Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny Samorząd we Włodowicach”

Zamówienie finansowane na podstawie umowy o powierzenie grantu nr FERC.02.02-CS.01-001/23/0751/ FERC.02.02-CS.01-001/23/2024 w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC). Priorytet II: Zaawansowane usługi cyfrowe. Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa.

1. Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny Samorząd we Włodowicach”.
2. Przedmiot zamówienia obejmuje dostawę:
   1) systemu antywirusowego zapewniającego ochronę z wykorzystaniem m.in. modułu antywirusowego, firewalla, szyfrowania dysków oraz EDR, 60 licencji, 2 lata,
   2) rozwiązania klasy NextGeneration Firewall (UTM) zabezpieczającego zasoby lokalnej sieci komputerowej urzędu na styku sieci LAN z internetem, 2 lata,
   3) systemu do zarządzania infrastrukturą i bezpieczeństwem IT, 2 lata,
   4) systemu informatycznego wspomagającego procesy zarządzania incydentami bezpieczeństwa oraz analizy ryzyka, 2 lata,
   5) systemu klasy PAM do zarządzania dostępem uprzywilejowanym, 5 licencji,
   6) systemu klasy DLP do identyfikacji oraz zapobiegania wyciekom danych,
   7) systemu klasy NAC zapewniającego kontrolę dostępu do sieci komputerowej urzędu oraz wgląd w działania urządzeń i użytkowników korzystających z zasobów sieciowych urzędu, 2 lata,
   8) serwerów do budowy systemu wysokiej dostępności – 2 sztuki,
   9) macierzy dysków – 1 sztuka,
   10) przełącznika sieciowego – 1 sztuka,
   11) zasilaczy awaryjnych – 22 sztuki

   wraz z usługą wdrożenia zakupionych rozwiązań.
3. Aby zachować regułę konkurencyjności dopuszcza się rozwiązania równoważne do rozwiązań wyspecyfikowanych przez Zamawiającego. Za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii, funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły, itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób. Za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic nie wpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, identycznych dla obu rozwiązań, dla których to warunków rozwiązania te są dedykowane.

4. W niniejszym dokumencie opisano wymagane parametry minimalne urządzeń, oprogramowania i usług. Wykonawca ma prawo zaoferować sprzęt i oprogramowanie o lepszych parametrach technicznych oraz szerszy zakres usług lub usługi o wyższym standardzie.

5. Dostarczane urządzenia i oprogramowanie muszą być sprawne, dobrej jakości i fabrycznie nowe, wyprodukowane nie wcześniej niż w 2024 r. Dostarczony sprzęt nie może posiadać wad fizycznych i prawnych oraz musi być gotów do użytkowania bez żadnych dodatkowych zakupów i inwestycji. Pod pojęciem „fabrycznie nowe" Zamawiający rozumie produkty wykonane z nowych, nieregenerowanych elementów, bez śladów uszkodzenia, nie poleasingowe, posiadające zgodne z właściwymi przepisami atesty, certyfikaty, licencje i dopuszczenia, w oryginalnych opakowaniach (pojemnikach, obudowach) stosowanych typowo dla danego produktu przez producenta, zaopatrzone w etykiety identyfikujące dany produkt.

6. Szczegółowy opis przedmiotu zamówienia (specyfikacja techniczna):

1) Dostawa systemu antywirusowego zapewniającego ochronę z wykorzystaniem m.in. modułu antywirusowego, firewalla, szyfrowania dysków oraz EDR – 60 licencji, okres ochrony: 2 lata

ADMINISTRACJA ZDALNA W CHMURZE

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

OCHRONA STACJI ROBOCZYCH

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.

5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. 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.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. 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).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. 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.
14. 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.
15. 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.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    1) tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    2) tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    3) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    4) 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,
    5) tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. 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.
18. 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.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

1) tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
2) tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
3) tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
4) tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. 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 oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
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. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
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.

<u>DODATKOWE WYMAGANIA DLA OCHRONY SERWERÓW WINDOWS:</u>

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
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.

DODATKOWE WYMAGANIA DLA OCHRONY SERWERÓW LINUX:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS/SAN, musi w pełni wspierać rozwiązanie DELL EMC Isilon.
21. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

SZYFROWANIE

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
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.

OCHRONA URZĄDZEŃ MOBILNYCH OPARTYCH O SYSTEM ANDROID

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
    1) usunięcie zawartości urządzenia,
    2) przywrócenie urządzenie do ustawień fabrycznych,
    3) zablokowania urządzenia,
    4) uruchomienie sygnału dźwiękowego,
    5) lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
    1) nazwę aplikacji,
    2) nazwę pakietu,
    3) kategorię sklepu Google Play,
    4) uprawnienia aplikacji,
    5) pochodzenie aplikacji z nieznanego źródła.

SANDBOX W CHMURZE

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.

3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    1) Czysty,
    2) Podejrzany,
    3) Bardzo podejrzany,
    4) Szkodliwy.
13. 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.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

MODUŁ XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji 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.

11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń Powershell.

2) Dostawa i wdrożenie rozwiązania klasy NextGeneration Firewall (UTM) zabezpieczającego zasoby lokalnej sieci komputerowej urzędu na styku sieci LAN z internetem, 2 lata

Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.

10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. Moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

1. Urządzenie ma być dostarczone wraz z komercyjnym, zaawansowanym skanerem antywirusowym oraz umożliwiać skanowanie plików w oparciu o sandboxing zlokalizowany w Internecie na serwerach producenta i na terenie Unii Europejskiej. Nie dopuszcza się aby analiza sandboxingu była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza sandboxingu była przeprowadzana przez firmy trzecie.
2. Skaner antywirusowy ma być dostarczany przez firmy trzecie (inne niż producent rozwiązania).
3. Administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem.
4. Skaner antywirusowy ma pochodzić od europejskiego producenta.
5. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
6. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

7. Urządzenie ma być dostarczone wraz z komercyjnym, europejskim skanerem Antywirusowym.

OCHRONA ANTYSPAM

1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o:
   1) białe/czarne listy,
   2) DNS RBL,
   3) Skaner heurystyczny.
3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
   1) PPTP VPN,
   2) IPSec VPN,
   3) SSL VPN.
3. SSL VPN ma działać w trybie tunelu.
4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 77 kategorii tematycznych stron internetowych. Rozszerzony URL Filtering posiada miliony sklasyfikowanych stron internetowych.
3. Klasyfikacja URL musi się odbywać w oparciu o komunikację z serwerami producenta znajdującymi się w sieci Internet, a nie na bazie danych przechowywanej lokalnie w urządzeniu.
4. Administrator ma mieć możliwość dodawania własnych kategorii URL.
5. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
   1) blokowanie dostępu do adresu URL,
   2) zezwolenie na dostęp do adresu URL,
   3) blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
6. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
7. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
8. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
9. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
10. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
11. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
   1) lokalną bazę użytkowników (wewnętrzny LDAP),
   2) zewnętrzną bazę użytkowników (zewnętrzny LDAP),
   3) usługę katalogową Microsoft Active Directory.
2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
   1) SSL,
   2) Radius,
   3) Kerberos.
4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
10. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
   1) równoważenie względem adresu źródłowego,
   2) równoważenie względem połączenia.
3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

ROUTING (TRASOWANIE)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
5. Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.

ADMINISTRACJA URZĄDZENIEM

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
15. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
16. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
17. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
18. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    1) manualnego eksportu do pliku w dowolnym momencie czasu,
    2) automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
19. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
20. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
21. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.

2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
2. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
3. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
4. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
5. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
6. Urządzenie ma posiadać usługę DNS Proxy.
7. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
8. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
9. Urządzenie musi mieć zaimplementowane Open API.
10. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

GWARANCJA I SERWIS

1. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
3. Urządzenie ma być objęte rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny.

