**załącznik nr 2.1 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA – Pakiet 1**

Strony zgodnie stwierdzają, że na potrzeby niniejszego OPZ wraz z załącznikami i przyszłej Umowy dotyczącej opisanego zamówienia, wymienionym w niniejszym paragrafie pojęciom nadają znaczenie określone poniżej, oraz że użyte w tekście poniżej wymienione pojęcia, rozumiane będą w sposób poniżej zdefiniowany. Dla podkreślenia, że pojęcia te rozumiane są w sposób zdefiniowany, ich pierwsze litery będą pisane w tekście wielką literą.

Strony ustalają następujące definicje:

1. **Zamawiający** – SPZOZ Szpital Powiatowy w Piszu
2. **Wykonawca** - podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez prowadzenia negocjacji na podstawie art. 275 pkt 1 Ustawy z dnia 11 września 2019r – prawo zamówień publicznych (Dz.U. z 2022 r. poz. 1710).o wartości zamówienia przekraczającej progi unijne, o jakich stanowi art. 3 ustawy z 11.09.2019r - Prawo zamówień publicznych
3. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawiązanej na podstawie rozstrzygnięcia podstępowania przetargowego.
4. **System informatyczny** - zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. W skład systemu wchodzą najczęściej elementy: Sprzęt komputerowy, Oprogramowanie narzędziowe, Oprogramowanie dziedzinowe.
5. **Infrastruktura sprzętowa -** znajdująca się w dyspozycji Zamawiającego, w tym stanowiąca jego własność oraz dostarczana w ramach realizacji przedmiotu zamówienia infrastruktura przetwarzania danych wszystkie połączenia, urządzenia fizyczne i oprogramowania aplikacyjne, które łącznie współpracując umożliwiają gromadzenie, przechowywanie, wytwarzanie danych i usług oraz udostępnianie danych i usług elektronicznych.
6. **Umowa** – umowa zawarta w ramach realizacji OPZ.
7. **SWZ –** Specyfikacja Warunków Zamówienia
8. **Gwarancja i Serwis Oprogramowania** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie w oraz w projekcie umowy.
9. **Gwarancja i Serwis Infrastruktury Sprzętowej** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie oraz w projekcie umowy.
10. **Sprzęt Komputerowy** – zestaw komputerów (w tym stacje robocze, sprzęt serwerowy, terminale) i oprzyrządowania, na którym pracuje oprogramowanie.
11. **System Komunikacyjny** – infrastruktura telekomunikacyjna, sieciowa, systemy separacji, systemy bezpieczeństwa oraz certyfikaty serwerów WWW, obejmujące elementy lokalnej sieci komputerowej, łącza i urządzenia rozległej sieci transmisji danych oraz urządzenia komutacji pakietów wraz z ich oprogramowaniem, odpowiedzialne za obsługę HIS.
12. **Oprogramowanie Narzędziowe** – elementy oprogramowania zainstalowane na Sprzęcie Komputerowym, obejmujące w szczególności:
    * + systemy operacyjne (np. Windows, LINUX, UNIX),
      + system zarządzania bazą danych (SZBD), zwane też oprogramowaniem bazodanowym (np. MSSQL, Oracle),
      + oprogramowanie służące do administracji i zarządzania Sprzętem Komputerowym, systemem operacyjnym i systemem zarządzania bazą danych,
      + oprogramowanie komunikacyjne umożliwiające podłączenie stacji dostępowych do serwera bazy;
13. **Szkolenie Administratora(ów)** – szkolenia użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora infrastruktury sprzętowej.
14. **Systemy Zewnętrzne** – systemy z którymi docelowo współpracować będzie wdrażany system.
15. **Wdrożenie** – etap cyklu życia systemu informatycznego, polegający na instalacji i dostosowaniu oprogramowania do wymagań Zamawiającego oraz testowaniu i uruchomieniu systemu informatycznego.

* Podstawowe etapy procesu wdrożenia:
* Przygotowanie dokumentacji,
* Przygotowanie i skonfigurowanie infrastruktury technicznej,
* Zainstalowanie i skonfigurowanie systemu informatycznego do eksploatacji,
* Testowanie systemu,
* Uruchomienie produkcyjne systemu.

1. **Środowisko Zapasowe** – kopia Środowiska Produkcyjnego lub jego części, służąca do gromadzenia kopii rzeczywistych danych biznesowych Zamawiającego i podjęcia ich przetwarzania w przypadku awarii Środowiska Produkcyjnego lub w celach przeprowadzenia testów wdrożeniowych aktualizacji/nowych funkcjonalności.
2. **Zdalny Dostęp** – analogowe lub cyfrowe łącze wydajnej transmisji danych pomiędzy węzłem infrastruktury siedziby Wykonawcy, a węzłem infrastruktury zapewnianym przez Zamawiającego, umożliwiające realizować usługi serwisowe lub konfiguracyjne.
3. **Szczegółowym Harmonogramem Realizacji Zadania** – szczegółowy terminarz realizacji przedmiotu Umowy wraz z podziałem na Etapy przygotowany przez Wykonawcę w terminie 14 dni roboczych od zawarcia umowy.
4. **Zadanie** – przedmiot zamówienia (przedmiot Umowy) wynikający łącznie z SWZ, Oferty Wykonawcy, Umowy.
5. **Etap** – główny element części Zadania, stanowiący funkcjonalną całość, podlegająca odrębnym odbiorom. Każdy Etap stanowi odrębną część (rozdział) niniejszego OPZ.
6. **Protokół Odbiorczy** – protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących przedmiotem poszczególnych Etapów.
7. **Protokół Uzgodnień** – dokument tworzony przez Wykonawcę i zatwierdzony przez Strony, na podstawie zapisu ze spotkania lub ustaleń zdalnych (mailowych, telefonicznych) z Zamawiającym. Dokument ten używany jest w trakcie prowadzenia analizy wymagań Zamawiającego i stanowi zobowiązanie obu Stron. Zamawiający zobowiązany jest, że wymagania zapisane w/w protokole nie zostaną zmienione, natomiast Wykonawca zobowiązany jest do realizacji zawartych w nim wymagań Zamawiającego. W przypadku zajścia konieczności wykonania zmian lub innych czynności niż te, które zostały opisane w Protokole Uzgodnień, należy utworzyć nowy Protokół Uzgodnień zawierający te zmiany. W Protokole Uzgodnień można zamieścić inne uzgodnienia, niezwiązane z wymaganiami projektu, tj. ustalenia organizacyjne.
8. **Dzień Roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
9. **Godziny Robocze** – godziny od 7:25 do 15:00 w każdym Dniu Roboczym.
10. **Kierownik Zamawiającego** – osoba wyznaczona przez Zamawiającego, koordynująca całość przedmiotu danego pakietu, posiadająca odpowiednie pełnomocnictwa. W szczególności odpowiedzialna ze strony Zamawiającego za realizację przedmiotu zamówienia.
11. **Kierownik Wykonawcy** - osoba wyznaczona przez Wykonawcę do koordynacji realizacji prac danego zadania. Upoważniona do podpisywania Dokumentacji Projektu z ramienia Wykonawcy.

