**Załącznik nr 3**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

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** – oznaczaSamodzielny Publiczny Zakład Opieki Zdrowotnej w Słupcy
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. poz. 2019 ze zm.), dalej PZP.
3. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawartej 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. **Plan Realizacji Projektu** – Dokument określający zasady współpracy pomiędzy Zamawiającym, a Wykonawcą. Zawiera m.in.:
    * strukturę organizacyjną projektu,
    * produkty projektu,
    * zasady komunikacji w projekcie,
14. **Szkolenie Administratora(ów)** – szkolenia użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora infrastruktury sprzętowej.
15. **Systemy Zewnętrzne** – systemy z którymi docelowo współpracować będzie wdrażany system.
16. **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 7:30 do 14:30 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.
12. **Elektroniczny System Zgłoszeń (ESZ)** – narzędzie posiadające interfejs WWW służące do rejestracji zgłoszeń (potencjalnych problemów, usterek) oraz kontroli ich cyklu życia (tzw. Issue Tracking System lub Defect Tracking System). System ESZ udostępniony zostanie przez Wykonawcę dla Zamawiającego na czas realizacji przedmiotu zamówienia oraz w okresie jego gwarancji.

**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 Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Słupcy.

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 Eskulap 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, w szczególności uwzględniając:

* posiadane środowisko domenowe,
* posiadaną konfigurację sieci wraz z segmentacją VLAN, oraz strefą DMZ,
* posiadaną konfiguracją baz danych i backupów,
* konfigurację stacji roboczych.

**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
   * Komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,
   * Dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim
   * Szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury szpitala, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
   * Zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni.
   * Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.

**Opis parametrów minimalnych dostarczanej infrastruktury oraz oprogramowania:**

Wymagania dla Wykonawcy który dostarczy infrastrukturę sprzętową oraz oprogramowanie:

Zamawiający wymaga, aby Wykonawca spełniała wymagania w zakresie:

|  |  |  |  |
| --- | --- | --- | --- |
| **1. System monitoringu infrastruktury IT (SOC) – usługa świadczona do 31.12.2022** | | | |
| **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 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 fizyczne i wirtualne 15 sztuk * Macierze 2 sztuk, * Przełączniki LAN 30 sztuk * Serwer Backupu 1 sztuk * Bibliotekę taśmowa LTO 1 sztuk * Macierz NAS 1 sztuk * UPS 3 sztuki * Kontroler WI-FI 2 Sztuki * Urządzenie typu UTM 2 sztuki * Serwerów aplikacji * IIS 4 sztuki * Serwer wirtualizacji 1 Sztuk * serwer AD 1 Sztuk * W ramach usługi wykonawca monitoruje krytyczne elementy systemu HIS: * Monitorowanie komunikacji z platformą P1 * Monitorowanie komunikacji bramek HL7 * Monitorowanie komunikacji EWUŚ * Monitorowanie KOWAL * Monitorowanie komunikacji AP-KOLCE * Monitorowanie RZM * Monitorowanie bazy danych systemu HIS | TAK |  |

|  |
| --- |
| **2. System EDR - 170 stanowisk** |
| W związku z posiadaniem przez Zamawiającego systemu antywirusowego ESET w wersji ESET PROTECT Entry ON-PREM (170 stanowisk, okres subskrypcji do 31.03.2024r), Zamawiający oczekuje dostarczenie licencji systemu ESET PROTECT Entry ON-PREM jako systemu EDR – licencje dostarczane w ramach zamówienia będą realizacją rozbudowy posiadanego już systemu ESET.  Ilość szt. Licencji ESET PROTECT Entry ON-PREM – 170 szt.  Okres subskrypcji 3 lata. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **3. Serwer bacupu** | | | | |
| **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 |
|  | obudowa do montażu w szafie typu rack | TAK | |  |
|  | zasilanie redundantne, przynajmniej 2 zasilacze typu HotPlug | TAK | |  |
|  | płyta główna z możliwością zainstalowania minimum dwóch procesorów | TAK | |  |
|  | zegar procesora minimum 2,6 GHz | TAK | |  |
