**Opis przedmiotu zamówienia**

| Lp. | Nazwa |  | Liczba sztuk | Opis techniczny –(**minimalne wymagania**) | Opis wdrożenia i adaptacji | Czas realizacji | Uwagi | CPV |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1.** | **Program do archiwizacji danych** | Z1 p.1 | 1 | Licencja musi pozwalać na wykonanie kopii min. 5 serwerów fizycznych i 4 maszyn wirtualnych.  Kopie wykonywane przez program muszą być szyfrowane i chronione przed kradzieżą. Program musi mieć możliwość replikacji *danych w celu ich przechowywania w kilku osobnych miejscach.*  1. Oprogramowanie musi współpracować z infrastrukturą VMware oraz Microsoft Hyper-V Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej 2. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. 3. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie  dowolnej platformy serwerowej oraz dyskowej 4. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji 5. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. 6. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API 7. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji 8. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji 9. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania 10. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji min. 2 szt. instancji konsoli administracyjnych. 11. Oprogramowanie musi posiadać mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej 12. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. 13. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji.  14. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) 15. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V  16.Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami 17. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL bezpośrednio z pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. 18. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków 19. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites 20. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender,  21. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. Rozwiązanie musi wykonywać kopię zapasową systemu Windows wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego 22. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów MS Windows  23. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również scentralizowany (poprzez centralną konsolę zarządzającą) 24. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster 25. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów 26. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym 27. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) 28. Rozwiązanie musi wspierać deduplikacje oraz kompresję.  29. Rozwiązanie musi wspierać kontrolę pasma sieciowego 30. Rozwiązanie musi wspierać technologię BitLocker 31. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania 32. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych 33. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V,  34. Rozwiązanie musi wspierać szyfrowanie kopii zapasowych 35. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych 36. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel 37. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora38. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. 39. System musi mieć możliwość eksportowania raportów do formatów DOC, XLS, PDF 40. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach 41. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych 42. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. | Wymagane jest aby wdrożenie przeprowadzone było przez Inżyniera Wykonawcy posiadającego certyfikat producenta potwierdzający kompetencje w tym zakresie.  Zamawiający wymaga dostarczenia licencji wieczystej.  Wsparcie Wykonawcy przez okres 24 miesięcy | 30 dni | Zamawiający wymaga by oprogramowanie było nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych | 48710000-8 (Pakiety oprogramowania do archiwizacji i odtwarzania danych). |
| **2.** | **Program do zarządzania stacjami roboczymi i siecią** | Z1;p.8 | 1 | Licencja powinna objąć co najmniej 120 stanowisk komputerowych. System powinien posiadać co najmniej 2 dostępy administracyjne.  Oprogramowanie musi umożliwiać inwentaryzację sprzętu IT i utrzymanie nadzoru nad oprogramowaniem i licencjami oraz zapewnić monitorowanie: infrastruktury, logowania, przeglądania stron, transferu plików, urządzeń USB, usług, procesów, wydajności sieci. System musi posiadać program klienta instalowanego na stacji roboczej odpowiedzialnego za zarządzanie tym komputerem, zbieranie danych oraz przesyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.  Komunikacja klient – serwer musi odbywać się z wykorzystaniem TLS 1.3. Konsola administracyjna – przeznaczona do zarządzania systemem musi być w formie aplikacji internetowej (webowej) i musi pozwalać na realizację pełnego zarządzania systemem oraz zasobami wraz z edycją/modyfikacją/usuwaniem i analizą danych (bez konieczności stosowania dodatkowych aplikacji). 1. Wszystkie komponenty systemu muszą się aktualizować samodzielnie z serwerów aktualizacji producenta systemu za pośrednictwem bezpiecznego połączenia.  2. W przypadku, gdy połączenie pomiędzy systemem a serwerem aktualizacji producenta nie jest dostępne musi być możliwość dokonania aktualizacji manualnie poprzez pobranie od producenta paczki aktualizacyjnej w postaci jednego pliku z kompletną aktualizacją.  3. Agent do działania nie może wymagać instalacji komponentów pomocniczych typu .NET Framework lub innych z wyłączeniem komponentów WMI. 4. Agent powinien być dostępny dla administratora z poziomu interfejsu konsoli administracyjnej zawsze w najnowszej wersji wydanej przez producenta (bez konieczności pobierania go ze strony producenta), w postaci pliku gotowego do zainstalowania (bez konieczności dodatkowego wykonywania zmian/ustalania parametrów). 5. Agent powinien być możliwy do zainstalowania za pośrednictwem MS Active Directory, za pomocą skryptów lub manualnie, poprzez uruchomienie na danej stacji roboczej. 6. Agent powinien wspierać wiele różnych adresów serwera rozumianych jako adresy w sieci lokalnej, rozległej (VPN) oraz za NATem.  7. System powinien umożliwiać komunikację pomiędzy agentami a serwerem w sieciach lokalnych, rozległych, także gdy komputery znajdują się za NATem.  8. System powinien mieć wbudowane mechanizmy automatycznej konserwacji/utrzymania zgodnie ze zdefiniowanym harmonogramem. 9. Harmonogram powinien mieć możliwość ustalenia częstotliwości wykonywania zadania (godzina, dzień, tydzień, miesiąc), możliwość zmiany wartość parametrów wejściowych do wykonania danej konserwacji, a także zatrzymania/uruchomienia wybranych pozycji harmonogramu w dowolnym momencie 10. Konsola administracyjna powinien 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). 11. Agent powinien działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 8.1/10/11 12. Serwer musi działać na systemach 64 bitowych: Windows Server 2012/2016/2019/2022 13. System powinien mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare. 14. System powinien umożliwiać import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory~~,~~  15. System musi umożliwiać import użytkowników z zewnętrznego pliku CSV. 16. System powinien posiadać wbudowany, w pełni definiowalny przez administratora interfejs do importu innych niż komputery urządzeń (np. pendrive, monitory, switche itp.) wraz z danymi o kosztach zakupu, nr dokumentu zakupowego, dostawcy, daty zakupu, gwarancji. Import powinien umożliwiać pobieranie danych z pliku CSV.  17. System musi umożliwiać pełne zdalne zarządzanie agentami (w sposób masowy i jednostkowy) w zakresie: uruchamiania i wyłączania agenta, zmiany konfiguracji, uruchamiania skanowania, przekazania dowolnych zadań do wykonania (poleceń systemu operacyjnego). 