**OPIS RÓWNOWAŻNOŚCI:**

W przypadku gdy w dokumencie stanowiącym element opisu przedmiotu zamówienia pojawią się wskazania znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego dostawcę (jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub jego produktów), należy rozumieć, zgodnie z przepisem art. 99 ust. 5 ustawy Pzp, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i w takich okolicznościach Zamawiający dopuszcza możliwość składania w ofercie rozwiązań równoważnych, wskazując, iż minimalne wymagania, jakim mają odpowiadać rozwiązania równoważne, to wymagania nie gorsze od parametrów wskazanych w tych dokumentach, a ich kryteria w celu oceny równoważności wskazane są w opisie przedmiotu zamówienia.

W przypadku, gdy Zamawiający opisuje przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy, zamawiający dopuszcza rozwiązania równoważne opisywanym.

Wykonawcy mogą składać oferty zawierające rozwiązania równoważne w stosunku do przedmiotu zamówienia przedstawionego w SWZ – zgodnie z art. 101 ust. 4, 5 i 6 ustawy PZP, jednak są zobowiązani wykazać, że oferowane przez nich rozwiązania spełniają wymagania określone przez Zamawiającego. Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów nie gorszych od założonych w niniejszym SWZ

Za równoważne uznaje się rozwiązania, jak również elementy, materiały, urządzenia o właściwościach funkcjonalnych i jakościowych takich samych, które zostały określone w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. Przy czym istotne jest to, że produkt równoważny to produkt, który nie jest identyczny, tożsamy z produktem referencyjnym, ale posiada pewne, istotne dla Zamawiającego, zbliżone do produktu referencyjnego cechy i parametry.

Istotne dla Zamawiającego cechy i parametry, to takie, które pozwolą zachować wszystkim systemom, urządzeniom, wyrobom, parametry i cechy pozwalające przede wszystkim na prawidłową współpracę z innymi systemami i/lub urządzeniami i/lub wyrobami w sposób założony przez Zamawiającego oraz pozwalające przy tym uzyskać parametry nie gorsze od założonych w niniejszym załączniku. Ciężar udowodnienia równoważności spoczywa na Wykonawcy

Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego poprzez złożenie opisu zaoferowanych produktów wraz z wykazaniem cech równoważności w stosunku do wymagań opisanych przez Zamawiającego w niniejszym załączniku oraz podanie nazwy handlowej i producenta.

W celu wykazania cech równoważności Zamawiający dopuszcza załączenie do opisu etykiet, zdjęć, kart katalogowych itp., z dopiskiem której pozycji asortymentowej (jakiego sprzętu) dotyczy dana informacja z zastrzeżeniem, że z tych dokumentów muszą wynikać parametry co najmniej określone przez Zamawiającego w załącznikach do OPZ i dane identyfikujące produkt.

**DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ OPROGRAMOWANIA**

Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w SPZOZ Szpital Powiatowy w Piszu .

Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

* Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2021.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 12 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej
* Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
* Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
* Wszystkie urządzenia muszą posiadać oznakowanie CE.
* Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
* Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
* Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
* Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).
* **Wykonawca w celu zabezpieczenia danych krytycznych przetwarzanych w systemie HIS Zamawiającego zobowiązany jest dołączyć do oferty potwierdzenie, że posiada uprawnienia lub autoryzację producenta systemu medycznego, z którego obecnie korzysta Zamawiający lub zrealizował przedmiot zamówienia w obszarze dotyczącym ingerencji w dane przetwarzane przez system medyczny Zamawiającego nie naruszając postanowień licencyjnych i gwarancyjnych dla systemu medycznego Medicus On-Line i gwarantował jego poprawne monitorowanie po zakończeniu prac integracyjnych.**

**Powyższe zobowiązanie wynika z konieczności monitoringu krytyczne elementy systemu HIS w ramach dostawy Systemu monitoringu infrastruktury IT.**

Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego.

**Wykonawca w ramach postępowania zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:**

1. Wykonanie Projektu Technicznego dostarczanej infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:
   * Dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,
   * Nazwy oraz szczegółowa adresacja poszczególnych elementów,
   * Planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca, zaprojektowanie kompleksowego systemu ochrony danych opartego na funkcjach macierzy oraz oprogramowania standardowego z uwzględnieniem specyfiki całego projektu,
   * Wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,
   * Harmonogram prac.

Projekt techniczny musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.

1. Konfiguracja serwerów oraz macierzy dyskowej.
2. Instalacja oraz konfiguracji oprogramowania.
3. Testy rozwiązania.
4. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.
5. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej i oprogramowania standardowego, która będzie składała się co najmniej z następujących elementów:
   * Specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,
   * Końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
   * Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
   * Dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim oraz angielskim
   * Szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury szpitala, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
   * Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.

**SOC   
W ramach realizacji zadania wykonawca dostarczy, zainstaluje (instalacja na maszynie wirtualnej), uruchomi w tym podłączy do systemu monitorowania infrastruktury IT urządzenia wykazane w poniższej specyfikacji. Wykonawca dostarczy licencje bezterminowe.**

