Zał. nr 8 do SWZ

Opis Przedmiotu Zamówienia do postępowania pn. „Podniesienie poziomu cyberbezpieczeństwa w Powiecie Kętrzyńskim”

Rozdział I: Założenia początkowe oraz wymagania ogólne

1. Wprowadzenie

1.1. Przedmiot zamówienia jest realizowany w ramach grantu pn. „Cyberbezpieczny Samorząd” współfinansowanego ze środków Unii Europejskiej: Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

1.2. Realizacja grantu ma na celu zwiększenie bezpieczeństwa informacji poprzez wzmacnianie odporności jednostek samorządu terytorialnego (JST) oraz ich zdolności do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego, wykrywania ich i reagowania na nie. Program jest odpowiedzią na wzrastającą liczbę ataków na podmioty administracji publicznej w Starostwie Powiatowym w Kętrzynie.

2. Ogólny opis przedmiotu zamówienia

2.1. Przedmiot zamówienia obejmuje systemy cyberbezpieczeństwa w zakresie:

Pozycja	OPIS
1	Dostawa, wdrożenie systemu do ochrony brzegu sieci klasy UTM, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu UTM.
2	Dostawa, wdrożenie nowego klastra HCI wraz z systemem tworzenia kopii zapasowych, migracja wszystkich systemów z minimum 10 maszyn wirtualnych Zamawiającego na nowe systemy operacyjne, przeniesienie bazy danych z SQL 2012 na nowy serwer bazodanowy oraz uruchomienie wszystkich maszyn wirtualnych na nowym klastrze HCI.
3	Dostawa, wdrożenie sieciowego serwera plikowego typu NAS na potrzeby tworzenia kopii zapasowych systemów z klastra HCI.
4	Przełączniki sieciowe do utworzenia sieci HCI oraz przełączniki sieciowe do utworzenia nowego rdzenia sieci LAN.
5	Dostawa, wdrożenie systemu SIEM (Security Information and Event Management) z usługą zewnętrznego SOC - Centrum Operacji Bezpieczeństwa (Security Operations Center), systemu monitoringu środowiska.
6	Szkolenia z zakresu Cyberbezpieczeństwa dla informatyków (administratorów – 2 osoby).
7	Szkolenia z zakresu Cyberbezpieczeństwa dla grup użytkowników (pracowników starostwa – 60 osób).

2.2. Przedmiot zamówienia musi być dostarczony, wdrożony i zainstalowany w całości w siedzibie Zamawiającego we wskazanym miejscu.

2.3. Wszystkie dostarczane Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem przedmiotu zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach) oraz Komponenty (rozumiane jako integralna część dostawy i wdrożenia przedmiotu zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.

2.4. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca musi przeprowadzić zgodnie z postanowieniami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.

2.5. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami OPZ oraz Wzoru Umowy.

2.6. Ilekroć w niniejszym OPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia, o których mowa w art. 101 ust. 1-3 ustawy PZP należy je rozumieć jako przykładowe. Zamawiający zgodnie z art. 101 ust. 4 ustawy PZP dopuszcza rozwiązanie równoważne opisywanym w treści OPZ. Jeżeli zapisy zawarte w OPZ wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający, zgodnie z art. 101 ust. 4 ustawy PZP dopuszcza składanie ofert na rozwiązania równoważne. Wszelkie „produkty" pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania stawiane przez Zamawiającego, stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dotyczący minimalnych wymagań parametrów jakościowych Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów /produktów/ ma wyłącznie charakter przykładowy. Zamawiający, przy opisie przedmiotu zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech.

3. Termin realizacji Przedmiotu Zamówienia

Zamawiający wymaga wykonania przedmiotu zamówienia w terminie 3 miesięcy od daty zawarcia umowy.

3.1. Organizacja wdrożenia

3.1.1. Założenia podstawowe:

3.1.2. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który musi być uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio utrzymywany w toku realizacji Przedmiotu Zamówienia. Wykonawca musi przedstawić Harmonogram wdrożenia w terminie 14 dni od daty podpisania umowy.

3.1.3. Wykonawca w Harmonogramie wdrożenia musi w szczególności uwzględnić podział na zadania takie jak: projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.

3.1.4. Wykonawca umożliwi Zamawiającemu udział we wszystkich realizowanych przez niego pracach w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostawach, instalacji/budowie, konfiguracji, wdrożeniu i testowaniu).

3.1.5. Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac w siedzibie Zamawiającego. Dopuszcza się narady prowadzone w trybie zdalnym z wykorzystaniem narzędzi komunikacji elektronicznej, które zapewni Wykonawca. Zamawiający przewiduje częstotliwość narad maksymalnie 1 raz w miesiącu, narad zdalnych maksymalnie 3 razy w miesiącu, chyba że nadzwyczajna sytuacja w realizacji przedmiotu umowy wymagała będzie częstszych spotkań w siedzibie lub odbywanych zdalnie.

3.1.6. Wykonawca zobowiązany jest przeprowadzić prace wdrożeniowe przedmiotu zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.

3.1.7. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie przedmiotu zamówienia.

3.1.8. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.

3.1.9. W ramach wdrożenia Wykonawca musi przygotować informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją przedmiotu zamówienia, w ramach której muszą zostać powołane minimum następujące role:

a) Kierownik Projektu ze strony Wykonawcy,
b) Zespół Wdrożeniowy ze strony Wykonawcy.

3.1.10 Wdrożenie, z zastrzeżeniami wskazanymi poniżej muszą realizować osoby wymienione w ofercie Wykonawcy, przy czym:

a) Osoby Zespołu Wykonawcy muszą być dyspozycyjne w trakcie wykonywania prac,
b) Wykonawca musi przekazać Zamawiającemu wykaz numerów telefonów kontaktowych do kluczowych osób biorących udział w realizacji Przedmiotu Zamówienia po stronie Wykonawcy.

3.2 Przygotowanie Dokumentacji

1. W ramach realizowanych prac Wykonawca musi opracować dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:
2. Dokumentacja powyższa musi zawierać bazowe zapisy opisujące budowane rozwiązania oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach przedmiotu zamówienia. Dokumenty te wraz ze SWZ z załącznikami będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
4. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem wdrożenia muszą być opracowane w oparciu o wymagania określone w niniejszym OPZ.

3.3 Analiza Przedwdrożeniowa

Analiza Przedwdrożeniowa obejmuje wszystkie czynności do wykonania przez Wykonawcę mające na celu analizę oraz wdrożenie środowiska informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy Przedwdrożeniowej Wykonawca przedstawi Zamawiającemu Dokumentację Analizy Przedwdrożeniowej (zwana dalej DAP) oraz harmonogram wdrożenia, na podstawie którego organizacyjnie i technicznie będzie realizowany przedmiot zamówienia. DAP będzie podlegał uzgodnieniu i akceptacji Zamawiającego. Termin wykonania analizy został określony w umowie. DAP musi zawierać w szczególności:

ZAWARTOŚĆ DOKUMENTACJI ANALIZY PRZEDWDROŻENIOWEJ (DAP)
1. **Wymagane dane ZARZĄDCZE:**
a) plan i sposób komunikacji Stron.
b) harmonogram wdrożenia
2. **Wymagane dane dotyczące systemów cyberbezpieczeństwa:**
a) podział przedmiotu zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty,
b) analiza wymagań przedmiotu zamówienia zawierająca opis sposobu realizacji wymagań, sposób testowania i odbioru,
c) Wykonawca określi w Analizie przedwdrożeniowej zalecaną specyfikację i optymalną konfigurację środowiska dla Systemu SIEM, SEOD EZD Proton m.in. pamięć, liczbę procesorów, wymagana powierzchnia dyskowa.
d) Dla każdego system cyberbezpieczeństwa Wykonawca opracuje: – Architekturę rozwiązania – Wersję oprogramowania wchodzące w skład Systemu – Konfigurację Systemu – Zastosowane licencje/subskrypcje.
3. Procedura testowania – scenariusze testowe dla wdrażanych systemów
4. Harmonogram wdrożenia
5. Opis instalacji i wdrożenia oprogramowania
6. Szczegółowy zakres i zawartość pozostałej Dokumentacji.

3.4 Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową i techniczną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej oraz w wersji elektronicznej w formacie edytowalnym.

2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.

3. W szczególności dokumentacja ta musi zawierać:
   a. Schemat infrastruktury i architekturę rozwiązania wraz z opisem.

b. Zasady licencjonowania dostarczonych elementów.
c. Konfigurację sprzętową i logiczną elementów infrastruktury dla wdrożonych systemów.
d. Procedury uruchamiania, zatrzymywania wdrożonych systemów oraz elementów infrastruktury.
e. Procedury konfiguracji kont w dostarczonych systemach.
f. Procedury awaryjne umożliwiające dostęp do infrastruktury w przypadku awarii.
g. Procedury wykonywania odtworzenia wdrożonych systemów z kopii zapasowej.
h. Procedury opisujące standardowe działania administracyjne.
i. Procedury odzyskania wdrożonych systemów po awarii.
j. Wytyczne (dobre praktyki) dla administratorów.
k. Spis dokumentacji zewnętrznej do której odwołuje się Dokumentacja Powykonawcza.

3.5 Odbiór Etapu/Dokumentacji/Końcowy

1. Odbiory Etapów/Dokumentacji będą się odbywać po zakończeniu określonych prac danego Etapu/Dokumentacji.
2. Odbiór końcowy przedmiotu zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym odebrania wszystkich Komponentów i Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji.
3. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej załącznik do SWZ.

3.6 Testy

1. W ramach odbioru przedmiotu zamówienia muszą zostać przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji przedmiotu zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale.
2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego przedmiotu zamówienia dokonać odbiorów w ramach poszczególnych Etapów i Odbioru Końcowego.
3. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
4. W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed Odbiorem Końcowym przedmiotu zamówienia.
5. Zamawiający wymaga, aby Wykonawca przeprowadził testy odbiorcze z zakresu:
   a) Uruchamianie i zatrzymywanie wdrożonych systemów
   b) Weryfikacja wdrożonych systemów zgodnie ze scenariuszami opisanymi w dokumentacji.
   c) Weryfikacja poprawności działania procedur.
   d) Symulację awarii wdrożonych systemów.

3.7 Dodatkowe zobowiązania Wykonawcy

1. Wykonanie przedmiotu zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi na każdym etapie realizacji.
3. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
4. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
5. Współdziałanie z osobami wskazanymi przez Zamawiającego.

Rozdział II. Szczegółowy opis przedmiotu zamówienia

1. Dostawa, wdrożenie systemu do ochrony brzegu sieci klasy UTM, instruktaż z zakresu administracji i bieżącej obsługi dostarczonego systemu UTM.

System UTM musi być dostarczony z gwarancją i wsparciem technicznym na okres min. 24 miesiące. System musi oferować poniższe funkcjonalności minimalne:

- Firewall
- IPS/IDS (Intrusion Detection and Prevention Firewal)
- Ochrona antywirusowa (Antywirus)
- Ochrona przed spamem (Antyspam)
- Zarządzanie ruchem (Traffic Control)
- Filtrowanie treści (Content Filtering)

1.1 Zaoferowany system musi posiadać następujące funkcjonalności w poniższych kategoriach:

A. Firewall

1. Filtrowanie ruchu na podstawie adresów IP źródłowych i docelowych, typu protokołu, portu źródłowego i docelowego TCP i UDP
2. Ustalenia limitów jednoczesnych połączeń z danego hosta źródłowego
3. Możliwość logowania ruchu sieciowego dla wybranych reguł firewall'a
4. Tworzenie aliasów do grupowania i nazywania adresów IP, sieci i portów
5. Normalizacja pakietów sieciowych
6. Tworzenie mostów sieciowych warstwy drugiej
7. Tworzenie kolejek sieciowych z podziałem pasma sieciowego

B. Translacja adresów

1. Przekazywanie pakietów z możliwością stosowania zakresów
2. Translacja NAT typu 1:1
3. Translacja wyjściowa adresów IP na adresy publiczne z możliwością ograniczania portów i protokołów ruchu wychodzącego

C. IDS/IPS

1. Rozpoznawanie wzorców w ruchu sieciowym na poziomie pakietu lub strumienia
2. Wykorzystywanie reguł dynamicznych do wykrywania tych nieprawidłowości, takich jak luki w protokołach, skanowanie portów, ataki typu „odmowa usługi”
3. Nasłuchiwanie komunikacji, rejestrator pakietów
4. Min. dwa zestawy gotowych reguł zabezpieczających

D. Antywirus

1. Przezroczysty serwer proxy skanujący cały ruch HTTP w poszukiwaniu sygnatur złośliwego oprogramowania
2. Sprawdzanie min. sygnatur wirusów, meta wzorców wirusów

E. Antyspam

1. Gotowe zestawy reguł blokowania, min. kraj pochodzenia, lista niebezpiecznych adresów IP, czarna lista DNS
2. Współpraca z modułem antywirusowym
3. Współpraca z modułem filtrowania zawartości
4. Wbudowany mechanizm dla ruchu SMTP w oparciu o szare listy

F. Zarzadzanie ruchem

1. Możliwość przydzielenia określonych poziomów przepustowości określonym aplikacjom/hostom lub protokołom
2. Możliwość ustalania priorytetów, ograniczania różnych typów ruchu lub miejsc docelowych ruchu
3. Możliwość ograniczenia przepustowości pojedynczego adresu IP lub pojedynczego zestawu adresów IP
4. Blokowanie dowolnych protokołów komunikacji
5. Blokowanie dowolnych aplikacji np. P2P, komunikatorów internetowych, gier lub ruchu TOR

G. Filtrowanie zawartości

1. Blokowanie domen według kategorii
2. Blokowanie domen z wybranego kraju
3. Blokowanie adresów IP w oparciu o dowolną listę
4. Filtr URL

H. Tablica stanów

Oferowane oprogramowanie musi działać w oparciu o filtrowanie z uwzględnieniem tablic stanów z następującymi właściwościami:

1. Ograniczenia w oparciu o ilość jednoczesnych połączeń od klienta
2. Ograniczenia ilości stanów połączeń z uwzględnieniem danego hosta
3. Ograniczenia ilości nowych połączeń z uwzględnieniem czasu (per second)
4. Zarządzanie stanami połączeń: utrzymywania stanu połączeń, brak śledzenia stanu połączeń itp.

I. Dodatkowe wbudowane funkcjonalności

Oferowane oprogramowanie musi oferować następujące dodatkowe funkcjonalności:

1. Wbudowany serwer usługi DNS
2. Wbudowany serwer usługi DHCP
3. Wbudowany serwer usługi NTP
4. Mechanizm wykrywania ataków sieciowych na wskazanych interfejsach sieciowych
5. Mechanizm monitorowania ruchu sieciowego i zbierania statystyk z uwzględnieniem typu ruchu, adresów źródłowych i docelowych i graficznej reprezentacji wyników
6. Wbudowanych mechanizm proxy z filtracją ruchu http

J. Wysoka dostępność

Zaoferowane oprogramowanie musi posiadać możliwość tworzenia rozwiązań wysokiej dostępności zawierającej minimum dwa węzły. Funkcjonalność wysokiej dostępności musi być dostarczona ze wszystkimi opcjami bez konieczności dokupowania dodatkowych licencji. Jeśli część funkcjonalności wymaga dodatkowych opcji licencyjnych muszą one być dostarczone w momencie oferowania produktu.

K. Koncentrator VPN

Koncentrator VPN musi umożliwiać tworzenie wirtualnych sieci w oparciu o następujące rodzaje VPN: IPsec, OpenVPN i PPTP.

Dostęp do koncentratora VPN musi być realizowany dla różnych urządzeń dostępowych, w tym dla OpenVPN z następujących urządzeń: komputerów z systemami Microsoft Windows 7 i 8, OpenSUSE i Ubuntu oraz Mac OS X, urządzeń mobilnych z systemami iOS oraz Android.

Koncentrator VPN musi umożliwiać swobodny wybór adresacji sieci IP używanych w tunelach VPN.

Zaoferowany system musi posiadać następujące funkcjonalności w poniższych kategoriach:

1.2 Zaoferowany system musi spełniać poniższe minimalne wymagania techniczne:

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do mocowania kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). Serwer wyposażony w zdejmowany panel przedni z zamkiem chroniącym przed nieuprawionym dostępem do dysków oraz możliwością dołożenia czujnika otwarcia obudowy współpracującego z BIOS/UEFI.
Procesor	Minimum jeden procesor max. dwunastordzeniowy, x86 - 64 bity, lub równoważny procesor dwunastordzeniowy pracujący z częstotliwością bazową min. 2.0GHz i osiągający w testach SPECrate2017_int_base wynik nie gorszy niż 215 punktów, dla testu oferowanego modelu serwera w konfiguracji z 2 procesorami. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org Płyta główna wspierająca zastosowanie procesorów od 8 do 60 rdzeni, mocy do min. 350W i taktowaniu CPU do min. 3.7GHz.