18. Agent powinien mieć możliwość wyświetlenia dowolnego komunikatu w postaci HTML wysłanego z poziomu konsoli administracyjnej, konsola powinna udostępnić dane o dacie i godzinie wyświetlenia komunikatu oraz użytkowniku, który go wyświetlił. 19. Konsola musi być w pełni polskojęzyczna  20. Konsola administracyjna powinna posiadać dashboardy, np. dashboard użytkownika, dashboard prezentujący parametry infrastruktury, dashboard prezentujący parametry sieci, dashboard prezentujący informacje o bezpieczeństwie. 21. System musi umożliwiać zbudowanie dashboardu użytkownika przez poprzez wybór szybkiego skrótu do dowolnego ekranu aplikacji lub wybór widgetu. 22. Konsola administracyjna powinna zawierać szczegółowe informacje dotyczące pracy wszystkich komputerów: wersja agenta, stanu agenta (włączony/wyłączony), zalogowanego użytkownika, historii czasu włączenia i wyłączenia komputera. System musi pokazywać następujące informacje: 23. Lista używanego oprogramowania (nazwa aplikacji, wersja, Producent, użycie w okresie ostatnich 3, 6, 12 miesięcy, data ostatniego uruchomienia). 24. Lista otwartych sesji pracownika (data zalogowania, nazwa komputera, IP, rodzaj połączenia (LAN, NAT, VPN), czas zalogowania). 25. Lista ostatnich sesji użytkownika (początek, koniec, czas trwania sesji, nazwa komputera, IP) 26. Lista używanego oprogramowania (nazwa aplikacji, wersja, producent, data ostatniego uruchomienia, użycie aplikacji w ostatnich 3, 6, 12 miesiącach). 27. Aktywność użytkownika w aplikacjach (aplikacja, kategoria aplikacji, łączny czas korzystania, czas korzystania aktywnego, czas korzystania pasywnego). 28. Aktywność użytkownika w Internecie (adres URL, informacja o stronie www –kategoria strony, czy strona jest produktywna, łączny czas korzystania, czas aktywności, czas pasywności). 29. System powinien umożliwiać zarządzanie licencjami w ramach dowolnego elementu struktury organizacyjnej (dla wybranej struktury organizacyjnej pokazuje liczbę instalacji i liczbę licencji w danym modelu licencjonowania wraz z listą komputerów). 30. System powinien dawać możliwość wykonywania wielu audytów legalności oprogramowania i zapamiętywać wyniki tych audytów w odniesieniu do systemów operacyjnych jak i aplikacji/pakietów~~,~~ 31. System powinien umożliwiać: automatyczną inwentaryzację komputerów znajdujących się w sieci lokalnej oraz komputerów znajdujących się poza siecią lokalną (za NATem). 32. System powinien zbierać szczegółowe informacje o sprzęcie (producent, model, data produkcji, numer seryjny) w oparciu o klasy WMI (Windows Management Instrumentation).  33. System powinien automatycznie identyfikować i klasyfikować urządzenia podłączane do komputera (pendrive, kamera, aparat, monitor zewnętrzny, pamięć masowa, telefon, urządzenie multimedialne itp.) 34. System powinien umożliwiać monitorowanie stanu zapory w czasie rzeczywistym,  35. System powinien zapewniać zdalne sterowanie zaporą na dowolnych komputerach,36. System powinien być wyposażony w mechanizmy informowania - wysyłania komunikatów (alerty) o: zasobach zakazanych (pliki erotyczne i pornograficzne), zasobach multimedialnych (pliki multimedialne), nowych komputerach w bazie danych, braku skanowania komputerów, brakach w licencjach, niewłaściwych datach systemowych komputerów, zdublowanych systemach operacyjnych, zakazanych procesach/stronach www /aplikacjach, nadmiernym obciążeniu dysków twardych, nadmiernym obciążeniu procesora, nadmiernym obciążeniu pamięci RAM, małej ilości wolnego miejsca na dysku  37. System powinien posiadać możliwość monitorowania daty włączenia i wyłączenia komputera niezależnie czy znajduje się w sieci lokalnej czy też poza nią 38. System powinien ewidencjonować zdarzenia związane z logowaniem się użytkowników do danego komputera39. Systemu powinien umożliwiać wyeksportowania wybranych lub wszystkich danych do formatu xls, csv, OpenOffice calc, html, jpeg, png. 40. System powinien umożliwiać tworzenie wybranych powiadomień wiele razy z określeniem innych grup obiorców41. System musi posiadać wbudowaną dokumentację pomocy użytkownika w języku polskim. | Zamawiający wymaga dostarczenia licencji wieczystej.  Wsparcie Wykonawcy przez okres 24 miesięcy | 30 dni | Zamawiający wymaga by oprogramowanie było nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych  Pomoc techniczna powinna być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.  Wykonawca przedstawi certyfikaty oraz referencji potwierdzających doświadczenie w ramach świadczonej usług wdrożenia | 48210000-3 (Pakiety oprogramowania do sieciowej komunikacji i zarządzania) |
| **3.** | **Urządzenie klasy UTM, zakup, wdrożenie oraz szkolenie** | Z1 p.9  Z1 p.13  Z2 p.1 | 2 | 1. 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. 2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 5. 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. 6. 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, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskaże 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 firewall-a niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe. 12. System detekcji i prewencji włamań (IPS) ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 13. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 14. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 15. Moduł IPS ma usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 16. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 17. 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. 18. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 19. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych. 22. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 20. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. 21. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. 22. Urządzenie ma umożliwiać zastosowanie wbudowanego skanera antywirusowego 23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 24. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji. 25. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 26. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. Skaner heurystyczny. 27. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. 28. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 29. Urządzenie ma wspierać co najmniej następujące typy sieci VPN: a. PPTP VPN, b. IPSec VPN, c. SSL VPN. 30. SSL VPN ma działać co najmniej w trybach tunelu i portalu. 31. Producent urządzenia musi umożliwiać pobranie bezpłatnego klienta SSL VPN współpracującego z oferowanym rozwiązaniem. 32. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 33. Urządzenie ma posiadać wbudowany filtr URL. 34. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 40 kategorii tematycznych stron internetowych. 35. Administrator ma mieć możliwość dodawania własnych kategorii URL. 36. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 37. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane. 38. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch 39. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 40. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory. 41. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA. 42. 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. 43. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 44. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 45. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 46. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). 47. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. 48. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 49. Urządzenie ma umożliwiać statyczne trasowanie pakietów. 50. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 51. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall. 52. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 53. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 54. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja musi się odbywać poprzez zaszyfrowany protokół HTTPS. 55. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 56. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 57. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH). 58. Interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 59. Interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 60. Interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 61. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych. 62. Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku. 63. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 64. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej raz w miesiącu 65. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji. 66. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego. 67. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 68. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 69. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 70. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 71. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 72. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 73. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI~~.~~ 74. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. 75. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. 76. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). 77. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. 78. 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). 79. Urządzenie ma posiadać usługę DNS Proxy. 80. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). 81. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. 82. Urządzenie musi posiadać min. dwie niezależne konfiguracje w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). Synchronizacja tych konfiguracji musi być możliwa w dowolnym innym momencie lub przed aktualizacją firmware. 83. Urządzenie musi dawać możliwość wyboru konfiguracji na etapie uruchamiania. 84. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. 85. W okresie obowiązywania gwarancji ma być zapewniona gwarancja oraz wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. 86. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB. 87. Urządzenie musi być wyposażone w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy. 88. Urządzenie musi posiadać min. 8 portów Ethernet 1/2,5Gbps. 89. Urządzenie musi posiadać min. 2 porty światłowodowe 1Gbps. 90. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. 91. Urządzenie ma być wyposażone port konsolowy RJ45. 92. Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps. 93. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps. 94. Przepustowość filtrowania Antywirusowego – minimum 1 Gbps. 95. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps. 96. Liczba tuneli VPN IPSec – minimum 500. 97. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50. 98. Obsługa interfejsów 802.11q (VLAN) – minimum 256. 99. Liczba równoczesnych sesji – minimum 500 000 i nie mniej niż 20 000 nowych sesji/sekundę. 100. Rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive. 101. Urządzenie nie może mieć limitu na liczbę użytkowników. 102. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U. 103. Urządzenie musi być wyposażone w moduł TPM. 104. Urządzenie muszą być objęte licencją gwarancją producenta na okres 24 miesięcy. W ramach licencji Zamawiający musi mieć możliwość wykorzystania i aktualizacji (bez dodatkowych kosztów) sygnatur bezpieczeństwa oraz mechanizmów takich jak: skaner antywirusowy, skaner antyspamowy, IPS/IDS, firewall, raportowanie, obserwacja ruchu i połączeń. | Urządzenia należy skonfigurować w siedzibie Zamawiającego i utworzyć funkcjonalny klaster wysokiej dostępności. Urządzenia mają być wyposażone w licencje niezbędne do działania klastra HA.  W ramach konfiguracji należy wykonać następujące zadania:   1. Instalacja i konfiguracja urządzenia zgodnie z wytycznymi Zamawiającego, w tym min.:  * odwzorowanie konfiguracji aktualnie używanego urządzenia UTM, * analiza odwzorowanych ustawień, ich optymalizacja i zaproponowanie zmian pod kątem zwiększenia bezpieczeństwa transmisji danych, * konfiguracja łączy internetowych wraz z mechanizmem SD-WAN, WAN Failover lub load balancing, * konfiguracja sieci LAN/VLAN w celu separacji sieci różnego przeznaczenia, * konfiguracja firewall-a oraz reguł filtrowania, * konfiguracja mechanizmu SSL Proxy,  1. Konfiguracja klastra HA, optymalizacja ważności interfejsów sieciowych, testy działania klastra (poprawność przełączania urządzeń aktywne/pasywne, utrzymanie ciągłości ruchu internetowego, szybkość przełączenia połączeń VoIP).   W ramach wdrożenia Wykonawca przeprowadzi szkolenie dla lokalnego administratora systemu informatycznego w siedzibie Zamawiającego. Czas trwania szkolenia **min. 8 godzin.** Program szkolenia musi obejmować min.:   * Rozpoczęcie pracy z urządzeniem UTM * Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego * Ustawienia systemowe i uprawnienia administratorów  Instalacja licencji i aktualizacja systemu * Tworzenie kopii zapasowej i przywracanie konfiguracji * Zbieranie logów i monitorowanie Przedstawienie kategorii zbieranych logów * Wykresy historyczne i monitorowanie * Typy obiektów oraz ich wykorzystanie * Obiekty sieciowe i obiekt typu „router” Konfiguracja sieci  Tryby pracy urządzenia  Typy interfejsów (Ethernet, modem, bridge, VLAN) * Typy routingu oraz ich priorytety * Translacja adresów sieciowych (NAT) * Translacja połączeń wychodzących (maskarada) * Translacja połączeń przychodzących (przekierowanie) * Translacja dwukierunkowa (jeden do jeden) * Filtrowanie ruchu sieciowego * Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection) * Kolejność przetwarzania reguł Firewall i NAT * Implementacja filtrowania URL dla ruchu http i https * Moduł IPS i stosowanie profili inspekcji * Konfiguracja usługi katalogowej * Rejestracja użytkowników * Wirtualne sieci prywatne (VPN)  SSL VPN   Gwarancja producenta: min 2 lata  Rodzaj gwarancji door-to-door.  **Przeprowadzenie szkolenia:**   * Szkolenie odbędzie się w siedzibie Zamawiającego. * Forma szkolenia - stacjonarna. * Czas trwania szkolenia min. 8 godzin. * Wykonawca zobowiązany jest do wystawienia uczestnikom szkolenia zaświadczeń o ukończeniu szkolenia. * Zaświadczenia powinny zawierać imię i nazwisko uczestnika, datę i miejsce przeprowadzenia szkolenia, tytuł szkolenia oraz program szkolenia. * Szkolenie przeprowadzać musi osoba posiadająca stosowną wiedzę, oraz m.in. 2 letnie doświadczenie w przygotowywaniu i przeprowadzaniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.. * Trener powinien posiadać certyfikat producenta UTM potwierdzający kwalifikacje. * Wykonawca powinien posiadać doświadczenie w prowadzeniu szkoleń z zakresu obsługi i konfiguracji urządzeń UTM | 60 dni | Zamawiający wymaga aby wdrożenie przeprowadzone było przez osobę posiadającą certyfikat producenta dostarczanego rozwiązania, który będzie potwierdzeniem jego umiejętności.  Po zakończeniu wdrożenia Wykonawca zobowiązany jest przekazać Zamawiającemu dokumentację powykonawczą szczegółowo opisującą konfigurację klastra UTM-ów. | 32420000-3 (Urządzenia sieciowe) oraz 80511000-9 (Usługi szkoleniowe). |