|  | zainstalowany 1 procesor minimum ośmiordzeniowy klasy x86 dedykowane do pracy w serwerach, zaprojektowane do pracy w układach wieloprocesorowych | TAK | |  |
|  | pamięć minimum 128GB ECC DIMM, rozszerzalna, z zabezpieczeniem typu: ECC | TAK | |  |
|  | dyski minimum 2x 960 GB SSD skonfigurowane w RAID1 , 6x8TB 7.2K | TAK | |  |
|  | sieć minimum 2x16Gb FC, 2x10Gb SFP+ SR | TAK | |  |
|  | z przodu obudowy: 1x USB 3.0, 1x USB 2.0 | TAK | |  |
|  | z tyłu obudowy: 2x USB 3.0, , 1x DB-15 | TAK | |  |
|  | Zarządzanie:   * Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania * Monitoring statusu i zdrowia systemu * Logowanie zdarzeń * Umożliwiający Update systemowego firmware * Umożliwiający zdalną konfigurację serwera * Monitoring i możliwość ograniczenia poboru prądu * Zdalne włączanie/wyłączanie/restart * Przekierowanie konsoli szeregowej przez IPMI * Zrzut ekranu w momencie zawieszenia system * Możliwość przejęcia zdalnego ekranu 1920x1200, 60 Hz,16 bpp * Zdalny dostęp do serwera * Możliwość zdalnej instalacji systemu operacyjnego * Alerty Syslog * Przekierowanie konsoli szeregowej przez SSH * Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera * Możliwość mapowania obrazów ISO z lokalnego dysku operatora * Możliwość mapowania obrazów ISO przez HTTPS * Możliwość jednoczesnej pracy użytkowników przez wirtualną konsolę * Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3 | TAK | |  |
|  | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID | TAK | |  |
|  | gwarancja: min. 36 m-cy , 3YNBD, producenta | TAK | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **4. Biblioteka taśmowa** | | | | |
| **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 |
| **Wymagania techniczne** | | | | |
|  | Obudowa przystosowana do montażu w standardowej szafie rack 19’’. Maksymalna wysokość oferowanego rozwiązania - 3U. | TAK | |  |
|  | Biblioteka taśmowa musi być wyposażona w min. 1 napęd taśmowy LTO8 z interfejsem FC min. 8 Gbit/s. | TAK | |  |
|  | Biblioteka taśmowa musi mieć możliwość rozbudowy do min. 8 napędów taśmowych. | TAK | |  |
|  | Biblioteka musi być wyposażona w nie mniej niż 20 slotów na taśmy i posiadać możliwość rozbudowy do co najmniej 100 slotów na taśmy. | TAK | |  |
|  | Biblioteka musi być wyposażona w przynajmniej 3 sloty wejścia/wyjścia, umożliwiający wymianę taśm bez konieczności wyłączania urządzenia. | TAK | |  |
|  | Biblioteka musi być wyposażona w czytnik kodów kreskowych. | TAK | |  |
|  | Biblioteka musi być wyposażona w komplet magazynków na taśmy, tak by możliwa była pełna obsada biblioteki taśmami LTO. | TAK | |  |
|  | Możliwość zdalnego zarządzania biblioteką poprzez interfejs WWW. | TAK | |  |
|  | Możliwość monitorowania stanu biblioteki i napędów. | TAK | |  |
|  | Biblioteka musi posiadać panel sterowania oraz wyświetlacz informujący o błędach urządzenia, aktywności napędów. | TAK | |  |
| **Wymagania dodatkowe** | | | | |
|  | Do biblioteki należy dostarczyć:  - niezbędne kable zasilające,  - taśmę LTO 8 – 10 szt.  - taśmę czyszczącą – 1 szt.  - przewód światłowodowy – 1 szt. | TAK | |  |
|  | Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu. | TAK | |  |
|  | Wszystkie oferowane urządzenia muszą być fabrycznie nowe. | TAK | |  |
|  | Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. | TAK | |  |
|  | Urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz. | TAK | |  |
|  | Oferowane produkty (urządzenia, sprzęty) w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE,  tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE. | TAK | |  |
|  | Urządzanie musi być objęta 36 miesięczną gwarancją | TAK | |  |
|  | Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji. | TAK | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **5. System Backupowy** | | | | |
| **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 |
| **1. MECHANIZMY ZABEZPIECZANIA DANYCH** | | | | |
| **Ogólne** | | | | |
|  | Rozwiązanie musi mieć możliwość konfigurowania liczby równoległych wątków wykonujących zadania tworzenia kopii zapasowej i odtwarzania | TAK | |  |
|  | Rozwiązanie musi umożliwiać bezagentowe (bez konieczności instalowania agenta w zabezpieczanym systemie operacyjnym) zabezpieczenie środowisk wirtualnych, kontenerowych , aplikacji, lub instancji pamięci masowej (wolumenu lub systemu plików) | TAK | |  |