PARAMETRY SPRZĘTOWE

1. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB.
2. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.
3. Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16.
4. Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10.
5. Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:
    1) Moduł z 8 interfejsami miedzianymi 2,5Gbps

   2) Moduł z 4 interfejsami miedzianymi 10Gbps.
   3) Moduł z 8 interfejsami miedzianymi 1Gbps (4 pary interfejsów w trybie bypass).
   4) Moduł z 8 interfejsami miedzianymi 1Gbps.
   5) Moduł z 8 interfejsami światłowodowymi 1Gbps.
   6) Moduł z 4 interfejsami światłowodowymi 10Gbps.
   7) Moduł z 2 interfejsami światłowodowymi 25Gbps.
6. Zainstalowany moduł z 4 interfejsami światłowodowymi 10Gbps.
7. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
8. Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.
9. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps.
10. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps.
11. Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps.
12. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps.
13. Liczba tuneli VPN IPSec – minimum 1000.
14. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150.
15. Obsługa interfejsów 802.11q (VLAN) – minimum 256.
16. Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę.
17. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie ActivePassive.
18. Urządzenie nie ma limitu na liczbę użytkowników.
19. Liczba reguł filtrowania – minimum 16 384.
20. Liczba tras statycznego routingu – minimum 5 120.
21. Liczba tras dynamicznego routingu – minimum 10 000.
22. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U. 141. Urządzenie musi być wyposażone w moduł TPM.

SYSTEM ZAAWANSOWANEGO ZARZĄDZANIA LOGAMI

1. W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
2. Rozwiązanie musi zostać dostarczone w postaci maszyny wirtualnej instalowanej w środowisku Vmware lub Windows Hyper-V.
3. Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
4. Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
5. Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.
6. Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.
7. Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
8. Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.
9. Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).
10. Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.
11. Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
12. Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).
13. Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.

14. Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).
15. Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów).
16. Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.
17. Rozwiązanie musi umożliwiać tworzenie statycznych raportów.
18. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
19. Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.
20. Rozwiązanie musi umożliwiać tworzenie własnych raportów.
21. Rozwiązanie musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) z funkcjonalnością „drill-down".
22. Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości e-mail.
23. Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.
24. Liczba zdarzeń na sekundę (EPS): min. 10 000.
25. Zarządzanie logami: 24 miesiące.
26. Liczba obsługiwanych urządzeń min. 500.
27. Liczba zapisu zdarzeń na dobę: min 13000 MB.
28. System logów musi wspierać hiperwizory: Vmware ESXi oraz Microsoft HyperV.

WDROŻENIE ROZWIĄZANIA KLASY NEXTGENERATION FIREWALL (UTM)

1. Dostarczone rozwiązanie musi być połączone z wdrożeniem w siedzibie i infrastrukturze Zamawiającego.
2. Wykonawca przeprowadzi szkolenie dla administratora sieci komputerowej Zamawiającego z administracji dostarczonym rozwiązaniem. Szczegółowy plan, zakres i termin szkolenia zostanie uzgodniony przez Wykonawcę z Zamawiającym.
3. Szkolenie musi odbywać się stacjonarnie w siedzibie Zamawiającego. Minimalny czas trwania szkolenia to 10 godzin zegarowych.
4. Wykonawca zapewni Zamawiającemu możliwość skorzystania z konsultacji z inżynierem do 12 miesięcy po odbytym szkoleniu w formie e-mail lub kontaktu telefonicznego.

3) Dostawa i wdrożenie systemu do zarządzania infrastrukturą i bezpieczeństwem IT, 2 lata

ARCHITEKTURA / BUDOWA

1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 50 Klientów jednocześnie.
2. Architektura / budowa:
   1) Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
   2) Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
   3) Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
   4) Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
   5) Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
3. Konfiguracja Architektury:

1) Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
2) System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

WYMAGANIA SYSTEMOWE

1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).
2. Klient musi działać na systemach 32- i 64-bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
3. Klient musi wspierać co najmniej poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera, Chrome, FireFox.
4. Serwer musi działać na systemach 64-bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.
5. Serwer www musi być oparty o platformę Microsoft 64-bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9.
6. Baza danych musi działać na bezpłatnym silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64-bitowych komercyjnych lub bezpłatnych (np. Microsoft SQL Server Express Edition).
7. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

INTERFEJSY

1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
3. System zapewnia integrację z modelem LLM.

FUNKCJONALNOŚCI SYSTEMU ZARZĄDZANIA INFRASTRUKTURĄ IT

1. Funkcjonalność Klienta: System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkowniku.
2. Funkcjonalność konsoli administracyjnej:
   1) Konsola administracyjna musi być wielojęzyczna (co najmniej język polski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.
   2) W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.
   3) Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.

3. Funkcjonalność panelu pracownika: Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.
4. Zarządzanie licencjami: System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej deinstalacji oprogramowania.
5. Wzorce aplikacji i pakietów: System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.
6. Inwentaryzacja sprzętu komputerowego i urządzeń: System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.
7. Inwentaryzacja urządzeń sieciowych: System musi posiadać zdolności do identyfikacji i zarządzania środowiskami wirtualizacji Hyper-V i VMware oraz urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP oraz dla środowisk wirtualizacji, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.
8. Inwentaryzacja sprzętu: System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.
9. Ochrona danych musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwolonymi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.
10. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.
11. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
12. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
13. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.
14. Automatyzacja: System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii

bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.

15. Zarządzanie magazynem IT: System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.
16. Repozytorium: Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.
17. Kody kreskowe: System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.
18. Wysyłanie wiadomości: System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.
19. System musi posiadać możliwość eksportu / importu treści.
20. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.
21. Monitorowanie stron www: System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.
22. Monitorowanie serwerów WWW: System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.
23. Monitorowanie dziennika zdarzeń: System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
24. System musi umożliwiać monitorowanie komunikatów Syslog.
25. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.
26. Monitorowanie sensorów: System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.
27. Repozytorium CMDB: System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.
28. Worktime manager: System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostepnienia w panelu pracownika.

29. Raportowanie i eksport danych: System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.
30. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.
31. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.
32. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

WSPARCIE I POMOC

1. Pomoc techniczna musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.
2. Zamawiający wymaga zapewnienia aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również świadczenia innych usług wspomagających korzystanie z Oprogramowania.
3. Czas trwania usługi SLA wynosi min. 24 miesiące od daty wdrożenia Oprogramowania.
4. System powinien zostać zainstalowany oraz skonfigurowany przez przedstawiciela wsparcia technicznego na infrastrukturze Zamawiającego. Proces wdrożenia musi obejmować pełne środowisko operacyjne umożliwiające prawidłowe funkcjonowanie systemu.
5. Powinny zostać przeprowadzone szkolenia administracyjne oraz użytkowe, o łącznym czasie trwania 4 godzin, w okresie nie dłuższym niż 90 dni od daty zakupu systemu.

WDROŻENIE SYSTEMU

1. Instalacja i konfiguracja środowiska systemowego, obejmująca komponenty niezbędne do prawidłowego funkcjonowania wdrażanego systemu, w tym: MS SQL Server, Java oraz Apache Tomcat.
2. Instalacja systemu, w tym wszystkich komponentów niezbędnych do jego prawidłowego funkcjonowania, a także opcjonalna konfiguracja routera.
3. Pierwsze uruchomienie systemu, obejmujące: rejestrację produktu, konfigurację agenta, utworzenie kopii zapasowej (backup), pobranie oraz instalację komponentu agenta.
4. Przesłanie dokumentacji wdrożeniowej do Zamawiającego, zawierającej szczegółowe informacje dotyczące instalacji oraz konfiguracji systemu.

SZKOLENIE WDROŻONEGO SYSTEMU

1. Szkolenie podstawowe wdrożonego systemu, przeprowadzone przez przedstawiciela wsparcia technicznego na infrastrukturze Zamawiającego.
2. Szkolenie obejmuje zarządzanie systemem, monitorowanie, inwentaryzację oraz zagadnienia związane z bezpieczeństwem.