Liczba procesorów	Min. 1 procesor
Pamięć operacyjna	Min. 64GB RDIMM DDR5 4800 MT/s w modułach pamięci o pojemności min. 32 GB każdy. Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB.
Sloty rozszerzeń	Min. 3 aktywnych gniazd PCI-Express generacji 5, x16 (szybkość slotu – bus width). 1x gniazda pełnej wysokości (full height) 2x gniazda połówkowej wysokości gotowe do obsadzenia kartami z portami zewnętrznymi. Dwa sloty OCP możliwe do obsadzenia poprzez kontrolery sprzętowe dla dysków lub karty sieciowe w dowolnej konfiguracji.
Dysk twardy	Serwer bez klatkowy z możliwością rozbudowy/rekonfiguracji w przyszłości serwera do 10 dysków typu Hot Swap, SAS/SATA/SSD/NVMe, 2,5” montowane z przodu obudowy. W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 10 zatoki dyskowe SFF gotowe do instalacji dysków SAS/SATA/SSD/NVMe 2,5”typu Hot Swap. Zainstalowane min. 2szt. dysków SSD SATA 6Gb/s 240GB pracujące w konfiguracji ze sprzętowym RAID 1.
Kontroler	Serwer wyposażony w kontroler software dla dysków SATA, obsługujący poziomy: RAID 0, 1, 10. Możliwość zastosowania/wymiany kontrolera na kontroler sprzętowy wyposażony w min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę napędów dyskowych SSD/SATA/SAS/NVMe. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.
Interfejsy sieciowe	Jedna 4-portowa karta 1Gb Base-T oparta o chipset BCM5719 oraz jedna dwuportowa karta 10/25Gb SFP28 oparta o chipset BCM57412, z czego jedna karta nie powinna zajmować slotów PCI-e i być zainstalowana w dedykowanym złączu dla karty sieciowej. Należy dostarczyć niezbędne moduły oraz przewody.
Karta graficzna	Zintegrowana karta graficzna
Porty	5 x USB, z czego min. 4szt w wersji USB 3.2 oraz jeden port USB 2.0 1x VGA Możliwość rozbudowy/rekonfiguracji o:

	- port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express - cyfrowy port video (Display Port lub HDMI), bez użycia przejściówek z portu VGA lub USB 8
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy max. 1000W
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Diagnostyka	Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze.
Bezpieczeństwo	Serwer wyposażony w moduł TPM 2.0.
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników

	• przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)
	• uwierzytelnianie oprogramowania sprzętowego PCIe z protokołem bezpieczeństwa i modelem danych (SPDM) zapewnia integralność komponentu
	• obsługa zdalnego serwera logowania (remote syslog)
	• wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów
	• mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii oraz ostatniego startu serwera a także nagrywanie na żądanie
	• funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności
	• monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
	• konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
	• zdalna aktualizacja oprogramowania (firmware)
	• zarządzanie grupami serwerów, w tym:
	  - tworzenie i konfiguracja grup serwerów
	  - sterowanie zasilaniem (wł/wył)
	  - ograniczenie poboru mocy dla grupy (power capping)
	  - aktualizacja oprogramowania (firmware)
	  - wspólne wirtualne media dla grupy
	• możliwość równoczesnej obsługi przez 6 administratorów
	• autentykacja dwuskładnikowa (Kerberos)
	• wsparcie dla Microsoft Active Directory
	• obsługa SSL i SSH
	• enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli
	• wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API
	• wsparcie dla Integrated Remote Console for Windows clients
	• możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)

Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Zapewnia wsparcie dla systemów operacyjnych: Microsoft Windows Server 2019, 2022 Ubuntu 22.04 LTS Red Hat Enterprise Linux (RHEL) 8.6 oraz 9.0 SUSE Linux Enterprise Server (SLES) 15 SP4 VMware ESXi 7.0 U3, 8.0
Wsparcie techniczne	24 miesięczna gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2-godzinnym czasem reakcji. Przybycie na

	miejsce w następnym dniu roboczym. Czas reakcji na zdarzenia krytyczne do 2 godzin. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.
Inne	Urządzenie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

1.3 Zakres wdrożenia.

Wykonawca dostarczy system UTM, zainstaluje, skonfiguruje oraz dokona przeniesienia całej obecnej konfiguracji z obecnie używanego systemu firewall. Wdrożenie obejmuje co najmniej:

a) konfiguracja ogólna systemu - adresy IP, DNS, DHCP, routing, NTP,
b) konfiguracja interfejsów sieciowych - WAN, LAN, DMZ. Konfiguracja dodatkowego łącza zapasowego, łącznie z ustawieniem routingu oraz przygotowanie odpowiednich polityk
c) integracja nowego systemu UTM z Active Directory,
d) przeniesienie całej konfiguracji z istniejącego urządzenia Firewall na nowy system UTM z najnowszą stabilną wersją oprogramowania
e) audyt reguł i ustawień, weryfikacja i poprawienie reguł oraz ustawień, optymalizacja używanych dotychczas reguł, zgodnie z dobrymi praktykami,
f) konfiguracja loadbalancingu dla min. dwóch łączy WAN,
g) konfiguracja QoS oraz kształtowania pasma dla co najmniej 5 profili,
h) przeniesienie istniejących obiektów sieciowych – około 200 obiektów,
i) przeniesienie istniejących reguł firewall oraz NAT – około 100 reguł,
j) przeniesienie konfiguracji openVPN,
k) przeniesienie filtrów URL oraz SSL, konfiguracja inspekcji SSL – około 80 obiektów URL oraz około 30 obiektów SSL,
l) opracowanie polityki deszyfracji danych szyfrowanych SSL (Secure Sockets Layer), opracowanie reguł działania w zależności od rodzaju ruchu, opracowanie polityki ponownego szyfrowania danych, konfiguracja systemu UTM
m) konfiguracja przesyłania logów do posiadanych przez Zamawiającego instancji zbierających i przechowujących logi,

Zamawiający może wymagać skonfigurowania dodatkowych parametrów systemu UTM, jeśli podczas wdrożenia zajdzie taka potrzeba.

Zamawiający wymaga, aby wdrożenie przeprowadził inżynier posiadający ważny certyfikat techniczny potwierdzający kompetencje z zakresu wdrażania systemów UTM. Wykonawca przed przystąpieniem do wdrożenia przygotuje harmonogram wdrożenia.

1.4 Instruktaże

Zamawiający wymaga przeprowadzenia instruktaży dla swoich administratorów zgodnie z poniższym opisem:

a) Instruktaż podstawowy (wdrożeniowy) – odbędzie się przy okazji wdrożenia i konfiguracji systemu UTM w siedzibie Zamawiającego, jego przedstawiciele będą uczestniczyć w wykonywanych pracach.

b) Instruktaż z zakresu wdrożonego systemu UTM (powdrożeniowy), dla grupy od 2 do 5 osób, średniozaawansowanych (wcześniej pracujących na systemach UTM), minimum 3 maksimum 5 dniowy, obejmujący cały niżej wymieniony zakres materiału szkoleniowego:
   - rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego; ustawienia systemowe i uprawnienia administratorów;
   - instalacja licencji i aktualizacja systemu; tworzenie kopii zapasowej i przywracanie konfiguracji;
   - zbieranie logów i monitorowanie; przedstawienie kategorii zbieranych logów;
   - wykresy historyczne i monitorowanie; obiekty: typy obiektów oraz ich wykorzystanie;
   - obiekty sieciowe i obiekt typu „router”;
   - konfiguracja sieci: tryby pracy urządzenia; typy interfejsów (ethernet, modem, bridge, vlan, gretap)
   - typy routingu oraz ich priorytety; translacja adresów sieciowych (nat); translacja połączeń wychodzących (maskarada); translacja połączeń przychodzących (przekierowanie); translacja dwukierunkowa (jeden do jeden);
   - filtrowanie ruchu sieciowego (firewall); ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (stateful inspection); szczegółowy opis parametrów reguły firewall; kolejność przetwarzania reguł firewall i nat;
   - ochrona aplikacji: implementacja filtrowania url dla ruchu http i https; konfigurowanie skanowania antywirusowego i modułu breach fighter;
   - moduł ips i stosowanie profili inspekcji; użytkownicy i uwierzytelnianie
   - konfiguracja usługi katalogowej: wprowadzenie do różnych metod uwierzytelniania (ldap, kerberos, radius, certyfikat ssl, spnego, sso);
   - rejestracja użytkowników; uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania; 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; ssl vpn - zasada działania, konfiguracja

c) Instruktaż powdrożeniowy musi zawierać elementy warsztatowe i opierać się na zadaniach praktycznych realizowanych w przygotowanym laboratorium (LAB) z oferowanymi systemami UTM. LAB musi być przygotowany w wersji oprogramowania zastosowanej podczas wdrożenia na systemie UTM Zamawiającego.

d) Instruktaże muszą być prowadzone przez praktyka posiadającego co najmniej 3-letnie doświadczenie w zakresie wdrażania systemów UTM oraz posiadającego ważny certyfikat inżynierski w zakresie administracji UTM.

W przypadku wykonania instruktażu powdrożeniowego w miejscu, gdzie łączny czas dojazdu transportem publicznym pracowników Zamawiającego jest dłuższy niż 1 godzina (od siedziby Zamawiającego), Wykonawca zapewni:

- zakwaterowanie w hotelu (co najmniej trzygwiazdkowym) począwszy od dnia poprzedzającego instruktaże
- pełne wyżywienia (śniadanie, obiad, kolacja). Zakwaterowanie w hotelu nie może być oddalone od miejsca szkolenia więcej niż 10 minut pieszo.

Instruktaż musi zakończyć się w ciągu maksymalnie 3 miesięcy licząc od dnia zakończenia wdrożenia. Instruktaż musi zostać zrealizowany w jednym terminie dla wszystkich osób, a termin Instruktażu Wykonawca musi ustalić z Zamawiającym.

1.5 Dokumentacja powykonawcza.

Wykonawca dostarczy co najmniej w formie elektronicznej dokumentację powykonawczą. Dokumentacja powinna zawierać wszystkie dane dostępowe do konfigurowanych urządzeń, systemów, schematy podłączenia urządzeń do sieci LAN, opis konfiguracji dostarczonego i wdrożonego systemu UTM, opis wdrożonych polityk.

1.6 Rozszerzone wsparcie serwisowe świadczone przez okres 24 miesięcy

System UTM będzie objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego partnera przez okres 24 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 27001.

System będzie objęty rozszerzonym wsparciem technicznym w zakresie:

- Wsparcie telefoniczne zespołu certyfikowanych inżynierów.
- Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu.
- Doradztwo w zakresie konfiguracji.
- Doradztwo w zakresie podnoszenia poziomu bezpieczeństwa.
- Zdalne wsparcie techniczne.
- Pomoc w zakładaniu zgłoszeń serwisowych u producenta.
- Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą).
- Przygotowanie systemu UTM do zdalnej konfiguracji.
- Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika.
- Nielimitowana rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika.
- Nielimitowana usługa zdalnego przeglądu konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich.
- Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich.

Dla zapewnienia wysokiego poziomu usług serwisowych, podmiot świadczący wsparcie musi posiadać certyfikat ISO 27001. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wymagany jest czas reakcji nie dłuższy niż 4 godziny dla połączeń telefonicznych lub nie dłuższy niż 6 godzin dla odpowiedzi w portalu serwisowym. Zamawiający wymaga, aby wsparcie serwisowe świadczył zespół certyfikowanych inżynierów w zakresie administracji systemami UTM, legitymujący się ważnymi certyfikatami.

Na żądanie Zamawiającego Wykonawca przedstawi oświadczanie o gotowości świadczenia wymaganego serwisu zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej oraz ważne certyfikaty techniczne inżynierów wystawione przez Producentów systemów UTM oraz certyfikat ISO 27001 Wykonawcy.

2. Dostawa, wdrożenie nowego klastra hiperkonwergentnego (HCI) wraz z systemem tworzenia kopii zapasowych, migracja wszystkich systemów z min. 10 maszyn wirtualnych Zamawiającego na nowe systemy operacyjne, przeniesienie bazy danych z SQL 2012 na nowy serwer bazodanowy oraz uruchomienie wszystkich maszyn wirtualnych na nowym klastrze HCI.

W celu podniesienia poziomu bezpieczeństwa systemów informatycznych Zamawiającego konieczna jest wymiana przestarzałych: serwerów, serwerowych systemów operacyjnych, serwera bazy danych. Wymagania ogólne w ramach zadania klaster HCI:

1. Dostawa trzech serwerów dla klastra HCI
2. Dostawa systemu wirtualizacji dla klastra HCI
3. Dostawa systemu backupu klastra HCI
4. Dostawa licencji systemów operacyjnych
5. Dostawa licencji serwera bazy danych
6. Wykonanie migracji wszystkich systemów Zamawiającego oraz serwera i bazy danych na nowy klaster HCI
7. Wykonanie instruktaży dla wszystkich dostarczanych systemów
8. Wykonanie dokumentacji powykonawczej

Na dostarczonych serwerach należy skonfigurować klaster hiperkonwergentny. Wszystkie obecne systemy Zamawiającego, zarówno te pracujące na serwerach fizycznych, jak i te zainstalowane na maszynach wirtualnych:

1. Serwer WWW dla Geoportalu (GEOBID, system Linux)
2. Serwer domeny Starostwa (Linux)
3. Serwer kopi zapasowej z podłączoną macierzą dyskową 50TB, harmonogramy (Linux)
4. Serwer bazy danych Firebird (GEOBID) i serwera plików (Linux)
5. Serwer proxy (linux)
6. System Response - baza danych PostgreSQL, JBOS, SMB (ZETO, Linux)
7. Serwer Microsoft SQL 2012 + System Elektronicznego Obiegu Dokumentów (SEOD) EZD Proton (Nefeni, Windows 2012)
8. Geoportal + oprogramowanie EWmapa + inne aplikacje dla geoportalu (Geobid, Windows 10)

należy przenieść na nowe systemy operacyjne, dla których będzie dostępne wsparcie techniczne, poprawki, aktualizacje przez okres 24 miesięcy. Należy wykonać migrację w/w baz danych na nowo dostarczone środowisko, w zakresie migracji wymagana jest instalacja najnowszych dostępnych wersji baz danych, zgodnie z wymaganiami producentów.

2.1 Minimalne wymagania techniczne dla każdego z 3 serwerów dedykowanych do pracy w klastrze HCI.

Element konfiguracji	**Wymagania minimalne**
Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami umożliwiającymi wysunięcie i wszystkimi elementami niezbędnymi do zamontowania serwera w szafie).

Procesor	Procesor max. 16 rdzeniowy, osiągający w teście SPECrate®2017_int_base wynik co najmniej 174 punktów. Płyta główna obsługująca procesory od 16 do 128 rdzeni, wymagających mocy 400W i obsługujących do 3TB pamięci RAM.
Zainstalowane procesorów	1
Pamięć operacyjna	Zainstalowanych min. osiem modułów 32 GB DDR5 4800MT/s. Płyta główna z minimum 12 slotami na pamięć, umożliwiająca instalację do minimum 3TB pamięci RAM, obsługująca moduły 4800 MT/s Obsługa zabezpieczeń: Advanced ECC.
Sloty rozszerzeń	Możliwość instalacji 2 karty PCI-Express generacji 5, x16(szybkość slotu – bus width), min. 1 karty pełnej wysokości (full height).
Dysk twardy	Możliwość instalacji do 10 dysków. Zainstalowane min. 2 dyski SSD SATA 240GB pracujące w konfiguracji ze sprzętowym RAID 1. Zainstalowanych min. 8 dysków SSD SATA 3.84TB z DWPD liczonym na okres 3 lat min. 1,66.
Interfejsy sieciowe	Zainstalowane dwie dwuportowe karty 10/25Gb SFP28 oparte o chipset BCM57412, nie zajmujące slotów PCI-e, zainstalowane w dedykowanym złączu dla karty sieciowej.
Karta HBA	Zainstalowana karta 1 portowa Fibre Channel min. 32 Gbit
Karta graficzna	Zintegrowana karta graficzna z pamięcią min. 16 MB, umożliwiająca wyświetlenie obrazu min. 1920 x 1200@60Hz
Porty	Min. 2x USB 3.2 (w tym min. 1 port wewnętrzny i 1 z przodu obudowy), min. 2x USB 3.1 z tyłu obudowy, min. 1 port VGA, port USB dedykowany dla modułu zarządzającego z przodu obudowy. Możliwość rozbudowy/rekonfiguracji o port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express 1x port RJ-45 dedykowany dla interfejsu zdalnego zarządzania
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy max. 1000W, efektywność zasilaczy 94%
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) z dedykowanym portem RJ45 pozwalającą na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe i nie zajmująca wymaganych slotów PCI. Jeśli jest wymagana to załączona odpowiednia licencja.
Karta/moduł zarządzający i system zarządzania	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe

	• praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii oraz ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów

	- sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power capping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2022 Red Hat Enterprise Linux (RHEL) 8.0 SUSE Linux Enterprise Server (SLES) 15 VMware ESXi 6.7 U3
Gwarancja	36 miesięczna gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2-godzinnym czasem reakcji. Przybycie na miejsce w następnym dniu roboczym. Czas reakcji na zdarzenia krytyczne do 2 godzin. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

2.2 Minimalne wymagania techniczne dla systemu Wirtualizacji HCI dla 3 serwerów.

Lp.	Wymagane minimalne parametry techniczne
1	Rozwiązanie musi zapewnić możliwość natywnej obsługi wielu instancji maszyn wirtualnych i kontenerów na każdym serwerze fizycznym.
2	Klaster fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji powinien skalować się bez nałożonych limitów licencyjnych.
3	Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej z funkcjonalnością przekazywania informacji TRIM/DISCARD do zasobów przechowywania danych oraz definiowanymi limitami prędkości odczytów i zapisów na utworzonym dysku, w wartościach MB/s oraz IOP/s wykonywanych na wybranym zasobie

4	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych na danym serwerze z możliwością sumarycznego przydzielenia puli pamięci operacyjnej RAM większej niż dostępna w działającym serwerze, nie mniej niż 192GB
5	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć skonfigurowanie od 1 do co najmniej 12 wirtualnych kart sieciowych.
6	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania przekierowania używanych portów USB do maszyn wirtualnych w trybie „hot plug", zarówno za pomocą nr portu jak i numerów identyfikacyjnych 'Producent/Urządzenie'.
7	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania przekierowania używanych fizycznych urządzeń zainstalowanych w gniazdach PCI/PCIe serwera wraz z przekierowaniem akceleratorów GPU.
8	Rozwiązanie wirtualizacyjne musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
9	Rozwiązanie wirtualizacyjne powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
10	Rozwiązanie wirtualizacyjne musi wspierać m.in. następujące systemy operacyjne: Windows XP/7/8/10/11, Windows Server 2012/2016/2019/2022, Systemy z rodziny Linux (kernel 2.4 – 6.0)
11	System wirtualizacji musi wspierać konfigurację w trybie graficznym rozwiązań zarówno dla obiektowego przechowywania danych jak i technik 'erasure coding' z użyciem osobnych urządzeń typu SSD do hybrydowych operacji z udziałem metadanych, w celu uzyskania redundancji bezpieczeństwa operacji na danych, ich przechowywania i maksymalnej wydajności.
12	Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania manualnych i zautomatyzowanych kopii pełnych oraz migawkowych (tzw. snapshot) instancji maszyn wirtualnych na potrzeby tworzenia kopii zapasowych bez przerywania pracy systemów. Wbudowana w interfejs graficzny konfiguracja zautomatyzowanych kopii maszyn wirtualnych oraz kontenerów powinna umożliwiać wyłączenie z procesu archiwizacji wybranych dysków wirtualnych w maszynach, dowolne harmonogramowanie zadań, wybór kompresji (m.in. ZSTD), poziomy ilościowe i jakościowe retencji oraz dodanie komentarzy.
13	System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji powyżej 4 000 portów.
14	Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii fizycznej karty sieciowej. Wspierane powinny być technologie redundancji i balansowania LACP (802.3ad) do warstwy 3+4 włącznie.