|  | Mechanizm tworzenia oraz odtwarzania maszyn wirtualnych musi być spójny dla wszystkich wymienionych platform wirtualizacyjnych pod kątem konfiguracji. | TAK | |  |
|  | Architektura rozwiązania powinna umożliwiać skalowanie horyzontalne (ang. scale-out) komponentów realizujących proces kopii zapasowej (ang. data-mover) | TAK | |  |
|  | System powinien przechowywać wszystkie metadane kopii zapasowych w relacyjnej bazie danych | TAK | |  |
|  | System powinien umożliwiać konfigurację w klastrze active-passive (komponent zarządzający rozwiązaniem) | TAK | |  |
|  | System powinien umożliwiać pracę w trybie autonomicznym (bez konieczności instalowania innych systemów backupów) | TAK | |  |
|  | Rozwiązanie musi umożliwić zarówno ręczne odtworzenie pojedynczej maszyny wirtualnej jak I zaplanowanie masowego odtworzenia wielu maszyn wirtualnych do wskazanego z góry środowiska (na żądanie oraz cyklicznie  z opcją nadpisania istniejących maszyn wirtualnych) | TAK | |  |
|  | Rozwiązanie powinno umożliwiać automatyczne wysyłanie raportów do centralnej bazy producenta (opcjonalnie z zawartością logów) w celu usprawnienia diagnostyki i świadczenia wsparcia przez producenta | TAK | |  |
| **Vmware vSphere/ESXi** | | | | |
|  | Obsługa Vmware vSphere/ESXi od wersji 6 korzystając z „VMware vSphere Storage API”. | TAK | |  |
|  | Wykonywanie kopii zapasowych w oparciu o technologie NBD & HotAdd. | TAK | |  |
|  | Wykonywanie przyrostowych kopii zapasowych z wykorzystaniem mechanizmu CBT. | TAK | |  |
|  | Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji | TAK | |  |
|  | Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej | TAK | |  |
|  | Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI. | TAK | |  |
|  | Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej | TAK | |  |
|  | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki) | TAK | |  |
|  | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o przypisane w środowisku tagi. | TAK | |  |
|  | Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej. | TAK | |  |
|  | Możliwość wykonywania cyklicznie migawek maszyny wirtualnej bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane) | TAK | |  |
|  | Możliwość użycia migawek spójnych na poziomie aplikacji (ang. quiesced snapshot) przy wykonywaniu kopii zapasowej | TAK | |  |
|  | Możliwość automatycznego uruchomienia maszyny wirtualnej po zakończonym procesie odtwarzania. | TAK | |  |
| Oracle VM | | | | |
|  | Obsługa Oracle VM od wersji 3.4 wzwyż. | TAK | |  |
|  | Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji | TAK | |  |
|  | Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej | TAK | |  |
|  | Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI. | TAK | |  |
|  | Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej | TAK | |  |
|  | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki) | TAK | |  |
|  | Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych  w oparciu o migawki (ang. snapshot) | TAK | |  |
| AWS EC2 | | | | |
|  | Wsparcie dla AWS EC2 | TAK | |  |
|  | Możliwość odtworzenia całej maszyny wirtualnej na środowisko wirtualizacji | TAK | |  |
|  | Możliwość odtworzenia pojedynczych plików/folderów z kopii zapasowej | TAK | |  |
|  | Możliwość udostępnienia dysków maszyny wirtualnych w kopii zapasowej do innych systemów poprzez protokół iSCSI. | TAK | |  |
|  | Możliwość pominięcia wybranych dysków maszyny wirtualnej z kopii zapasowej | TAK | |  |
|  | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa maszyn wirtualnych (np. maszyny o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki) | TAK | |  |
|  | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o przypisane w środowisku tagi. | TAK | |  |
|  | Możliwość tworzenia pełnych kopii zapasowych maszyn wirtualnych  w oparciu o migawki (ang. snapshot) | TAK | |  |
|  | Możliwość automatycznego wykonania polecenia na maszynie wirtualnej (której kopia zapasowa jest wykonywana) bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej. | TAK | |  |
|  | Możliwość wykonania migawki (snapshot). | TAK | |  |
|  | Możliwość automatycznego uruchomienia maszyny wirtualnej po zakończonym procesie odtwarzania. | TAK | |  |
| **Aplikacje** | | | | |