4) Dostawa i wdrożenie systemu informatycznego wspomagającego procesy zarządzania incydentami bezpieczeństwa oraz analizy ryzyka – okres subskrypcji: min. 2 lata

PODSTAWOWA FUNKCJONALNOŚĆ SYSTEMU:

1. Wykonawca wdroży system informatyczny wspomagający procesy zarządzania incydentami bezpieczeństwa i ochroną danych osobowych oraz analizy ryzyka usprawniającego, przyczyniając się jednocześnie do realizacji kluczowych celów dyrektywy NIS2, ustawy KSC oraz stosowania przepisów RODO.
2. Zamawiający oczekuje systemu utrzymywanego w modelu model SAAS
3. Zamawiający oczekuje możliwości korzystania z systemu bez dodatkowych aplikacji dedykowanych
4. W chwili obecnej Zamawiający nie posiada systemu informatycznego wspierającego i monitorującego poprawne funkcjonowanie procedur SZBI; dzięki wdrożeniu systemu ma zostać zapewnione wsparcie realizacji wymaganych przepisami prawa procesów z zakresu bezpieczeństwa informacji oraz zarządzania procesami, w szczególności:
   1) upoważnieniami dopuszczającymi (nadawanie, zarządzanie zmianą, odbieranie uprawnień),
   2) incydentami i zgłoszeniami naruszeń bezpieczeństwa i ochrony danych osobowych,
   3) analiza ryzyka w bezpieczeństwie informacji i ochrony danych osobowych,
   4) zbieranie dowodów na zgodność z procedurami,
   5) wspomaganie szkoleń w systemie e-learningowym,
   6) prowadzeniem rejestrów wymaganych przepisami prawa.
5. Zamawiający oczekuje, że System będzie dostępny dla min. 5 użytkowników w modelu subskrypcyjnym; okres subskrypcji: 2 lata
6. System ma zapewnić funkcjonalności w zakresie nie mniejszym niż:
   1) zdefiniowania własnej skali ryzyka i jej późniejszej modyfikacji przez Zamawiającego,
   2) przeprowadzenia analiz ryzyka dla elementów pochodzących ze stworzonych słowników oraz tych utworzonych przez Zamawiającego,
   3) uwzględniania w analizie zmodyfikowanych wartości z utworzonych słowników, definiowania własnych reguł obliczeń dla pól formularzy, definiowania własnych arkuszy analizy ryzyka,
   4) realizacji wszystkich rodzajów analiz określonych w przepisach dot. ochrony danych osobowych, m.in.: analizy ryzyka, oceny ryzyka naruszenia, testów równowagi, oceny skutków przetwarzania,
   5) realizacji analiz ryzyka naruszeń i incydentów dotyczących cyberbezpieczeństwa,
   6) zdalnego audytu podmiotów przetwarzających,
   7) prowadzenia dowolnych rejestrów dotyczących zarządzania bezpieczeństwem informacji, w tym w szczególności rejestrów dot. systemów IT, w tym: rejestr zasobów IT, typy zasobów IT, rejestrów zniszczenia/usunięcia danych i nośników, rejestry uprawnień, rejestry kopii zapasowych itp.
   8) klasyfikacji informacji oraz zarządzania aktywami,
   9) definiowania i generowania dowolnych raportów w formatach: *.docx, *.xlsx z automatycznym wypełnieniem pól na podstawie tagów referujących do pól formularza,
   10) sugestii podczas przeprowadzania analizy, np. poprzez proponowanie odpowiednich zagrożeń na podstawie ustalonej listy podatności,
   11) dokumentowania realizowanych audytów,
   12) automatycznej analizy udzielanych odpowiedzi w ankietach oraz opracowana protokołu identyfikującego kluczowe obszary ryzyka,
   13) korzystania z funkcjonalności bazy wiedzy, która automatycznie wspiera w wypełnianiu formularzy związanych z cyberbezpieczeństwem i RODO np. w opisie zasobów, analizie ryzyka. Przykład: na podstawie opisu charakteru przetwarzania, aplikacja będzie miała funkcjonalność proponowania potencjalnego ryzyka, zagrożenia i podatności,
   14) logowania MFA - z wykorzystaniem tokenów autoryzacyjnych Google/Microsoft Authenticator,

15) zarządzania uprawnieniami opartymi na rolach, w tym możliwość tworzenia grup lokalnych, definicja uprawnień dla właścicieli grupy,
16) definiowania i dziedziczenia uprawnień,
17) pełnej konfiguracji słowników, w tym zmiany schematu struktury słowników przez Zamawiającego,
18) zarządzania słownikami, w tym nielimitowanego dodawania nowych rozwiązań bez koniecznej ingerencji w kod źródłowy aplikacji,
19) zarządzania workflow i procesami, w tym tworzenia nowych i modyfikacja procesów dotyczących wprowadzania informacji do formularzy przez określonych pracowników, na poszczególnych etapach procesów,
20) definiowania czasowych dostępów dla użytkowników do zasobów, w tym np. możliwość zmiany przypisania licencji do innych użytkowników w trakcie trwania umowy – w ramach dostępnej puli,
21) możliwość wykorzystania epodpisu wewnętrznego,
22) definiowania procesów składających się z dowolnej ilości akcji, których kolejność warunkowana jest wynikiem walidacji formularzy na podstawie zdefiniowanych warunków przez Zamawiającego,
23) wysyłania powiadomień o zmianie statusu dla danego procesu, w kontekście danego rekordu,
24) definiowania szablonów zadań, które będą automatycznie uruchomione po wystąpieniu określonych przez Zamawiającego warunków,
25) generowania dokumentów na podstawie szablonów,
26) generowania umów powierzenia na podstawie zdefiniowanych szablonów *.docx,
27) definiowania filtrów i ich zapisania do przeszukiwania rekordów wg zawartości,
28) zmiany nazwy dla elementów menu wg wymagań Zamawiającego,
29) tworzenia obiegów dot. nadawania lub zmiany uprawnień i upoważnień,
30) importu danych z dowolnego pliku *.xlsx bez konieczności dostosowania do zadanego szablonu importu, na podstawie przyporządkowania w trakcie importu kolumn z pliku do zawartości słowników,
31) exportu wszystkich danych merytorycznych wraz z powiązaniami w postaci plików co najmniej w *.xlsx

7. System musi zapewniać:
   1) dokumentację w formie elektronicznej z samouczkami w języku polskim,
   2) dostępność z powszechnie stosowanych przeglądarek internetowych z możliwością dostępu do wszystkich funkcjonalności na tabletach i smartfonach z Android/iOS/Windows, w tym w szczególności Edge i Firefox,
   3) aktualizację w okresie dostępu do systemu do najnowszej wersji w tym w szczególności dostosowujący system do zmieniających się przepisów prawa i wymagań bezpieczeństwa.
8. Wymagania dodatkowe - Zamawiający oczekuje:
   1) możliwości logowania się do systemu bez konieczności instalowania jakichkolwiek dodatkowych komponentów oprócz z przeglądarki internetowej w aktualnej stabilnej wersji,
   2) utrzymania systemu w formule oprogramowanie jako usługa tj. zapewnienie architektury i ciągłości działania usługi bez konieczności zapewnienia hostingu przez Zamawiającego,
   3) w pełni funkcjonującego oprogramowania; oprogramowanie ma zawierać wszystkie funkcjonalności gotowe do użycia.
9. Wymagania wobec Wykonawcy/Producenta Systemu:
   1) Zapewnienie i realizacja wsparcia technicznego w godzinach pracy Zamawiającego;
   2) Aktualizację systemu wg aktualnych wytycznych, jego dostosowanie i implementacja zmian wynikających z przepisów prawa;
   3) Przegląd systemu i logów, celem podnoszenia jakości i wdrażania uwag użytkowników tzw. User experience;
   4) Wykonywanie kopii zapasowej systemu oraz danych i udostępniane ich na życzenie Zamawiającego w terminie do 3 dni roboczych; odtworzenie kopii zapasowej na życzenie Zamawiającego ma nastąpić w ciągu 12 godzin roboczych;