|  |  |  |  |
| --- | --- | --- | --- |
| **1. System monitoringu infrastruktury IT** | | | |
| **Lp.** | **Wymagane minimalne parametry techniczne** | **Wymóg do spełnienia (warunek graniczny)** | **OFEROWANE PARAMETRY TECHNICZNE – podaje Wykonawca**  **Wymogi dotyczące opisu oferowanych parametrów:**  **TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcę**  **NIE – wykonawca nie spełnia konkretnego parametru** |
| Użytkownicy | | | |
| 1. | * Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat. * Zapewnienia równoległego dostępu do systemu dla wielu użytkowników. * Ograniczania użytkownikom dostępu do wybranych grup hostów. | TAK |  |
| Monitorowanie | | | |
| 1. | * Monitorowania serwerów fizycznych. * Monitorowania urządzeń sieciowych. * Monitorowania stanu połączeń. * Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów * Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux. * Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych. * Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń. * Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu. * Grupowanie hostów. * Definiowanie planowanych przerw serwisowych dla hostów i usług. * Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK). * Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych). * Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www). * Monitorowanie serwerów za pomocą agentów * Monitorowanie serwerów aplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server . * Monitorowanie Active Directory. * Monitorowanie serwerów plików, udziałów sieciowych. * Monitorowanie statusu serwerów Apache. * Monitorowanie baz danych: * ORACLE, * MySQL, * Postgress. * MSSQL Server * DB2 * Monitorowanie urządzeń przez następujące protokoły: * SNMP, * WMI, * IPMI. * Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW. * Monitorowanie poprawności działania DNS. * Monitorowanie środowiska VMware. * Monitorowanie środowiska Hyper-V. * Monitorowanie środowisk Proxmox * Monitorowanie działania serwera czasu NTP. * Monitorowanie offsetu czasu na serwerach. * Monitorowanie ping - czasy odpowiedzi, straty pakietów. * Monitorowanie zajętości miejsca na poszczególnych partycjach. * Monitorowanie obciążenia dysków. * Monitorowanie wykorzystania pamięci RAM. * Monitorowanie obciążenia CPU. * Monitorowanie logów systemowych Windows. * Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia. * Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane. * Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix. * Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence) * Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe * Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów). * Wykrywanie niestabilnie działających usług. * Monitorowanie dostępności stron internetowych. * Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń). | TAK |  |
| Prezentacja | | | |
| 1. | * Prezentację stanu urządzeń na mapie. * Prezentację danych na dashboardach. * Elastyczną konfigurację dashboardów, wybór elementów. * Wizualizację stanu działania całej infrastruktury na jednym dashboardzie. * Tworzenie indywidualnych dashboardów przez użytkowników | TAK |  |
| Powiadomienia | | | |
| 1. | * Globalne wyłączanie powiadomień. * Powiadamianie użytkownika o problemach przez e-mail. * Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie. * Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników. * Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług | TAK |  |
| Konfiguracja | | | |
| 1. | * Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW * Automatyczna konfiguracja i działanie z REST-API * Centralne zarządzanie agentami * Integracja danych z różnych źródeł danych (JSON, XML, SNMP) | TAK |  |
| Monitoring bazy danych systemu HIS | | | |
| 1. | Możliwość monitorowania bazy danych systemu HIS w zakresie co najmniej:   * Instance state * Version * Jobs * Locks * Processes * Number of active sessions * Recovery area * Log switch activity * General tablespace information * Tablespaces performance * Long active sessions * Undo retention * Checkpoint and online backup state * Custom SQLs * RMAN backup status * RMAN backups * ASM disk groups * Apply and transport lag of Oracle Data-Guard * Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości | TAK |  |
| Kolektor logów | | | |
| 1. | * System posiada własny kolektor logów syslog * Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps * Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event * Klasyfikuje wiadomości bazując zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe. | TAK |  |
| Cyberbezpieczeństwo | | | |
| 1. | * System monitoruje urządzenia klasy UTM minimum w zakresie: * wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika * monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany” jest uważany za OK, a status „niezsynchronizowany” CRIT. * monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz” (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda” (1). * monitoruje aktualną liczbę sesji na urządzeniu * monitoruje liczbę dostępnych tuneli IPSec VPN * monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika. * monitoruje poziom wykorzystania procesora * Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne. * System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog * System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog. | TAK |  |
| SOC i NOC | | | |
| 1. | * Operacyjne Centrum Bezpieczeństwa; centrum kompetencyjne, które zajmować się będzie monitorowaniem infrastruktury teleinformatycznej, analizą zdarzeń, detekcją zagrożeń bezpieczeństwa i reagowaniem na wykryte incydenty naruszające bezpieczeństwo teleinformatyczne chronionych organizacji za pomocą analizy zbieranych logów z urządzeń, systemów IT oraz aplikacji, korelacją zdarzeń i detekcją zagrożeń oraz odpowiednią reakcję na pojawiające się incydenty * W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie monitorowania zgodnie z opisanymi poniżej wymaganiami. * Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24 / 7 / 365, zgodnie z określonymi warunkami SLA. * Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji. * Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza * Reakcji. * Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji. * W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT: * Serwery 7 sztuk fizycznych * maszyny wirtualne 12 sztuk * Macierze 2 sztuk, * Przełączniki LAN 21 sztuk * Serwer Backupu 1 sztuk * Macierz NAS 1 sztuk * UPS 6 sztuk * Serwerów aplikacji 2 sztuk * Serwer bazodanowy 2 sztuk * serwer AD 1 Sztuk * W ramach usługi wykonawca monitoruje krytyczne elementy systemu HIS: * Monitorowanie komunikacji z platformą P1 w pełnym zakresie wymiany danych * Monitorowanie systemu HIS w zakresie wystawianych dokumentów EDM * Monitorowanie systemu HIS w zakresie pobieranej przez podmioty zewnętrzne z repozytorium dokumentacji EDM * Monitorowanie systemu His w ramach raportowania zdarzeń medycznych * Monitorowanie komunikacji modułu HL7 * Monitorowanie komunikacji EWUŚ * Monitorowanie KOWAL * Monitorowanie komunikacji AP-KOLCE * Monitorowanie RZM * Monitorowanie bazy danych systemu HIS * Monitorowanie środowiska Tomcat | TAK |  |

1. **System zaawansowanej ochrony antywirusowej stacji roboczych, serwerów, wyposażony w funkcję szyfrowania dysków oraz Endpoint Detection and Response (EDR), spełniający poniższe funkcje : 150 stanowisk na min. 2 lata**
2. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
3. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
4. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
5. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
6. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
7. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
8. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.
9. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
10. Rozwiązanie musi zapewniać weryfikację 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).
11. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
12. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
13. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
14. 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.
15. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
16. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
17. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
18. Rozwiązanie musi informować administratora o nieaktualnych komponentach w tym przynajmniej JAVA i serwer SQL.

**Ochrona stacji roboczych**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11), MacOS 10.15 lub nowszy.
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 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).
11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12. 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.
13. 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.
14. 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.
15. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

* tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
* tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
* tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
* tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

1. 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.
2. 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.
3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
4. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
5. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
6. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
7. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

* tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
* tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
* tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

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

1. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
3. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
4. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
5. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
6. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
7. 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.
8. Rozwiązanie musi wykorzystywać do działania chmurę producenta (Sandbox w chmurze).
9. 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.
10. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
11. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
12. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.

**Ochrona serwera**

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2008 R2 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, 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.

Dodatkowe wymagania dla ochrony serwerów Windows:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. 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.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. 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 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Endpoint Detection and Response

1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta.
2. Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica”.
6. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
7. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
9. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania.
10. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.
11. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
12. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania poleceń powershell.