|  | Rozwiązanie musi umożliwiać wykonanie kopii zapasowej przy użyciu natywnych poleceń zabezpieczanej aplikacji (wykonujących np. spójną kopię zapasową bazy danych) na zdalnych maszynach oraz poprzez opracowane dedykowane skrypty administracyjne bez konieczności wykonania obrazu całej maszyny wirtualnej lub instancji pamięci masowej (wolumenu lub systemu plików) | TAK | |  |
|  | Rozwiązanie musi umożliwiać zdefiniowanie w jaki sposób kopia zapasowa będzie wykonana (jakie polecenie, jakie parametry, gdzie znajdują się pliki do zabezpieczenia) a następnie umożliwiać wielokrotne przypisanie takiej konfiguracji do wielu instancji aplikacji z różnymi wartościami parametrów, tak aby nie było konieczności wielokrotnego podawania argumentów polecenia dla każdej z aplikacji z osobna | TAK | |  |
|  | Rozwiązanie musi umożliwiać wykonywanie skryptów i poleceń zarówno poprzez SSH (zdalnie) jak i z maszyny na której jest zainstalowane rozwiązanie producenta (tak, żeby nie było konieczności uruchamiania usług zdalnych takich jak SSH w celu wykonania kopii zapasowej) | TAK | |  |
|  | Rozwiązanie powinno umożliwiać wkopiowanie danych backupu do innego systemu z użyciem SSH – np. transfer danych kopii zapasowej z aplikacji produkcyjnej na środowisko aplikacji testowej | TAK | |  |
| File System | | | | |
|  | Możliwość wykonywania kopii zapasowych filesystemu podłączonego do noda vProtect (katalogi, pliki zwykłe, dowiązania symboliczne) | TAK | |  |
|  | Możliwość wykonania kopii zapasowej pełnej. | TAK | |  |
|  | Możliwość wykonania kopii zapasowej przyrostowej. | TAK | |  |
|  | Możliwość odtworzenia pojedynczego pliku. | TAK | |  |
|  | Możliwość podłączenia zasobu po interfejsie ISCSI, jako dysk z filesystemem XFS. | TAK | |  |
| **Nutanix Files (AFS)** | | | | |
|  | Możliwość wykonywania kopii zapasowych Nutanix Files (AFS), zasobów NFS/SMB, z wykorzystaniem funkcjonalności CFT. | TAK | |  |
|  | Możliwość wykonania kopii zapasowej pełnej. | TAK | |  |
|  | Możliwość wykonania kopii zapasowej przyrostowej. | TAK | |  |
|  | Możliwość odtworzenia pojedynczego pliku. | TAK | |  |
|  | Możliwość podłączenia zasobu po interfejsie ISCSI, jako dysk z filesystemem XFS. | TAK | |  |
| **Ceph RBD** | | | | |
|  | Możliwość wykonania kopii zapasowych wolumenów Ceph RBD. | TAK | |  |
|  | Możliwość wykonania kopii zapasowej pełnej. | TAK | |  |
|  | Możliwość wykonania kopii zapasowej przyrostowej. | TAK | |  |
|  | Możliwość odtworzenia pojedynczego pliku. | TAK | |  |
|  | Możliwość podłączenia zasobu po interfejsie ISCSI | TAK | |  |
|  | Możliwość wykonywania cyklicznie migawek wolumenu bez eksportu danych i ich automatyczna rotacja (usuwanie najstarszych – polityka powinna umożliwiać wskazanie liczby migawek i okres przez jaki powinny być przetrzymywane) | TAK | |  |
|  | Możliwość automatycznego wykonania polecenia bezpośrednio przed jak I po wykonaniu migawki w celu np. wstrzymania działania usługi na czas wykonywania migawki i zapewnienia lepszej spójności kopii zapasowej. | TAK | |  |
|  | Możliwość automatycznego przypisywania polityk do maszyn wirtualnych w oparciu o reguły nazewnictwa wolumenów RBD (np. wolumeny RBD o nazwie zawierającej wskazany ciąg znaków powinny być przypisywane do wskazanej polityki) | TAK | |  |
| **2. SKŁADOWANIE DANYCH KOPII ZAPASOWYCH** | | | | |
| Ogólne | | | | |
|  | Rozwiązanie musi umożliwiać wykonanie polecenia/skryptu administracyjnego przed i po dostępie do pamięci masowej – np. w celu wywołania mechanizmów replikacji danych lub wysyłania powiadomień | TAK | |  |
|  | Rozwiązanie musi umożliwiać synchronizację obecności kopii zapasowej  w danej lokalizacji składowania z wewnętrzna bazą danych, np. gdyby ręcznie kopie zostały usunięte, nie powinny widnieć w interfejsie użytkownika; analogicznie gdyby ponownie były dostępne, np. po tymczasowej awarii systemu plików, powinny ponownie zostać zaznaczone jako dostępne | TAK | |  |
| **System plików** | | | | |
|  | Rozwiązanie musi umożliwiać składowanie kopii zapasowej na lokalnych lub zdalnych zasobach dyskowych podmontowanych do rozwiązania jako systemy plików | TAK | |  |
|  | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK | |  |
|  | Rozwiązanie musi oferować deduplikację danych | TAK | |  |
|  | Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie | TAK | |  |
|  | Rozwiązanie powinno umożliwiać wykorzystanie mechanizmu ochrony nadpisania zabezpieczonych kopii zapasowych (ang. retention lock), gdy używany jest Dell-EMC PowerProtect (DataDomain) | TAK | |  |
| **System plików (syntetyczny)** | | | | |
|  | Rozwiązanie musi umożliwiać składowanie kopii zapasowej na lokalnych lub zdalnych zasobach dyskowych podmontowanych do rozwiązania jako systemy plików | TAK | |  |
|  | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK | |  |
|  | Rozwiązanie musi umożliwiać składować dane w postaci syntetycznej bez konieczności scalania przyrostowych kopii zapasowych w trakcie odtwarzania | TAK | |  |
| **IBM Spectrum Protect** | | | | |
|  | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie IBM Spectrum Protect od wersji 7 | TAK | |  |
|  | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK | |  |
|  | Rozwiązanie musi oferować deduplikację danych po stronie zarówno rozwiązania jak i serwera IBM Spectrum Protect | TAK | |  |
| **Dell EMC Avamar** | | | | |
|  | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie Dell EMC Avamar od wersji 7.5 | TAK | |  |
|  | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK | |  |
|  | Integracja powinna używać narzędzi administracyjnych dostarczanych przez Dell EMC | TAK | |  |
| **Dell EMC NetWorker** | | | | |
|  | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie Dell EMC NetWorker od wersji 9 | TAK | |  |
|  | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK | |  |
|  | Integracja powinna używać narzędzi administracyjnych dostarczanych przez Dell EMC | TAK | |  |
| **Veritas NetBackup** | | | | |
|  | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie Versitas NetBackup od wersji 7.6 | TAK | |  |
|  | Rozwiązanie musi oferować deduplikację danych po stronie serwera Veritas NetBackup | TAK | |  |
| **Amazon S3**  **Scality S3**  **IBM Cloud Object Storage**  **Alibaba Cloud OSS**  **Claudian S3** | | | | |
|  | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie pamięci masowej oferowanej z użyciem interfejsu obiektowego S3 | TAK | |  |
|  | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK | |  |
|  | Rozwiązanie musi umożliwiać przenoszenie starszych kopii zapasowych  z Amazon S3 do Amazon Glacier w celu redukcji kosztów przechowywania danych | TAK | |  |
|  | Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie | TAK | |  |
|  | Rozwiązanie musi umożliwiać wsparcie dla systemów które wspierają wersjonowanie oraz takich, które nie posiadają takiej możliwości | TAK | |  |
| **Microsoft Azure Blob** | | | | |
|  | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w chmurze pamięci masowej Microsoft Azure Blob | TAK | |  |
|  | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK | |  |
|  | Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie | TAK | |  |
| **Google Cloud Storage** | | | | |
|  | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w chmurze pamięci masowej Google Cloud Storage | TAK | |  |
|  | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK | |  |
|  | Rozwiązanie musi oferować szyfrowanie danych kluczem generowanym przez rozwiązanie | TAK | |  |
| **OpenStack Swift** | | | | |
|  | Rozwiązanie musi umożliwiać składowanie kopii zapasowej w systemie pamięci masowej oferowanej z użyciem interfejsu obiektowego Swift  w wersji 3 | TAK | |  |
|  | Rozwiązanie musi umożliwiać retencję składowania kopii zapasowych (liczba wersji, liczba dni – osobno dla pełnych i przyrostowych kopii) | TAK | |  |
|  | Rozwiązanie musi oferować kompresję danych przed składowaniem  ich w Swift | TAK | |  |
| **Biblioteki Taśmowe** | | | | |
|  | Obsługa bibliotek taśmowych fc/sas , mozliwość ustawienia retencji , oraz zapisu jednoprzebiegowego – kopia wykonywana raz zapisywana najpierw na dysk I potem na taśmę (disk 2 disk 2 tape) | TAK | |  |
| **3. INTERFEJS ADMINISTRACYJNY I API** | | | | |
| **Ogólne** | | | | |
|  | Rozwiązanie musi oferować możliwość dostęp administracyjny za pośrednictwem interfejsu web’owego (przeglądarka internetowa), tekstowego (CLI) oraz API | TAK | |  |
|  | Interfejsy powinny umożliwiać administratorom logowanie z użyciem poświadczeń Active Directory lub LDAP | TAK | |  |
|  | System powinien umożliwiać nadawanie uprawnień i dostępów administratorom do na podstawie definiowalnych ról (ang. RBAC) na poziomie globalnym systemu (sekcji interfejsu użytkownika) oraz do poszczególnych instancji środowisk wirtualnych, aplikacji i instancji pamięci masowych (wolumenów lub systemów plików) | TAK | |  |
| **Interfejs webowy** | | | | |
|  | Interfejs musi umożliwiać wyświetlenie podstawowych statystyk, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona | TAK | |  |
|  | Interfejs musi umożliwiać wyświetlenie statystyk prędkości wykonywania kopii (ilość danych w jednostce czasu) i czasu trwania, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona z podziałem na fazy wykonywania zadań kopii zapasowych (eksport danych ze środowiska i zapis w miejscu składowania danych) | TAK | |  |
|  | Interfejs musi umożliwiać konfigurację cyklicznie przesyłanych raportów  ze statusem ostatnio wykonanych kopii zapasowych | TAK | |  |
|  | Interfejs musi umożliwiać konfigurację cyklicznie przesyłanych raportów  ze statusem kopii zapasowych, które nie powiodły się w ostatnim czasie –  np. w ciągu ostatnich kilkunastu minut, niedostępności komponentu wykonującego kopie zapasowe (ang. data-mover) | TAK | |  |
|  | Interfejs musi umożliwiać wyświetlenie statystyk takich jak rozmiar kopii zapasowej oraz czas potrzebny na wykonanie kopii zapasowej  lub odtworzenia w perspektywie czasu, np. w celu analizy przyrostu rozmiarów backupu lub czasu jego wykonywania | TAK | |  |
|  | Interfejs powinien umożliwiać raportowanie zajętość przestrzeni dyskowej w miejscach składowania danych z podziałem na środowiska wirtualne, polityki, maszyny wirtualne, instancje pamięci masowej | TAK | |  |
|  | Interfejs musi umożliwiać centralne zarządzanie konfiguracją komponentów realizujących proces kopii zapasowej (ang. data-mover), danych dostępowych i metod wykonywania kopii zapasowych wirtualizatorów oraz konfiguracji miejsc składowania danych | TAK | |  |
|  | Interfejs musi umożliwiać wykonanie na żądanie kopii zapasowej wskazanego środowiska, aplikacji lub instancji pamięci masowej (systemu plików lub wolumenu) | TAK | |  |
|  | Interfejs musi umożliwiać wykonanie odtworzenia kopii zapasowej wskazanego środowiska lub instancji pamięci masowej (systemu plików lub wolumenu) | TAK | |  |
|  | Interfejs musi umożliwiać wykonanie operacji montowania kopii zapasowej w celu dostępu do pojedynczych plików (jeśli wspierane dla danego wirtualizatora) – odtworzenie plików lub folderów musi również odbywać się za pośrednictwem interfejsu web’owego | TAK | |  |
|  | Interfejs musi umożliwiać konfigurację cyklicznego wykonywania kopii zapasowej wskazanych środowisk wirtualnych, aplikacji, instancji pamięci masowej (systemu plików lub wolumenu), migawek środowisk wirtualnych oraz okresowego przywracania wskazanych maszyn wirtualnych | TAK | |  |
|  | Harmonogramy cyklicznego wykonywania kopii zapasowych, migawek i przywracania środowisk wirtualnych powinny umożliwiać wskazywanie: godziny rozpoczęcia, dni tygodnia oraz ich kolejne wystąpienie w miesiącu (np. drugi wtorek miesiąca), miesiące | TAK | |  |
|  | Harmonogramy cyklicznego wykonywania kopii zapasowych, migawek i przywracania środowisk wirtualnych powinny umożliwiać interwałowe wykonywania zadania - wskazywanie: godziny rozpoczęcia, i godziny zakończenia i odstępu | TAK | |  |
|  | Interfejs musi umożliwiać monitorowanie na żywo postępu i ewentualne anulowanie zadań wykonywanych przez rozwiązanie | TAK | |  |
|  | Interfejs musi umożliwiać szybkie wyszukiwanie elementów konfiguracji, środowisk wirtualnych, aplikacji i instancji pamięci masowej (systemu plików lub wolumenu) | TAK | |  |
|  | Interfejs musi udostępniać kreatora konfiguracji podstawowych elementów rozwiązania takich jak dodanie środowiska wirtualnego, rozwiązań pamięci masowych, polityk i harmonogramów | TAK | |  |
|  | Interfejs powinien umożliwiać wykonanie testu połączenia ze środowiskiem zabezpieczanym oraz miejsca składowania kopii zapasowych | TAK | |  |
| **Interfejs tekstowy** | | | | |
|  | Interfejs musi umożliwiać wyświetlenie podstawowych statystyk, czy dane środowisko wirtualne lub aplikacja jest zabezpieczona | TAK | |  |
|  | Interfejs musi umożliwiać wykonanie na żądanie kopii zapasowej wskazanego środowiska, aplikacji, lub instancji pamięci masowej (systemu plików lub wolumenu) | TAK | |  |