5) Zapewnienie obsługi gwarancyjnej;
6) Przeprowadzanie okresowych szkoleń z nowych funkcjonalności i aktualizację dokumentacji wchodzącej w skład instrukcji, w tym samouczków;
7) Jeżeli oferowane oprogramowanie opiera się lub wykorzystuje technologię firm trzecich to komponenty te, dla Zamawiającego muszą być legalne i na bieżąco aktualizowane oraz zgodne z polityką licencjonowania firmy trzeciej; powinna zawierać na bieżąco pojawiające się poprawki bezpieczeństwa;
8) Jeżeli oferowane oprogramowanie opiera się o komponenty wymagające odpłatnego licencjonowania ze strony Zamawiającego to koszty z tym związane muszą być sfinansowane przez dostawcę usługi, a licencje przekazane Zamawiającemu;
9) Zapewnienie kompatybilności Systemu z najnowszą wersją każdego z komponentów programowych niezbędnych do prawidłowego ich działania oraz z najnowszą wersją przeglądarki internetowej. W przypadku wykrycia braku wyżej określonej kompatybilności Wykonawca/Producent Systemu niezwłocznie dostarczy wersję kompatybilną, jednak nie później niż w ciągu 30 dni od czasu wykrycia i zgłoszenia przez Zamawiającego lub pozyskania przez Wykonawcę informacji o ww. niekompatybilności za pomocą ogólnodostępnych źródeł informacji. Za zgodą Zamawiającego termin 30 dni może ulec wydłużeniu w przypadku, jeśli niekompatybilność ta nie wpływa rażąco na funkcjonalność Systemu lub nowsza wersja komponentu, który stracił kompatybilność nie jest konieczna z punktu widzenia bezpieczeństwa systemów Zamawiającego.
10) Regularnego przeprowadzania testów bezpieczeństwa Systemu prowadzonego przez zewnętrzne podmioty specjalizujące się w zagadnieniach cyberbezpieczeństwa. Przedstawianie na życzenie Zamawiającego wyników testów potwierdzających odpowiedni poziom bezpieczeństwa Systemu.
11) Zapewnienia w sposób ciągły usuwania wad Systemu wpływających na obniżenie bezpieczeństwa informacji.
12) Zamawiający zastrzega sobie możliwość przeprowadzania testów bezpieczeństwa Systemu. Wykonawca jest zobowiązany do usunięcia wykrytych wad Systemu do 30 dni od czasu powiadomienia przez Zamawiającego.
13) Bieżącego przekazywania informacji mogących mieć wpływ na cyberbezpieczeństwo Systemu i wszystkich elementów konfiguracji środowiska, w którym System działa.
14) Wykorzystywanie nowoczesnych rozwijanych technologii w celu podnoszenia bezpieczeństwa Systemu.
15) Zapewnienie prawidłowej konfiguracji i odpowiedniego poziomu zabezpieczeń dla modułów udostępnionych w sieci Internet.

10. W zakresie obsługi awarii Zamawiający oczekuje:
    1) udzielania konsultacji telefonicznych w dni robocze w godzinach 8.00 – 16.00 przez chat oraz pod wskazanym numerem telefonu.
    2) udzielania konsultacji zdalnych.
    3) czasy obsługi:
        a) czas reakcji na zgłoszoną awarię – do 10 godzin po dokonaniu zgłoszenia przez Zamawiającego, liczony w pełnych godzinach, w dni robocze, w godzinach pracy Urzędu, od momentu dokonania zgłoszenia przez Zamawiającego do momentu przyjazdu serwisu do siedziby Zamawiającego w okresie gwarancji i rękojmi za wady
        b) czas usunięcia awarii lub zapewnienie alternatywnego sposobu pracy na Systemie – do 14 dni kalendarzowych,.
    4) analizy, wskazania przyczyny i usunięcia nieprawidłowego działania systemu objętego umową.

ZAKRES WDROŻENIA SYSTEMU:

1. Wstępna konfiguracja systemu.
2. Ustawienie predefiniowanych ról dopasowanych do specyfiki Zamawiającego oraz grup uprawnień (wstępna konfiguracja RBAC).

3. Udostępnienie predefiniowanych słowników obejmujących: zagrożenia, podatności, podstawy przetwarzania, kategorie danych, kategorie osób.
4. Udostępnienie predefiniowanych szablonów raportów, w tym raportów dla analizy ryzyka.
5. Udostępnienie predefiniowanej konfiguracji dla analiz, w tym dla analizy ryzyka, testów równowagi, oceny wagi naruszenia.
6. Wstępna konfiguracja pulpitów z wykresami analitycznymi.
7. Udostępnienie możliwości logowania MFA dla użytkowników.
8. Konfiguracja automatycznych codziennych backupów.
9. Udostępnienie pakietu tokenów AI wraz np. z funkcjonalnością opracowań podsumowań raportów z analizy ryzyka.

SZKOLENIE WDROŻONEGO SYSTEMU:

1. Prezentacja konfiguracji i najistotniejszych funkcjonalności systemu.
2. Dostęp do dokumentacji oraz bazy kompetencji obejmującej tutoriale prezentujące funkcjonalność w języku polskim.
3. Dostęp do filmów instruktażowych.
4. Bezpłatne aktualizacje.
5. Dostęp do wsparcia technicznego w dni robocze w godz. 9:00 – 15:00.

DOSTAWA, GWARANCJA I USŁUGA WDROŻENIOWA:

1. Zamawiający wymaga zapewnienia aktualizacji Systemu (asysta techniczna) oraz nieprzerwanego działania Systemu (SLA) przez cały okres dostępu do Systemu
2. Ciągłość działania usługi musi być zapewniona bez konieczności zapewnienia hostingu przez Zamawiającego (System utrzymywany w formule SAAS)
3. Wykonawca lub producent Systemu zapewni wsparcie techniczne w godzinach pracy Zamawiającego
4. Wykonawca lub producent Systemu zapewni SLA w formie czasu reakcji na zgłoszenia o problemach do 4 godzin oraz czasu naprawy w przypadku awarii Systemu, tj. niezgodności ze specyfikacją określoną w niniejszym opisie przedmiotu zamówienia do 5 dni roboczych
5. Dostawa musi obejmować przeprowadzenie szkolenia dla wybranych pracowników Zamawiającego do 60 dni od wdrożenia Systemu
6. Zamawiający oczekuje zapewnienia dokumentacji w formie elektronicznej z samouczkami w języku polskim

5) Dostawa i wdrożenie systemu klasy PAM do zarządzania dostępem uprzywilejowanym – 5 licencji

ARCHITEKTURA I FUNKCJONALNOŚĆ SYSTEMU PAM:

1. System PAM musi być rozwiązaniem bezagentowym tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy bez potrzeby instalacji oprogramowania (agenta) na systemie, do którego będzie nawiązywana sesja, umożliwiającym uwierzytelnianie wieloskładnikowe i obsługujące wiele platform i systemów operacyjnych.
2. System PAM ma zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego m.in. routery, przełączniki, zapory sieciowe, aplikacje, bazy danych itp.
3. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze Hyper-V lub VMware. Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu.
4. Rozwiązanie nie może wymagać wdrożenia kolejnych komponentów jako osobne maszyny wirtualne lub fizyczne. Do prawidłowego działania wszystkich dostępnych funkcjonalności wymagane jest posiadanie tylko jednej maszyny wirtualnej.

