Portal z autentyfikacją opartą na Self-registration.

4.Dostawca sprawdzi i dostosuje oprogramowanie na przełącznikach Zamawiającego do wersji zalecanej przez producenta systemu NAC.
5.Zamawiający wymaga, aby wraz z rozwiązaniem oraz kontraktem serwisowym oferta obejmowała minimum 2 dniowy instruktaż powdrożeniowy dla 3 pracowników Zamawiającego obejmujące zakresem obsługę systemu NAC. Warsztaty muszą być przeprowadzone w siedzibie Zamawiającego lub za pomocą platformy umożlwiającej zdalne prowadzenie szkoleń.
6.Przeprowadzenie szkoleń.
7.Dostarczenie dokumentacji powykonawczej.

VI. Wymagania dodatkowe

1. Całość oprogramowania musi zostać dostarczona i uruchomiona w siedzibie Zamawiającego.
2. Oferowane rozwiązanie musi być produktem fabrycznie nowym.
3. Oferowane rozwiązanie w dniu składania ofert nie może być przeznaczone przez producenta do wycofania z produkcji lub ze sprzedaży.
4. Zamawiający wymaga zapewnienia Wykonawcy, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
5. Wykonawca zobowiązuje się do wykonania wszelkich prac z zachowaniem najwyższej staranności.
6. Dostawca musi dostarczyć wszystkie niezbędne komponenty do wdrożenia.
7. Wdrożenie musi zakończyć wykonanie testów poprawności pracy systemu kontroli dostępu do sieci oraz sporządzenie protokołu odbioru.
8. Dostawca rozwiązania musi zatrudniać minimum 1 inżyniera wsparcia technicznego posiadającego techniczny certyfikat producenta w ścieżce Security (np. CCIE Security lub równoważny).
9. Zamawiający wymaga wdrożenia najnowszej, dostępnej wersji systemu NAC wspieranej przez producenta systemu.

VII. Wymagania obsługi serwisowej

1. Oferowane rozwiązanie musi posiadać bezterminową (dożywotnią) licencję.
2. Oferowane rozwiązanie musi posiadać 36-miesięczną usługę serwisową, gwarancję i wsparcie producenta oraz możliwość aktualizacji mechanizmów bezpieczeństwa.
3. W czasie obowiązywania usługi serwisowej, Zamawiający musi mieć prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade) na posiadanej przez siebie platformie.
4. W czasie obowiązywania usługi serwisowej Zamawiający musi mieć dostęp do wsparcia technicznego producenta lub autoryzowanego partnera producenta, świadczonego w dni robocze od poniedziałku do piątku w godzinach 9:00-17:00.
5. Zamawiający może zgłaszać sprawy z zakresu pomocy technicznej kontaktując się poprzez dedykowany adres email lub numer infolinii.
6. Dostarczone oprogramowanie musi posiadać gwarancję producenta na cały czas obowiązywania usługi serwisowej.
7. Dokumentacja do systemu zarządzania musi być publicznie dostępna na stronie internetowej producenta.
8. Producent musi publikować na swojej stronie internetowej informacje o wykrytych lukach bezpieczeństwa w systemie.