|  | Interfejs musi umożliwiać wykonanie na odtworzenia kopii zapasowej wskazanego środowiska lub instancji pamięci masowej (systemu plików lub wolumenu) | TAK | |  |
|  | Interfejs musi umożliwiać wykonanie operacji montowania kopii zapasowej w celu dostępu do pojedynczych plików (jeśli wspierane dla danego wirtualizatora) – odtworzenie plików lub folderów musi wówczas odbywać się bezpośrednio ze wskazanej ścieżki na systemie rozwiązania | TAK | |  |
|  | Interfejs musi umożliwiać konfigurację cyklicznego wykonywania kopii zapasowej wskazanych środowisk wirtualnych lub aplikacji, migawek środowisk wirtualnych oraz okresowego przywracania wskazanych maszyn wirtualnych | TAK | |  |
|  | Interfejs musi umożliwiać monitorowanie postępu i ewentualne anulowanie zadań wykonywanych przez rozwiązanie | TAK | |  |
|  | Interfejs tekstowy musi być umożliwiać wykonywanie poleceń w trybie  nie-interakcyjnym (z poziomu skryptu) | TAK | |  |
| **Interfejs programistyczny (API)** | | | | |
|  | Rozwiązanie musi umożliwiać pełną konfigurację, wykonywanie wszystkich operacji oraz odczyt wszystkich dostępnych statystyk z poziomu API | TAK | |  |
|  | Rozwiązanie musi udostępniać wszystkie API z użyciem technologii REST  i JSON | TAK | |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **6. Zapora sieciowa UTM** | | | |
| **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 |
| **Wymagania Ogólne** | | | |
| 1. | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe  i bezpieczeństwa niezależnie od dostawcy łącza. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System musi wspierać IPv4 oraz IPv6 w zakresie:  • Firewall.  • Ochrony w warstwie aplikacji.  • Protokołów routingu dynamicznego. Redundancja, monitoring i wykrywanie awarii  1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.  2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.  3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  4. Monitoring stanu realizowanych połączeń VPN.  5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP.  Powinna istnieć możliwość tworzenia interfejsów redundantnych.  6. Dostarczone urządzenia musza pracować w klastrze active-active | TAK |  |
| **Interfejsy, Dysk, Zasilanie** | | | |
| 2. | 1. System realizujący funkcję Firewall musi dysponować minimum:   • 10 portami GigabitEthernet RJ-45  • 2 gniazdami SFP 1 Gbps.  2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.  4. System musi być wyposażony w zasilanie AC | TAK |  |
| **Parametry wydajnościowe** | | | |
| 3. | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.  2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.  3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.6 Gbps.  4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.  5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.  6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.  7. Wydajność systemu w zakresie inspekcji komunik. szyfrowanej SSL dla ruchu http – min. 700 Mbps. | TAK |  |
| **Funkcje Systemu Bezpieczeństwa** | | | |
| 4. | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:  1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.  2. Kontrola Aplikacji.  3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.  4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.  5. Ochrona przed atakami - Intrusion Prevention System.  6. Kontrola stron WWW.  7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.  8. Zarządzanie pasmem (QoS, Traffic shaping).  9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).  10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.  11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.  12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system Polityki,  **Firewall**  13. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  14. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  • Translację jeden do jeden oraz jeden do wielu.  • Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.  17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.  • Amazon Web Services (AWS).  • Microsoft Azure  • Google Cloud Platform (GCP).  • OpenStack.  • VMware NSX. | TAK |  |
| **Połączenia VPN** | | | |