15	Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
16	Oprogramowanie wirtualizacyjne powinno być licencjonowane w oparciu o licencję GNU Affero GPL, v3. W innym przypadku polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego, bez względu na ilość dostępnych zasobów sprzętowych tj. ilość gniazd/rdzeni CPU, pamięci RAM, wszelkich kontrolerów i zasobów magazynów danych. Wsparcie techniczne dla błędów oprogramowania musi być świadczone bezpośrednio przez producenta oprogramowania. Sposób licencjonowania lub subskrypcji musi umożliwiać rozszerzenie wsparcia o dodatkowe usługi zdalnego łączenia się inżyniera producenta oprogramowania do zgłoszonego serwera.
17	Oprogramowanie do wirtualizacji musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora.
18	Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi, również w trybie działającej maszyny która jest klonowana.
19	Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
20	Rozwiązanie wirtualizacyjne musi posiadać wbudowany interfejs programistyczny (API) zapewniający integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
21	Rozwiązanie wirtualizacyjne musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna dostarczana jest w postaci gotowej, wstępnie skonfigurowanej. Dostęp do konsoli powinien być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5 i zabezpieczony certyfikatem SSL
22	Rozwiązanie wirtualizacyjne 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 historyczne.
23	Rozwiązanie wirtualizacyjne musi mieć zaimplementowany firewall, natywnie konfigurowalny w web GUI, z rozróżnieniem dla każdego serwera w klastrze.
24	Rozwiązanie wirtualizacyjne musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
25	Rozwiązanie wirtualizacyjne musi mieć możliwość migracji maszyn wirtualnych w czasie ich pracy oraz w trybie wyłączonym pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać konfigurację min. 8 procesów przenoszenia jednocześnie.
26	Rozwiązanie wirtualizacyjne musi zapewniać funkcjonalność z poziomu konsoli graficznej przypisywania dla konkretnej maszyny wirtualnej wybranych rdzeni konkretnego procesora lub grupy rdzeni procesorów w serwerze.

27	System zapewnia odpowiednią redundancję dla uruchomionych usług w oparciu o mechanizm wysokiej dostępności (HA), aby w przypadku awarii lub niedostępności co najmniej 2 serwerów fizycznych w klastrze, wybrane przez administratora i uruchomione w nim wirtualne maszyny oraz kontenery zostały uruchomione na innych serwerach w tym samym klastrze. Rozwiązanie musi posiadać co najmniej dwie, dedykowane, dodatkowo redundantne sieci wzajemnej komunikacji między serwerami w klastrze, niezależnie dla warstwy synchronizacji pracy (hypervisorów) klastra oraz niezależnie dla warstwy współdzielonej w klastrze przestrzeni danych, gwarantujące właściwe działanie mechanizmów wysokiej dostępności dla usług na wypadek izolacji sieciowej serwerów fizycznych, awarii samych serwerów lub poszczególnych komponentów krytycznych w nich zawartych. Wymaga się, aby minimalnym pułapem poprawnego działania infrastruktury HCI z pełnym dostępem administracyjnym do danych było 60% sprawnie działających wszystkich zasobów.
28	Dla wdrożonego rozwiązania wymagane jest 24 miesięczne wsparcie producenta oprogramowania w zakresie dostępu do poprawek i uaktualnień. Dla tego samego okresu, wsparcie serwisowe musi być świadczone przez dostawcę rozwiązania, ze zgłoszeniami w trybie dni roboczych i czasem reakcji do 1 dnia roboczego.
29	Wdrożenie wymaga przedstawienia finalnej dokumentacji opisującej infrastrukturę, jej konfigurację i wszelkie dane dostępowe na poziomie najwyższym do wszystkich elementów systemu. Wdrożenie zakończone będzie min. 32 godzinnym instruktażem stanowiskowym (4 dni robocze) dla zespołu administratorów**.**

2.3 Minimalne wymagania techniczne dla systemu backupu środowiska HCI

Lp.	Wymagane minimalne parametry techniczne
1	System wspiera kopie zapasowe maszyn wirtualnych, kontenerów i danych z fizycznych hostów
2	Rozwiązanie “chmurowe”, skonfigurowane w komunikacji z wdrożonym klastrem wirtualizacyjnym i wskazanymi przez Zamawiającego zasobami fizycznych hostów za pośrednictwem bezpiecznego, dedykowanego połączenia VPN.
3	System uruchomiony z licencją lub subskrypcją, lub w abonamencie, zapewniający dostęp w trybie ‘online’ do repozytorium o przestrzeni roboczej min. 2TB, dla archiwum skonfigurowanych kopii zapasowych, na okres minimum 12 miesięcy.
4	Możliwość przywracania pojedynczych plików lub katalogów, kopii zapasowych kontenerów i maszyn wirtualnych
5	Obsługa inkrementacyjnych kopii zapasowych
6	Obsługa deduplikacji przechowywanych kopii zapasowych, również pochodzących z różnych źródeł
7	Integracja z dostarczonym systemem wirtualizacyjnym umożliwiająca tworzenie kopii

	zapasowych bez wyłączania maszyn wirtualnych.
8	Wsparcie kompresji zstandard przed wysyłką kopii do magazynu docelowego
9	Funkcjonalność terminarza wyzwalającego w sposób automatyczny wykonywanie kopii zapasowych
10	Możliwość wywołania realizacji kopii zapasowej manualnie z poziomu klienta
11	Funkcjonalność umożliwiająca zautomatyzowane zarządzanie retencji kopii zapasowych w zakresie: zachowaj X kopii, zachowaj kopie z X godzin, zachowaj kopie z X tygodni, zachowaj kopię z X miesięcy.
12	System umożliwia szyfrowanie danych po stronie klienta w trybie AES-256 dla metody Galois/Counter Mode (GCM). Ponadto dostęp do zaszyfrowanych danych działa wyłącznie na podstawie pary kluczy RSA - system umożliwia z konsoli graficznej zapisać/drukować klucz szyfrujący.
13	System posiada wewnętrzny mechanizm autentykacji i praw dostępu dla użytkowników oraz posiada możliwość połączenia przez OpenID Connect w celu realizacji SSO
14	System posiada wbudowany mechanizm sprawdzania spójności backupów oparty między innymi na sumach kontrolnych SHA-256. Rozwiązanie umożliwia automatyzację okresowego sprawdzania spójności odczytu kopii zapasowych.
15	Rozwiązanie wspiera tryb serwisowy w którym uwidacznia aktywne operacje
16	` wraz z interfejsem do przywracania kopii, tworzenie i zarządzanie miejscami przechowywania, wgląd w statystyki wydajności i aktywne zadania, zintegrowaną dokumentację, wykonywanie aktualizacji i zarządzanie przepustowością sieci w celu uniknięcia wysycenia łącz
17	System pozwala na zautomatyzowaną, regularną synchronizację kopii zapasowych między różnymi instancjami systemu backupu w celu przechowywania kopii w kilku niezależnych lokalizacjach
18	System wspiera bezpieczeństwo logowania przy pomocy technologii “Two Factor Authentication (2FA)” przez GUI oraz “Time-based One Time Passwords (TOTP)”.
19	System umożliwia obsługę przez konsolę web archiwizacji długoterminowej LTO-5 i nowszych.
20	Dla wdrożonego rozwiązania wymagane jest 24 miesięczne wsparcie producenta oprogramowania w zakresie dostępu do poprawek i uaktualnień. Dla tego samego okresu czasu, wsparcie serwisowe musi być świadczone przez dostawcę rozwiązania, ze zgłoszeniami w trybie dni roboczych i czasem reakcji do 1 dnia roboczego.
21	Wdrożenie wymaga przedstawienia finalnej dokumentacji opisującej infrastrukturę, jej konfigurację i wszelkie dane dostępowe na poziomie najwyższym do wszystkich elementów systemu. Wdrożenie zakończone będzie min. 16-godzinnym instruktażem stanowiskowym (2 dni robocze) dla zespołu administratorów**.**

2.4 Zakres wymaganych prac wdrożeniowych.

Lp.	Nazwa	Zakres prac wdrożeniowych
1	Instalacja serwerów i systemu wirtualizacji	Należy zainstalować, uruchomić i skonfigurować dostarczone serwery w miejscach uzgodnionych z Zamawiającym. Dostarczone serwery należy podpiąć do istniejącej infrastruktury (zasilanie, sieć LAN, sieć HCI). Serwery muszą zostać skonfigurowane i podpięte zgodnie z wytycznymi Zamawiającego. W zakres czynności wchodzi między innymi: – instalacja fizyczna serwerów w szafie RACK, we wskazanej serwerowni, – instalacja i konfiguracja hiperkonwergentnego systemu klastra wirtualizacji wraz z podpięciem do zasobów dodatkowych zgodnie z wytycznymi Zamawiającego (istniejąca macierz Fibre Channel) – instalacja niezbędnych usług monitoringu infrastruktury i konfiguracja powiadomień, – konfiguracja kont użytkowników i uprawnień zgodnie z przekazaną listą od Zamawiającego, – konfiguracja reguł bezpieczeństwa dla infrastruktury,
2	Migracja systemów Zamawiającego	Należy utworzyć min. 10 maszyn wirtualnych w nowym środowisku HCI, w tym: – 2 maszyny wirtualne z zainstalowanym systemem Windows Serwer 2022, zainstalowane wszystkie dostępne poprawki, aktualizacje – Min. 8 maszyn wirtualnych z systemem Linux, dla którego będzie dostępne wsparcie techniczne, poprawki, aktualizacje przez okres min 24 miesiące. Należy zainstalować wszystkie dostępne poprawki, aktualizacje Należy skonfigurować maszyny wirtualne zgodnie z zaakceptowanym przez Zamawiającego Harmonogramem wdrożenia. Należy zainstalować Microsoft SQL Serwer 2022 Standard 0na w/w maszynie z Windows Serwer 2022. Należy przenieść systemy Zamawiającego zgodnie z zaakceptowanym przez Zamawiającego Harmonogramem wdrożenia. Należy przenieść bazy danych Zamawiającego zgodnie z zaakceptowanym przez Zamawiającego Harmonogramem wdrożenia. Należy przenieść System Elektronicznego Obiegu Dokumentów EZD Proton użytkowany przez Zamawiającego, zgodnie z zaakceptowanym przez Zamawiającego Harmonogramem wdrożenia. W celu zapewnienia najwyższej jakości usługi Zamawiający wymaga, aby migracja została przeprowadzona zgodnie z wymaganiami oraz procedurami producenta. Wykonawca musi dostarczyć oświadczenie producenta tj. firmy Nefeni sp. z o.o. potwierdzające, że migracja SEOD będzie przeprowadzona przez producenta lub pod jego nadzorem merytorycznym.

3	Instalacja Systemu backupu	Należy zainstalować, uruchomić i skonfigurować dostarczone środowisko backupu na zasobach lokalnych oraz urządzeniach wirtualnych i fizycznych, uzgodnionych z Zamawiającym. W skład usług wymaganych w OPZ polegających na instalacji, uruchomieniu i konfiguracji dostarczonego środowiska backupu Zamawiający wymaga: – utworzenie reguł kopii zapasowych w systemie dla serwerów, środowiska wirtualizacji oraz stacji roboczych, – sprawdzenie poprawności wykonania kopii zapasowych serwera i stacji roboczej – konfiguracja mechanizmu tworzenia kopii zapasowej bazy danych SQL Serwer
4	Instruktaż stanowiskowy	Zamawiający wymaga przeprowadzenia instruktaży stanowiskowych z wszystkich dostarczanych elementów zamówienia. Instruktaże stanowiskowe powinny obejmować łącznie min 48h dla zespołu max. 5 osób Zamawiającego.
5	Testy zainstalowanego środowiska Zamawiającego	Zamawiający uzna wykonanie prac za zakończone w momencie przedstawienia przez Wykonawcę dokumentów potwierdzających wykonanie testów całego dostarczonego w tym postępowaniu środowiska w obecności przedstawiciela Zamawiającego. Wykonawca wykona dokumentację powykonawczą dla całego dostarczonego rozwiązania.
6	Prowadzenie prac	Wszystkie wymagane prace, które w jakikolwiek sposób mogą zakłócić pracę Starostwa, muszą się odbywać w oknie serwisowym: niedziela od godz. 20:00 do 5:00.

2.5 Kryteria równoważności dla Serwerowego Systemu Operacyjnego (SSO) Microsoft Windows Serwer 2022 oraz dla Serwera Bazy Danych (SBD) Microsoft SQL Serwer 2022 Standard.

W związku z podaniem przez Zamawiającego nazw konkretnych licencji oraz wskazaniem producenta, poniżej podano kryteria równoważności, czyli wymagane cechy minimalne dla oprogramowania równoważnego.

1. Serwer Bazy Danych (SBD) licencjonowany na min. 4 rdzenie procesora musi spełniać następujące wymagania minimalne (poprzez wbudowane mechanizmy):

1) Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.
2) Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
3) Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
4) Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.

5) Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
6) SBD musi umożliwiać tworzenie klastrów niezawodnościowych.
7) Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:
   - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
   - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
   - klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,
8) Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (backup) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
9) Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.
10) Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory.
11) Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.
12) Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń:
   - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),
   - wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),
   - para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).
13) Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.
14) Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków” obiektu, „rodzica”

itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Wykonawcę języku

15) programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.
16) Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:
    - udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
    - udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
    - udostępniać język zapytań do struktur XML,
    - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
    - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.

16) Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:

    - zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
    - oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
    - obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,
    - typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja - punkt, seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).

17) Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania.
18) Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożliwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.
19) Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.
20) Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.
21) Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam
22) sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.

23) System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:
   - mechanizm debuggowania tworzonego rozwiązania,
   - mechanizm stawiania „pułapek" (breakpoints),
   - mechanizm logowania do pliku wykonywanych przez transformację operacji,
   - możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),
   - możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo),
   - mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),
   - mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),
   - mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,
   - mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych.
24) Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.
25) Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).
26) Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).
27) Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.
28) Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).

29) Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
30) Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.
31) System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać:
    - raporty parametryzowane,
    - cache raportów (generacja raportów bez dostępu do źródła danych),
    - cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów),
    - współdzielenie predefiniowanych zapytań do źródeł danych,
    - wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
    - możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,
    - możliwość wizualizacji wskaźników KPI,
    - możliwość wizualizacji danych w postaci obiektów sparkline.
32) Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
33) Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF, PowerPoint.
34) SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.
35) SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja).
36) Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.
37) W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.
38) System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.
39) W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).

40) SBD musi posiadać wbudowane mechanizmy do obsług danych grafowych (struktur złożonych z węzłów i krawędzi - reprezentujących relacje między węzłami). System musi mieć wbudowane funkcje (dostępne z poziomu kodu SQL) do analizy powiązań między węzłami grafu oraz wyszukiwania najkrótszej ścieżki w grafie.
41) SBD musi posiadać mechanizmy klasyfikacji informacji przechowywanych w bazie danych w celu łatwej identyfikacji obszarów (obiektów) w bazie danych, gdzie składowane są dane wrażliwe. Mechanizm ten powinien umożliwiać przypisanie kolumnom w tabeli m.in. takich atrybutów jak: typ przechowywanych informacji oraz poziom wrażliwości danych. Dodatkowo SBD powinien udostępniać zestaw predefiniowanych raportów prezentujących m.in. listę sklasyfikowanych tabel i kolumn oraz liczbę tabel zawierających dane wrażliwe.