| **4.** | **UPS Serwerowy** | Z1 p.7 | 2 | UPS z wyświetlaczem LCD plus moduł bateryjny  Moc pozorna: min. 6000VA  Moc rzeczywista: min. 6000W  Technologia: on-line (VFI), podwójna konwersja  Typ obudowy: RACK  Kształt napięcia wyjściowego: sinusoidalny  Czas przełączania sieć – UPS: 0ms  Kształt napięcia wyjściowego na pracy bateryjnej: sinusoidalny  Zabezpieczenie przeciwzwarciowe gniazd wyjściowych: Bezpiecznik automatyczny  Zabezpieczenie przeciążeniowe: elektroniczne  Akumulatory w module bateryjnym: 12V 9Ah lub 12V 7Ah; szczelne, bezobsługowe  Czas podtrzymania UPS + moduł bateryjny dla obciążenia 100% / 80% / 50%:  minimum 7 /10 /19 min  Ilość i typ gniazd wyjściowych w UPS minimum 2x IEC 320 C13  Sygnalizacja: Wyświetlacz LCD (informacje wskazujące pracę sieciową, bateryjną, przeciążenie i ładowanie akumulatora).  RS232, USB HID, karta SNMP/http - wymagana na wyposażeniu  Złącze EPO: wymagane  Szyny do montażu w szafie RACK (z możliwością wysuwania serwisowego)  Gwarancja producenta min. 36 miesięcy na podzespoły elektroniczne i min 24 miesiące na akumulatory,  autoryzowany serwis producenta zlokalizowany w Polsce.  serwis realizowany w systemie door to door  Oprogramowanie: w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji VMware, Hyper-V, bez ograniczeń co do ilości monitorowanych stanowisk (bez dodatkowych opłat za licencje).  deklaracja CE producenta sprzętu lub normy równoważnej | Wykonawca zobowiązany jest do podłączenia urządzeń w szafie RACK Zamawiającego  Gwarancja min 24 miesiące na urządzenie i 12 miesięcy na akumulatory; | 30 dni |  | 31154000-0 (UPS – Zasilacze awaryjne) |
| **5.** | **UPS biurkowy** | Z1 p.7 | 37 | Moc pozorna: min. 550VA Moc rzeczywista: min. 330W Czas przełączania sieć – UPS: <6ms AKUMULATORY I CZAS PODTRZYMANIA Czas podtrzymania (P 0,8max/P 0,5max): minimum 2/6 min Akumulatory wewnętrzne bezobsługowe VRLA Technologia: line interactive Typ obudowy: wolnostojąca Gniazda IEC C130 – minimum 1 szt. Gniazda typu E. lub Gniazda schucko - minimum 2 szt Akumulatory wymienialne przez użytkownika. Sygnalizacja: Akustyczno-optyczna, sygnalizacja pracy sieciowej i bateryjną, niski poziom baterii, przeciążenie, awarię,  Zimny Start: tak Interfejs komunikacyjny: USB HID (kabel w komplecie) Oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS, ~~,~~ deklaracja CE producenta sprzętu  Autoryzowany serwis producenta zlokalizowany w Polsce Serwis realizowany w systemie door-to-door | Gwarancja min 24 miesiące na urządzenie i 12 miesięcy na akumulatory; | 30 dni |  | 31154000-0 (UPS – Zasilacze awaryjne) |
| **6.** | **Serwer NAS typ 1** | Z1 p.2 | 1 | Rodzaj obudowy: Rack Czterordzeniowy procesor o taktowaniu min. 2 GHz min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB Urządzenie musi umożliwiać obsługę dysków HDD SATA III o pojemności 12 TB. Prędkość odczytu - min. 500 MB/s Prędkość zapisu - min. 500 MB/s Sprzęt powinien być wyposażony w min.8 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 12 dysków łącznie przy użyciu dodatkowej jednostki rozszerzającej  Minimum: • 2 porty USB 3.2.1 Minimum: • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego) • Możliwość podłączenia dodatkowych kart sieciowych 10G poprzez gniazdo rozszerzeń  Tak Obsługiwane protokoły: SMB2, SMB3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTPs, SFTP, SNMP, LDAP Obsługa RAID: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 • Minimalna liczba kont użytkowników: 500 • Minimalna liczba grup użytkowników: 50 • Minimalna liczba folderów współdzielonych: 100 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 5000 Obsługa VMware vSphere®, Microsoft Hyper-V®,  Możliwość połączenia z serwerami Windows® AD/LDAP, Szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH,  • Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o system plików, który będzie zapewniał obsługę migawek,  • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym 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 oprogramowania • Urządzenie musi posiadać możliwość utworzenia bezpłatnej chmury prywatnej z graficzną konsolą zarządzającą, agentami na urządzenia PC oraz aplikacją mobilną na Android. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. Urządzenie musi by c wyposażone w szyny Rack umożliwiające wysuwanie do celów serwisowych  Urządzenie musi być wyposażone w zasilacz redundantny | Gwarancja producenta: min 3 lata | 30 dni |  | 48820000-2 (Serwery komputerowe). |
| **7.** | **Serwer NAS typ 2** | Z1 p.2 | 2 | Obudowa tower Czterordzeniowy procesor o taktowaniu min. 3GHz Pamięć RAM min. 8 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB   Urządzenie musi umożliwiać obsługę dysków HDD SATA III o pojemności 12 TB. Prędkość odczytu - min. 281 MB/s ●Sprzęt powinien być wyposażony w min. 8 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 18 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą dedykowanych przewodów rozszerzeń ●Wbudowane minimum 2 gniazda M.2 obsługujące dyski NVMe  Minimum 2 porty USB 3.2.1  Porty sieciowe - minimum:  • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)  • 1 port 10GbE RJ45 (nie dopuszcza się realizacji połączenia 10GbE za pomocą zewnętrznej karty sieciowej PCIe)  Funkcja Wake on LAN/WAN Obsługiwane protokoły sieciowe Min. SMB, NFS, FTP, iSCSI, SSH, SNMP i VPN (PPTP, OpenVPN™, L2TP)  Obsługiwane typy macierzy RAID RAID 0, RAID 1, RAID 5, RAID 6, RAID 10  Funkcja udostępniania plików  • Minimalna liczba kont użytkowników: 500  • Minimalna liczba grup użytkowników: 50  • Minimalna liczba folderów współdzielonych: 50  Wirtualizacja VMware® vSphere™, Microsoft® Hyper-V®,  Usługa katalogowa Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP  Bezpieczeństwo szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt i HTTPS (dostosowywane mechanizmy szyfrowania)  Oprogramowanie • Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC • Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o system plików, który będzie zapewniał obsługę migawek  • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym 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 oprogramowania • Urządzenie musi posiadać możliwość utworzenia bezpłatnej chmury prywatnej z graficzną konsolą zarządzającą, agentami na urządzenia PC oraz aplikacją mobilną na Android. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Urządzenie musi być wyposażone w zasilacz redundantny | Gwarancja producenta: min 3 lata | 30 dni |  | 48820000-2 (Serwery komputerowe). |
| **8.** | **Dyski do NAS** | Z1 p.2 | 12 | Typ dysku: HDD Format: 3,5” Pojemność: 12 TB Prędkość obrotowa 7200 obr./min Bufor: 256 MB Interfejs: SATA III – 6 Gb/s Przeznaczenie Dedykowane do pracy w NAS | Wykonawca zobowiązany będzie zamontować dostarczone dyski w zamawianych urządzeniach NAS-1 i NAS-2 oraz dokonać ich konfiguracji zgodnie ze wskazaniami Zamawiającego.  Gwarancja: minimum 5 lat | 30 dni |  | 30233132-0 (Dyski twarde) |