| 5. | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  • Wsparcie dla IKE v1 oraz v2.  • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).  • Obsługa protokołu Diffie-Hellman grup 19 i 20.  • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.  • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.  • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.  • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.  • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.  • Mechanizm „Split tunneling” dla połączeń Client-to-Site.  2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.  • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.  • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. | TAK |  |
| **Routing i obsługa łączy WAN** | | | |
|  | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:  • Routingu statycznego.  • Policy Based Routingu.  • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. | TAK |  |
| **Funkcje SD-WAN** | | | |
|  | 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. | TAK |  |
| **Zarządzanie pasmem** | | | |
|  | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.  3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. | TAK |  |
| **Ochrona przed malware** | | | |
|  | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.  3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.  5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.  6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. | TAK |  |
| **Ochrona przed atakami** | | | |
|  | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.  3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.  5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów  7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. Kontrola aplikacji | TAK |  |
| **URL, Cookies** | | | |
|  | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. | TAK |  |
| **Kontrola WWW** | | | |
|  | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.  3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.  4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.  6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.  7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. | TAK |  |
| **Uwierzytelnianie użytkowników w ramach sesji** | | | |
|  | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.  • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.  •Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.  3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.  4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | TAK |  |
| **Zarządzanie** | | | |
|  | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.  2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.  3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.  4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.  5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. | TAK |  |
| **Logowanie** | | | |
|  | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.  2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.  3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.  4. Musi istnieć możliwość logowania do serwera SYSLOG. | TAK |  |
| **Certyfikaty** | | | |
|  | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:  • ICSA lub EAL4 dla funkcji Firewall. | TAK |  |
| **Serwisy i licencje** | | | |
|  | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 36 miesięcy.  b) Gwarancja oraz wsparcie  Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. | TAK |  |

**Wymagania w zakresie instalacji i konfiguracji serwera, biblioteki i systemu backupowego**

1. Montaż serwerów w posiadanej szafie rack 42U w pomieszczeniu udostępnionym przez Zamawiającego.
2. Podłączenie serwera i biblioteki do listw zasilających PDU.
3. Aktualizacja oprogramowania układowego wszystkich komponentów.
4. Podłączenie do sieci LAN ( rekonfiguracja przełączników )
5. Konfiguracja RAID serwera.
6. Instalacja i konfiguracja systemu operacyjnego.
7. Konfiguracja systemu zdalnego zarządzania.
8. Instalacja , uruchomienie i konfiguracja systemu backupowego.
9. Opracowanie polityki backupu .
10. Wymagane jest wykonanie testowego backupu oraz odtworzenia z weryfikacją prawidłowości działania systemów odtworzonych .
11. Wykonawca po zainstalowaniu i skonfigurowaniu sprzętu i oprogramowania będzie miał obowiązek przeprowadzenia instruktażu dla administratorów Zamawiającego w zakresie konfiguracji i zarządzania dostarczonego sprzętu oraz oprogramowania.