2. Serwerowy System Operacyjny (SSO):

Licencje muszą uprawniać do uruchamiania w dostarczonym klastrze HCI min. dwóch maszyn wirtualnych oferowanego systemu operacyjnego. Dostarczone licencje muszą obejmować wszystkie rdzenie, wszystkich procesorów w dostarczonym klastrze HCI. Równoważny system operacyjny musi posiadać następujące, wbudowane cechy:

1. możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,
2. możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,
3. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,
4. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,
5. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
6. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,
7. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),
8. wbudowane wsparcie instalacji i pracy na wolumenach, które:
   - pozwalają na zmianę rozmiaru w czasie pracy systemu,
   - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   - umożliwiają zdefiniowanie list kontroli dostępu (ACL),
9. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
10. wbudowane szyfrowanie dysków
11. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,
12. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,
13. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,
14. graficzny interfejs użytkownika,
15. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

16. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),
17. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,
18. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
19. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    - podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    - usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        a) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        b) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        c) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
    - zdalna dystrybucja oprogramowania na stacje robocze,
    - praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
    - centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        a) dystrybucję certyfikatów poprzez http,
        b) konsolidację CA dla wielu lasów domeny,
        c) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
    - szyfrowanie plików i folderów,
    - szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
    - możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
    - serwis udostępniania stron WWW,
    - wsparcie dla protokołu IP w wersji 6 (IPv6),
    - wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
        a) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
        b) obsługi ramek typu jumbo frames dla maszyn wirtualnych,
        c) obsługi 4-KB sektorów dysków,
        d) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
        e) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),
        f) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,
        g) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),
        h) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,
        i) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez

skrypty,

możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF

3. Dostawa, wdrożenie sieciowego serwera plikowego typu NAS na potrzeby tworzenia kopii zapasowych systemów z klastra HCI, podłączenie zasobu do środowiska backupu klastra HCI.

Element konfiguracji	Wymagania minimalne
Procesor	Procesor o taktowaniu nie mniejszym niż 1,7 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 2GB DDR4
Pamięć RAM liczba slotów	Minimum 1 slot
Pamięć RAM - możliwość rozszerzenia	nie mniej niż do 16GB
Pamięć Flash	Nie mniej niż 512MB
Liczba zatok na dyski twarde	Minimum 4
Obsługiwane dyski twarde	3.5" SATA
Pojemność obsługiwanych dysków twardych	do 22TB
Zainstalowane dyski twarde	Min 4 dyski 20TB każdy, dyski klasy Enterprise przystosowane do pracy 24x7.
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej dwóch
Porty LAN 2,5 Gb/s	Minimum 2 RJ-45
Porty LAN 10 Gb/s	Minimum 2 na złączu SFP+
Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2 Gen 1	Minimum 4
Port PCI-Ex	Tak, minimum 1
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 1U
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Min. dwa redundantne zasilacze wewnętrzne o mocy min. 250 W każdy, 100-240 V
Specyfikacja oprogramowania	
Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie wolumenów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak

Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping oraz Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S Migawka oraz kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla pod folderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików, producenta urządzenia dla systemów Windows Backup na zewnętrzne dyski twarde
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / Obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików / Serwer FTP /Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia

	DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Możliwość aktualizacji oprogramowania Ustawienia: Back up, przywracania, resetowania systemu
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym adresów IP Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Zdalna replikacja Rsync Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS(bramka zewnętrzna)
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji aplikacji z paczek
Maksymalna liczba użytkowników	4096
Gwarancja	36 miesięcy gwarancji producenta na urządzenie oraz 60 miesięcy gwarancji na dyski twarde

4. Przełączniki sieciowe zarządzalne do utworzenia sieci HCI oraz przełączniki sieciowe do utworzenia nowego rdzenia sieci LAN.

Obecnie używane przez Zamawiającego przełączniki tworzące rdzeń sieci LAN są przestarzałe, nie ma możliwości instalacji nowego oprogramowania wewnętrznego. Przedmiotem zadania jest dostawa 2 nowych przełączników umożliwiających utworzenia nowego rdzenia sieci LAN. Ponadto należy dostarczyć dwa nowe przełączniki umożliwiające utworzenie dedykowanej, odseparowanej sieci LAN na potrzeby klastra HCI.

4.1 Przełącznik sieciowy, zarządzalny do dedykowanej sieci LAN dla klastra HCI – 2 sztuki

Element konfiguracji	Wymagania minimalne
Fizyczne	Wysokość w szafie 19” – 1U, głębokość nie większa niż 250mm, możliwość montażu w szafie rack

Techniczne	Minimum 1 port ethernet 10/000BaseT Minimum 8 portów SFP28, pozwalających na instalację wkładek 25Gbit. Minimum 2 porty QSFP28, pozwalające na instalację wkładek 100Gbit. Minimum 1 port konsoli: RJ45
Wydajność	Pojemość matrycy przełączania: minimum 710Gbps Wydajność: minimum 350Gbps Tablica adresów MAC o wielkości minimum 120k pozycji
Procesor	Min. 1 procesor 650Mhz
Pamięć RAM	Min. 128MB
Pamięć wbudowana	Min. 32MB
Stackowanie / MLAG	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) lub możliwość wykonania MLAG (Multichassis Link Aggregation)
Funkcje minimalne	Obsługa ramek Jumbo minimum 9k Routing IPv4 – minimum: statyczny, RIP, OSPF, BFD,VRF, VRRP Routing IPv6 – minimum: statyczny, RIPng, OSPF Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping Obsługa vxlan Obsługa Port isolation Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol Obsługa funkcji Loop Protect Obsługa funkcji Traffic Shaping Obsługa 4094 tagów IEEE 802.1Qoraz minimum 1000 jednoczesnych sieci VLAN z BPDU protection Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie lub MLAG Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping ze wsparciem opcji 82 Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI Obsługa standardu 802.1p Funkcja mirroringu portów Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) lub CDP Cisco Discovery Protocol Funkcja autoryzacji użytkowników zgodna z 802.1x Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo RADIUS Accounting

Zarządzanie	Zarządzanie poprzez port konsoli (pełne), Musi wspierać możliwość zarządzania przez następujące protokoły: • SNMP v.1, 2c i 3, • Telnet, SSH v.2, • http • https • Syslog • NTP Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
Zasilanie	Urządzenie musi być wyposażone w dwa redundantne, dedykowane zasilacze Możliwość zasilania PoE.
Wyposażenie	Wraz z przełącznikiem należy dostarczyć niezbędne wkładki, przewody do redundantnego podłączenia serwerów i utworzenia dedykowanej sieci dla klastra HCI. Zestaw do montażu w szafie rack
Gwarancja	24 miesiące gwarancji w miejscu instalacji

4.2 Zakres wdrożenia przełączników dla dedykowanej sieci LAN dla klastra HCI:

Wykonawca dostarczy nowe urządzenia, przedstawi projekt wydzielenia sieci LAN dla serwerów klastra HCI do akceptacji Zamawiającego. Na podstawie zaakceptowanego projektu zainstaluje przełączniki w wskazanej szafie rack, skonfiguruje do pracy w sieci LAN Zamawiającego. Wszystkie prace muszą się odbywać w oknie serwisowym: niedziela od godz. 20:00 do 5:00. Projekt musi obejmować minimum:

- aktualizacja oprogramowania układowego serwerów składowych klastra
- instalacja oprogramowania wirtualizacji w najnowszej dostępnej stabilnej wersji
- aktualizacja oprogramowania układowego przełączników do najnowszej stabilnej wersji
- konfiguracja portów do zarządzania (management port)
- konfiguracja dedykowanych przełączników dla sieci HCI do współdzielenia klastrowego zasobu dyskowego
- konfiguracja przełączników rdzenia sieci do działania w trybie redundantnym (zestawienie połączeń w trybie LACP lub LAG do serwerów)
- konfiguracja serwerów dla sieci HCI prywatnej
- konfiguracja serwerów dla sieci LAN publicznej (dostępowej)
- konfiguracja rozproszonych zasobów dyskowych HCI
- konfiguracja klastra wirtualizacji z wykorzystaniem zasobów dyskowych HCI

4.3 Przełącznik sieciowy, zarządzalny do utworzenia rdzenia sieci LAN – 2 sztuki

Element konfiguracji	Wymagania minimalne
Fizyczne	Wysokość w szafie 19” – 1U, głębokość nie większa niż 250mm, możliwość montażu w szafie rack
Techniczne	Minimum 1 port ethernet 10/000BaseT Minimum 24 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Minimum 2 porty SFP28, pozwalające na instalację wkładek 25Gbit. Minimum 1 port konsoli: RJ45
Wydajność	Pojemość matrycy przełączania: minimum 216 Gbps Wydajność: minimum 108 Gbps Tablica adresów MAC o wielkości minimum 32k pozycji
Procesor	Min. 1 procesor 650Mhz
Pamięć RAM	Min. 64 MB
Pamięć wbudowana	Min. 16 MB
Stackowanie / MLAG	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) lub możliwość wykonania MLAG (Multichassis Link Aggregation)
Funkcje minimalne	Obsługa ramek Jumbo minimum 9k Routing IPv4 – minimum: statyczny, RIP, OSPF, BFD,VRF, VRRP Routing IPv6 – minimum: statyczny, RIPng, OSPF Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping Obsługa vxlan Obsługa Port isolation Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol Obsługa funkcji Loop Protect Obsługa funkcji Traffic Shaping Obsługa 4094 tagów IEEE 802.1Qoraz minimum 1000 jednoczesnych sieci VLAN z BPDU protection Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie lub MLAG Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping ze wsparciem opcji 82 Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI Obsługa standardu 802.1p Funkcja mirroringu portów Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) lub CDP Cisco Discovery Protocol Funkcja autoryzacji użytkowników zgodna z 802.1x Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo RADIUS Accounting

Zarządzanie	Zarządzanie poprzez port konsoli (pełne), Musi wspierać możliwość zarządzania przez następujące protokoły: • SNMP v.1, 2c i 3, • Telnet, SSH v.2, • http • https • Syslog • NTP Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
Zasilanie	Urządzenie musi być wyposażone w dwa redundantne, dedykowane zasilacze Możliwość zasilania PoE
Wyposażenie	Wraz z przełącznikiem należy dostarczyć niezbędne wkładki, przewody do redundantnego podłączenia wszystkich wskazanych przez Zamawiającego urządzeń do tworzonego rdzenia sieci LAN. Zestaw do montażu w szafie rack
Gwarancja	24 miesiące gwarancji w miejscu instalacji

4.4 Zakres wdrożenia przełączników do rdzenia sieci LAN:

Wykonawca dostarczy nowe urządzenia, przedstawi projekt wdrożenia przełączników do rdzenia sieci LAN Zamawiającego. Na podstawie zaakceptowanego projektu zainstaluje przełączniki w wskazanej szafie rack, skonfiguruje do pracy w sieci LAN Zamawiającego. Wszystkie prace muszą się odbywać w oknie serwisowym: niedziela od godz. 20:00 do 5:00. Projekt musi obejmować minimum:

- aktualizacja oprogramowania układowego przełączników do najnowszej stabilnej wersji
- konfiguracja sieci wirtualnych przełącznika na podstawie obecnej infrastruktury
- konfiguracja agregacji połączeń do serwerów pomiędzy przełącznikami
- konfiguracja agregacji połączeń dla przełączników dostępowych
- konfiguracja syslog dla przełączników
- konfiguracja protokołu SNMP zgodnie z obecnym systemem monitoringu
- konfiguracja użytkowników administracyjnych przełącznika zgodnie z wytycznymi bezpieczeństwa

5. Migracja

Systemu Elektronicznego Obiegu Dokumentów (SEOD) EZD Proton na nowy system operacyjny oraz nowy serwer bazodanowy, zgodnie z zaleceniami producenta. Szkolenie pracowników z zakresu Cyberbezpieczeństwa z elementami dobrych praktyk bezpiecznej korespondencji dokumentacji elektronicznej.

Podniesienie poziomu bezpieczeństwa użytkowanego Systemu Elektronicznego Obiegu Dokumentów (SEOD) EZD Proton. Obecnie system jest zainstalowany na serwerze fizycznym z systemem operacyjnym Windows 2012 oraz

wykorzystuje bazę danych na serwerze SQL 2012. Zarówno dla Windows Serwer 2012 jak i Serwera SQL 2012 nie są już dostępne poprawki, aktualizacje oraz wsparcie techniczne producenta, systemy są przestarzałe. W celu podniesienia poziomu bezpieczeństwa Systemu Elektronicznego Obiegu Dokumentów EZD Proton Zamawiający zamierza przenieść system na najnowsza dostępną wersję systemu operacyjnego Windows Serwer oraz najnowszą dostępną bazę danych SQL Serwer 2022. Wykonawca dostarczy licencje niezbędne do pracy SEOD EZD Proton w nowym klastrze HCI, zainstaluje min. dwie maszyny wirtualne Windows Serwer 2022 wraz w wszystkim dostępnymi aktualizacjami. Zainstaluje, skonfiguruje Serwer SQL 2022 Standard, skonfiguruje Windows Serwer 2022 zgodnie z wymaganiami SEOD EZD Proton, dokona przeniesienia SEOD EZD Proton na Windows Serwer 2022, przeniesie bazę danych na nowy Serwer SQL 2022 Standard, przeprowadzi testy poprawności działania SEOD EZD Proton na nowym systemie operacyjnym i bazodanowym. Ponadto Wykonawca przeprowadzi szkolenia w zakresie użytkowanego Systemu Elektronicznego Obiegu Dokumentów EZD Proton autorstwa Nefeni sp. Zo.o. dla 60 pracowników Zamawiającego. Szkolenia musza być przeprowadzane w grupach max 10 osobowych. Wykonawca zapewni szkolenia zarówno dla pracowników merytorycznych jak i administratorów przenoszonego systemu SEOD EZD Proton.

Lp.	Opis wymagania
WSZ1	Szczegółowy plan szkolenia wraz z harmonogramem przygotowany zostanie na etapie planu realizacji projektu.
WSZ2	Wykonawca na etapie uzgadniania materiałów szkoleniowych przekaże minimalne wymagania, jakie powinni spełniać oddelegowani przez Zamawiającego, uczestnicy szkolenia
WSZ3	Do każdego modułu wspomagającego obsługę obszarów działalności Urzędu, Zamawiający wskaże osoby, które Wykonawca przeszkoli
WSZ4	Szkolenia będą prowadzone w siedzibie zamawiającego na sprzęcie dostarczonym przez Wykonawcę (laptopy) w godzinach pracy Zamawiającego w terminach uzgodnionych wcześniej. Wykonawca w ramach zamówienia dostarczy na potrzeby szkoleń rzutnik oraz ekran.
WSZ5	Zamawiający nie dopuszcza przeprowadzania szkoleń typu e-learning w zastępstwie szkoleń tradycyjnych.
WSZ6	Zamawiający dopuszcza przeprowadzanie szkoleń grupowych, w grupach do 10 użytkowników oraz szkoleń indywidualnych przy stanowiskowych dla grup jedno-, dwu- lub trzyosobowych.
WSZ7	Wykonawca przeszkoli osoby pełniące obowiązki administratorów wskazanych przez Zamawiający w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych.
WSZ8	Wykonawca zapewni przeszkolenie administratora wskazanego przez Zamawiającego w zakresie administracji i konfiguracji zaoferowanego systemu bazodanowego. Szkolenie musi obejmować co najmniej instalację, konfigurację bazy danych, obsługę narzędzi

	administratora, architekturę systemu, zagadnienia związane z zachowaniem bezpieczeństwa, integralności i zabezpieczenia przed utratą danych, przywracaniem danych po awarii.
WSZ9	Uzgodnieniu pomiędzy stornami podlegają: - Minimalne wymagania dla uczestników szkoleń, - Harmonogram szkoleń grupowych i indywidualnych, - Materiały szkoleniowe dla szkoleń grupowych, - Listy obecności ze szkoleń grupowych i indywidualnych, - Protokoły Odbioru Zadania dot. Szkoleń.
WSZ10	Zamawiający oczekuje, że ilość oraz program szkoleń powinny gwarantować użytkownikom systemu zapoznanie się z wszystkimi funkcjonalnościami jakie system oferuje.

Zakres materiału na szkolenia dla poszczególnych grup

Pracownik kancelarii [**KANCELARIA**]:

- dodawanie interesanta
- rejestracja pism przychodzących tradycyjnych
- rejestracja pism przychodzących z ePUAPu
- wydruk rejestru pism przychodzących
- przekazywanie pism do dekretacji oraz dekretacja skrócona
- wysyłanie pism poprzez rejestr pocztowy
- wydruk rejestru pocztowego

Pracownik na stanowisku kierowniczym [**KIEROWNICY**]:

- odebranie pisma z kancelarii i przedekretowanie na pracownika merytorycznego
- ustawianie zastępstw w obrębie komórki organizacyjnej
- rodzaje dekretacji
- przeglądanie pism pracowników podległych

Pracownik na stanowisku merytorycznym [**MERYTORYCZNI**]:

- odbieranie pism po dekretacji
- prowadzenie dokumentacji nietworzącej akt spraw
- prowadzenie dokumentacji tworzącej akt spraw
- prowadzenie sprawy
- pisanie pism wychodzących tradycyjnych i elektronicznych
- ustawianie zastępstw za siebie w obrębie komórki organizacyjnej

Administratorzy [**ADMINISTRATORZY**]
Zakres przewidziany jest na cały dzień szkoleniowy:

- zarządzanie użytkownikami
- zarządzanie strukturą organizacyjną
- zaawansowane czynności administracyjne
- administracja dokumentacją przy pismach / sprawach / teczkach pracowników
- opcje systemu wraz z parametryzacją
- schematy pism
- obiegi automatyczne

W związku z podaniem przez Zamawiającego nazw licencji, poniżej podano kryteria równoważności, czyli wymagane cechy dla równoważnego Oprogramowania typu Microsoft SQL Server Standard 2022:

System bazodanowy (SBD) licencjonowany na min. 4 rdzenie procesora musi spełniać następujące wymagania minimalne (poprzez wbudowane mechanizmy):

42) Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.
43) Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
44) Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
45) Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
46) Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
47) SBD musi umożliwiać tworzenie klastrów niezawodnościowych.
48) Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:
    - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
    - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
    - klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,
49) Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (backup) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
50) Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.
51) Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł

użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory.

52) Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.
53) Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń:
   - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),
   - wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),
   - para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).
54) Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.
55) Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków" obiektu, „rodzica" itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Wykonawcę języku
56) programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.
57) Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:
   - udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
   - udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
   - udostępniać język zapytań do struktur XML,
   - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
   - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.

16) Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:

   - zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,

- oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
- obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,
- typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja - punkt, seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).

58) Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania.
59) Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożliwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.
60) Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.
61) Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.
62) Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam
63) sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.
64) System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:
    - mechanizm debuggowania tworzonego rozwiązania,
    - mechanizm stawiania „pułapek” (breakpoints),
    - mechanizm logowania do pliku wykonywanych przez transformację operacji,
    - możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),
    - możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo),
    - mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),

- mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),
- mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,
- mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych.

65) Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.
66) Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).
67) Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).
68) Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.
69) Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).
70) Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
71) Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.
72) System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać:
    - raporty parametryzowane,
    - cache raportów (generacja raportów bez dostępu do źródła danych),

- cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów),
- współdzielenie predefiniowanych zapytań do źródeł danych,
- wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
- możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,
- możliwość wizualizacji wskaźników KPI,
- możliwość wizualizacji danych w postaci obiektów sparkline.

73) Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
74) Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF, PowerPoint.
75) SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.
76) SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja).
77) Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.
78) W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.
79) System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.
80) W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).
81) SBD musi posiadać wbudowane mechanizmy do obsług danych grafowych (struktur złożonych z węzłów i krawędzi - reprezentujących relacje między węzłami). System musi mieć wbudowane funkcje (dostępne z poziomu kodu SQL) do analizy powiązań między węzłami grafu oraz wyszukiwania najkrótszej ścieżki w grafie.
82) SBD musi posiadać mechanizmy klasyfikacji informacji przechowywanych w bazie danych w celu łatwej identyfikacji obszarów (obiektów) w bazie danych, gdzie składowane są dane wrażliwe. Mechanizm ten powinien umożliwiać przypisanie kolumnom w tabeli m.in. takich atrybutów jak: typ przechowywanych informacji oraz poziom wrażliwości danych. Dodatkowo SBD powinien udostępniać zestaw predefiniowanych raportów prezentujących m.in. listę sklasyfikowanych tabel i kolumn oraz liczbę tabel zawierających dane wrażliwe.

oraz Microsoft Windows Serwer 2022:

Licencje muszą uprawniać do uruchamiania w dostarczonym klastrze HCI min. dwóch maszyn wirtualnych oferowanego systemu operacyjnego. Dostarczone licencje muszą obejmować wszystkie rdzenie, wszystkich procesorów w dostarczonym klastrze HCI. Równoważny system operacyjny musi posiadać następujące, wbudowane cechy:

20. możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,
21. możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,
22. możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,
23. możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,
24. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
25. wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,
26. automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),
27. wbudowane wsparcie instalacji i pracy na wolumenach, które:
    - pozwalają na zmianę rozmiaru w czasie pracy systemu,
    - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    - umożliwiają zdefiniowanie list kontroli dostępu (ACL),
28. wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
29. wbudowane szyfrowanie dysków
30. możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,
31. możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,
32. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,
33. graficzny interfejs użytkownika,
34. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
35. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),
36. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,
37. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
38. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    - podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    - usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        d) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        e) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        f) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
    - zdalna dystrybucja oprogramowania na stacje robocze,

- praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
- centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
  d) dystrybucję certyfikatów poprzez http,
  e) konsolidację CA dla wielu lasów domeny,
  f) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
- szyfrowanie plików i folderów,
- szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
- możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
- serwis udostępniania stron WWW,
- wsparcie dla protokołu IP w wersji 6 (IPv6),
- wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
  j) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
  k) obsługi ramek typu jumbo frames dla maszyn wirtualnych,
  l) obsługi 4-KB sektorów dysków,
  m) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
  n) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),
  o) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,
  p) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),
  q) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,
  r) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,

5. Dostawa, wdrożenie systemu SIEM (Security Information and Event Management) z usługą zewnętrznego SOC - Centrum Operacji Bezpieczeństwa (Security Operations Center), systemu monitoringu środowiska.

Zamawiający wymaga dostarczenia systemu SIEM z gwarancją oraz wsparciem technicznym na okres min. 12 miesięcy (parametr punktowany dodatkowo) oraz świadczenie usługi SOC (Security Operations Center) przez okres min. 12 miesięcy (parametr punktowany dodatkowo).

5.1 Słownik pojęć:

Skrót lub Pojęcie	Opis
Best Effort	Stan realizacji usługi, w którym zostały przekroczone ograniczenia SLA ze względu na wystąpienie zwiększonego zapotrzebowania na usługę. W przypadku przekroczenia ograniczeń SLA Wykonawca niezwłocznie poinformuje Zamawiającego o zaistniałej sytuacji.

Cyberbezpieczeństwo	Adekwatny do potrzeb stan ochrony zapewniający możliwość wykrycia oraz reagowania na zdarzenia niepożądane oraz wskazane w dokumentacji systemu zarządzania bezpieczeństwem informacji Zamawiającego.
Cyberprzestrzeń	Przestrzeń, w której następuje wymiana, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikacja między człowiekiem i komputerem.
Czas	Wszystkie wskazania w dokumencie w zakresie czasu dotyczą czasu w aktualnej strefie czasowej przyjętej jako czas urzędowy obowiązujący w Polsce.
Departament Bezpieczeństwa	Komórka organizacyjna w strukturach Zamawiającego, odpowiedzialna za bezpieczeństwo informacji.
Dzień roboczy	Od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego.
Incydent Bezpieczeństwa Informacji (Incydent)	Pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
Koordynator Wykonawcy	Osoba z ramienia Wykonawcy odpowiedzialna za podejmowanie decyzji w zakresie realizacji spełniania warunków SLA usługi oraz za kontakt z Zamawiającym. Koordynator może mieć jednego lub wielu zastępców.
Okres przejściowy	Czas, w którym Wykonawca zobowiązany będzie do podjęcia działań, których celem będzie przejęcie wiedzy od Zamawiającego o jego systemie monitoringu, uzgodnienia z Zamawiającym wzoru Miesięcznego Raportu Rozliczenia Usług, ustalenia z Zmawiającym harmonogramu wdrożenia dla pierwszych scenariuszy użycia oraz dopasowanie i uzgodnienie zasad współpracy Zamawiającego z systemami Wykonawcy. Zakończenie okresu przejściowego potwierdzone zostanie Protokołem Odbioru.
Koordynator Zamawiającego	Osoba z ramienia Zamawiającego odpowiedzialna za podejmowanie decyzji w zakresie realizacji usługi. Koordynator może mieć jednego lub wielu zastępców.
Miejsce świadczenia usługi monitorowania cyberbezpieczeństwa	Miejsce świadczenia usługi Monitorowania Cyberbezpieczeństwa przez zespół Wykonawcy spełniające wymagania ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).

Pierwsza Linia Wsparcia	Pierwsza Linia Wsparcia SOC – usługa realizująca w szczególności zadania: • Identyfikacji zdarzeń; • Analizy i eliminacji najprostszych znanych zdarzeń
Druga Linia Wsparcia	Druga Linia Wsparcia SOC – usługa realizująca w szczególności zadania: • Współpracy w reakcji na zdarzenia skomplikowane i nieznane; • Tworzenie Scenariuszy Reakcji na powtarzalne zdarzenia; • Nadzór nad poprawnością działania konfiguracji scenariuszy użycia;
On-call	Dyżur pod telefonem, czekanie w gotowości na zgłoszenie Drugiej Linii Wsparcia, wyłącznie dla Incydentów o priorytecie Poważnym.
CTI/OSINT	Ang. Cyber Threat Inelligence/OpenSource Inteligence - narzędzia dostarczające szczegółowe informacje o technikach hakerskich, zagrożeniach, podatnościach, artefaktach lub umiejętności ich interpretowania i dekodowania oraz czynności pozwalające na pozyskanie informacji z powszechnie dostępnych źródeł umożliwiających powiększenie zakresu wiedzy na temat potencjalnych zagrożeń.
Praca ciągła	Praca systemu w trybie 24/7/365 dni.
PUODO	Prezes Urzędu Ochrony Danych Osobowych – organ właściwy do spraw ochrony danych osobowych na terytorium Polski, utworzony ustawą z 10 maja 2018 roku o ochronie danych osobowych. Jest również organem nadzorczym w rozumieniu ogólnego rozporządzenia o ochronie danych.
RODO	Ustawa o ochronie danych osobowych z dnia 28 maja 2018 roku uszczegółowiające wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) jest odpowiedzią na wyzwania związane ze zmieniającą się gospodarką dupa osobowymi.
SOC	Security Operations Center – centrum operacji bezpieczeństwa, którego zadaniem jest monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na cyber zagrożenia.
Scenariusz Reakcji	Dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia nieporządnego, składający się z: • Zestawu możliwości technicznych wykrycia zdarzenia; • Zdefiniowanych warunków wywołania zdarzenia niepożądanego; • Opisu identyfikacji zdarzeń zależnych; • Instrukcji reakcji na zdarzenie; • Instrukcji uruchomienia działań korekcyjnych; • Instrukcji wykonywania działań informacyjnych; • Ogólnych i szczegółowych ścieżek eskalacyjnych.

Scenariusz użycia systemu bezpieczeństwa	Dokument opisujący zestaw zadań wymaganych do wykonania w ramach Drugiej Linii Wsparcia, w skład którego wchodzą między innymi: • Skonfigurowanie jednego lub kilku źródeł zdarzeń; • Przygotowanie Scenariuszy Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia.
SLA	Zestaw wartości granicznych dla kluczowych wskaźników wydajności, dla których określona realizacja usługi jest wymagany w zakresie jakościowym.
System analizy logów	System umożliwiający zbieranie i analizę logów z urządzeń, sieci i systemów informatycznych
Transfer Wiedzy	Usługa przekazywania kompetencji w zakresie realizacji usług Pierwszej i Drugiej Linii Wsparcia.
Usługa monitorowania Cyberbezpieczeństwa	Zestaw czynności wykonywanych przez Wykonawcę w ramach umowy w celu identyfikacji Incydentów Bezpieczeństwa Informacji.
Zdarzenia niepożądane	Zdarzenie mogące wskazywać na wystąpienie incydentu bezpieczeństwa w środowisku chronionym.
Zdarzenie False-Negative	Wykrycie przez Drugą Linię Wsparcia, zdarzenia nie poprawnie rozpoznanego przy zastosowaniu ustalonych i zaakceptowanych procedur bezpieczeństwa. Realizacja i rozpoznawanie zdarzeń „False-Negative”.
Zdarzenie False-Positive	Wykrycie przez automatyczne systemy zdarzenia, które po analizie zostało uznane jako zdarzenie poprawne. W przypadku notorycznego występowania, statystycznie rozumianego jako więcej niż 100 zdarzeń „False - Positive” na 1 incydent bezpieczeństwa w miesiącu, należy uznać regułę automatyczną tworzącą takie zdarzenia jako błędną konfigurację systemu bezpieczeństwa.
Przypadek testowy	Celowe wykonanie pełnego przebiegu zdarzenia od momentu wystąpienia sytuacji niepożądanej do momentu zakończenia przetwarzania fazy analizy incydentu. Gdy jest to możliwe, obejmuje wykonanie odwracalnych kroków reakcji na incydent, sprawdzenie scenariusza end-to-end łącznie z zablokowaniem wskaźników kompromitacji w narzędziach prewencyjnych.

5.2 Termin realizacji usługi SOC

1. Świadczenie Usługi SOC rozpoczęte zostanie w terminie określonym na etapie tworzenia planu wdrożenia.
2. Termin, o którym mowa w punkcie 6.2 podpunkt 1 licząc od dnia podpisania umowy do rozpoczęcia świadczenia usługi, traktuje się jako okres przejściowy, w którym Wykonawca zobowiązany będzie do podjęcia działań, których celem będzie dopasowanie i uzgodnienie zasad współpracy. Zakończenie okresu przejściowego potwierdzone zostanie Protokołem Odbioru.
3. Wykonawca do świadczenia usługi będzie wykorzystywał narzędzia dostarczone w niniejszym

postępowaniu oraz udostępnione przez Zamawiającego. Dostęp do narzędzi i systemów Zamawiającego musi być zrealizowany za pomocą bezpiecznego połączenia szyfrowanego.

5.3 Wymagania dla Usługi SOC (Security Operations Center)

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie Analizy Logów zgodnie z opisanymi poniżej wymaganiami.

5.4 Pierwsza i Druga Linia Wsparcia

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie Analizy Logów zgodnie z opisanymi poniżej wymaganiami.

1) Pierwsza Linia Wsparcia

W ramach realizacji zadań Pierwszej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

a) Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa zgodnie warunkami określonymi w punkcie 8 (Ogólne warunki SLA).
b) Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.
c) Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji.
d) Łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa.
e) Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszy Reakcji.
f) Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.
g) Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive).
h) Priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa.
i) Przygotowywanie dziennych raportów wykrytych zdarzeń bezpieczeństwa.

2) Druga Linia Wsparcia

W ramach realizacji zadań Drugiej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

a) Dostępność usługi dla Zamawiającego zgodnie z określonymi warunkami SLA (Ogólne warunki SLA).
b) Analizę zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych.
c) Przygotowywanie i realizację Scenariuszy użycia systemu bezpieczeństwa zgodnie z wymaganiami przedstawionymi przez Zamawiającego.
d) Przygotowanie Scenariuszy Reakcji.
e) Przygotowanie Miesięcznych raportów z realizacji prac.

5.5 Scenariusze

1. Scenariusz użycia systemu bezpieczeństwa

Zamawiający wymaga przygotowania i wdrożenia możliwych scenariuszy użycia dla zidentyfikowanych przez Zamawiającego ryzyk. Harmonogram wdrożenia zostanie ustalony w okresie przejściowym dla pierwszych scenariuszy użycia, pozostałe scenariusze zostaną przygotowane w uzgodnionym terminie. Każdorazowo Scenariusz użycia musi zostać zaakceptowany przez Zamawiającego. Zamawiający posiada listę przykładowych scenariuszy użycia, które należy przygotować i wdrożyć. Przykładowe scenariusz użycia:

- Wykrywanie logowania z pominięciem systemu klasy PAM
- Wykrywanie utworzenia użytkownika (lokalnego i domenowego)
- Wykrycie złośliwego oprogramowania na chronionym obiekcie

a) *Minimalny zakres zadań, z których ma być zbudowany Scenariusz użycia systemu bezpieczeństwa zawiera:*
   - Skonfigurowanie jednego lub kilku źródeł zdarzeń,
   - Stworzenie Scenariusza Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia,
   - Opisanie szczegółowej ścieżki eskalacji,

b) *Opracowanie scenariusza manualnego lub automatycznego sprawdzania poprawności działania. W przypadku pojawienia się nowych skuteczniejszych technik identyfikacji zagrożeń, Wykonawca ma obowiązek zaktualizować w porozumieniu z Zamawiającym istniejące Scenariusze użycia systemu bezpieczeństwa.*

2. Scenariusz Reakcji

Przygotowany przez Wykonawcę oraz zatwierdzony przez Zamawiającego Scenariusz Reakcji określa minimalny zestaw czynności konieczny do udokumentowania oraz wyciągnięcia powtarzalnych wniosków, na podstawie których zostaną podjęte określone czynności. Scenariusz Reakcji składa się z podzadań realizujących funkcje:

- **Wzbogacenia** wiedzy o artefaktach tj. adresy IP, domeny, hash'e plików, nazwy plików, rozpoznawalność wskaźników kompromitacji przez udostępnione narzędzia klasy CTI / OSINT, w celu wyciągania adekwatnych wniosków i podejmowania trafnych decyzji,
- **Analizy** zidentyfikowanego zdarzenia, w tym w szczególności potwierdzenia, że zagrożenie w przypadku uruchomienia w środowisku Zamawiającego może stać się incydentem lub jest incydentem, jak również rozpoczęcia pobierania lub zabezpieczenia dodatkowych danych z zaatakowanego źródła ataku zasobu na potrzeby realizacji Pierwszej Linii Wsparcia,
- **Reakcji** rozumianej jako ograniczenie możliwości wystąpienia zdarzenia niepożądanego, uruchomienia procesu eskalacyjnego lub innych czynności stosownych do zagrożenia w zakresie uzgodnionym z Zamawiającym,
- **Informowania i raportowania** obejmującego dokumentowanie wykonanych czynności oraz rezultatów przeprowadzonej analizy lub zasadności czynności reakcji.