**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.
6. **System kopi bezpieczeństwa wraz z niezbędnymi elementami**

Wykonawca w ramach wykonania zadania zainstaluje i skonfiguruje system do tworzenia kopii bezpieczeństwa maszyn wirtualnych oraz kontenerów. System kopii ma zostać zainstalowany jako maszyna wirtualna na dwóch serwerach fizycznych pomiędzy którymi wykonawca stworzy automatycznie replikującą się przestrzeń.

|  |  |  |
| --- | --- | --- |
| lp | Wymagania funkcjonalno-techniczne | Tak / Nie |
|  | Licencja na oprogramowanie musi pozwalać na pełne wykorzystanie sprzętowych zasobów serwera oraz przestrzeni przeznaczonych do wykonywania kopii bezpieczeństwa. Licencja nie może ograniczać ilości przechowywanych kopii bezpieczeństwa, a także nie może ograniczać ilości maszyn wirtualnych z których ma być wykonana kopia bezpieczeństwa. |  |
|  | System kopii bezpieczeństwa musi być zarządzany przez graficzny panel. |  |
|  | System kopii bezpieczeństwa musi być kompatybilny z obecnym rozwiązaniem wirtualizacyjnym zamawiającego. obecnie Zamawiający posiada środowisko HA oparte na Proxmox 5.4  Zamawiający dopuszcza w ramach postepowania wymianę środowiska wirtualizacyjnego lub jego aktualizację do najnowszej wersji.  min wymagania dotyczące środowiska wirtualizacyjnego : - Licencja na oprogramowanie musi pozwalać na pełne wykorzystanie sprzętowych zasobów serwera  - Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych  - Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.  - Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 320 logicznych wątków oraz do 4TB pamięci fizycznej RAM  - Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-64 procesorowych  - Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB  - Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM.  - Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-10 wirtualnych kart sieciowych  - Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.  - Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej  - Rozwiązanie musi umożliwiać poprawne zainstalowanie następujących systemów operacyjnych: Windows Server 2008,2012,2016,2019 , Windows 7, Windows 8, Windows 10,Windows 11, SLES 11, SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris 11,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6, NetWare 5, OEL 4, OEL 5, Debian, CentOS,  - Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance  - Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.  - Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.  Z możliwością wysyłania maila o wykonanej kopii bezpieczeństwa  - Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.  - System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej.  - Musi zostać zapewniona odpowiednia redundancja i mechanizm (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.  Wykonawca zmieniając środowisko wirtualizacje zobowiązany jest do przeniesienia obecnych maszyn wirtualnych na nowe środowisko w sposób bezpieczny, nie powodujący dłuższej przerwy technicznej niż 4 godziny. W przypadku wykonywania Update środowiska wirtualizacyjnego wykonawca zobowiązany jest do podniesienia systemów operacyjnych maszyn wirtualnych systemu medycznego Medicus-Online. |  |
|  | Możliwość szyfrowania kopii po stronie klienta w celu zapewnienia bezpieczeństwa danych przed dotarciem do serwera backupowego |  |
|  | Możliwość korzystania z różnych typów przestrzeni dyskowych do składowania kopii bezpieczeństwa |  |
|  | Automatyczna weryfikacja kopii bezpieczeństwa |  |
|  | Możliwość tworzenia kopii min. na LTO-5 |  |
|  | Powiadomienia e-mail o wykonanych / niewykonanych kopiach bezpieczeństwa |  |
|  | System działający w modelu serwer – klient |  |
|  | Możliwość tworzenia kopi zapasowych fizycznych hostów opartych o systemy operacyjne z rodziny Linux, min. Debian, ubuntu |  |
|  | Wykonywanie kopii bezpieczeństwa maszyn wirtualnych oraz kontenerów z poziomu konsoli wirtualizatora. |  |
|  | Możliwość tworzenia kopii bezpieczeństwa na żądanie z panelu wirtualizatora |  |
|  | Możliwość konfigurowania harmonogramu kopii bezpieczeństwa - administrator wykonuje z panelu zarządzania środowiskiem wirtualnym |  |
|  | Możliwość podłączenia drugiego serwera kopii zapasowej w celu synchronizacji wykonanych kopii bezpieczeństwa |  |
|  | Możliwość zaplanowania maksymalnej liczy przechowywanych kopii |  |
|  | W ramach instalacji i konfiguracji systemu backupowego wykonawca na serwerach z klastra HA rozszerzy przestrzeń dyskową co umożliwi przeprowadzenie manualnego odtwarzania kopii zapasowych maszyn wirtualnych w celu weryfikacji poprawności ich wykonania.  Każdy z trzech serwerów fizycznych pracujących w klastrze HA musi zostać rozszerzony przynajmniej o dwa dyski o poniższych parametrach (razem min. 6 dysków): Dedykowany dysk SSD 480GB od serwera DL360 G10  Typ dysku: SSD  Format szerokości : 2,5'' (SFF)  Typ napędu: Wewnętrzny  Pojemność dysku: min. 480 GB  Interfejs dysku: SATA III - 6 Gb/s  Typ pamięci: MLC  Ilość operacji odczytu IOPS : min 79 000  Ilość operacji zapisu IOPS : min 29 000  Pobór mocy: max. 2.16 W  Gwarancja : min. 36 miesięcy |  |

**W ramach zadania wykonawca dostarczy zainstaluje i skonfiguruje sieciowy serwer plikowy dla archiwizacji  
kopii bezpieczeństwa. Konfiguracja sieciowego serwera plików musi zakładać podział przestrzeni dyskowej do przechowywania kopii przyrostowych maszyn wirtualnych jak i kopii pełnych maszyn wirtualnych**

|  |  |
| --- | --- |
| Architektura procesora | 64 bit |
| Procesor liczba rdzeni | Procesor osiągający wynik co najmniej 22 700 punktów w teście „PassMark Performance Test”, wynik opublikowany na stronie : <https://www.cpubenchmark.net/high_end_cpus.html> na dzień składania oferty. |
| Pamięć RAM | Nie mniej niż 32GB DDR4 |
| Pamieć RAM liczba slotów | Minimum 4 sloty |
| Pamięć RAM - możliwość rozszerzenia | Nie mniej niż do 128 GB |
| Możliwość instalacji dysków 3,5" SATA | Minimum 4 |
| Możliwość instalacji dysków 2,5" SATA | Minimum 5 |
| Pojemność dysków twardych jakie można stosować | do 18 TB |
| Zaintalowane dyski twarde | Min. 4 dyski o pojemności min. 10TB, przeznaczone do pracy w trybie 24x7, pamięc cache min 256MB |
| Możliwość podłączenia modułu rozszerzającego | Tak, minimum 5, rozbudowa może wymagać instalacji dodatkowej karty nie dostarczonej z urządzeniem |
| Porty LAN | Minimum 2 x 1 Gb/s Ethernet, 2 x 10 Gb/s SFP+, 2 x 10 Gbase-T |
| Diody LED | HDD 1–9, stan urządzenia, LAN |
| Porty USB | min. 2 gniazda typu USB 3.2 Gen 1 min. 1 gniazdo typu A USB 3.2 Gen2 10 Gb/s |
| Przyciski | Reset, Zasilanie |
| Typ obudowy | RACK, maksymalnie 1U |
| Dopuszczalna temperatura pracy | od 0 do 40˚C |
| Wilgotność względna podczas pracy | 5-95% R.H. |
| Zasilanie | Redundatne min. 300 W(x2), 100–240 V |
| Agregacja łączy | Tak |
| Obsługiwane systemy plików | Dyski wewnętrzne: ZFS Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+ |
| Możliwość podłączenia karty WLAN na USB | Tak |
| Łączenie usług z interfejsem | Tak |
| Szyfrowanie udziałów sieciowych | Tak, min AES 256 |
| Szyfrowanie dysków zewnętrznych | Tak |
| Zarządzanie dyskami | RAID 0,1,5,50,6,60,10, Triple Parity, Triple Mirror Konfiguracja priorytetu odbudowy grup RAID RAID HotSpare i Global HotSpare SSD Trim HDD S.M.A.R.T. Skanowanie uszkodzonych bloków  Wykrywanie uszkodzenia i naprawa danych Cache odczytu z wykorzystaniem dysków SSD Cache odczytu i dziennik zapisu z wykorzystaniem dysków SSD Funkcjonalność migawek udziałów oraz LUN, wraz z możliwością ich replikacji na drugie urządzenie |
| Wbudowana obsługa iSCSI | Obsługa wielu jednostek LUN na Target Obsługa mapowania i maskowania LUN Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S  Wykonywanie migawek oraz kopii zapasowej LUN |
| Obsługa Fiber Channel (FC SAN) | Wsparcie opcjonalnych kart FC Mapowanie LUN |
| Zarządzanie prawami dostępu | Przypisanie pojemności dla użytkowników Importowanie listy użytkowników Zarządzanie kontami użytkowników  Zarządzanie grupą użytkowników  Zarządzanie uprawnieniami dla użytkowników i grup Obsługa zaawansowanych uprawnień dla podfolderów |
| Obsługa Windows AD | Logowanie użytkowników domenowych poprzez protokoły CIFS/SMB, FTP oraz menadżera plików sieci Web Funkcja serwera i klienta LDAP |
| Funkcje backup | Oprogramowanie do tworzenia kopii bezpieczeństwa plików, opracowane przez producenta urządzenia dla systemów Windows.  Backup na zewnętrzne dyski twarde. |
| Współpraca z zewnętrznymi dostawcami usług chmury | Przynajmniej: Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox, OneDrive for Business, Google Drive |
| Darmowe aplikacje na urządzenia mobilne | Monitoring i zarządzanie urządzeniem / Współdzielenie plików / Obsługa kamer  Dostępne na systemy iOS oraz Android |
| Minimum obsługiwane aplikacje | Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer pobierania (Bittorrent/HTTP/HTTPS/FTP) |
| VPN | VPN client / VPN server Minimum obsługa PPTP, OpenVPN |
| Administracja systemu | Połączenia HTTP/HTTPS Powiadamianie przez e-mail Powiadamianie przez SMS (z wykorzystaniem zewnętrznych usług) DDNS oraz zdalny dostęp w chmurze producenta SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP oraz lokalnych przez USB Monitorowanie zasobów urządzenia Monitorowanie zasobów systemu w czasie rzeczywistym Rejestr zdarzeń Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Możliwość aktualizacji oprogramowania z powiadomieniem z serwerów producenta Ustawienia systemowe: kopia zapasowa, przywracanie, resetowanie systemu |
| Wirtualizacja | Możliwość uruchomienia maszyn wirtualnych z systemem Windows, Linux, Unix i Android Import maszyn wirtualnych  Klonowanie maszyn wirtualnych Migawki maszyn wirtualnych |
| Zabezpieczenia | Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem połączeń Obsługa HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Import certyfikatu SSL |
| Możliwość instalacji dodatkowego oprogramowania | Tak, sklep z aplikacjami producenta i aplikacjami firm zewnętrznych Możliwość instalacji z gotowych paczek oraz wbudowane narzędzia wirtualizacji umożliwiającee zarówno obsługę kontenerów Docker/LXC jak i pełnych maszyn wirtualnych |
| Gwarancja | Min. 3 lata producenta na serwer, min. 60 miesięcy na dyski twarde |

**4.1 Voucher na szkolenie certyfikowane : CERTIFIED STORMSHIELD NETWORK** ADMINISTRATOR, **24 h**(3 dni x 8 h) – 2 sztuki zgodnie z zakresem :

1. Uruchomienie urządzenia
   * Rejestracja w strefie klienta i dostęp zasobów
   * 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
2. Zbieranie logów i monitorowanie
   * Przedstawienie kategorii zbieranych logów
   * Wykresy historyczne i monitorowanie
3. Obiekty
   * Typy obiektów oraz ich wykorzystanie
   * Obiekty sieciowe i obiekt typu „router”
4. Konfiguracja sieci
   * Tryby pracy urządzenia
   * Typy interfejsów (Ethernet, modem, bridge, VLAN, GRETAP)
   * Typy routingu oraz ich priorytety
5. Translacja adresów sieciowych (NAT)
6. Translacja połączeń wychodzących (maskarada)
7. Translacja połączeń przychodzących (przekierowanie)
8. Translacja dwukierunkowa (jeden do jeden)
9. Filtrowanie ruchu sieciowego (Firewall)
10. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)
    * Szczegółowy opis parametrów reguły Firewall
    * Kolejność przetwarzania reguł Firewall i NAT
11. Ochrona aplikacji
    * Implementacja filtrowania URL dla ruchu http i https
    * Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
    * Moduł IPS i stosowanie profili inspekcji
12. Użytkownicy i uwierzytelnianie
13. Konfiguracja usługi katalogowej
    * Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)
    * Rejestracja użytkowników
    * Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania
14. Wirtualne sieci prywatne (VPN)
    * Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)
    * Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)
    * Tunele VTI
15. SSL VPN
    * Zasada działania
    * Konfiguracja

**4.2 Voucher na szkolenie : Konfigurowanie Active Directory Federation Services – 2 sztuki, zgodnie z zakresem :**

* + - 1. Wprowadzenie do tożsamości opartych na oświadczeniach
  1. istniejące rozwiązania do zarządzania tożsamościami
  2. zalety wykorzystania tożsamości opartych na oświadczeniach
  3. scenariusze wykorzystania AD FS
  4. terminologia AD FS i tożsamości opartych na oświadczeniach
     + 1. Wymagania wstępne AD FS

1. wymagania dot. konfiguracji wstępnej Windows
2. wprowadzenie do PKI
3. Omówienie Group Managed Service Accounts (gMSA)
   * + 1. Komponenty AD FS
   1. rola serwera federacji
   2. rodzaje oświadczeń, punkty końcowe oraz magazyn atrybutów
   3. zabezpieczenia AD FS
   4. rola Web Application Proxy
   5. administracja AD FS
      * 1. Uwierzytelnianie oparte na oświadczeniach dla organizacji
   6. przygotowanie AD FS
   7. AD FS w jednej organizacji
   8. idea i rodzaje oświadczeń
   9. reguły i szablony oświadczeń
   10. tworzenie reguł i szablonów oświadczeń
   11. konfiguracja AD FS
       * 1. Uwierzytelnianie oparte na oświadczeniach w federacji typu Business-to-Business (B2B)
4. wdrażanie AD FS w środowisku federacyjnym
5. konfiguracja relacji dla zaufanych dostawców oświadczeń
6. zarządzanie oświadczeniami w ramach organizacji
   * + 1. Zaawansowane scenariusze wdrażania AD FS
   1. implementacja roli Web Application Proxy
   2. planowanie wysokiej dostępności
   3. konfigurowanie rejestracji urządzeń w ADFS (opcjonalnie)
   4. konfigurowanie graficznego interfejsu użytkownika ADFS (opcjonalnie)
   5. dodatkowe scenariusze konfiguracyjne AD FS
      * 1. Rozwiązywanie problemów z AD FS
7. konfiguracja audytu dla AD FS
8. rozwiązywanie problemów z AD FS
9. Narzędzia dodatkowe: Claims X-Ray, AD FS Event Module, PowerShell Diagnostics Module, AD FS Rapid Restore Tool.

**4.3 Szkolenia dla personelu szpitala z cyberbezpieczeństwa**

Wykonawca przeprowadzi w uzgodnionym terminie z Zamawiającym szkolenia dla pracowników szpitala z zakresu cyberbezpieczeństwa . Szkolenia odbędą się w placówce zamawiającego w dwóch terminach maksymalna liczba grup 8.   
Zamawiający wymaga przeprowadzenia szkolenia dotyczącego:

1. Cyberbezpieczeństwo
   1. Cyberprzestrzeń, cyberbezpieczeństwo – czyli co?
   2. Ramy prawne i organizacyjne cyberbezpieczeństwa
   3. Dlaczego te zagadnienia są takie ważne?
2. Najsłabszy element systemu? Człowiek!
   1. Socjotechnika głównym narzędziem przestępców
   2. Sposoby przeprowadzania ataków i wykradania danych
   3. Jak należy reagować i bronić się przed próbami manipulacji
   4. Większa świadomość najlepszym zabezpieczeniem
3. Codzienne narzędzia pracy
   1. Niebezpieczny e-mail
   2. Zagrożenia na stronach internetowych
   3. Ataki przez telefon
   4. Sieci bezprzewodowe
4. Co robić, żeby było bezpiecznie?
   1. Bezpieczeństwo fizyczne
   2. Polityka haseł
   3. Bezpieczna praca z programem pocztowym i przeglądarką internetową
   4. Szyfrowanie danych
5. Informacja o stanie zdrowia i dokumentacja medyczna
   1. Zasady udostępniania
   2. Przetwarzanie danych pacjentów
   3. Archiwizacja i utylizacja
6. Odpowiedzialność pracownika
   1. Nieuprawnione ujawnienie informacji
   2. Zaniedbania w zakresie nadzoru nad informacją
   3. Z kim kontaktować się w przypadku incydentu?

Zamawiający wymaga po przeprowadzeniu szkoleń dostarczenia materiałów szkoleniowych z powyższego zakresu

**5. Oprogramowanie do zarządzanie zasobami IT**

Wykonawca dostarczy, zainstaluje oprogramowanie do zarządzania zasobami IT, wraz z oprogramowaniem musi zostać dostarczona licencja na system operacyjny na którym zostanie zainstalowane oprogramowanie. Zamawiający przewidział instalację systemu wraz z oprogramowaniem jako maszynę wirtualną.

*150 urządzeń, dwa stanowiska administracyjne ( umożliwiające równoczesna pracę). Licencja na minimum dwa lata.*

|  |  |  |
| --- | --- | --- |
| **LP** | Wymaganie | **Tak /nie** |
| 1. 1 | Pozyskiwanie informacji o sprzęcie, zarządzanie widokami, funkcje ogólne |  |
| 1. 2 | Centralne zarządzanie wynikami skanowania sprzętu i oprogramowania, pozyskiwanie informacji o sprzęcie (dane techniczne koputera) |  |
|  | Zdalne wykrywanie urządzeń w sieci za pomocą protokołów PING, ARP oraz SNMP |  |
|  | Automatyczne wykrywanie adresów IP, MAC, DNS, Systemu Operacyjnego wraz z informacją o aktualizacji |  |
|  | Automatyczne wykrywanie, czy komputer jest członkiem domeny oraz do jakiej domeny lub grupy roboczej należy |  |
|  | Odwzorowanie struktury organizacji w oparciu o Active Directory |  |
|  | Jednostronna synchronizacja komputerów oraz drukarek z AD (Odwzorowanie wszystkich wprowadzonych zmian w rekordach Active Directory) |  |
|  | Automatyczne skanowanie całości lub wybranych grup Active Directory oraz sieci |  |
|  | Mapowanie atrybutów obiektów AD do obiektów |  |
|  | Grupowanie wyposażenia z podziałem na jednostki organizacyjne w firmie (np. względem działów, lokalizacji, statusów) |  |
|  | Inwentaryzacja dowolnych elementów wyposażenia (biurka, szafy, telefony, etc.) |  |
|  | Utworzenie własnych typów elementów wyposażenia |  |
|  | Łączenie elementów wyposażenia w zestawy |  |
|  | Przypisywanie zasobu do wielu zestawów |  |
|  | Makrodefinicje w celu spersonalizowania nazw elementów w drzewku wyposażenia |  |
|  | Grupowanie, sortowanie i filtrowanie po dowolnie nadanych atrybutach |  |
|  | Podpięcie dowolnych załączników, np. skany faktur, gwarancji oraz wszelkich innych plików |  |
|  | Przypisywanie sprzętu do konkretnych osób |  |
|  | Przypisywanie sprzętu do wybranej firmy |  |
|  | Automatyczne wyznaczanie 'Głównego użytkownika' komputera |  |
|  | Wiązanie wielu rekordów wyposażenia z użytkownikiem |  |
|  | Przypisywanie sprzętu do dowolnej lokalizacji |  |
|  | Definiowanie własnych, dowolnych atrybutów sprzętu |  |
|  | Aktywnym komputerom (bez określonego statusu) przydzielany jest status 'W użyciu' |  |
|  | Wydruk etykiet z kodami kreskowymi do inwentaryzacji wyposażenia |  |
|  | Określanie loga firmy oraz użycia go na wydrukach |  |
|  | Grupowa zmiana domeny/grupy roboczej zasobu |  |
|  | **Informacje o sprzęcie** |  |
|  | Automatyczne wykrywanie typu komputera (Desktop\Notebook\Serwer\Kontroler domeny) na podstawie wyników skanowania sprzętu |  |
|  | Wykrywanie komputerów typu All-In-One |  |
|  | Automatyczne wykrywanie typów stacji roboczej (Tower\Desktop\SFF\uSFF) |  |
|  | Automatyczne uzupełnianie informacji o procesorze, liczbie rdzeni, ilości pamięci RAM, rozmiarze dysku, nazwie karty graficznej i rozdzielczości monitora w obiekcie zasobu po wykonaniu skanowania sprzętu |  |
|  | Odczytywanie indeksów wydajności poszczególnych komponentów komputera: CPU, GPU, HDD, RAM |  |
|  | Automatyczna aktualizacja nazwy komputera w przypadku jej zmiany |  |
|  | Definiowanie statusów dla sprzętu (Nowy, Do kasacji, W serwisie, itd. ) |  |
|  | Szczegółowa informacja na temat podzespołów sprzętu (procesor, bios, płyta główna, pamięć, dyski twarde, monitory, karty graficzne i muzyczne, etc. ) |  |
|  | Odczyt informacji o module TPM |  |
|  | Odczyt D3Dscore z WinSAT |  |
|  | Inwentaryzacja osprzętu komputerowego (monitory, drukarki, myszki, urządzenia sieciowe: Switch, Router, Access Point, Bridge, Modem, NAS, UPS, itd.) |  |
|  | Automatyczne wykrywanie lokalnych drukarek (USB) na podstawie wyników skanowania sprzętu |  |
|  | Automatyczne wykrywanie i tworzenie monitorów (producent, numer seryjny, rozdzielczość, odczyt firmy, działu, osoby odpowiedzialnej, głównego użytkownika) |  |
|  | Automatyczne tworzenie zestawów: Komputer + Monitor |  |
|  | Automatyczne utworzenie zestawów: Komputer + drukarka lokalna |  |
|  | Automatyczne utworzenie zestawów: host + maszyny wirtualne |  |
|  | Automatyczne wykrywanie czy komputer jest maszyną wirtualną |  |
|  | Wykrywanie maszyn wirtualnych typu: Parallels Virtual Platform |  |
|  | Określanie informacji o wykorzystywanej wirtualizacji |  |
|  | Podgląd zestawów, do których należy zasób |  |
|  | Cykliczne wykonywanie skanowania sprzętu z różnymi ustawieniami |  |
|  | Przypisywanie stałego atrybutu COA, który będzie uwzględniany na raportach wyposażenia i audytu |  |
|  | Definiowanie szczegółowych informacji finansowych |  |
|  | Obsługa walut w danych finansowych |  |
|  | Definiowanie bazy dostawców sprzętu i oprogramowania |  |
|  | Automatyczne odczytywanie ServiceTag oraz modelu komputera (na podstawie wyników skanowania sprzętu) |  |
|  | Automatyczna aktualizacja adresów IP komputerów bez zainstalowanego agenta |  |
|  | Agent odczytuje identyfikator SID komputera |  |
|  | Określanie adresu interfejsu webowego urządzenia sieciowego |  |
|  | Określanie typu gwarancji dla zasobu |  |
|  | Określenie wpływu biznesowego wybranego zasobu |  |
|  | Tworzenie własnych typów gwarancji |  |
|  | Określanie ikony dla typów zasobów |  |
|  | **Raporty zasobów** |  |
|  | Automatyczne tworzenie historii zmian sprzętu |  |
|  | Raport zbiorczy historii zmian w sprzęcie |  |
|  | Ewidencja zdarzeń serwisowych |  |
|  | Dodanie notatek\komentarzy dla zdefiniowanych obiektów zasobów |  |
|  | Informacja na temat pojemności dysków twardych oraz wolnego miejsca |  |
|  | Wydruk\dodanie jako załącznik protokołu przekazania\zwrotu\utylizacji sprzętu |  |
|  | Wydruk\dodanie jako załącznik protokołu przekazania dla całego zestawu |  |
|  | Kreator szablonów wydruków WYSIWYG |  |
|  | Definiowanie dedykowanych profili protokołów |  |
|  | Zapisywanie protokołów podczas generowania jako załącznik do zasobu |  |
|  | Wydruk\dodanie jako załącznik Karty informacyjnej dla elementu wyposażenia |  |
|  | Wydruk lub zapisanie do pliku raportów ze szczegółami sprzętu |  |
|  | Porównywarka wyników skanowania sprzętu |  |
|  | Dzienniki zdarzeń systemu Windows |  |
|  | Automatyczny monitoring i raportowanie zmian w podzespołach sprzętu |  |
|  | **Funkcje dodatkowe** |  |
|  | Zdalne wykonywanie skryptów (batch) - Obsługa zadań jednorazowych i cyklicznych |  |
|  | Wykonywanie zadań dla wszystkich komputerów (uwzględnia komputery, które zostaną dodane w przyszłości) |  |
|  | Edytor skryptów (batch) z funkcją kolorowania składni |  |
|  | Wykorzystywanie predefiniowanych skryptów (batch) |  |
|  | Import informacji o wyposażeniu z pliku CSV |  |
|  | Wyszukiwanie sterowników, informacji o komputerze, informacji o gwarancji w bazie producenta (DELL) |  |
|  | Mechanizm automatycznego tworzenia rekordów producenta sprzętu (na podstawie wyników skanowania sprzętu) |  |
|  | Generowanie kodów paskowych, QR dla każdego elementu wyposażenia |  |
|  | Obsługa kodów QR |  |
|  | Archiwum zasobów |  |
|  | Przeniesienie utylizowanego wyposażenia do archiwum |  |
|  | Automatyczne usunięcie informacji sieciowych oraz licencji agenta dla zasobu archiwizowanego |  |
|  | Zarządzanie sprzętem przez aplikacje mobilną (Android, Windows Phone) |  |
|  | Powiadomienia o kończącej się gwarancji\umowie serwisowej dla zasobu |  |
|  | Zachowanie ostatniego skanu sprzętu podczas konserwacji bazy danych |  |
|  | Powiadomienia o utworzeniu monitora, wykryciu maszyny wirtualnej |  |
|  | Grupowa zmiana atrybutów |  |
|  | Personalizacja statusów zasobów |  |

**6. Urządzenie klasy UTM do ochrony brzegu sieci 3 szt.**

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, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. 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.
13. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
14. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
15. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
16. 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.
17. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
18. 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.
19. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
20. Po zakupie stosownej licencji 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).
21. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
22. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
23. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
24. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
25. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
26. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
27. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
28. 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.

Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

1. Ochrona antyspam ma działać w oparciu o:
   1. białe/czarne listy,
   2. DNS RBL,
   3. Skaner heurystyczny.
2. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
3. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
4. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
5. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
   1. PPTP VPN,
   2. IPSec VPN,
   3. SSL VPN.
6. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
7. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
8. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
9. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
10. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
11. Urządzenie ma posiadać wbudowany filtr URL.
12. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
13. Administrator ma mieć możliwość dodawania własnych kategorii URL.
14. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
15. blokowanie dostępu do adresu URL,
16. zezwolenie na dostęp do adresu URL,
17. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
18. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
19. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
20. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
21. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
22. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
23. 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.
24. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
25. 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.
26. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
27. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
28. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
29. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
30. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    1. równoważenie względem adresu źródłowego,
    2. równoważenie względem połączenia.
31. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
32. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
33. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
34. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
35. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
36. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
37. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
38. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
39. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
40. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
41. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
42. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
43. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
44. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
45. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
46. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
47. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
48. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
49. 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 chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
50. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
51. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
52. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
53. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
54. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
55. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
56. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
57. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
58. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
59. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
60. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
61. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
62. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
63. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
64. Urządzenie ma posiadać usługę DNS Proxy.
65. 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.
66. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
67. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
68. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
69. Urządzenie ma umożliwiać podłączenie karty SD w celu zapisywania logów.
70. Liczba portów Ethernet 10/100/1000Mbps – min.8.
71. Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
72. Przepustowość Firewall (1518 bajtów UDP) – minimum 2Gbps.
73. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1.6Gbps.
74. Przepustowość filtrowania Antywirusowego – minimum 400Mbps.
75. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 350Mbps.
76. Maksymalna liczba tuneli VPN IPSec – minimum 50.
77. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 20.
78. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 20.
79. Obsługa interfejsów 802.11q (VLAN) – minimum 128
80. Liczba równoczesnych sesji – minimum 200 000 i nie mniej niż 15 000 nowych sesji/sekundę.
81. Urządzenie nie ma limitu na liczbę użytkowników.
82. Liczba reguł filtrowania – minimum 4 096.
83. Liczba tras statycznego routingu – minimum 512.
84. Liczba tras dynamicznego routingu – minimum 10 000.

Ponadto Zamawiający oczekuje dostarczenia pakietu zawierającego przedłużenie wszystkich licencji oraz gwarancji na okres min. 24 miesięcy dla dwóch posiadanych urządzeń Stormshield SN510.

1. **Konfiguracja urządzeń aktywnych sieci i urządzeń bezpieczeństwa UTM**

Zamawiający posiada następujący sprzęt aktywny sieci w postaci przełączników sieciowych, rdzeniowych, przełączników dostępowych oraz klastra urządzeń bezpieczeństwa sieci klasy UTM generacji drugiej

- przełączniki rdzeniowe sieci LAN – HPE FLEXFABRIC 5700 32XGT 8XG 2QSFP+ - 2 szt

- serwer HPE PROLIANT DL360G10 – działający jako klaster HA – 3 szt

- serwer HPE PROLIANT DL360G10 – działający w trybie replikacji – 2 szt

- macierz dyskowa, blokowa HPE MSA2052 – 2 szt

- UTM Stormshield SN510 – 2 szt

- Przełączniki dostępowe sieci LAN – HPE ARUBA 2540 48G 4SFP+ – 14 SZT

- urządzenia sieci WIFI – HPE ARUBA IAP-207 RW Instant – 20 szt

1. W ramach realizacji zamówienia usług wdrożeniowych, Wykonawca wykona plan oraz harmonogram wdrożenia obejmujący rekonfigurację posiadanej przez Zamawiającego infrastruktury teleinformatycznej a w szczególności urządzeń aktywnych sieci oraz urządzeń bezpieczeństwa sieci. W ramach usługi rekonfiguracji, Wykonawca dokona pełnej inwentaryzacji zainstalowanego sprzętu sieciowego, serwerowego oraz bezpieczeństwa sieci w sposób pozwalający na prawidłowe przygotowanie planu wdrożenia. Plan wdrożenia musi przewidywać osiągnięcie celu jakim jest poprawa bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego z wykorzystaniem posiadanego przez Zamawiającego sprzętu oraz rozwiązań oraz z wykorzystaniem najlepszych praktyk stosowanych w zakresie cyber-bezpieczeństwa. Jeśli posiadane infrastruktura będzie wymagała zastosowania dodatkowych kabli lub modułów połączeniowych to Wykonawca, musi takie elementy dostarczyć w ramach realizowanej usługi rekonfiguracji infrastruktury teleinformatycznej Zamawiającego.

2. Wykonawca wykona ponowną konfigurację klastra urządzenia typu firewall wraz z aktualizacją oprogramowania układowego do najnowszej, stabilnej wersji. Wymagania konfiguracyjne obejmują:

- konfiguracje klastra UTM

- konfiguracje wszystkich interfejsów sieciowych,

- konfiguracje obiektów i grup obiektów,

- ustanowienie nowych polityk firewall i odpowiednich profili bezpieczeństwa kontrolujących i prowadzących inspekcję ruchu sieciowego dla istniejących oraz nowych usług i systemów z ekspozycją zewnętrzną oraz wewnętrzną

- translację NAT,

- identyfikację użytkowników,

- routingi,

- logowanie,

- ustawienia systemowe (m.in. dostęp administracyjny wg wymagań Zamawiającego),

- modyfikację obecnie działającej konfiguracji z urządzeń UTM Stormshield SN510 w sposób zgodny z przygotowanym planem wdrożenia

- konfiguracje wymaganych routingów w/g potrzeb Zamawiającego,

- konfiguracje tuneli VPN w/g koncepcji Zamawiającego (do 20 połączeń)

- aktualizacja oprogramowania układowego wszystkich przełączników aktywnych sieci do najnowszej stabilnej wersji

- segmentacja sieci zgodnie z przyjętym przez Zamawiajacego podziału na podstawie planu wdrożenia, przedstawionego przez Wykonawcę

- konfiguracja stosu logicznego dla przełączników sieciowych - rdzeniowych

- adresacja IP, podział na podsieci, utworzenie VLANów, konfiguracja routingu pomiędzy vlanami,

- rekonfiguracja systemu sieci WIFI

- integracja przełączników sieciowych oraz urządzeń sieci bezprzewodowej z urządzeniami bezpieczeństwa

3. Wykonawca wykona również konfiguracje polityk bezpieczeństwa, a w szczególności :

- identyfikację użytkowników sieci i egzekwowanie zasad opartych na tożsamości w sieci szpitala,

- konfiguracje pozostałych parametrów pracy urządzeń, nie wymienionych powyżej, a uznanych przez Zamawiającego za istotne do skonfigurowania, w terminach podanych przez Zamawiającego

4. Wykonawca wykona testy działania urządzeń sieciowych odbędą się zgodnie z zaakceptowanym przez Zamawiającego planem i harmonogramem wdrożenia, w tym testów:

- Poprawność działania sprzętu,

- Poprawność działania skonfigurowanych sieci LAN,

- Poprawność komunikacji pomiędzy serwerami systemu, stacji klienckich

- poprawność działania urządzeń bezpieczeństwa sieci w tym testy działania wybranych reguł i polityk bezpieczeństwa