| **9.** | **Sieci bezprzewodowe i ich wdrożenie oraz przeprowadzenie szkolenia dla informatyka – „Bezpieczeństwo sieci WI-FI** | Z1 p.4  Z2 p.2 | 4 | Zintegrowana dwupolaryzacyjna antena dookólna 1. Dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach oraz obsługujące następujące standardy: a. 2.4 GHz 802.11 b/g/n/ax b. 5 GHz 802.11 a/n/ac Wave 2/ax 2. Zgodność z normami IEEE 802.11 a/ac/ax/b/d/e/g/h/i/k/n/r/u/v 3. Moc transmisyjna: min. 32dBm dla 2.4 GHz oraz 33dBm dla 5GHz 4. Zysk anteny: min. 5dBi dla 2.4 GHz oraz 6dBi dla 5 GHz 5. Obudowa zapewniająca prawidłową pracę w poniższych warunkach: - Temperatura: 0⁰ C do +50⁰ C - Wilgotność pracy: do 95% 6. Zasilanie: 802.3af PoE 7. Port Rj45 (10/100/1000 Mbps) 8, Interfejs radiowy wspierający funkcję 2x2:2 MU-MIMO 9. Jednoczesne rozgłaszanie 16 SSID łącznie na obu modułach radiowych 10. Do 16 profili WLAN per radio 11. Deklarowana liczba klientów na moduł radiowy: do 128 12. Możliwość kształtowania wiązki (beamforming) 13. Tryb zarządzania – standalone bez kontrolera, z wykorzystaniem kontrolera chmurowego lub kontrolera na maszynie wirtualnej 14. Obsługa maksymalnej szybkość transmisji danych: a. 2,4 GHz – 573,5Mbps b. 5 GHz – 2402Mbps 15. Wsparcie dla metod uwierzytelniania: Hotspot 2.0, 802.1x EAP-SIM/AKA 16. Możliwość ustawienia harmonogramu włączania i wyłączania sieci WLAN z podziałem na dni, tygodnie lub godziny. 17. Możliwość ustawienia limitu danych dla klienta z wykorzystaniem bitrate, czasu sesji, przepustowości konfigurowane per SSID 18. Możliwość tunelowania ruchu: L2TPv2, L2GRE, PPPoE 19. Współczynnik MTBF przy pracy w temperaturze max. 50ºC na poziomie minimum 500 000 godzin 20. Urządzenie w komplecie musi zawierać uchwyt do montażu naściennego | Wykonawca przeprowadzi montaż (okablowanie zostało przygotowane przez zamawiającego) i konfigurację urządzeń w budynku Starostwa Powiatowego w Głogowie wraz z szkoleniem dla lokalnego informatyka  w siedzibie Zamawiającego. Punkty dostępowe będą pracowały w osobnej sieci VLAN, użytkownicy będą autoryzowani, utworzony zostanie HOTSPOT.  Skonfigurowana zostanie konsola do zarządzania użytkownikami i urządzeniami połączonymi z siecią bezprzewodową  Gwarancja producenta: 2 lata.  **Wykonawca zapewni szkolenie dla Administratora (1 osoba) z wdrażanego rozwiązania.**. Program szkolenia musi obejmować w zakresie minimum:  •Wprowadzenie do bezprzewodowych systemów telekomunikacyjnych.  •Standard 802.11 i jego warianty. Specyfika medium, podstawowe pojęcia: kanał, moc.  •Typy połączeń, punkt-punkt, punkt-wielopunkt.  •Podstawowa konfiguracja urządzeń Access Point.  •Podstawowa konfiguracja komputerów klienckich (Windows, Linux).  •Roaming komputerów klienckich pomiędzy wieloma AP.  •Konfiguracja bezprzewodowego mostu (bridge) w oparciu o tryb WDS.  •Podstawowe zagadnienia bezpieczeństwa  •Mechanizmy szyfrowania  **Przeprowadzenie szkolenia:**   1. Szkolenie odbędzie się w siedzibie Zamawiającego. 2. Forma stacjonarna. 3. Czas szkolenia min. 8 godz. 4. Wykonawca zobowiązany jest do wystawienia uczestnikom szkolenia zaświadczeń o ukończeniu szkolenia. Zaświadczenia powinny zawierać imię i nazwisko uczestnika, datę  i miejsce przeprowadzenia szkolenia, tytuł szkolenia oraz jego program 5. Szkolenie przeprowadzać musi osoba posiadająca stosowną wiedzę, oraz m.in. 2 letnie doświadczenie w przygotowywaniu i przeprowadzaniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń. 6. Trenerzy powinni posiadać certyfikaty potwierdzające ich kwalifikacje. | 30 dni | Po zakończeniu wdrożenia Wykonawca zobowiązany jest przekazać Zamawiającemu dokumentację powykonawczą szczegółowo opisującą konfigurację  Wykonawca przedstawi certyfikaty oraz referencje potwierdzające doświadczenie w ramach świadczonej usługi wdrożenia i szkolenia | 32412110-8 (Sieci bezprzewodowe) oraz 80511000-9 (Usługi szkoleniowe). |
| **10.** | **Przełącznik sieciowy typu 1** | Z1 p.11 | 1 | Przełącznik zarządzalny w obudowie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz,  Minimum 48 portów 10/100/1000 Mbps RJ45 z obsługą PoE+ 802.3af/at, minimum 4 porty SFP/SFP+ 1/10GbE, Budżet mocy PoE: min. 400 W 1 port konsolowy  Minimum 10 000 adresów MAC Pamięć flash min. 128 MB Pamięć RAM min. 512 MB Funkcjonalność warstwy II  Obsługa minimum 2000 wirtualnych sieci Wsparcie dla agregacji statycznej oraz LACP (802.3ad) Obsługa min. 8 grup LACP i 8 portów fizycznych per grupa Obsługa ramek Ethernet typu Jumbo min. 9k Funkcjonalność warstwy III  Obsługa list kontroli dostępu opartych o adresy MAC DHCP Snooping DHCP Relay DHCP Server IGMP Snooping Querier IGMP Proxy PVST/PVRST BPDU Guard, BPDU filtering, Root Guard Authentication, Authorization, and Accounting (AAA) Private VLAN Port Mirroring Port Security/MAC Locking OoS – kolejki priorytetowe oraz Weighted Round Robin (WRR),TFTP, FTP,SSH v2 SNMP v1/v2/v3 Zarządzanie przez CLI, wbudowane WebGUI (HTTP/HTTPS)  Zgodność z protokołami  802.1ab LLDP ANSI/TIA-1057- LLDP-MED. 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority 802.1Q VLAN Tagging 802.1S Multiple Spanning Tree (MSTP) 802.1W Rapid Spanning Tree (RSTP) 802.3ad Link Aggregation with LACP 802.3x Flow Control RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 2030 SNTP RFC 2865 RADIUS Client RFC 3579 RADIUS Support for EAP RFC 3164 Syslog | Wdrożenie musi obejmować minimum:  -Demontaż starych przełączników 7 sztuk  -Instalacja w szafach rack zamawiającego nowych przełączników Typ 1, 2 oraz 3  -Aktualizacja oprogramowania przełączników do najnowszej dostępnej wersji  -Podstawowa konfiguracja przełączników tj. interfejsy do zarządzania, konto administracyjne  -Konfiguracja na przełącznikach protokołu typu RSTP wraz z oferowanymi przez dany sprzęt zabezpieczeniami typu Root Guard, Loop Guard, BPDU Guard w sposób zgodny z tzw. dobrymi branżowymi praktykami  -Odpowiednie połączenie przełączników Typ 1 i 2 z zachowaniem wysokiej dostępności do przełączników rdzeniowych Typ 3  -Odpowiednie połączenie urządzeń UTM z zachowaniem wysokiej dostępności do przełączników rdzeniowych Typ 3  -Do przełączników Typ 1 i 2 należy dostarczyć 12 szt kabli DAC 1m SFP+ 10GbE  -Do przełączników Typ 3 należy dostarczyć 6 szt modułów optycznych SFP+ 10GbE SR, 8 szt modułów SFP+ do RJ-45 10GbE, 2 szt kabli DAC 1m QSFP28 100GbE, 2 szt kabli DAC typu breakout QSFP+ 40GbE -> 4x10GbE o długości 5m  -Kompatybilność dostarczonego okablowania typu DAC oraz modułów optycznych powinna zostać odpowiednio dobrana przez Wykonawcę w celu poprawnego działania ze wszystkimi dostarczonymi przez Wykonawcę urządzeniami  -Przeniesienie konfiguracji VLAN ze starych przełączników (w tym ustawienia dla konkretnych gniazd na patch panelach, serwerów) Zamawiający posiada w swojej sieci nie więcej niż 8 skonfigurowanych VLAN.  -Opisanie interfejsów przełącznika numerami gniazd z patch paneli, do których interfejsy przełącznika są podłączone, w przypadku połączeń między przełącznikami i/lub serwerami powinny być opisy do którego sprzętu jest podłączone urządzenie.  -Wykonanie konfiguracji wysokiej dostępności typu MLAG (ang. Multichassis Link Agreggation Group) na przełącznikach Typ 3  Zamawiający wymaga dostarczenia licencji wieczystej.  Wsparcie Wykonawcy przez okres 24 miesięcy | 60 dni | Po zakończeniu wdrożenia Wykonawca zobowiązany jest przekazać Zamawiającemu dokumentację powykonawczą szczegółowo opisującą konfigurację.  Wykonawca przedstawi certyfikaty oraz referencje potwierdzające doświadczenie w ramach świadczonej usług wdrożenia | 2422000-7 (Urządzenia sieciowe). |