5. Rozwiązanie musi oferować wdrożenie drugiej instancji i konfiguracji klastra typu active-active.
6. System PAM musi zapewniać możliwość zarządzania (w szczególności):
   1) Użytkownikami na systemach operacyjnych: Windows, Unix/Linux,
   2) Kontami domenowymi: MS Active Directory,
   3) Kontami lokalnymi: VMware ESX/ESXi,
   4) Kontami na urządzeniach m.in.: Cisco, Aruba, Alcatel, CheckPoint, Fortigate, Huawei, IBM AIX, Brocade,
   5) Kontami baz danych: Microsoft SQL, Oracle, MySQL, PostgreSQL
   6) Kontami do zarządzania i monitorowania serwerów: m.in. iLO, iDRAC,
   7) Kontami aplikacji webowych: Facebook, Google, Twitter, Linkedin, Instagram, Openstack, AWS
   8) Kontami w innych nie wymienionych systemach/urządzeniach do których dostęp odbywa się po protokołach: SSH, RDP,VNC, TELNET, HTTP/HTTPS,
   9) Kluczami SSH.
7. System PAM musi umożliwiać utworzenie poświadczeń typu Just-in-Time (JIT), które będą tworzone lub aktywowane na czas trwania sesji.
8. System PAM musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP,VNC, TELNET, HTTP/HTTPS, X11.
9. System PAM musi wspierać również protokoły bez rejestracji sesji: Cassandra, Elasticsearch, LDAP, LDAPS, MongoDB, MySQL, Oracle, PostgreSQL, Redis, Solr, SQL Server, RDS Sybase, Windows RM, Windows RPC, Windows SMB.
10. System PAM musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami:
    1) przeglądarka internetowa,
    2) klient RDP,
    3) klient protokołu SSH/Telnet (np. putty),
    4) klient serwerów bazodanowych m.in. DBeaver.
11. System PAM musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, TACACS Active Directory, OpenID, SAML.
12. System PAM musi zapewniać możliwość dwuskładnikowego uwierzytelniania.
13. System PAM musi wspierać integrację z rozwiązaniami dwuskładnikowego uwierzytelnienia takimi jak Google Authenticator i Microsoft Authenticator.
14. System PAM musi obsługiwać monitorowanie i ochronę kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane.
15. System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd do haseł uprzywilejowanych.
16. System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.
17. System PAM musi umożliwiać budowanie polityk kontroli dostępu wymuszającej:
    1) podanie powodu rozpoczęcia sesji,
    2) podanie powodu podglądu hasła,
    3) konieczność akceptacji rozpoczęcia sesji przez innego administratora/ów,
    4) konieczność akceptacji podglądu hasła przez innego administratora/ów,
    5) zakresu godzin, dni oraz dat kiedy użytkownik systemu będzie miał dostęp do poświadczeń.
18. System PAM musi umożliwiać udostępnienie poświadczenia do użytku dla użytkownika poza polityką dostępową, która jest do niego przypisana. Udostępnienie musi dawać możliwość wyboru długości trwania takiego dostępu.
19. System PAM musi posiadać log dla wszystkich zdarzeń systemowych.
20. System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji/serwera.

21. System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.
22. System PAM musi umożliwiać raportowanie wszystkich logowań do systemu.
23. System PAM musi umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego.
24. Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.
25. System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.
26. System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.:
    1) umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i duże litery, cyfry, znaki specjalne),
    2) generować automatycznie hasła kont systemów docelowych w sposób pseudo losowy,
    3) generować unikalne hasła dla konta systemów docelowych,
    4) wymuszać automatyczną zmianę hasła po jego podglądzie.
27. System PAM musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.
28. System PAM musi umożliwiać podgląd zestawionej sesji w czasie rzeczywistym.
29. System PAM musi umożliwiać przerwanie i/lub zawieszenie trwającej sesji.
30. System PAM musi posiadać menu pozwalające na zawieszenie lub przerwanie wszystkich sieci oraz zablokowanie dostępu do samego rozwiązania w przypadku sytuacji krytycznej.
31. System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń).
32. Audyt poleceń musi umożliwiać podjęcie co najmniej akcji, zablokuj polecenie i rozłącz sesję po wykryciu audytowanego polecenia a także automatyczne umieszczenie na liście blokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie.
33. Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.
34. System PAM musi umożliwiać konfigurację parametrów nagrań, w tym:
    1) ilości klatek na sekundę,
    2) jakości pojedynczej klatki,
    3) formatu pojedynczej klatki: jpg lub png,
    4) długości przechowywania nagrań.
35. System PAM musi rejestrować znaki wprowadzone z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych.
36. System PAM musi umożliwiać utworzenie oddzielnego zestawu ustawień w oparciu o:
    1) politykę dostępową,
    2) urządzenie docelowe,
    3) poświadczenie,
    4) adresu źródłowego.
37. System PAM musi umożliwiać odtworzenie i pobranie zarejestrowanych nagrań sesji.
38. Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie producenta na terenie Polski.
39. System PAM musi być kompletny i pozwalać na uruchomienie minimum następujących funkcjonalności:
    1) zarządzać kontami uprzywilejowanymi w ramach organizacji,
    2) monitorować wykorzystanie kont uprzywilejowanych,
    3) nagrywać i archiwizować sesje zdalne,
    4) gwarantować skalowalność rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług.

40. System PAM musi umożliwiać personalizację wyglądu aplikacji co najmniej po przez umieszczenie logo Zamawiającego w głównym oknie aplikacji.

LICENCJONOWANIE I WDROŻENIE SYSTEMU PAM:

1. System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 5 użytkowników, którzy będą korzystali z Systemu PAM, minimum dla następującej liczby funkcjonalności:
   1) Ochrona kont uprzywilejowanych,
   2) Ochrona kluczy SSH,
   3) Zarządzanie i monitorowanie sesji uprzywilejowanych,
   4) Rejestrowanie sesji uprzywilejowanych,
   5) Raportowanie wykorzystania kont uprzywilejowanych.
2. Dostarczone licencje na System PAM do ochrony kont uprzywilejowanych nie mogą mieć ograniczeń czasowych. Dostarczone licencje będą udzielone bezterminowo.
3. Dostarczone licencje na System PAM nie mogą w żaden sposób limitować ilości chronionych systemów docelowych.
4. System powinien być dostarczony wraz z rocznym serwisem umożliwiającym korzystanie ze wsparcia producenta oraz dystrybutora oraz pobieranie aktualizacji przygotowanych przez producenta.
5. W ramach zakupionych licencji użytkownicy Systemu PAM muszą posiadać możliwość skorzystania z mechanizmu prywatnego sejfu.
6. W ramach realizacji zamówienia Wykonawca zainstaluje i skonfiguruje System PAM w środowisku Zamawiającego.
7. Wykonawca przeprowadzi szkolenie dla administratora sieci komputerowej Zamawiającego z obsługi Systemu PAM. Szczegółowy plan, zakres i termin szkolenia zostanie uzgodniony przez Wykonawcę z Zamawiającym.
8. Szkolenie musi odbywać się stacjonarnie w siedzibie Zamawiającego. Minimalny czas trwania szkolenia to 10 godzin zegarowych.
9. Wykonawca zapewni Zamawiającemu możliwość skorzystania z konsultacji z inżynierem do 12 miesięcy po odbytym szkoleniu w formie e-mail lub kontaktu telefonicznego.

6) Dostawa i wdrożenie systemu klasy DLP do identyfikacji oraz zapobiegania wyciekom danych

FUNKCJONALNOŚĆ SYSTEMU DLP:

1. System musi zapewniać ochronę danych na urządzeniach pracującymi pod kontrolą systemów operacyjnych: Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi, Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi, MacOS 12 lub nowszy.
2. Serwer administracyjny musi obsługiwać instalację na systemach: Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych: MS SQL Server 2016 lub nowsze, MS SQL Express, AzureSQL S3 lub nowsze.
4. Konsola administracyjna i komunikaty klienta DLP muszą być w języku polskim.
5. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
6. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
7. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
8. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
9. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.

10. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
11. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
12. Administrator musi mieć możliwość tworzenia i usuwania kont w konsoli programu.
13. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
14. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
15. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
16. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
17. Administrator musi mieć możliwość wykonania audytu stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e-mail oraz czynności na plikach.
18. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
19. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
20. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości e-mail.
21. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
22. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
23. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
24. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
25. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
26. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
27. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
28. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
29. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
30. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
31. System musi wykorzystywać mechanizm OCR (*Optical Character Recognition*), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.
32. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.).
33. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych.

LICENCJONOWANIE I WDROŻENIE SYSTEMU DLP:

1. System DLP musi zostać dostarczony z kompletem licencji dla co najmniej 30 użytkowników.
2. Dostarczone licencje na System DLP nie mogą mieć ograniczeń czasowych. Dostarczone licencje będą udzielone bezterminowo.

3. System powinien być dostarczony wraz z rocznym serwisem umożliwiającym korzystanie ze wsparcia producenta oraz dystrybutora oraz pobieranie aktualizacji przygotowanych przez producenta.
4. W ramach realizacji zamówienia Wykonawca zainstaluje i skonfiguruje System DLP w środowisku Zamawiającego.
5. Wykonawca przeprowadzi szkolenie dla administratora sieci komputerowej Zamawiającego z obsługi Systemu DLP. Szczegółowy plan, zakres i termin szkolenia zostanie uzgodniony przez Wykonawcę z Zamawiającym.
6. Szkolenie musi odbywać się stacjonarnie w siedzibie Zamawiającego. Minimalny czas trwania szkolenia to 10 godzin zegarowych.
7. Wykonawca zapewni Zamawiającemu możliwość skorzystania z konsultacji z inżynierem do 12 miesięcy po odbytym szkoleniu w formie e-mail lub kontaktu telefonicznego.

7) Dostawa i wdrożenie systemu klasy NAC zapewniającego kontrolę dostępu do sieci komputerowej urzędu oraz wgląd w działania urządzeń i użytkowników korzystających z zasobów sieciowych urzędu, 2 lata

PODSTAWOWA FUNKCJONALNOŚĆ SYSTEMU NAC:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor).
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 2500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
    1) VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x,
    2) Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
    1) serwera RADIUS dla infrastruktury sieciowej,
    2) serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    3) serwera SYSLOG,
    4) serwera TACACS+,
    5) serwera Monitoringu,
    6) serwera DHCP,
    7) serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    8) serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.

12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez e-mail.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. login, hasło, imię, nazwisko, e-mail, status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. tożsamość, MAC adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony VLAN z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, autoryzacji, statusu, opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.

34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem SYSLOG informacji z serwerów autoryzacji, DHCP, VPN, OTP, TACACS+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM.
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
    1) Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
    2) Czy włączony jest firewall
    3) Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur

4) Czy jest włączone szyfrowanie dysku systemowego
5) Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
6) Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
7) Czy w systemie są uruchomione procesy wskazane przez administratora
8) Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
9) Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
   a) Wartości klucza rejestru,
   b) Typu wartości: Number, String, Version.

60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania informatyka urzędu co najmniej dla systemów: Microsoft Windows, Mac OS, iOS, Android.
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

MECHANIZMY UWIERZYTELNIANIA

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły: MAC, PAP/ASCII, CHAP, SNMP, 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), TEAP, itp.
3. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
4. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
5. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
6. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
   1) Tożsamość/Urządzenie końcowe,
   2) Grupa tożsamości/urządzeń końcowych,
   3) Parametry urządzeń końcowych, min: system operacyjny, wersja,
   4) Atrybuty Active Directory,
   5) Jednostka organizacyjna tożsamości/urządzeń końcowych,
   6) Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
   7) Grupy urządzeń sieciowych,
   8) Porty urządzeń sieciowych,
   9) Grupy portów urządzeń sieciowych,
   10) Jednostka organizacyjna portów,
   11) Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
   12) Data, czas ważności polityki,
   13) Wewnętrzny Captive Portal,
   14) Metoda autoryzacji.
7. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.

8. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
9. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
10. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
11. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
12. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
14. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
15. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
16. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
17. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
18. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
19. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

OBSŁUGA SERWERÓW CERTYFIKATÓW CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
   1) możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
   2) możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
   3) Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
   4) usługę OCSP (Online Certificate Status Protocol).

OBSŁUGA SERWERÓW DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
   1) Uruchamianie usługi dla wybranych podsieci,
   2) Przypisanie ustalonego adresu IP dla adresu MAC.
   3) Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
   4) Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
   5) Możliwość określania braku dostępu dla wybranych adresów MAC,
   6) Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
   7) Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,

8) Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
9) Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
10) Dokonywanie zmian bez konieczności wyłączania usług.

OBSŁUGA SERWERÓW TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

RAPORTOWANIE I MONITORING

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu e-mail.
8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności VLANów w urządzeniach sieciowych działających w środowisku.
14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.

18. Raport zdarzeń Microsoft Active Directory, minimum:
    1) Logowania, wylogowania z system w tym błędne logowania,
    2) Logowania do sieci 802.1X**.**

ALARMY

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
    1) wiadomości e-mail,
    2) Syslog,
    3) notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
    1) Ilości obsługiwanych transakcji RADIUS,
    2) Opóźnienie obsługi transkacji RADIUS,
    3) Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
    1) badanie łączności IP za pomocą ping, traceroute,
    2) tcpdump protokołów RADIUS, TACACS+,
    3) wyszukiwanie zdarzeń RADIUS z uwzględnieniem: nazwy użytkownika, adresu MAC, statusu uwierzytelnienia (udana lub nieudana), powodu, jeżeli uwierzytelnienie nieudane, zakresu czasowego, co do dnia, godziny i minuty,
    4) wykonanie zdalnego polecenia na urządzeniu sieciowym.

WYMAGANIA DOTYCZĄCE WDROŻENIA:

1. Dostawa, instalacja, licencjonowanie Systemu NAC oraz konfiguracja zostanie wykonana w środowisku Zamawiającego.
2. Podstawowa konfiguracja Systemu NAC: integracja z domeną AD, konfiguracja urzędu certyfikacji.
3. Konfiguracja urządzenia firewall: dodatnie VLAN-u gościnnego, ustawienie polityk, etc.
4. Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
5. Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
6. Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii; przeprowadzenie testów.
7. Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów; przeprowadzenie testów.
8. Przeprowadzenie szkolenia dla administratora sieci komputerowej Zamawiającego z konfiguracji i administrowania Systemem NAC.
9. Szczegółowy plan, zakres i termin szkolenia zostanie uzgodniony przez Wykonawcę z Zamawiającym.
10. Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 30 dni po zakończeniu wdrożenia.

LICENCJA WSPARCIA TECHNICZNEGO PRODUCENTA OPROGRAMOWANIA:

Wykonawca dostarczy wraz z dożywotnią licencją Systemu NAC – **24 miesięczną licencję na wsparcie producenta oprogramowania**. Licencja ta powinna obejmować minimum:

1) Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą Systemu NAC
2) Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
3) Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
4) Dostęp do dokumentacji i instrukcji na stronie internetowej.

5) Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

8) Dostawa i wdrożenie serwerów do budowy systemu wysokiej dostępności - 2 sztuki

Lp.	Element konfiguracji	Opis minimalnych wymagań technicznych
1	Obudowa	Obudowa typu RACK maksymalnie 2U dedykowana dla rozwiązań wirtualizacyjnych i Data Center. Obudowa musi posiadać minimum 25 wnęk na dyski hot-plug. Minimum 3 porty USB oraz 1 port VGA dostępne bezpośrednio z przodu obudowy (bez stosowania zewnętrznych, to jest poza obudową, kabli / przejściówek / rozgałęziaczy / konwerterów). Dodatkowy panel/bezel zamykany, chroniący przed nieuprawnionym dostępem do dysków). Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack.
2	Płyta główna	Płyta główna dwuprocesorowa dedykowana do pracy w serwerach. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
3	Procesory	Jeden procesor wprowadzony przez producenta procesora do sprzedaży nie wcześniej niż w połowie 2023 roku 16 rdzeniowy z zegarem bazowym minimum 2,0GHz umożliwiające osiągnięcie w oferowanym serwerze dla konfiguracji dwuprocesorowej (wydruk wyniku, dostępnego publicznie na stronie spec.org nie później niż w dniu składania oferty, dla konkretnego oferowanego serwera należy dołączyć w formacie PDF do oferty): - min. 12.3 pkt. w teście SPECspeed2017_int_base - min. 267 pkt. w teście SPECrate2017_int_base
4	Pamięć RAM	Minimum 32 sloty DIMM wbudowane w płytę główną. Co najmniej 384 GB zainstalowanej pamięci RAM DDR5 o szybkości transmisji danych nie mniejszej niż 4800MT/s z systemem kodowania korekcyjnego ECC.
5	Karta graficzna	Karta graficzna zintegrowana z płytą główną. Minimum 2 porty graficzne VGA, z czego minimum 1 na froncie obudowy.
6	Dyski twarde	Zainstalowane dyski: Dwa dyski SSD SATA dedykowane do rozwiązań serwerowych, o pojemności minimum 480GB każdy, skonfigurowane w sprzętowy RAID1. Dwa dyski SSD SATA o pojemności minimum 7,68 TB każdy w kieszeniach hot-swap z przodu obudowy. Dyski mają być dostarczone przez producenta serwera i objęte gwarancją w ramach gwarancji serwera.
7	Kontroler dyskowy	Kontroler dyskowy SAS/SATA z pamięcią minimum 8GB obsługujący poziomy RAID 0, 1, 5, 6, 10, 50, 60 z możliwością zainstalowania podtrzymania cache.
8	Interfejsy sieciowe (LAN)	Zintegrowane, nie zajmujące żadnych standardowych slotów PCIe (wbudowane w płytę jako LOM lub na kartach typu OCP) porty: 2x 1Gb RJ45. Możliwość rozbudowy o dodatkowe 2x 25/10 Gb SFP28 nie zajmujące żadnych standardowych slotów PCIe (wbudowane w płytę jako LOM lub na kartach typu OCP).
9	Interfesjsy sieciowe w slotach PCIe	Minimum 2 porty 25/10 Gb SFP28 oraz 2 porty 10Gb RJ45.

10	Porty zarządzające	Minimum 1 port sieciowy RJ45 1Gb dedykowany dla interfejsu zdalnego zarządzania (karty zarządzającej) dostępny z tyłu serwera, oraz minimum 1 port USB dedykowany do bezpośredniego zarządzania z wykorzystaniem karty zarządzającej, dostępny z przodu serwera.
11	Zasilacze i Wentylatory	Zainstalowane dwa redundantne zasilacze o mocy minimum 900W każdy, w klasie Titanium.
12	System diagnostyczny	Serwer musi posiadać kontroler zarządzania płytą główną (BMC), niezależny od OS, który jest zgodny ze specyfikacją Intelligent Platform Management Interface 2.0 (IPMI 2.0) i zapewnia monitorowanie i zarządzanie sprzętem. Wspierać musi on następujące interfejsy zarządzania: - Interfejs DCMI 1.5- Interfejs IPMI 1.5/IPMI 2.0- Interfejs wiersza poleceń- Interfejs Redfish- Interfejs Hypertext Transfer Protocol Secure (HTTPS)- Interfejs Simple Network Management Protocol (SNMP).
13	Bezpieczeństwo	Serwer musi posiadać Trusted Platform Module (TPM) w wersji 2.0. Czujnik otwarcia obudowy komunikający się z BIOS lub kartą zarządzającą serwera. Spełnia wymagania NIST SP 800-193. Spełnia następujące wymaganie NIST SP 800-147B:- Obsługiwany jest mechanizm aktualizacji podpisu cyfrowego oprogramowania układowego BIOS. Podczas aktualizacji podpis cyfrowy jest weryfikowany, aby zapobiec nieautoryzowanej aktualizacji oprogramowania układowego BIOS.
14	Certyfikaty, kompatybilność	Serwer musi posiadać deklarację CE. Serwer musi widnieć na stronie www.windowsservercatalog.com jako certyfikowany do pracy z systemami Windows Server 2025, 2022, 2019 Serwer musi widnieć na stronie https://partnerweb.vmware.com/comp_guide2/search.php?deviceCategory=server jako certyfikowany do pracy z systemami ESXi 7.0 U3, 8.0 U1, 8.0 U2, 8.0 U.3
15	Gwarancja i serwis	Serwer powinien posiadać oficjalną gwarancję i wsparcie serwisowe producenta przez okres minimum 5 lat realizowane w miejscu instalacji sprzętu z czasem reakcji serwisu w następnym dniu roboczym od momentu zgłoszenia usterki w miejscu instalacji serwera. W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia producenta o tym, że zaoferowane serwery będą objęte wsparciem serwisowym przez firmę z siedzibą w Polsce, która jest autoryzowanym partnerem serwisowym producenta. Oświadczenie zawierać powinno ponadto deklarację, że w przypadku niewywiązania się firmy serwisującej z obowiązani serwisowych, producent bierze bezpośrednio na siebie wsparcie serwisowe w zaoferowanym reżimie serwisowym.
16	Ekologia	Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC.

		Potwierdzeniem spełnienia powyższego wymogu jest umieszczenie oferowanego urządzenia w rejestrze internetowym www.epeat.net na poziomie min. Epeat bronze.
17	Wdrożenie	Dostarczone serwery muszą być zainstalowane w siedzibie i infrastrukturze Zamawiającego. W ramach realizacji zamówienia Wykonawca: 1) zainstaluje na dostarczonych serwerach oprogramowanie wirtualizacyjne (oprogramowanie nie może ograniczać liczby wirtualnych maszyn; oprogramowanie nie może być ograniczone czasowo; musi działać w trybie permanentnym; oprogramowanie musi posiadać przyjazny interfejs graficzny; musi mieć możliwość pracy w środowisku LXC - kontenery Linux; oprogramowanie musi wspierać LVM, katalogi oraz system ZFS, iSCSI, Fiber Channel, NFS, GlusterFS, CEPH i DRBD), umożliwiające łączenie serwerów w klastry o wysokiej dostępności, dające możliwość zarządzania węzłami klastra poprzez interfejs GUI i skonfiguruje je zgodnie ze wskazaniami Zamawiającego (Wykonawca musi dostarczyć odpowiednie oprogramowanie wirtualizacyjne) 2) przygotuje dostarczone fizyczne serwery do roli węzła klastra HA, przeprowadzi tuning roli klastra HA, wykona testy nowego środowiska na awarie oraz wydajność pracy. 3) skonfiguruje i podłączy oferowane macierze do systemu wirtualizacyjnego jako datastor'y wykorzystując protokół iSCSI. 4) Wykonawca przeprowadzi szkolenie z zakresu wykonanych prac i administracji nowym środowiskiem. Minimalny czas trwania szkolenia to 10 godzin zegarowych. 5) Wykonawca musi zapewnić możliwość skorzystania z konsultacji z inżynierem do 12 miesięcy po odbytym szkoleniu w formie e-mail lub kontaktu telefonicznego.

9) Dostawa macierzy dysków – 1 sztuka

Lp.	Element konfiguracji	Opis minimalnych wymagań technicznych
1	Obudowa	Urządzenie musi być przystosowane do montażu w szafie rack 19”, zajmowana wysokość maksymalnie 2U. Urządzenie musi być wyposażone w zestaw szyn do montażu w szafie rack 19”.
2	Procesor	Ośmiordzeniowy procesor o taktowaniu 2,1 GHz, maksymalnie 2,7 GHz z technologią Turbo Boost osiągający w teście PassMark na wrzesień 2024 co najmniej 10 050 punktów
3	Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
4	Pamięć RAM	min. 16GB pamięci DDR4 ECC RDIMM z możliwością rozszerzenia do min. 128GB
5	Przestrzeń dyskowa	Urządzenie musi być wyposażone w min. 12 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 96 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą gniazda rozszerzeń z interfejsem SAS. Macierz musi umożliwiać podłączenie dysków SATA oraz SAS. Zainstalowane min. 4 dyski SAS 12Gb/s każdy o pojemności min. 12 TB.

6	Porty zewnętrzne	Minimum: 1) 2 porty USB 3.2.1 2) 1 gniazdo rozszerzenia (półka dyskowa)
7	Porty sieciowe	Minimum: 1) 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) 2) 2 porty 10GbE RJ45
8	Port zarządzający	1 port LAN do zarządzania
9	Funkcja Wake on LAN/WAN	Tak
10	Gniazdo rozszerzeń PCIe 3.0	Min. 2x 8-liniowe gniazdo x8
11	Wentylator obudowy	Min. 4 wentylatory
12	Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, Fibre Channel, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
13	Obsługiwane systemy plików	Min.: 1) Wewnętrzny: Btrfs, ext4 2) Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+
14	Zarządzanie pamięcią masową	1) Maksymalny rozmiar pojedynczego wolumenu: a) 1 PB (wymagana pamięć 64 GB, tylko grupy RAID 6) b) 200 TB (wymagana pamięć 32 GB) c) 108 TB 2) Minimalny liczba wewnętrznych wolumenów: 256 3) Minimalna liczba obsługiwanych migawek w systemie: 65 536 4) Minimalny liczba obiektów iSCSI Target: 256 5) Minimalny liczba jednostek iSCSI LUN: 512 6) Obsługa klonowania/migawek jednostek iSCSI LUN
15	Obsługiwane typy macierzy RAID	Podstawowy (basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID F1
16	Funkcja udostępniania plików	1) Minimalna liczba kont użytkowników: 16 000 2) Minimalna liczba grup użytkowników: 512 3) Minimalna liczba folderów współdzielonych: 512 4) Minimalna liczba jednoczesnych połączeń CIFS/NFS/AFP/FTP: 4 000 5) Minimalna liczba jednoczesnych połączeń protokołu SMB/AFP/FTP (z rozbudową pamięci RAM): 10 000
17	Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
18	Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
19	Usługa katalogowa	Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
20	Bezpieczeństwo	Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
21	Obsługiwane systemy klienckie	Windows 7 i nowsze, Mac OS X® 10.11 i nowszy
22	Obsługiwane przeglądarki	Chrome®, Firefox®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze; Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
23	Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w nadmiarowy zasilacz
24	Oprogramowanie	1) Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek,

		generowania sum kontrolnych CRC, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych; dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych 2) Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie; ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia 3) Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI, a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS; usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń, a także wspierać algorytm Intelliversioning; ponadto usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym 4) Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA), aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system)
25	Konserwacja	1) Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack dostarczonych z zestawem 2) Wymiana modułu zasilacza ma przebiegać w szybki i bezpieczny sposób bez wyłączania urządzenia oraz bez użycia narzędzi 3) Wymiana wentylatora systemowego musi przebiegać w szybki i bezpieczny sposób bez użycia narzędzi
26	Gwarancja	1) 5 lat na urządzenia główne oraz dodatkowe karty sieciowe 2) 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack

10) Dostawa przełącznika sieciowego – 1 sztuka

Lp.	Parametr	Wymagania minimalne i opis
1	Typ urządzenia	Przełącznik zarządzalny, warstwy 3
2	Rodzaj obudowy	Umożliwiająca montaż w szafie RACK 19”, wysokość 1U, wyposażona w 3 wentylatory, redundantny zasilacz
3	Ilość portów	RJ45 Gigabit Ethernet (10/100/1000) - 48 szt. 1 x Fast Ethernet (10/100), port konsoli SFP+ (10G) - 4 sloty QSFP+ (40G) - 2 sloty
4	Pamięć RAM	64MB

5	Wydajność	Całkowita przepustowość przełącznika: min. 168 Gb/s Zdolność do przełączania: min. 336 Gb/s Szybkość przesyłania: min. 235 Mp/s
6	Moduł SFP+	Wyposażony w 4x moduł SFP+ (10GbE)
7	Gwarancja	Okres gwarancji: 3 lata

11) Dostawa zasilaczy awaryjnych – 22 sztuki

Lp.	Nazwa	Wymagane minimalne cechy i parametry techniczne sprzętu
1	Zastosowanie	Urządzenie poprzez zapewnienie czystej i stabilnej mocy wyjściowej podczas przerw w dostawie prądu lub wahań napięcia będzie wykorzystywane do zapewnienia nieprzerwanej pracy komputerów
2	Typ	Line-interactive
3	Obudowa	Tower
4	Pojemność energetyczna	600VA / 360W
5	Współczynnik mocy wyjściowej	0,6
6	Czas przełączania	Max 10ms z trybu AC/liniowego do trybu bateryjnego
7	Czas podtrzymania	Minimum: 9 minut przy połowie obciążenia
8	Wejście	Zakres napięcia wejściowego: 170-280V AC Zakres częstotliwości: 45Hz – 65Hz (samoczynna adaptacja do 50/60Hz)
9	Wyjście	Czysta fala sinusoidalna Nominalne napięcie wyjściowe: 230V AC Regulacja napięcia (w trybie bateryjnym): +/- 10% Częstotliwość (praca baterii): +/- 1Hz
10	Ochrona linii danych	Port RJ11, port RJ45
11	Gniazda wyjściowe	Minimum: 4x 230V (10A) z uziemieniem
12	Sprawność	W trybie LINE: min. 98% przy pełnym obciążeniu W trybie bateryjnym: min. 82% przy pełnym obciążeniu
13	Poziom hałasu	Max 40 dB
14	Dodatkowe cechy urządzenia	Baterie z możliwością wymiany w czasie pracy Wielofunkcyjny wyświetlacz LCD z funkcją automatycznego przyciemniania Automatyczny regulator napięcia (AVR) Połączenie USB zgodne z Human Interface Device (HID)
15	Oprogramowanie	Dołączone oprogramowanie monitorujące
16	Gwarancja	24 miesiące

Wykonawca będzie zobowiązany do wdrożenia zakupionych rozwiązań zgodnie z wymaganiami określonymi w szczegółowym opisie przedmiotu zamówienia.

7. Przedmiotowe środki dowodowe

1) Zamawiający wymaga złożenia wraz z ofertą przedmiotowych środków dowodowych środków dowodowych w zakresie potwierdzenia, że oferowane dostawy spełniają wymagania Zamawiającego co do przedmiotu zamówienia.
2) Dotyczy dostawy i wdrożenia serwerów do budowy systemu wysokiej dostępności - Wymagane dołączenie do oferty oświadczenia producenta o tym, że zaoferowane serwery będą objęte wsparciem serwisowym przez firmę z siedzibą w Polsce, która jest autoryzowanym partnerem serwisowym producenta. Oświadczenie zawierać powinno ponadto deklarację, że w przypadku niewywiązania się firmy serwisującej z obowiązani serwisowych, producent bierze bezpośrednio na siebie wsparcie serwisowe w zaoferowanym reżimie serwisowym.
3) Zamawiający nie przewiduje możliwości uzupełnienia przedmiotowych środków dowodowych.