5.6 Raport Poincydentalny

Zamawiający wymaga przygotowania Raportu Poincydentalnego dla incydentów o priorytecie Poważnym i Wysokim nie później niż do 2 dni roboczych od zakończenia realizacji zawierającego informacje:

- Unikalny identyfikator zdarzenia
- Kiedy incydent wystąpił?
- Kiedy incydent został zauważony / wykryty?
- Kto lub jaki proces był sprawcą incydentu?
- Co się wydarzyło?
- Gdzie wydarzenie miało miejsce?
- Dlaczego zdarzenie mogło wystąpić?
- Jakie czynności zostały przeprowadzone w celu powstrzymania incydentu?
- Zalecenia Poincydentalne zawierające informację jakie zabezpieczenia zostały ustanowione lub powinny zostać ustanowione w celu zapobieżenia ponownemu wystąpieniu incydentu.

W przypadku przygotowania zaleceń, dla których konieczne jest wprowadzenie istotnych zmian do systemów bezpieczeństwa lub jakiejkolwiek rekonfiguracji systemów Zamawiającego Koordynator Wykonawcy przedstawi do akceptacji Koordynatorowi Zamawiającego zakres i szczegółową listę zmian. Zwolnione z takiej czynności są Zalecenia Poincydentalne konieczne do powstrzymania zidentyfikowanego Incydentu zagrażającego cyberbezpieczeństwu infrastruktury lub danych Zamawiającego.

5.7 Systemy Zamawiającego wymagające monitorowania

Usługa monitorowania, będąca przedmiotem zamówienia, może być oparta o logi/dane z poniższych systemów Zamawiającego (źródła logów) udostępnionych przez Zamawiającego:

Rodzaj usługi lub urządzenia	Liczba urządzeń / nodów będących źródłami logów
Active Directory (liczba serwerów)	
Windows Server	
Linux Server	
DNS, DHCP	
Systemy bezpieczeństwa np.: serwer systemu antywirusowego, web application firewall, inne	
Centralny Firewall / UTM	
Pomocniczy Firewall / UTM	
IPS / IDS	
VPN	
Przełączniki sieci LAN, punkty dostępowe WiFi	

Zamawiający na bieżąco będzie aktualizował listę źródeł logów wysyłających nowe dane do Wykonawcy.

5.8 Wymagania dla Systemu Zbierania i Analizy Logów oraz Systemu SIEM.

1) Wymagania dla Systemu Analizy Logów
   a) W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
   b) Rozwiązanie musi zostać dostarczone w postaci maszyn wirtualnej instalowanych w środowisku Vmware lub Windows Hyper-V
   c) Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach.
   d) Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie

zdarzenia z logów.

e) Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.

f) Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.

g) Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.

h) Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.

i) Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).

j) Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.

k) Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie. –

l) Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).

m) Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.

n) Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).

o) Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów)

p) Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.

q) Rozwiązanie musi umożliwiać tworzenie statycznych raportów.

r) Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF.

s) Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.

t) Rozwiązanie musi umożliwiać tworzenie własnych raportów.

u) Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.

v) Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.

Wymagania systemowe

a) Liczba zdarzeń na sekundę (EPS): min. 9 500

b) Zarządzanie logami: min. 2 lata

c) Liczba obsługiwanych urządzeń min. 600

d) Liczba zapisu zdarzeń na dobę: min 12000 MB

e) System logów musi wspierać hiperwizory: Vmware ESXi oraz Microsoft HyperV

5.9 Wymagania dla Systemu SIEM.

a) W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące incydenty na urządzeniach sieciowych Zamawiającego

b) Rozwiązanie musi w pełni realizować swoją funkcjonalność lokalnie (instalacja on-prem)

c) Architektura rozwiązania musi być oparta o fizyczne lub wirtualne sondy monitorujące, których rolą jest

odbieranie kopii ruchu sieciowego, generowanie alarmów oraz/lub metadanych o zdarzeniach, przygotowanie przechwyconych plików do dalszej analizy oraz przekazywanie przetworzonych danych do urządzenia administracyjnego.

d) Architektura rozwiązania musi być oparta także o fizyczne urządzenie administrujące, którego rolą jest zarządzanie sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu, dogłębna analiza odebranych plików, prezentacja wyników detekcji, a także przekazywanie danych do rozwiązań stron trzecich

e) Platformy muszą obsługiwać szyfrowanie dysków w standardzie LUKS.

f) Rozwiązanie musi wspierać implementację na środowisku wirtualnym takim jak m.in. VMWare, Hyper-V, Proxmox, KVM, OVM, OVF.

g) Serwer dedykowany musi posiadać redundantne zasilanie oraz musi być objęty 3 letnim okresem gwarancyjnym w miejscu instalacji.

h) Sonda musi posiadać co najmniej 4 porty monitorujące i muszą być w stanie przetworzyć dane dla maksymalnego odbieranego ruchu sieciowego na poziomie 4Gb/s.

i) Serwer dedykowany musi obsługiwać do 3 900 zdarzeń na sekundę, musi przechowywać do 9 milionów zdarzeń, musi mieć możliwość detekcji malware, a także musi analizować przy pomocy silnika detekcji shellcode/powershell do 3 na sekundę.

j) Licencja na zakup i serwis oprogramowania musi bazować na ilości aktywnie występujących w ruchu sieciowym adresów IP. Ilość adresów, objętych monitorowaniem: 250.

k) Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce

l) Konsola rozwiązania musi zawierać informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, sygnatury czasowe.

m) Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia oraz musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).

n) Rozwiązanie musi obsługiwać silniki detekcji takie jak Analiza Shellcode i Powershell, tj. detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wywoływania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.

o) Rozwiązanie musi umożliwiać analizowanie całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń.

5.10 Administracja Systemem Analizy Logów:

W ramach realizacji zadań administracji Systemem Analizy Logów Wykonawca będzie odpowiedzialny za:

a) Informowanie Zamawiającego o awariach Systemu Analizy Logów, mogących uniemożliwić poprawne działanie systemów informacyjnych Zamawiającego i/lub świadczenie usług ujętych w niniejszym dokumencie;
b) Rekomendowanie zmiany zasobów takich jak: vCPU, vRAM, pamięć masowa;
c) Optymalizowanie konfiguracji Systemu Analizy Logów w celu nieprzekraczania wartości licencji Systemu posiadanego przez Zamawiającego oraz niezwłocznego zgłaszania sytuacji przekroczenia poziomu utylizacji licencji;
d) Konfigurację Systemu Analizy Logów w celu gromadzenia i normalizowania logów ze wskazanych systemów Zamawiającego zgodnie z punktem 6.7;
e) Weryfikację czy System Analizy Logów prawidłowo analizuje logi ;

f) Tworzenie wymagań dla systemów Zamawiającego wysyłających logi w zakresie poziomu logowania zdarzeń.

5.11 Testowanie Systemu Analizy Logów:

W ramach realizacji zadań testowania Systemu Analizy Logów Wykonawca będzie odpowiedzialny za:

a) Przygotowanie i uzyskanie aprobaty Zamawiającego dla scenariuszy testów Systemu Analizy Logów,
b) Weryfikację wdrożonych scenariuszy użycia oraz implementacji nowych przypadków zgłoszonych przez Zamawiającego,
c) Weryfikację możliwości wdrożenia przypadków użycia w środowisku Zamawiającego,

5.12 Analiza złośliwego oprogramowania:

a) W ramach realizacji umowy, Zamawiający będzie mógł zlecić Wykonawcy wykonanie analizy złośliwego oprogramowania, nie więcej niż 6 w ciągu roku. Sposób zgłaszania analizy złośliwego oprogramowania zostanie uzgodniony po podpisaniu umowy.
b) Zakres analizy złośliwego oprogramowania będzie nie mniejszy niż:
c) Analiza statyczna wskazanej próbki złośliwego oprogramowania,
d) Analizy dynamiczna w kontrolowanym środowisku pozwalającym na wyłączenie funkcji ukrywania lub wykrywania analizy,
e) W przypadku wykorzystywania rodziny malware określenia wersji
f) Każdorazowo po wykonanej analizie złośliwego oprogramowania Wykonawca przekaże drogą mailową raport z wykonanej analizy. Zakres raportu zostanie ustalony po podpisaniu umowy.

5.13 Ogólne warunki SLA

Wykonawca zapewni świadczenie Usługi monitorowania zgodnie z określonym poziomem SLA.

<table>
<tr><th>Nazwa usługi</th><th>Poziom świadczonej usługi</th></tr>
<tr><td>Pierwsza Linia Wsparcia

Czasy dla pierwszych zdarzeń każdego dnia w wymiarze 30 zdarzeń, pozostałe zadania realizowane będą w trybie „Best Effort”</td><td>Dostępność usługi w dni robocze pomiędzy godzinami 7:00 a 15:00.

<table>
<tr><td rowspan="2">Priorytet zdarzenia</td><td colspan="2">Czas od wykrycia przez L1 do</td></tr>
<tr><td>Podjęcia</td><td>Realizacji</td></tr>
<tr><td>Poważny</td><td>30 min</td><td>2 h</td></tr>
<tr><td>Wysoki</td><td>60 min</td><td>6 h</td></tr>
<tr><td>Średni</td><td>2 h</td><td>12 h</td></tr>
<tr><td>Niski</td><td>4 h</td><td>24 h</td></tr>
</table></td></tr>
<tr><td>Druga Linia Wsparcia

Czasy dla pierwszych Incydentów każdego dnia w wymiarze 5 incydentów, pozostałe zadania realizowane w trybie „Best Effort”</td><td>Dostępność usługi w dni robocze pomiędzy godzinami 7:00 a 15:00.

<table>
<tr><td rowspan="2">Priorytet incydentu</td><td colspan="2">Czas od eskalacji pierwszej linii wsparcia do</td></tr>
<tr><td>Podjęcia</td><td>Realizacji</td></tr>
<tr><td>Poważny</td><td>30 min</td><td>24 h</td></tr>
<tr><td>Wysoki</td><td>60 min</td><td>2 dni</td></tr>
<tr><td>Średni</td><td>2 h</td><td>4 dni</td></tr>
</table></td></tr>
<tr><td>Analiza złośliwego oprogramowania</td><td>Rozpoczęcie analizy w terminie do 2 dni roboczych od przekazania podejrzanej próbki oprogramowania przez Koordynatora Zamawiającego do Koordynatora Wykonawcy oraz potwierdzenia otrzymania próbki przez Koordynatora Wykonawcy.</td></tr>
</table>

Scenariusz użycia systemu bezpieczeństwa	Przygotowanie i wdrożenie scenariusza użycia systemu wraz ze scenariuszami reakcji w terminie do 5 dni roboczych od przekazania informacji od Koordynatora Zamawiającego do Koordynatora Wykonawcy z wyjątkiem scenariuszy ujętych w harmonogramie przygotowanym w okresie przejściowym.

1. W uzasadnionych przypadkach Wykonawca ma prawo zwrócenia się do Zamawiającego o zgodę na zawieszenie SLA na usługę Pierwszej i Drugiej Linii Wsparcia na uzgodniony z Zamawiającym okres jednak nie dłuższy niż 14 dni. Wniosek o zawieszenie SLA musi zawierać uzasadnienie. Zamawiający w takim przypadku zobowiązany jest do rozpatrzenia prośby w ciągu 1 dnia roboczego od chwili uzyskania informacji o tym fakcie. W przypadku odmowy Zamawiający jest zobowiązany w ciągu 3 Dni Roboczych do przedstawienia pisemnego uzasadnienia odmowy, wskazując obiektywne czynniki świadczące o bezzasadności wniosku Wykonawcy.
2. Czas podjęcia Incydentu będzie liczony jako delta czasu pomiędzy odnotowaniem wystąpienia zdarzenia przez L1 a czasem nadania priorytetu.
3. Czas realizacji Incydentu będzie liczony jako delta czasu pomiędzy podjęciem incydentu a zakończeniem obsługi podsumowanym wydanymi wstępnymi rekomendacjami i/lub raportem, w zależności od przypisanego scenariusza reakcji.
4. Zamawiający wyróżnia cztery poziomy incydentów: Poważny, Wysoki, Średni, Niski. Domyślnie każdy incydent zarejestrowany, jeżeli nie zostanie to uszczegółowione inaczej ma priorytet Średni.

Priorytet	Opis
Poważny	• Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO; • Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika; • Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min); • Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych; • Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers; • Potwierdzona informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; • Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; • Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; • Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności; • Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych; • Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej;
	• Zgłoszenie incydentu Poważnego skutkuje bezzwłocznym uruchomieniem u Zamawiającego procesu eskalacyjnego KSC lub RODO;
Wysoki	• Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym; • Ujawnienie zestawionej sesji zwrotnej z C&C, trwającej co najmniej od 30 minut, aktywnie wykorzystywanej przez atakującego (więcej niż 1kb/min); • Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej; • Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszony w ramach inicjatywy Trusted Introducers; • Potwierdzona Informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową;

Priorytet	Opis
Poważny	• Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO; • Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika; • Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min); • Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych; • Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers; • Potwierdzona informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; • Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; • Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; • Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności; • Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych; • Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej;
	• Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; • Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; • Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności; • Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, upload na dyski webowe lub przenoszenie przez nieautoryzowane pendrive; • Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware); • Ujawnienie nieznanego przez VirusTotal lub inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu;

Priorytet	Opis
Poważny	• Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO; • Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika; • Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min); • Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych; • Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers; • Potwierdzona informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; • Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; • Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; • Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności; • Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych; • Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej;
	• Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;
Średni	• Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym; • Nieautoryzowane dysponowanie uprawnieniami administracyjnymi; • Częściowo personalizowany atak na personel zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;
	• Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy, ale nie zostało zatrzymane przez inny system bezpieczeństwa;

Priorytet	Opis
Poważny	• Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO; • Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika; • Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min); • Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych; • Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers; • Potwierdzona informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; • Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; • Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; • Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności; • Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych; • Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej;
	• Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome lub nieświadome działanie;
Niski	• Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa.

5.14 Transfer wiedzy.

1. Zamawiający wymaga, aby w każdym półroczu trwania umowy, Wykonawca przeprowadził dla grupy nie większej niż 6 osób wskazanych przez Koordynatora Zamawiającego warsztaty. Łączny wymiar godzin w półroczu wynosi nie więcej niż 4. Spotkanie ma formę Warsztatów prowadzonych w formie zdalnej. Niewykorzystane godziny nie kumulują się i nie przechodzą na kolejne okresy.
2. Warsztaty swoim zakresem będą obejmować:
   - Wyjaśnianie zagrożeń płynących z wykrytych i opisanych incydentów

- Wyjaśnianie sposobów implementacji zaleceń opisanych w Raportach Miesięcznych
- Szczegółowy harmonogram warsztatów oraz lista uczestników zostaną uzgodnione przez Koordynatorów stron.

3. Raportowanie i rozliczanie pracy

4. Miesięczny Raport Rozliczenia Usług

a) Każdy miesiąc świadczenia Usług podsumowany zostanie Raportem Miesięcznym wg według wzoru przedstawionego przez Wykonawcę. Wykonawca zobowiązany jest przedstawić Raport wraz z listą zaleceń do wykonania przez personel Zamawiającego w terminie 5 Dni Roboczych od dnia zakończenia miesiąca kalendarzowego, w którym była świadczona Usługa.

b) Zamawiający zastrzega sobie prawo zgłoszenia zastrzeżeń do Raportu, w terminie do 5 Dni roboczych od dnia jego otrzymania i zażądać uzupełnienia lub poprawy Raportu w terminie do 3 dni roboczych. Po uwzględnieniu przez Wykonawcę uwag do Raportu, Zamawiający w terminie kolejnych 3 Dni roboczych zweryfikuje ostateczną treść Raportu.

c) Dostarczony Raport Miesięczny bez uwag jest potwierdzeniem prawidłowego wykonania Usługi w miesiącu, którego dotyczy.

d) Raport składa się z sekcji:

- *Monitorowanie cyberbezpieczeństwa*
  - Data świadczenia usług
  - Zestawienie obsłużonych incydentów
    - Identyfikator incydentu
    - Nazwa
    - Klasyfikacja priorytetu Incydentu
    - Dokładna data i godzina ujawienia incydentu
    - Statusy końcowe
  - Ogólne rekomendacje i zalecenia Zamawiającego w zakresie cyberbezpieczeństwa w nawiązaniu do obsłużonych Incydentów w celu eliminacji możliwości pojawienia się incydentów w przyszłości.
- *Analiza złośliwego oprogramowania*
  - Data świadczenia usług
  - Lista zgłoszonych analiz złośliwego oprogramowania
  - Liczba analiz przeprowadzonych zgodnie z SLA

5.15 Wymagania dodatkowe

1. Cała dokumentacja powinna być dostarczana w edytowalnej postaci elektronicznej, w formacie przetwarzanym przez MS Word, Excel (od wersji 2007) lub PDF.
2. Zamawiający wymaga zatrudnienia przez Wykonawcę na podstawie umowy o pracę przez cały okres realizacji zamówienia 2 (dwóch) osób, wykonujących usługi w zakresie czynności Pierwszej oraz Drugiej Linii Wsparcia związanych z obsługą realizacji przedmiotu zamówienia, jeżeli wykonywane przez nich czynności polegają na wykonywaniu pracy w rozumieniu przepisu art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t. j. Dz. U. z 2018 r., poz. 917, z późn. zm.). Zamawiający uzna za spełniony obowiązek zatrudnienia osób wykonujących usługi w zakresie czynności pierwszej linii wsparcia przy realizacji przedmiotu zamówienia na podstawie umowy o pracę w przypadku, gdy Wykonawca skieruje do realizacji zamówienia własnych pracowników (dwóch) lub pracowników zatrudnionych na umowę o pracę. Zamawiający nie będzie ingerować w sposób prowadzenia działalności oraz organizację pracy administracyjno-biurowej Wykonawcy.

3. Wykonawca zobowiązany zostanie do przestrzegania polityki bezpieczeństwa opisanej w Polityce Bezpieczeństwa Informacji dla dostawców, która stanowi załącznik do umowy. O zmianach polityki mogących mieć wpływ na realizację umowy Wykonawca zostanie bezzwłocznie poinformowany.

5.16 Zespół SOC

Dla zapewnia prawidłowej realizacji usługi SOC Zamawiający stawia minimalny wymóg dla składu zespołu SOC:

1. Operatorzy I linii SOC – 2 osoby
2. Operatorzy II linii SOC – 1 osoba
3. SOC manager – 1 osoba
4. Zarządzania podatnościami – 1 osoba
5. Eksperci od bezpieczeństwa urządzeń – 1 osoba
6. Eksperci od ochrony danych osobowych – 1 osoba
7. Eksperci od zgodności z NIS2 i KSC – 1 osoba

5.17 Opcjonalny moduł EDR (Endpoint Detection and Response - moduł punktowany dodatkowo).

Wykonawca wraz z system SIEM może dostarczyć system klasy Endpoint Detection and Response wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla 250 urządzeń wraz z wsparciem technicznym na okres min. 12 miesięcy (parametr punktowany dodatkowo). Minimalne wymagania dla systemu EDR:

1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS umożliwiające bezproblemową współpracę z systemem antywirusowym do ochrony stacji roboczych, użytkowanym przez Zamawiającego.
2. Rozwiązanie musi zawierać centralną konsolę administracyjną umożliwiającą monitorowanie oraz wizualizację zebranych danych z zarządzanych urządzeń.
3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej.
4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
6. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, nazwę komputera, grupę, użytkownika.
7. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, rozmiar pliku.
8. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne lub niebezpieczne.
9. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
10. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania komend zdalnych.
11. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
12. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.

13. Rozwiązanie musi umożliwiać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
14. Rozwiązanie musi zapewniać integrację z przynajmniej takimi systemami jak: konsola programu antywirusowego, moduł EDR.
15. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: numer seryjny, informacje o systemie, procesor, pamięć RAM, karty sieciowe.
16. Serwer administracyjny musi posiadać możliwość tworzenia grup komputerów.
17. Rozwiązanie musi zapewniać korzystanie z min. 100 szablonów raportów, przygotowanych przez producenta lub własnych raportów tworzonych przez administratora.
18. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email oraz do dziennika syslog.
19. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami.
20. Rozwiązanie musi informować administratora o niezainstalowanych aktualizacjach systemowych.

5.18 Opcjonalny moduł NDR (Network Detection and Response - moduł punktowany dodatkowo).

Wykonawca wraz z system SIEM może dostarczyć system klasy Network Detection and Response wraz z centralną konsolą zarządzającą w postaci licencji bezterminowej dla 250 adresów IP wraz z wsparciem technicznym na okres min. 12 miesięcy (parametr punktowany dodatkowo). Minimalne wymagania dla systemu NDR:

1. Wielowątkowy silnik detekcji umożliwiający obsługę ruchu liczonego w dziesiątkach Gigabitów
   - Możliwość obsługi wielu podsieci VLAN
   - Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
   - Obsługa biblioteki wyrażeń regularnych HyperScan
   - Możliwość aktualizacji reguł bez wyłączania/ponownego uruchamiania silnika detekcji
2. Obsługa wielowątkowości procesora
3. Możliwość analizy kopii ruchu w sieci LAN w czasie rzeczywistym bez ingerencji w ruch sieciowy
4. Rejestracja żądań HTTP
5. Rejestracja i przechowywanie certyfikatów TLS
6. Możliwość wyodrębnienia plików z analizowanego ruchu sieciowego i zapisania ich na dysku do późniejszej analizy
7. Możliwość przechwytywania pakietów danych przesyłanych w sieci LAN i zapisywanie ich dla późniejszej analizy offline
8. Tworzenie raportów w przypadku wykrycia ruchu opisanego regułami jako ruch niebezpieczny
9. Rejestrowanie i dogłębna analiza ruchu szyfrowanego TLS/SSL
10. Rejestrowanie wszystkich kluczy wymiany do analizy oraz w celu zapobiegania podmianie
11. Rejestrowanie, zapisywanie ruchu HTTP z dowolnego portu do pliku w celu późniejszej analizy
12. Możliwość identyfikacji, wyodrębniania i rejestrowania plików w ruchu HTTP
13. Rejestracja wszystkich zapytań i odpowiedzi DNS
14. Funkcja wykrywania włamań sieciowych
15. Funkcja zapobiegania włamaniom sieciowym
16. funkcja monitorowania bezpieczeństwa sieci LAN
17. Pełne wsparcie dla protokołu IPv6

18. Możliwość dekodowania tuneli: IP-IP, IP6-IP4, IP4-IP6, GRE, VXLAN, Geneve, Teredo
19. Silnik analizy strumienia danych TCP
20. Defragmentacja pakietów w celu poddania ich analizie IPS
21. Możliwość obsługi wielu podsieci VLAN
22. Możliwość obsługi wielu fizycznych połączeń sieciowych do różnych segmentów sieci LAN
23. Możliwość modyfikacji reguł
24. Możliwość zdefiniowania niebezpiecznych plików przez parametry: wielkość, nazwa, rozszerzenie
25. Możliwość wykrywania złośliwego oprogramowania w oparciu o odcisk palca JA3, JA3S
26. Możliwość wykrywania złośliwego oprogramowania w oparciu o metodę HASSH
27. Obsługa dekodowania pakietów: IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ, MPLS, ERSPAN, VXLAN
28. Dekodowanie warstwy aplikacji: HTTP, HTTP/2, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, ENIP/CIP, DNP3, NFS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP, RDP, RFB
29. Możliwość tworzenia raportów zgodnych z standardem JSON, SYSLOG,
30. Możliwość filtrowania alertów z podziałem na wagę/priorytet
31. Możliwość filtrowania alertów dla wybranej reguły z podziałem na wagę/priorytet
32. Wspierane systemy operacyjne: Windows, Linux, FreeBSD, OpenBSD, MacOS, Mac OS X
33. Obsługa przekazywania alertów „dalej” do systemów takich jak: syslog, eve.log, JSON, Unified 2
34. Filtrowanie alertów na poziomie: reguł, hostów, sieci

5.19 System monitoringu systemu wirtualizacji oraz infrastruktury IT

W ramach realizacji zadania Wykonawca dostarczy licencje bezterminowe z wsparciem technicznym na okres min. 24 miesięcy, dokona instalacji, konfiguracji oraz podłączenie wszystkich wymaganych systemów będących celem monitorowania. System musi spełniać poniższe wymagania minimalne:

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.
Monitorowanie	
2	▪ 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).
Prezentacja	
3	▪ 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
Powiadomienia	
4	▪ 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
Konfiguracja	
5	▪ 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)
Monitoring bazy danych systemu HIS	
6	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
Kolektor logów	
7	▪ 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.
Cyberbezpieczeństwo	
8	▪ 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.
Monitoring	
9	W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT: – Serwer fizyczny - 10 sztuk – maszyna wirtualna Windows / Linux – do 30 sztuk – serwer AD - 2 sztuki – Macierz - 4 sztuki, – Przełącznik Fibre Channel – 2 sztuki – Przełącznik rdzeniowy – 4 sztuki – Przełącznik dostępowy (LAN) – do 20 sztuk – Macierz NAS 1 sztuka – Zasilacz awaryjny (UPS) - 2 sztuki – Serwer bazodanowy - 2 sztuki – Serwer wirtualizacji (Host, hypervizor) - 3 sztuki – Serwer wirtualizacji (konsola zarządzająca) – 1 sztuka – Serwer Backupu - 1 sztuka ▪ W ramach usługi wykonawca monitoruje krytyczne systemy Zamawiającego: ▪ Baza danych SQL dla systemu obiegu dokumentów

	▪ System obiegu dokumentów (użytkowany przez Zamawiającego)

6. Szkolenia z zakresu Cyberbezpieczeństwa dla administratorów.

Przedmiotem zadania jest pakiet szkoleń dla administratorów, mający na celu podniesienie poziomu wiedzy z zakresu Cyberbezpieczeństwa, ustalania polityki bezpieczeństwa oraz konfiguracji posiadanych systemów w sposób zapewniający najwyższy możliwy poziom ochrony. Zamawiający wymaga dostarczenia voucherów na okaziciela, które można zrealizować w terminie do 12 miesięcy licząc od dnia wystawienia i dostarczenia do Zamawiającego. Wymagane jest ustalenie z Zamawiającym terminu wystawienia każdego vouchera.

6.1 Szkolenie z zakresu elementów systemu zabezpieczeń infrastruktury teleinformatycznej – 1 voucher na szkolenie ważny przez okres min. 12 miesięcy

Szkolenie zakończenie egzaminem oraz certyfikatem, czas trwania min. 5 dni roboczych. Szkolenie musi łączyć teorię oraz zajęcia praktyczne (warsztaty) przy użyciu nowoczesnego sprzętu i oprogramowania. Po zakończeniu szkolenia Zamawiający będzie miał możliwość kontaktu z trenerem w terminie do 30 dni od zakończenia szkolenia. Zakres szkolenia:

Moduł 1: Zapoznanie z elementami podatnymi na niebezpieczeństwo oraz metodami ich wykorzystywania przez intruza

Moduł 2: Przewidywanie zagrożeń bezpieczeństwa na podstawie modelu STRIDE:

- tworzenie planu zarządzania ryzykiem
- projektowanie zabezpieczeń dla zasobów fizycznych
- wyznaczenie zagrożeń i analiza ryzyka w sieci

Moduł 3: Wyznaczenie zagrożeń i analiza ryzyka dla kont w organizacji

- projektowanie zabezpieczeń kont – polityki blokowania konta, granularne zasady haseł
- wyznaczenie zagrożeń i analiza ryzyka dla procesu uwierzytelniania

Moduł 4: Typowe zagrożenia usług katalogowych i DNS oraz zastosowanie metod zabezpieczających te usługi

- znaczenie i ograniczenia funkcjonalności Credential Guard w systemach Windows
- działanie i konfiguracja DNSSEC

Moduł 5: Wyznaczenie zagrożeń, projektowanie zabezpieczeń i analiza ryzyka dla danych

- implementacja i konfiguracja Encrypted File System i Bitlocker w oparciu o dobre praktyki

Moduł 6: Wyznaczenie zagrożeń, projektowanie zabezpieczeń i analiza ryzyka dla transmisji danych

Moduł 7: Projektowanie polis inspekcji dostępu do zasobów

Moduł 8: Analiza ryzyka tworzonego przez użytkowników sieci, projektowanie polityki bezpiecznego używania komputera

Moduł 9: Analiza ryzyka zarządzania sieci, projektowanie polityki bezpieczeństwa dla zarządzania siecią

Moduł 10: Elementy kryptografii

- sposoby wykorzystania kryptografii do zabezpieczania informacji
- metody szyfrowania
- zabezpieczanie informacji w organizacji przy użyciu uwierzytelniania oraz kontroli dostępu

Moduł 11: Dystrybucja i zarządzanie certyfikatami, tworzenie struktury PKI

- zabezpieczanie transmisji danych (SSL/TLS)
- implementacja zabezpieczeń dla typowych metod transmisji danych (IPSec), i uwierzytelniania do sieci bezprzewodowych (RADIUS/WPA2-Enterprise)
- dystrybucja i wykorzystanie kart inteligentnych w środowisku Windows

Moduł 12: Identyfikacja, odpowiedź na incydenty oraz asystowanie przy formalnym śledztwie w przypadku włamania

6.2 Certyfikowane szkolenie z zakresu bezpieczeństwa głównych systemów informatycznych w organizacji – 1 voucher na szkolenie ważny przez okres min. 12 miesięcy.

Szkolenie zakończenie egzaminem oraz certyfikatem, czas trwania min. 5 dni roboczych. Szkolenie musi łączyć teorię oraz zajęcia praktyczne (warsztaty) przy użyciu nowoczesnego sprzętu i oprogramowania. Po zakończeniu szkolenia Zamawiający będzie miał możliwość kontaktu z trenerem w terminie do 30 dni od zakończenia szkolenia. Minimalny zakres szkolenia:

1. Bezpieczeństwo stacji roboczych:
   - zarządzanie uprawnieniami
   - filtrowanie URL
   - konfiguracja programu antywirusowego
   - kopia zapasowa systemu operacyjnego, danych użytkownika, kopia profilu użytkownika na zasób sieciowy
   - kontrola podłączanych nośników
2. Ochrona serwerów: DMZ; Firewall; WWW; OWASP Top10; Szukanie podatności; IPS/IDS; Poczta; Serwery pośredniczące; Skanowanie AV; Ochrona sieci; Jak szukać luk w zabezpieczeniach; Sniffing
3. Domena Microsoft Active Directory:
   - Instalacja i konfiguracja kontrolerów domeny: omówienie usług AD DS.
   - Omówienie kontrolerów domeny usług AD DS.
   - Wdrożenie kontrolera domeny
   - Encrypted DNS – szyfrowana usługa rozpoznawania nazw w Windows Server 2022
   - Zarządzanie obiektami w AD DS. zarządzanie kontami użytkowników
   - Zarządzanie grupami w usługach AD DS.
   - Zarządzanie obiektami typu komputer w AD DS.
   - Wdrażanie i zarządzanie OU
   - Zarządzanie zaawansowaną infrastrukturą AD DS.
   - Wprowadzenie do zaawansowanych wdrożeń AD DS.
   - Wdrożenie rozproszonego środowiska AD DS.
   - Konfiguracja relacji zaufania AD DS.
   - Wdrażanie i zarządzanie lokacjami i repliką AD DS.

- Omówienie replikacji usług AD DS.
- Konfigurowanie lokacji usług AD DS.
- Konfigurowanie i monitorowanie replikacji usług AD DS.
- Wdrażanie zasad grupy: Wprowadzenie do zasad grupy
- Wdrażanie i zarządzanie obiektami GPO (Group Policy Object)
- Konfiguracja zakresu i przetwarzania obiektów GPO
- Rozwiązywanie problemów z GPO
- Zarządzanie ustawieniami użytkowników za pomocą zasad grupy
- Wdrażanie szablonów administracyjnych
- Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów
- Konfiguracja preferencji zasad grupowych

4. Instalacja i konfiguracja oprogramowania antywirusowego:
   - instalacja konsoli zarządzającej
   - zarządzanie administratorami i ich uprawnieniami
   - polityki i dziedziczenie; apache HTTP Proxy
   - zdalna instalacja i omówienie możliwość
   - grupy statyczne i dynamiczne
   - zadania klienta, serwera oraz wyzwalacze, typowe scenariusze
   - omówienie funkcji podstawowych i zaawansowanych klienta AV
   - ochrona antywirusowa
   - zarządzanie aktualizacją
   - konfiguracja zapora osobiste
   - moduł antyspamowy
   - kontrola dostępu do stron internetowych
   - kontrola dostępu do urządzeń
   - chmura publiczna, prywatna
   - wirtualizacja środowiska produkcyjnego, sandbox
   - rozwiązywanie najczęściej pojawiających się problemów
5. Podstawy budowy sieci:
   - urządzenia sieci komputerowych; wielkości sieci; składniki sieci, nośniki transmisji danych, przewodowe i bezprzewodowe; model sieci ISO OSI oraz TCP/IP;
   - protokoły warstw TCP/IP; nagłówek pakietu IPv4; adresacja IPv4, maski podsieci; klasy adresów, zakresy prywatne, APIPA;
   - adresacja IPv6, przyczyny powstania; adresy specjalne, zastosowanie; Translacja adresów NAT; adres fizyczny MAC, protokół ARP;
   - protokół TCP; Usługa DNS i DHCP, działanie i zagrożenia; routery, firewall, IDS/IPS, Proxy; VPN, bezpieczeństwo sieci;
6. Podstawowe narzędzia administratora wraz ze sposobem ich wykorzystywania do monitoringu sieci:
   - Ping; tracert/traceroute; tcpdump/windump;
   - Wireshark: graficzne narzędzie do analizy ruchu sieciowego

- Cacti: narzędzie do monitorowania ruchu w sieci
- Observium: monitorowanie sieci
- nmap (Zenmap): czyli sprawdź co masz w sieci

7. Tworzenie kopii zapasowych serwerów fizycznych oraz wirtualnych:
   - instalacja i konfiguracja oprogramowania do backupu na hoście i serwerze fizycznym
   - metody wdrożenia, automatyzacja wdrożenia,
   - opracowanie, konfiguracja, modyfikacja planów backupowych
   - backup systemów Microsoft (Windows, Active Directory, SQL Server)
   - sposoby aktualizacji agentów.
   - tworzenie planów kopii zapasowej: typy chronionych danych/zasobów/usług; lokalizacje przechowywania kopii zapasowych; weryfikacja kopii zapasowej; usuwanie planu kopii zapasowej; dodatkowe ustawienia;
   - odzyskiwanie kopii zapasowej danych/zasobów/usług: metody odtwarzania, tworzenie i zastosowanie nośnika startowego (wykorzystanie pxe); administracja kontami i uprawnieniami;

8. Konfiguracja urządzenia brzegowego typu UTM:
   - rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego; ustawienia systemowe i uprawnienia administratorów; instalacja licencji i aktualizacja systemu; tworzenie kopii zapasowej i przywracanie konfiguracji; zbieranie logów i monitorowanie; przedstawienie kategorii zbieranych logów; wykresy historyczne i monitorowanie; obiekty: typy obiektów oraz ich wykorzystanie; obiekty sieciowe i obiekt typu „router”;
   - konfiguracja sieci: tryby pracy urządzenia; typy interfejsów (ethernet, modem, bridge, vlan, gretap)
   - typy routingu oraz ich priorytety; translacja adresów sieciowych (nat); translacja połączeń wychodzących (maskarada); translacja połączeń przychodzących (przekierowanie); translacja dwukierunkowa (jeden do jeden); filtrowanie ruchu sieciowego (firewall); ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (stateful inspection); szczegółowy opis parametrów reguły firewall; kolejność przetwarzania reguł firewall i nat;
   - ochrona aplikacji: implementacja filtrowania url dla ruchu http i https; konfigurowanie skanowania antywirusowego i modułu breach fighter; moduł ips i stosowanie profili inspekcji; użytkownicy i uwierzytelnianie
   - konfiguracja usługi katalogowej: wprowadzenie do różnych metod uwierzytelniania (ldap, kerberos, radius, certyfikat ssl, spnego, sso); rejestracja użytkowników; uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania; 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; ssl vpn - zasada działania, konfiguracja

6.3 Certyfikowane szkolenie z zakresu oferowanego i wdrożonego przez Wykonawcę systemu monitorowanie infrastruktury IT – 1 voucher na szkolenie ważny przez okres min. 12 miesięcy.