| **11.** | **Przełączniki sieciowe typ 2** | Z1 p.11 | 6 | Przełącznik zarządzalny w obudowie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażony w zintegrowany zasilacz~~,~~ Minimum 48 portów 10/100/1000 Mbps RJ45, minimum 4 porty SFP/SFP+ 1/10GbE, 1 port konsolowy  Minimum 10000 adresów MAC Pamięć flash min. 128 MB Pamięć RAM min. 512 MB Obsługa minimum 2000 wirtualnych sieci Wsparcie dla agregacji statycznej oraz LACP (802.3ad) Obsługa 8 grup LACP i 8 portów fizycznych per grupa Obsługa ramek Ethernet typu Jumbo min. 9k Obsługa list kontroli dostępu opartych o adresy MAC i IP Storm Control Broadcast/Multicast/Unknown Unicast DHCP Snooping DHCP Relay DHCP Server IGMP Snooping Querier IGMP Proxy PVST/PVRST BPDU Guard, BPDU filtering, Root Guard Authentication, Authorization, and Accounting (AAA) Private VLAN Port Mirroring Port Security/MAC Locking OoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), TFTP, FTP, SSH v2 SNMP v1/v2/v3 Zarządzanie przez CLI, wbudowane WebGUI (HTTP/HTTPS)  Zgodność z protokołami  802.1ab LLDP ANSI/TIA-1057- LLDP-MED. 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority 802.1Q VLAN Tagging 802.1S Multiple Spanning Tree (MSTP) 802.1W Rapid Spanning Tree (RSTP) 802.3ad Link Aggregation with LACP RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 2030 SNTP RFC 2132 DHCP options and BOOTP vendor extensions RFC 2865 RADIUS Client RFC 3579 RADIUS Support for EAP RFC 3164 Syslog | Opis zawarty przy przełączniku typu 1  Gwarancja Minimum 60 miesięcy. Bezpłatny dostęp do aktualizacji na okres minimum 24 miesięcy. | 60 dni | Po zakończeniu wdrożenia Wykonawca zobowiązany jest przekazać Zamawiającemu dokumentację powykonawczą szczegółowo opisującą konfigurację.  Wykonawca przedstawi certyfikaty oraz referencje potwierdzające doświadczenie w ramach świadczonej usługi wdrożenia | 2422000-7 (Urządzenia sieciowe). |
| **12.** | **Przełącznik sieciowe typ 3** | Z1 p.12 | 2 | Przełącznik zarządzalny w obudowie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażony w dwa wbudowane zasilacze -min. 12 portów 10GbE SFP+  -min. 3 porty 100GbE (QSFP28)  -min. 1 port konsoli  Wymagane jest dostarczenie kabla min. 1m DAC QSFP28 100GbE do każdego przełącznika Możliwość wykorzystania okablowania i modułów 40GbE QSFP+ w portach 100GbE QSFP28. Możliwość rozszycia portów 100GbE za pomocą odpowiedniego okablowania na: -100GbE QSFP28 -> 4x25GbE SFP28 -40GbE QSFP+ -> 4x10GbE SFP+ Dostarczone kable i moduły powinny być kompatybilne z dostarczonym urządzeniem. Wydajność przełącznika •Throughput: min. 500 Mpps •Switching capacity min. 600Gbps •Bufor pakietów: min. 12MB •Pamięć CPU: min 4GB •Obsługa minimum 2000 wirtualnych sieci •Obsługa minimum 1000 000 adresów MAC w trybie Scaled L2 Zgodność z protokołami  802.1AB LLDP TIA-1057 LLDP-MED. 802.1s MSTP 802.1w RSTP 802.1t RPVST+ 802.3ab Gigabit Ethernet (1000Base-T) 802.3ad Link Aggregation with LACP 802.3ba 40 Gigabit Ethernet (40GBase-X) 802.3z Gigabit Ethernet (1000BaseX) 802.1D Bridging, STP 802.1p L2 Prioritization 802.1Q VLAN Tagging, GVRP 802.1s MSTP 802.1w RSTP 802.1X Network Access Control 802.3ad Link Aggregation with LACP 802.3bj 100 Gigabit Ethernet ANSI/TIA-1057 LLDP-MED. 768 UDP 793 TCP 3164 Syslog 4254 SSHv2 791 IPv4 792 ICMP 826 ARP 1027 Proxy ARP 1035 DNS (client) 1305 NTPv4 3046 DHCP Option 82 (Relay) 2460 IPv6 2463 ICMPv6 4291 IPv6 Addressing 2464 Transmission of IPv6 Packets over Ethernet Networks Zarządzenie przez CLI  2865 RADIUS 3162 Radius and IPv6 SSHv2, SNMPv1/2 FTP, TFTP, SCP Syslog Port Mirroring Access Control Lists Round Robin Weighted Round Robin  Zamawiający wymaga aby oferowany przełącznik:  - posiadał deklarację CE (dokument załączyć do oferty) - był zgodny z standardem RoHS (oświadczenie producenta lub przedstawiciela producenta załączyć do oferty) Gwarancja  Minimum trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez linię telefoniczną producenta. | Opis zawarty przy przełączniku typu 1  Gwarancja Minimum 60 miesięcy. Bezpłatny dostęp do aktualizacji na okres minimum 24 miesięcy. | 60 dni | Po zakończeniu wdrożenia Wykonawca zobowiązany jest przekazać Zamawiającemu dokumentację powykonawczą szczegółowo opisującą konfigurację  Wykonawca przedstawi certyfikaty oraz referencji potwierdzających doświadczenie w ramach świadczonej usług wdrożenia | 2422000-7 (Urządzenia sieciowe). |
| **13.** | **Program do zarządzania SZBI** | Z1 p.3 | 1 | Oprogramowanie wspomagającego zarządzanie w zakresie bezpieczeństwa informacji i ochrony danych osobowych.  Oprogramowanie ma być dostarczone w najnowszej wersji w języku polskim.  Oprogramowanie powinno posiadać dokumentację użytkownika opisującą funkcjonalność każdego z modułów oprogramowania oraz dokumentację administratora opisującą sposób administrowania programem w tym jego instalowania, konfiguracji, sposobu tworzenia kopii zapasowych oraz odtwarzania w przypadku awarii,  1. Koszt zakupu oprogramowania powinien uwzględniać koszt wszystkich składników oprogramowania (poza systemem operacyjnym zainstalowanym na serwerze Zamawiającego), które są niezbędne do jego pracy zgodnie z niniejszą specyfikacją.  2. W ramach zamówienia Zamawiający otrzyma wersję instalacyjną oprogramowania oraz licencję uprawniającą do korzystania z przedmiotowego oprogramowania.  3. Program powinien pracować jako aplikacja intranetowa uruchamiana i prawidłowo pracująca w aktualnych wersjach przeglądarek internetowych (MS Edge, Google Chrome, FireFox).  4. Wszystkie dane gromadzone w oprogramowaniu powinny być zapisywane wyłącznie centralnie, na komputerze pełniącym rolę serwera pracującego w trybie ciągłym przez 24 godziny na dobę.  5. Serwer będzie dostarczony przez Zamawiającego i będzie znajdował się w jego siedzibie.  6. Program powinien pracować na serwerze z procesorem 8-rdzeniowy w architekturze 64 bit, min. 1TB SSD, min. 16GB RAM z zainstalowanym systemem operacyjny Windows lub Linux (inne składniki oprogramowania niezbędne do pracy programu dostarcza Wykonawca).  7. Aplikacja instalowana na serwerze działającym w systemie Windows powinna posiadać automatyczny instalator wszystkich składników niezbędnych do prawidłowego działania oprogramowania.  8. Poza instalatorem dla systemu Windows aplikacja powinna mieć możliwość uruchomienia na serwerze pracującym pod systemem Linux (konfiguracja instalacji niestandardowych powinna być określona w dokumentacji programu).  9. Program ma mieć możliwość importu użytkowników z przygotowanego zgodnie ze specyfikacją pliku lub ich importu bezpośrednio z Active Directory.  oprogramowanie musi:  - posiadać rejestr zidentyfikowanych procesów w tym procesów z zakresu ochrony danych,  - posiadać rejestr komórek organizacyjnych, który będzie oparty na regulaminie organizacyjnym,  - posiadać możliwość opisu komórki organizacyjnej poprzez określenie jej podrzędności w strukturze organizacyjnej, przypisania do niej stanowisk pracy oraz zakresu zadań jaki realizuje,  - posiadać rejestr wszystkich pracowników, praktykantów i stażystów oraz osób świadczących pracę na umowach cywilnoprawnych,  - posiadać rejestr wszystkich dokumentów określających wymagania (m.in.: polityk, zarządzeń, decyzji, instrukcji, procedur) obowiązujących na poszczególnych stanowiskach pracy w urzędzie,  - posiadać możliwość opisania dokumentu poprzez m.in.: określenie osoby odpowiedzialnej za dokument, przypisanie do procesu, który realizuje oraz wskazanie właściwych stanowisk pracy na jakich obowiązuje,  - posiadać możliwość udostępniania treści dokumentu pracownikom,  - wspomagać opisywanie kontekstu organizacji w tym dokumentować okresowe analizy czynników mających wpływ na zdolność organizacji do osiągania zamierzonych celów, umożliwiać opisanie zakresu i wyłączeń systemu  - umożliwiać prowadzenie rejestru zidentyfikowanych aktywów informacyjnych oraz zasobów wspomagających,  - wspomagać opisywanie aktywów m.in. poprzez wskazanie procesów przetwarzających informacje oraz istotności informacji dla realizacji danego procesu, wskazanie zasobów wykorzystywanych przy przetwarzaniu informacji oraz określenie poziomu istotności zasobu dla informacji,  - umożliwiać ustalenie wymaganego poziomu podstawowych oraz dodatkowych atrybutów informacji i adekwatnie do tego ustalać klasyfikacje aktywów.  - umożliwiać prowadzenie zgodnie z przepisami prawa rejestru czynności przetwarzania i kategorii czynności przetwarzania danych osobowych w Urzędzie,  - posiadać możliwość rejestrowania klauzul informacyjnych  - posiadać możliwość ewidencji zawartych umów powierzenia przetwarzania danych osobowych,  - wspomagać wystawianie upoważnień do przetwarzania danych osobowych oraz prowadzić rejestr osób upoważnionych do przetwarzania danych osobowych,  - posiadać elektroniczny rejestr udostępnionych danych osobowych, który zawiera m.in. informacje o wnioskującym, dacie wniosku, podstawie prawnej upoważniającej do udostępnienia danych, zakresie udostępnionej informacji oraz terminie i osobie udostępniającej,  - umożliwiać ewidencjonowanie oraz wspomagać obsługę wniosków wynikających z RODO tj.:  - dostęp do danych osobowych (art. 15 RODO),  - sprostowanie danych osobowych (art. 16 RODO),  - usunięcie danych osobowych (art. 17 RODO),  - ograniczenie przetwarzania danych osobowych (art. 18 RODO),  - przeniesienie danych osobowych (art. 20 RODO),  - sprzeciw wobec przetwarzania danych osobowych (art. 21 RODO),  - posiadać rejestr zidentyfikowanych ryzyk w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych,  - posiadać możliwość przypisania stanowiska odpowiedzialnego za zidentyfikowane ryzyko i jego cyklicznej oceny,  - posiadać możliwość identyfikacji i ewidencji czynników ryzyka (źródeł zagrożeń i szans), podatności na zagrożenia lub szanse, opisania skutków ryzyka, estymację i ocenę ryzyka, ustalenia reakcji na ryzyko oraz monitorowania i raportowania ryzyka,  - posiadać możliwość przeprowadzania cyklicznej oceny ryzyka,  - prezentować ryzyka w formie graficznych zestawień m.in. mapy ryzyka,  - posiadać rejestr wszystkich użytkowanych aplikacji,  - posiadać rejestr nadanych w Urzędzie uprawnień do przetwarzania danych w aplikacjach komputerowych zgodnie z zakresem zadań wykonywanych przez pracownika,  - posiadać możliwość elektronicznego wnioskowania o nadanie właściwych uprawnień dla pracowników zgodnie z ich zakresem obowiązków do obsługi programów komputerowych, w których są przetwarzane dane osobowe,  - w przypadku aplikacji przetwarzających dane osobowe weryfikować czy pracownik posiada upoważnienie do przetwarzania danych osobowych,  - posiadać rejestr zaistniałych incydentów oraz słabości systemu,  - podsiadać możliwość zgłoszenia zidentyfikowanego zdarzenia lub słabości systemu bezpieczeństwa informacji (w tym naruszenia ochrony danych osobowych),  - umożliwiać analizę i klasyfikację zgłoszonego zdarzenia,  - wspomagać obsługę incydentów bezpieczeństwa informacji w tym określenia operatora incydentu oraz ewidencjonować podejmowane działania,  - posiadać stosowne zestawienia dotyczące zidentyfikowanych incydentów i słabości systemów~~,~~  - posiadać rejestr certyfikatów bezpieczeństwa,  - posiadać możliwość wnioskowania o nadanie certyfikatu bezpieczeństwa,  - umożliwiać ewidencjonowanie certyfikatów bezpieczeństwa,  - posiadać możliwość unieważniania certyfikatu bezpieczeństwa,  - posiadać rejestr przeprowadzonych audytów wewnętrznych w tym auditów w zakresie bezpieczeństwa informacji i ochrony danych osobowych,  - posiadać możliwość tworzenia programów auditów wewnętrznych na danych rok oraz planowania auditów z określeniem m.in.: zakresu auditu, przedmiotu auditu, komórek organizacyjnych uczestniczących w działaniach auditowych, terminu przeprowadzenia auditu oraz osób przeprowadzających audit,  - możliwość dokumentowania podjętych działań auditowych tj. przygotowanie m.in.: programu auditów na dany rok, protokołu końcowego z auditu,  - możliwość dokumentowania wszystkich spostrzeżeń, niezgodności i wniosków wynikłych podczas podjętych działań auditiwych,  - posiadać rejestr wszystkich zidentyfikowanych nieprawidłowości (niezgodności) w zakresie bezpieczeństwa informacji i ochrony danych osobowych,  - możliwość określenia działań korygujących i korekcyjnych względem zidentyfikowanej nieprawidłowości oraz głoszenia wykonania działań korygujących,  - posiadać rejestr przeprowadzanych w Urzędzie cyklicznych przeglądów zarządzania w zakresie m.in. bezpieczeństwa informacji i ochrony danych osobowych,  - możliwość automatycznego przygotowania raportu do analizy z zakresu m.in. bezpieczeństwa informacji i ochrony danych osobowych.  10. Wszystkie moduły programu muszą być ze sobą kompatybilne i wzajemnie powiązane (moduły powinny korzystać z danych wprowadzanych w innych modułach bez konieczności ponownego ewidencjonowania tych samych danych).  11 Program musi informować ~~użytkownika o~~ działaniach, które należy podjąć w ~~aplikacji~~ ze względu na posiadane w aplikacji uprawnienia lub zajmowane w organizacji stanowisko pracy.  12. Komunikaty adresowane do użytkowników muszą być wysyłane na adres e-mail użytkownika.  Licencja  1. Licencja ma zezwalać na jednoczesną pracę w programie wszystkich pracowników Urzędu.  2. Licencja nie może ograniczać liczby końcówek jednocześnie korzystających z oprogramowania.  3. Licencja musi dopuszczać tworzenie przez Zamawiającego dowolnej ilości kopii oprogramowania dla celów testowych lub szkoleniowych.  4. Od dnia przekazania przez 24 miesiące Wykonawca zapewnia wsparcie, w ramach którego Zamawiający zostanie uprawniony do nieodpłatnego pobierania poprawek i aktualizacji oraz na bieżąco pomocy (nadzoru) w obsłudze programu.  5. Pomoc techniczna powinna być świadczona co najmniej w dni robocze w godzinach pracy Urzędu | W ramach dostawy systemu Wykonawca zobowiązany jest do jego instalacji i konfiguracji na zasobach wskazanych przez Zamawiającego | 30 dni | Zamawiający wymaga by oprogramowanie było nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych  Wykonawca przedstawi certyfikaty oraz referencji potwierdzających doświadczenie w ramach świadczonej usług wdrożenia | 72212730-5 (Usługi w zakresie opracowywania oprogramowania dla systemów zarządzania bezpieczeństwem). |
| **14.** | **Oprogramowanie typu SIEM** | Z1 p.6 | 1 | 1. Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyber zagrożeniom, umożliwiającego ich wykrywanie oraz zapewniającego automatyzację~~.~~  2. System musi umożliwić odbieranie logów wygenerowanych przez systemy zabezpieczeń, systemy sieciowe, systemy operacyjne i aplikacje następującymi protokołami: Syslog, TLS syslog, NetFlow, Windows Event Forwarding.  3. Logi pozyskiwane z systemów Microsoft Windows nie mogą wymagać instalowania dedykowanego oprogramowania bezpośrednio na tych systemach.  4. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych.  5. Proces normalizacji musi wspierać min. następujące typy składni: SYSLOG (zgodny z RFC 3164) i automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie.  6. System musi umożliwiać automatyczne nadawanie kategorii zdarzeń w formie nowych pól, np.: logowanie, wylogowanie, zmiana uprawnień, błąd konfiguracji, wykryte skanowanie systemu czy zablokowany malware.  7. System musi rejestrować i przechowywać pozyskane logi w postaci surowej (RAW) oraz znormalizowanej (przetworzonej).  8. System musi umożliwiać fizyczne rozdzielenie repozytoriów logów pobieranych z systemów informatycznych od repozytoriów zdarzeń generowanych w ramach systemu,9. System musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych w postaci skompresowanej.  10. System musi zapewnić mechanizmy bezpieczeństwa dla danych przechowywanych w repozytoriach uniemożliwiające ich nieautoryzowaną modyfikację oraz zapewnić operatorom mechanizmy weryfikacyjne integralność danych.  11. System musi udostępniać możliwość konfiguracji automatycznego odrzucenia logów niezawierających istotnych dla zamawiającego informacji. Definiowanie, które logi mają zostać odrzucone i niezapisane w repozytorium logów musi być realizowane za pomocą reguł, które pozwolą zdefiniować warunki po wszystkich sparsowanych polach.  