Szkolenie zakończenie egzaminem oraz certyfikatem, czas trwania min. 7 dni roboczych. Szkolenie musi łączyć teorię oraz zajęcia praktyczne (warsztaty) przy użyciu nowoczesnego sprzętu i oprogramowania. Po zakończeniu szkolenia Zamawiający będzie miał możliwość kontaktu z trenerem w terminie do 30 dni od zakończenia szkolenia. Minimalny zakres szkolenia:

Moduł 1: Funkcjonalności, kluczowe założenia, istotne informacje,

Moduł 2: Komponenty systemu, przegląd modułu proxy

Moduł 3: Network Time Protocol, strefy czasowe, Firewall, SELinux

Moduł 4: Wymagania instalacyjne; instalacja, tworzenie bazy danych systemu; Serwer: instalacja z pakietów; narzędzia wiersza poleceń, GUI; instalowanie nakładek dla systemu z pakietów, ćwiczenia praktyczne

Moduł 5: Interfejs systemu; przegląd, uprawnienia użytkownika, wyszukiwanie globalne

Moduł 6: Profil użytkownika, ustawienia, motywy, media i powiadamianie

Moduł 7: Administracja, tworzenie nowego użytkownika, ćwiczenia praktyczne

Moduł 8: Definicje, lista pojęć wykorzystywanych w pracy z systemem

Moduł 9: Monitoring, urządzenia, przegląd, hosty, ostatnie dane: proste wykresy, wykresy dla wielu urządzeń, aplikacje

Moduł 10: Konfiguracja grupy urządzeń, urządzenia, nazywanie urządzeń, ćwiczenia praktyczne

Moduł 11: Zbieranie danych, pozycje, klucze pozycji, jednostki pozycji, standardowe, elastyczne i zaplanowane interwały aktualizacji pozycji, mapowanie wartości, historia i trendy, testowanie elementów głównego interfejsu, filtrowanie pozycji/edycja masowa, czyszczenie historii, przetwarzanie wstępne, pozycje nieobsługiwane, monitorowanie bez agentowe, proste sprawdzenia, testy ICMP, ćwiczenia praktyczne

Moduł 12: Instalacja agenta przy użyciu pakietów, agent dla Windowsa i MacOS, ćwiczenia praktyczne

Moduł 13: Zbieranie danych, pasywne sprawdzenia przy pomocy Agenta, aktywne sprawdzanie przy pomocy Agenta, narzędzia wiersza poleceń, ćwiczenia praktyczne

Moduł 14: Monitoring Windows poprzez agenta systemowego dla Windows, logi zdarzeń, liczniki wydajności, zapytania WMI

Moduł 14: Makra wbudowane makra, makra użytkownika

Moduł 15: Wykrywanie problemów, wyzwalacze, wyrażenia i funkcje wyzwalaczy, konstruktor wyrażenia wyzwalacza, testowanie wyrażenia wyzwalaczy, zamykanie i potwierdzanie problemów, zależności wyzwalające, zaawansowane wykrywanie problemów, ćwiczenia praktyczne

Moduł 16: Znaczniki zdarzeń, definiowanie znaczników niestandardowych, wiele poziomów znaczników, przypadki zastosowania

Moduł 17: Szablony: właściwości szablonu, łączenie szablonów, wiele poziomów szablonów, ćwiczenia praktyczne

Moduł 18: Zbieranie danych, parametry użytkownika dla Agenta, ćwiczenia praktyczne

Moduł 19: Zbieranie danych w praktyce, sprawdzenia SSH, sprawdzenia Telnet, sprawdzenia HTTP, ćwiczenia praktyczne

Moduł 20: Pozycje zależne, definicja, konfiguracja pozycji nadrzędnych, konfiguracja pozycji zależnych, ćwiczenia praktyczne

Moduł 21: Zbieranie danych: sprawdzenia obliczane, demonstracja, sprawdzenia agregowane, monitoring SNMP, interfejsy SNMP, SNMP OID i MIB, narzędzia wiersza poleceń SNMP, rozwiązywanie problemów SNMP, pułapki SNMP, monitoring plików logów, typy pozycji monitoringu plików logów, wyzwalacze monitoringu plików logów,

zaawansowany monitoring plików logów, notatki monitoringu logów, scenariusze web, kroki scenariusza web, raporty ze scenariusza web, wyzwalacze scenariusza web, ćwiczenia praktyczne

Moduł 22: Raporty: informacje o systemie, raporty dostępności, najczęściej uruchamiające się wyzwalacze

Moduł 22: Tryby inwentarza, automatyczne uzupełnianie danych, przegląd, szczegóły, ćwiczenia praktyczne

Moduł 23: Powiadomienia: typy mediów, szablony wiadomości, konfiguracja mediów użytkownika

Moduł 24: Akcje/Działania: funkcjonalność, warunki, operacje i kroki, operacje odzyskiwania i aktualizacji, eskalacje, stosowanie makr, rozwiązywanie problemów, działania wewnętrzne, wykrywanie błędnej konfiguracji, ćwiczenia praktyczne

Moduł 25: Powiadomienia: niestandardowe typy mediów, ćwiczenia praktyczne

Moduł 26: funkcjonalność, okresy konserwacji, konserwacja oparta na hostach i wyzwalaczach, wstrzymywanie eskalacji, ćwiczenia praktyczne

Moduł 27: Monitoring na poziomie biznesowym: usługi, relacja rodzic – dziecko, kalkulacja SLA, raporty, czas pracy i przestój; wykrywanie niskopoziomowe: przegląd, workflow, przykłady, ćwiczenia praktyczne; eksport konfiguracji: Import/eksport XML

Moduł 28: Automatyzacja: przegląd wykrywania sieci, przegląd automatycznej rejestracji, omówienie API systemu, ćwiczenia praktyczne

Moduł 29: Kopia zapasowa - najlepsze praktyki

Moduł 30: Kondycja serwera: korzystanie z szablonów, główne komponenty wewnętrzne, wbudowany dashboard, demonstracja; przegląd plików konfiguracyjnych

Moduł 31: Administracja: ustawienia ogólne, ustawienia housekeepera, globalne wyrażenia regularne, makra, poziomy i opcje wyzwalaczy, proxy, grupy użytkowników, specjalne grupy użytkowników, uprawnienia, skrypty frontend, audyt, logi działań, kolejka, ćwiczenia praktyczne

Moduł 32: Wizualizacja danych: niestandardowe grafy, konstruktor map, mapowanie ikon na mapach, hierarchia map, uprawnienia, opcje wyświetlania problemów, ekrany, prezentacje, dashboardy, ćwiczenia praktyczne

6.4 Certyfikowane szkolenie z zakresu oferowanego i wdrożonego przez Wykonawcę systemu SIEM – 1 voucher na szkolenie ważny przez okres min. 12 miesięcy.

Szkolenie zakończenie egzaminem oraz certyfikatem, czas trwania min. 6 dni roboczych. Szkolenie musi łączyć teorię oraz zajęcia praktyczne (warsztaty) przy użyciu nowoczesnego sprzętu i oprogramowania. Po zakończeniu szkolenia Zamawiający będzie miał możliwość kontaktu z trenerem w terminie do 30 dni od zakończenia szkolenia.

Minimalny zakres szkolenia:

Moduł 1: Wprowadzenie do systemu bezpieczeństwa informatycznego

- Zasady działania systemu
- Kluczowe funkcjonalności systemu
- Model architektury
- Rola systemu w kompleksowym systemie bezpieczeństwa

Moduł 2: Architektura i komponenty systemu

- Składniki systemu: zbieranie, analiza, reakcja
- Określone moduły systemu w ramach systemu bezpieczeństwa
- Struktura i przepływ danych w systemie

Moduł 3: Instalacja i konfiguracja systemu SIEM

- Wymagania instalacyjne
- Proces instalacji systemu
- Konfiguracja podstawowych ustawień systemu

Moduł 4: Zarządzanie logami

- Zbieranie, przetwarzanie i przechowywanie logów
- Konfiguracja źródeł logów
- Analiza struktury logów i identyfikacja kluczowych informacji

Moduł 5: Monitorowanie zdarzeń i incydentów

- Detekcja zagrożeń na podstawie logów i danych z systemu
- Klasyfikacja incydentów zgodnie z poziomem zagrożenia
- Ostrzeżenia i powiadomienia w przypadku wykrycia nieprawidłowości

Moduł 6: Analiza zachowań użytkowników

- Monitorowanie aktywności użytkowników
- Wykrywanie podejrzanych zachowań i anomalii
- Analiza przywilejów i dostępów użytkowników

Moduł 7: Badanie ruchu sieciowego

- Monitorowanie ruchu w sieci
- Wykrywanie ataków sieciowych i analiza danych przesyłanych w sieci
- Analiza protokołów sieciowych i identyfikacja podejrzanych aktywności

Moduł 8: Reakcja na incydenty

- Proces reakcji na incydenty w systemie
- Konfiguracja reguł reakcji automatycznej
- Rola analityków bezpieczeństwa w reakcji na incydenty

Moduł 9: Audyt i raportowanie

- Generowanie raportów z działalności systemu
- Przegląd audytu zgodności z normami i przepisami
- Przechowywanie i archiwizacja danych audytowych

Moduł 10: Zarządzanie zabezpieczeniami

- Konfiguracja reguł detekcji i alertów
- Utrzymywanie bazy danych o zabezpieczeniach
- Doskonalenie strategii obronnej w oparciu o analizę danych z systemu

Moduł 11: Praktyczne scenariusze zagrożeń

- Symulacja rzeczywistych scenariuszy ataków
- Testowanie reakcji systemu na różne rodzaje incydentów
- Doskonalenie umiejętności analitycznych i reakcyjnych uczestników

Moduł 12: Integracja z zewnętrznymi systemami

- Integracja systemu z innymi narzędziami bezpieczeństwa
- Współpraca z systemami kontroli dostępu, antywirusowymi itp.
- Konfiguracja interfejsów API

Moduł 13: Doskonalenie umiejętności praktycznych

- Objaśnienie praktycznej analizy logów, incydentów i raportowania
- Testowanie reakcji systemu na symulowane ataki i zagrożenia
- Indywidualne zadania praktyczne, w których uczestnicy stosują zdobytą wiedzę

Moduł 14: Optymalizacja i skalowalność systemu

- Tuning wydajności systemu
- Zarządzanie skalowalnością infrastruktury
- Przegląd najlepszych praktyk w optymalizacji systemu

Moduł 15: Zarządzanie zdarzeniami bezpieczeństwa

- Kategoryzacja, analiza i zarządzanie zgłoszonymi incydentami
- Weryfikacja incydentów i ocena poziomu zagrożenia
- Implementacja procedur zarządzania incydentami

Moduł 16: Doskonalenie umiejętności analitycznych

- Zaawansowana analiza danych
- Wykorzystanie narzędzi analitycznych do identyfikacji trendów i wzorców
- Wnioskowanie i podejmowanie decyzji na podstawie danych

Moduł 17: Praktyczna symulacja ataków

- Realistyczne symulacje ataków z wykorzystaniem różnych technik
- Testowanie skuteczności reakcji systemu na różne scenariusze ataków
- Indywidualne i zespołowe ćwiczenia praktyczne

Moduł 18: Zarządzanie ryzykiem i zgodnością

- Ocena ryzyka związana z działalnością systemu informatycznego
- Przegląd wymogów zgodności z przepisami i standardami branżowymi
- Implementacja strategii minimalizacji ryzyka i zapewnienia zgodności

Moduł 19: Praktyczna konfiguracja i objaśnienie rozwoju systemu

- Konfiguracja systemu zgodnie z wymaganiami organizacji
- Rozwój funkcjonalności systemu w oparciu o specyficzne potrzeby branżowe
- Test nowych funkcji i ich integracja z istniejącą infrastrukturą

Moduł 20: Zrozumienie istoty praktycznej analizy danych i raportowania

- Praktyczne ćwiczenia z analizy danych logów i generowania raportów
- Testowanie różnych scenariuszy raportowania danych z systemu
- Doskonalenie umiejętności interpretacji danych i komunikacji wyników

7. Szkolenia z zakresu Cyberbezpieczeństwa dla grup użytkowników.

Wykonawca przeprowadzi szkolenia dla użytkowników w grupach 5-10 osób (minimum 60 osób). Wielkość grup będzie uzależniona od liczby osób, które w tym samym czasie będą mogły opuścić stanowisko pracy bez zakłócania ciągłości działania Starostwa. Szkolenia odbędą się w formie wykładów połączonych z ćwiczeniami praktycznymi.

Minimalny zakres szkolenia:

Moduł 1: Wprowadzenie

Czy w cyfrowym świecie naprawdę jest niebezpiecznie?

Czym ryzykujemy zaniedbując bezpieczeństwo?

Co zrobić, gdy popełniliśmy błąd w security?

Co można stracić

Moduł 2: Wiedza podstawowa

Jak dbać o swoje stanowisko pracy

Unikanie ryzykownego sprzętu elektronicznego

Podstawowe oprogramowanie zabezpieczające

Wewnętrzne szkolenia z bezpieczeństwa

Moduł 3: Jak nas podejść, popularne techniki ataków

Socjotechnika
Phishing
Ransomware

Moduł 4: Jak się bronić

- hasła

- jako korzystać i chronić
- zabezpieczenie wieloczynnikowe
- antywirus
- kopie zapasowe
- aktualizacja oprogramwania
- zaufanie, a właściwie jego brak
- szyfrowanie danych

Moduł 5: Co chronimy

Twoje dane
Email -dlaczego należy chronić
Przeglądarka
Telefon
Karty
Komputer

Moduł 6: użyteczne oprogramowanie

Samodzielne rozwijanie wiedzy o bezpieczeństwie

Jeśli wyjdziesz z zamku, jego mury Cię nie obronią - dyscyplina

Polityka prywatności, RODO i prawidłowe przetwarzanie danych wrażliwych

Jak to jest z zasłanianiem kamerki, odłączaniem mikrofonu...?

Moduł 7: Bezpieczne hasła

Jakie hasła są naprawdę bezpieczne?

Korzyści ze sprawdzonego narzędzia - KeePass

Instalacja i konfiguracja KeePass

Dodawanie i używanie własnych haseł w KeePass

Jak współdzielić hasła firmowe za pomocą KeePass

Moduł 8: Uwierzytelnianie dwuskładnikowe

Obrona przed wyciekiem haseł

Czym jest uwierzytelnianie dwuskładnikowe?

Jakie rodzaje dodatkowych poświadczeń możemy wykorzystać?

Konfiguracja uwierzytelniania dwuskładnikowego na przykładzie Google

Konfiguracja uwierzytelniania dwuskładnikowego na przykładzie Facebook

Do jakich usług zaleca się koniecznie korzystać z uwierzytelnienia dwuskładnikowego?

Moduł 9: Email oraz przeglądarka internetowa

Co robimy, a co nie w przeglądarce

Jak bezpiecznie używać poczty elektronicznej

Moduł 10: Smartfony i tablety

Może lepiej nie korzystać ze wzoru bezpieczeństwa?

Ile zajmuje włamywaczowi zainstalowanie szkodliwego programu na smartfonie?

Czy można instalować aplikacje spoza sklepu google play?

Ogranicz zaufanie do osób kontaktujących się telefonicznie

Moduł 11: Zagrożenia w pracy zdalnej

Domownicy i własne dzieci mogą niecelowo Ci zaszkodzić

Jak nie dać sobie ukraść danych osobowych

Przechwycenie tożsamości i oszuści na portalach społecznościowych

Okazje, zaskakująco dobre oferty i wygrane w konkursach

Moduł 12: Szkodliwe oprogramowanie, "robaki"

Czym jest Bloatware i jak można się go pozbyć

Jak sprawdzić czy jakiś plik jest bezpieczny

Jak poznać się, że program spowalnia komputer