12. System musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych zdarzeń w formie przetworzonej i pierwotnej. Interfejs musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, ~~złożonych z~~ wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych. Interfejs wyszukiwania musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości. Tworzenie zapytań musi być możliwe poprzez bezpośrednie wskazanie pola zdarzenia za pomocą wskaźnika myszy i dodanie tego pola do filtra wyszukiwania, wraz z określeniem warunków wyszukiwania przez wyrażenie logiczne. 13. System musi zapewniać możliwość utrzymywania dokumentacji sieci, systemów oraz usług, umożliwiającej na gromadzenie i edycję danych istotnych w kontekście oceny generowanych przez system zdarzeń bezpieczeństwa. 14. System musi być zintegrowany z usługą katalogową Microsoft Active Directory celem pobrania informacji o poświadczeniach oraz atrybutach użytkowników i komputerów zarejestrowanych w domenie.~~.~~  15. System powinien umożliwiać zdefiniowanie struktury organizacyjnej oraz zapewniać możliwość jej synchronizacji z usługą katalogową Microsoft Active Directory.  16. System musi umożliwiać analizę konfiguracji systemów IT poprzez ich skanowanie bezpośrednio w ramach mechanizmów dostępnych w samym rozwiązaniu oraz poprzez integrację ze skanerami podatności. 17. System powinien posiadać zestaw predefiniowanych reguł weryfikacji konfiguracji zasobów IT.  18. System musi pozwalać na zautomatyzowaną ocenę wpływu incydentu bezpieczeństwa IT na działalność organizacji względem zagrożeń natury informatycznej  19. System musi zapewniać kontrolę dostępu do systemu i oferowanych przez niego funkcjonalności w oparciu o zdefiniowane role.  20. Dostarczone rozwiązanie musi umożliwiać gromadzenie i korelacje zdarzeń przesyłanych lub pobieranych z innych systemów. Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł oraz ich agregację.  21. Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości: a. centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej;  b. możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows; c. możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application; d. zdolność do monitorowania integralności plików; e. zdolność do monitorowania rejestru systemowego; f. zdolność do monitorowania urządzeń zewnętrznych (removable devices); g. agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS; h. musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu; i. musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS; j. musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu. interfejs użytkownika musi umożliwiać obsługę w języku polskim  22. Produkt musi umożliwiać równoczesną pracę co najmniej 2 operatorów oraz obsługiwać min. 100 źródeł logów dotyczących wszystkich zdarzeń związanych z komputerami oraz serwerami wykorzystywanymi w organizacji oraz zapewnić dla tych źródeł detekcję i obsługę cyberzagrożeń w ramach wszystkich oferowanych w tym postępowaniu funkcjonalności.  2.3 System ma gwarantować możliwość elastycznej rozbudowy o kolejne źródła logów.  24. System musi umożliwiać instalację na jednej z platform systemowych: Microsoft Windows (minimum Server 2016), ~~Oracle~~ Linux~~.~~  25. Wsparcie musi obejmować bezpłatne dostarczanie aktualizacji oprogramowania, reagowanie na zgłaszane błędy systemowe oraz usługę konsultacji powdrożeniowej w formie spotkań z dedykowanym inżynierem, certyfikowanym z procesu konfiguracji i obsługi oferowanego systemu. Przez okres 24 miesięcy. 26. Wykonawca zapewni bezpłatne szkolenia w zakresie użytkowania i administrowania wdrożonego systemu. Szkolenie ma zostać przeprowadzone dla maksymalnie 2 osób .Szkolenia mogą odbyć się w formie zdalnej | Zamawiający wymaga dostarczenia licencji wieczystej.  Wsparcie Wykonawcy przez okres 24 miesięcy  Zamawiający wymaga dostarczenia licencji wieczystej ze wsparciem producenta na okres m.in. 24 miesięcy. Powinna objąć co najmniej 120 stanowisk komputerowych.  Instalacja, konfiguracja, szkolenie dla administratorów  Wykonawca przeprowadzi kompleksową implementację oprogramowania, obejmującą instalację, konfigurację oraz indywidualne szkolenie administratora Starostwa. Szkolenie skupi się na umiejętnościach analizy i interpretacji zdarzeń, co umożliwi efektywne zarządzanie systemem.  Szkolenie przeprowadzać musi osoba posiadająca stosowną wiedzę, oraz m.in. 2 letnie doświadczenie w przygotowywaniu i przeprowadzaniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.  Trenerzy powinni posiadać certyfikaty potwierdzające ich kwalifikacje.  Wykonawca powinien posiadać doświadczenie w prowadzeniu szkoleń z zakresu zgodną z tematyką szkolenia.  **Przeprowadzenie szkolenia:**   1. Szkolenie odbędzie się u Zamawiającego. 2. Forma stacjonarna. 3. Szkolenie będzie miało czas realizacji 8 godzin. 4. Wykonawca zobowiązany jest do wystawienia uczestnikom szkolenia zaświadczeń o ukończeniu szkolenia. . Zaświadczenia powinny zawierać imię i nazwisko uczestnika, datę i miejsce przeprowadzenia szkolenia, tytuł szkolenia oraz program szkolenia | 120 dni | Zamawiający wymaga by oprogramowanie było nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne od wad fizycznych i prawnych  Wykonawca przedstawi certyfikaty oraz referencji potwierdzających doświadczenie w ramach świadczonej usług wdrożenia | 48730000-4 (Systemy monitorowania i zarządzania bezpieczeństwem IT). |
| **15.** | **Hardening** | Z1 p.10 | 1 | Zamawiający oczekuje realizacji następujących zadań:   * aktualizacja systemów i oprogramowania (innych niż dziedzinowe) występujących na wykazie oprogramowania dozwolonego do stosowania prowadzonego przez Zamawiającego; Zamawiający nie będzie wymagał aktualizacji, które pojawią się w okresie 30 dni przed podpisaniem protokołu odbioru; obszar działania: stacje robocze oraz serwery, * wyłączenie zbędnych usług i odinstalowanie zbędnych programów; obszar działania: serwery, * zablokowanie nieużywanych portów; obszar działania: serwery, serwery NAS, przełączniki, punkty dostępu bezprzewodowego), * wyłączenie zbędnych protokołów oraz protokołów bez mechanizmów szyfrowania (np. ftp, telnet, pop3, smtp, http); obszar działania: serwery, serwery NAS, przełączniki, punkty dostępu bezprzewodowego), * zmiana domyślnych poświadczeń obszar działania: serwery, serwery NAS, przełączniki, punkty dostępu bezprzewodowego), drukarki sieciowe, telefony, kontrolery. | Działania należy wykonać z wykorzystaniem wdrażanego oprogramowania ITSM z punktu 2, którego funkcjonalność została opisana wcześniej. | 60 dni | Wykonawca przedstawi certyfikaty oraz referencje potwierdzające doświadczenie w ramach świadczonej usług wdrożenia wykonania Hardeningu w obszarach: serwery, serwery NAS, przełączniki, punkty dostępu bezprzewodowego | 72250000-2 (Usługi systemów zabezpieczeń IT). |

**Wymagania dodatkowe**  
Sprzęt dostarczony w ramach projektu musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w styczniu 2023r., dostarczony w opakowaniu oryginalnym (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie oraz musi pochodzić   
z autoryzowanego kanału dystrybucyjnego. Nie dopuszcza się zastosowania urządzeń tzw. „refurbished”.   
Zamawiający zastrzega sobie możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów u producenta.

Zamawiający w ogłaszanych postępowaniach na dostawy/ usługi będzie określał dla Wykonawcy oraz osób które będą realizowały zamówienie wymagania wskazane w dokumentach programowych Projektu grantowego „Cyberbezpieczny Samorząd” dostępne na stronie internetowej: <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad>