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.

2. Ogólny opis przedmiotu zamówienia

2.1. Przedmiot zamówienia obejmuje systemy cyberbezpieczeństwa w zakresie:

Lp.	OPIS
1	Ochrona brzegu sieci – dostawa i wdrożenie klastra składającego się z dwóch urządzeń UTM, konfiguracja polityk bezpieczeństwa, inspekcja ruchu SSL, segmentacja sieci LAN.
2	Usługa katalogowa - dostawa licencji, wdrożenie usługi katalogowej, konfiguracja polityk bezpieczeństwa.
3	Podłączenie komputera do domeny - konfiguracja DNS, przyłączenie do drzewa AD
4	Migracja danych z profilu użytkownika lokalnego na profil domenowy
5	Dostawa i wdrożenie serwera do przechowywania kopii zapasowych (serwer backupowy)
6	Dostawa i wdrożenie biblioteki taśmowa wraz z taśmami LTO-8
7	Dostawa i wdrożenie oprogramowania do tworzenia kopii zapasowych, opracowanie i wdrożenie polityki backup 3-2-1.
8	Dostawa i wdrożenie przełączników sieci LAN, wdrożenie systemu NAC.
9	Dostawa, wdrożenie systemu SIEM (Security Information and Event Management) z usługą zewnętrznego SOC - Centrum Operacji Bezpieczeństwa (Security Operations Center)
10	Aktualizacja polityki Zarządzania Bezpieczeństwem Informacji dla Gminy.
11	Szkolenia z zakresu Cyberbezpieczeństwa dla administratorów.

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 do 3 miesięcy od daty zawarcia umowy.

3.1. Organizacja wdrożenia

1. Założenia podstawowe:
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. Wykonawca w Harmonogramie wdrożenia musi w szczególności uwzględnić podział na zadania takie jak: projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
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).
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.
6. Wykonawca zobowiązany jest przeprowadzić prace wdrożeniowe przedmiotu zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
7. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie przedmiotu zamówienia.
8. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.

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.
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.

3.1 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.

3.2 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, migrowanych systemów Zamawiającego 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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. Ochrona brzegu sieci – dostawa i wdrożenie klastra składającego się z dwóch urządzeń UTM, konfiguracja polityk bezpieczeństwa, segmentacja sieci LAN.

Zamawiający oczekuje dostarczenia dwóch nowych, identycznych urządzeń klasy UTM wraz z gwarancją oraz dostępem do aktualizacji oprogramowania zabezpieczającego przez okres min. 24 miesięcy. Wykonawca musi opracować: projekt wymiany obecnych urządzeń brzegowych (tj. urządzeń pracujących na styku sieci LAN oraz WAN), projekt podziału sieci LAN na wirtualne podsieci, harmonogram wdrożenia oraz zakres wdrożenia, który przedstawi Zamawiającemu do akceptacji. Wykonawca musi: wdrożyć dostarczane urządzenia, w tym min. skonfigurować je do pracy w klastrze wysokiej dostępności; wykonać instruktaż z zakresu administracji dostarczonych urządzeń UTM; opracować dokumentację powykonawczą; świadczyć rozszerzone wsparcie serwisowe przez okres min. 24 miesięcy. Wymagany klaster dwóch urządzeń UTM musi spełniać wszystkie wymienione poniżej funkcje sieciowe oraz bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.

1.1 Urządzenie klasy UTM z gwarancją i wsparciem na okres min. 36 miesięcy – 2 sztuki

System UTM realizujący funkcję Firewall musi zapewniać pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System musi umożliwiać budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Musi być możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.

4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
   - 10 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1400 tys. jednoczesnych połączeń oraz min. 90 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3500 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 7 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2,4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 200 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure.
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - OpenStack.
   - VMware NSX.
   - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode (GCM).
   - Obsługa protokołu Diffie-Hellman grup 19, 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.

- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łącz WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5 000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2 000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagany jest pakiet licencji zawierający funkcjonalności minimalne: kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres min. 36 miesięcy.

Gwarancja oraz wsparcie

1. Urządzenia muszą być objęte standardowym serwisem gwarancyjnym producenta przez okres min. 36 miesięcy.
2. Dodatkowo wymagana jest rozszerzona gwarancja na urządzenia, polegająca na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement) w czasie nie dłuższym niż 24 godziny w dni robocze, dla zgłoszeń utworzonych do godz. 14:00 w dni robocze.
3. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie Zamawiającego, realizowana przez producenta lub autoryzowanego partnera w języku polskim.

1.2 Zakres wdrożenia.

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

a) konfigurację ogólną 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 70 obiektów,
i) przeniesienie istniejących reguł firewall oraz NAT – około 30 reguł,
j) przeniesienie konfiguracji IPSec VPN,
k) przeniesienie filtrów URL oraz SSL, konfiguracja inspekcji SSL – około 60 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 urządzeń UTM
m) konfiguracja przesyłania logów do posiadanych przez Zamawiającego instancji zbierających i przechowujących logi,
n) wykonanie projektu podziału sieci LAN Zamawiającego
o) utworzenie wirtualnych sieci LAN, konfiguracja przełączników, urządzeń UTM, konfiguracja polityk

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

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

1.3 Instruktaż

Zamawiający wymaga przeprowadzenia instruktażu dla swoich administratorów zgodnie z poniższym opisem:
Instruktaż podstawowy (wdrożeniowy) – odbędzie się przy okazji wdrożenia i konfiguracji systemu UTM w siedzibie Zamawiającego, jego przedstawiciele będą uczestniczyć w wykonywanych pracach. Instruktaż z zakresu wdrożonego systemu UTM (powdrożeniowy), dla grupy od 2 do 5 osób, średniozaawansowanych (wcześniej pracujących na systemach UTM), minimum 2 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

Instruktaż powdrożeniowy musi zawierać elementy warsztatowe i opierać się na zadaniach praktycznych realizowanych na oferowanych systemach UTM.

Instruktaż musi być prowadzony przez praktyka posiadającego co najmniej 3-letnie doświadczenie w zakresie wdrażania systemów UTM oraz posiadającego ważny certyfikat inżynierski wystawiony przez producenta UTM w zakresie administracji UTM.

1.4 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.

1.5 Opcjonalne rozszerzone wsparcie serwisowe świadczone przez okres 12 miesięcy (usługa punktowana dodatkowo)

Opcjonalnie Wykonawca może zaoferować rozszerzone wsparcie techniczne gwarantujące 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 12 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 27001. System UTM 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.
- Łączny czas wsparcia do wykorzystania na w/w usługi: do 12 roboczogodzin w roku kalendarzowym

Wsparcie techniczne inżyniera będzie realizowane zdalnie, świadczone w języku polskim. W ramach realizacji usługi zostanie wyznaczony dedykowany inżynier legitymujący się certyfikatem, wystawionym przez producenta oferowanego systemu UTM, z zakresu administracji, konfiguracji systemów UTM. Wsparcie powdrożeniowe musi być świadczone 5 dni w tygodniu w godzinach 8:00 – 17:00 – kontakt z inżynierem poprzez dedykowaną tylko dla Zamawiającego infolinię – dostęp po podaniu hasła lub PIN-u.

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. Wymagany jest czas reakcji nie dłuższy niż 2 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 wystawionymi przez producentów urządzeń UTM.

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. Usługa katalogowa: dostawa licencji, wdrożenie usługi katalogowej, konfiguracja polityk bezpieczeństwa.

2.1 Wymagania ogólne w ramach zadania Usługa Katalogowa:

- Dostarczenia min. 2 licencji SSO, po jednej dla każdego z dwóch serwerów fizycznych (hostów) Zamawiającego, gdzie każdy z serwerów posiada procesory o łącznej liczbie rdzeni 16 lub mniej. Typ licencji musi umożliwiać przeniesienie jej na inny serwer fizyczny (host) w przyszłości (np. w przypadku awarii lub wymiany serwera, hosta), musi umożliwiać uruchomienie min. 2 maszyn wirtualnych SSO na serwerze
- Dostarczenia min. 50 licencji dostępowych dla użytkowników (User CAL)
- Utworzenia projektu opisującego wdrożenie usługi katalogowej opartej o harmonogram
- Wdrożenia usługi katalogowej zgodnie z przedstawionym, zaakceptowanym projektem
- Wdrożenia polityk bezpieczeństwa opartych o dobre praktyki, doświadczenie Wykonawcy oraz zalecenia producenta oprogramowania
- Podłączenia wszystkich stacji roboczych Zamawiającego do domeny
- Migracji profili lokalnych do nowych profili domenowych
- Przeprowadzenia instruktażu dla administratorów Zamawiającego
- Opracowania i dostarczenia dokumentacji powdrożeniowej

Wdrożenie Usługi Katalogowej będzie poprzedzone utworzeniem projektu opisującego wdrożenie usługi katalogowej począwszy od zaplanowania liczby serwerów na potrzeby usługi katalogowej oraz serwerów plików zapewniającej, w przypadku awarii pojedynczego serwera, ciągły dostęp do usługi katalogowej, a w szczególności do mechanizmów uwierzytelniania oraz rozwiązywania nazw oraz serwera plików, poprzez harmonogram, a skończywszy na dokumentacji powdrożeniowej.

Wymagana jest instalacja systemów operacyjnych serwerów w taki sposób, aby w łatwy sposób możliwe było włączenie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego.

Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem.

Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.

Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi:

- Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości;
- Śledzenie zmian dotyczących tworzenia, usuwania obiektów.

Zamawiający wymaga skonfigurowania dwóch stacji zarządzających. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów).

Konfiguracja globalnej polityki haseł dla domeny.
Konfiguracja polityki haseł dla kadry zarządzającej.
Szczegółowe dane zostaną przekazane na etapie konfiguracji.
Stworzenie skryptów służących do tworzenia struktury usługi katalogowej. Po oddaniu wdrożonego systemu do eksploatacji konieczne będzie tworzenie nowych kont użytkowników, grup zabezpieczeń oraz jednostek organizacyjnych.

Zamawiający wymaga wygenerowania kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń za pomocą opracowanych skryptów.

Skonfigurowanie mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows. Zamawiający wymaga skonfigurowanie mapowania dysków sieciowych za pomocą zasad grup na dwa sposoby:

Z wykorzystaniem skryptów logowania.

Z wykorzystaniem mechanizmów zaimplementowanych w systemach Microsoft Windows 10 i nowszych. Wymagane jest także skonfigurowanie automatycznej instalacji niezbędnych składników na stacjach klienckich. Zamawiający nie dopuszcza instalacji wymaganych składników ręcznie. Zamawiający wymaga zintegrowania z urządzeniem UTM oraz weryfikację nawiązywania połączenia poprzez nazwę użytkownika z domeny.

2.2 Uruchomienie i skonfigurowanie serwera plików oraz wydruków

Serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów mechanizmów zwiększających dostępność danych poprzez zastosowanie technologii replikacji systemu plików. Konieczność taka podyktowana jest zapewnieniem ciągłości dostępu do krytycznych danych Wnioskodawcy w przypadku awarii jednego z serwera plików. Zastosowane mechanizmy replikacji systemu plików muszą zapewniać:

- Replikację multi-master z rozwiązywaniem konfliktów;
- Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki.

Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu.

Na serwerach plików muszą być skonfigurowana przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów. Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików. Konieczne jest także skonfigurowanie mechanizmów raportujących.

Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty” oraz „Pulpit” ze stacji roboczych na serwery plików. Funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego.

Zamawiający wymaga opracowania koszyka dozwolonych aplikacji wraz z implementacją polityk globalnych ograniczających dostęp do aplikacji z wykorzystaniem np.: dedykowanych ustawień związanych z polityką kontroli uruchomienia aplikacji.

Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi:

- Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder;
- Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder;
- Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień.

Zamawiający wymaga uruchomienia serwera wydruków oraz podłączenia i skonfigurowania 3 wybranych drukarek sieciowych. Zamawiający wymaga opracowania i skonfigurowania odpowiednich polityk globalnych mapujących odpowiednie drukarki użytkownikom. Niedopuszczalne jest przyłączenie wszystkim użytkownikom wszystkich dostępnych drukarek. Użytkownicy powinni mieć przyłączone drukarki znajdujące się najbliżej jego komputera.

2.3 Przygotowanie infrastruktury PKI

Zamawiający wymaga przygotowania i uruchomienia wewnętrznej infrastruktury PKI. Zamawiający posiada stacje robocze pracujące w oparciu o następujące systemy operacyjne: Windows 10 i nowsze.
Wymagana przez Zamawiającego konfiguracja musi uwzględniać:

- Zaplanowanie i uruchomienie wewnętrznej struktury CA;
- Konfigurację szablonów certyfikatów;
- Wydanie certyfikatów dla serwerów oraz stacji roboczych;
- Zastosowanie mechanizmów bezpieczeństwa poprzez możliwość backupu archiwizacji kluczy prywatnych wydawanych certyfikatów;
- Wskazanie wszystkich możliwych dróg publikacji list CRL;

2.4 Wymagania minimalne dla serwerowych systemów operacyjnych (SSO) przeznaczonych dla Usługi Katalogowej:

Każda z licencji musi uprawniać do uruchamiania na serwerze Zamawiającego (max. 16 rdzeni ma serwer) min. dwóch maszyn wirtualnych oferowanego systemu operacyjnego. 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,
        j) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

2.5 Wymagania minimalne dla licencji dostępowych do usługi katalogowej.

Wraz z licencjami na Serwerowy Systemem Operacyjnym SSO należy dostarczyć licencje dostępowe dla min. 50 użytkowników, które umożliwią konkretnemu użytkownikowi dostęp do serwerów z SSO z dowolnego urządzenia. Licencje dostępowe muszą umożliwiać dostęp do: usługi katalogowej, plików na dyskach sieciowych serwerów oraz usługi drukowania sieciowego.

3. Podłączenie komputera do domeny - konfiguracja DNS, przyłączenie do drzewa AD

Zamawiający wymaga dołączenia wszystkich 50 stacji roboczych do domeny oraz przeszkolenia personelu Zamawiającego do samodzielnego podłączania stacji oraz migracji profili użytkowników.

Zamawiający wymaga uruchomienia i skonfigurowania usług dostępnych w dostarczonych systemach operacyjnych serwerów umożliwiających zarządzanie aktualizacjami stacji roboczych i serwerów według założeń:

- Aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet;
- Administrator zatwierdza aktualizacje do instalacji;
- Stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu.

Zamawiający wymaga skonfigurowania co najmniej następujących parametrów:

- Systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje;
- Kategorii aktualizacji;
- Grup komputerów;
- Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów;
- Zasad automatycznego zatwierdzania nowych aktualizacji;
- Mechanizmów raportowania (e-mail).

4. Migracja danych z profilu użytkownika lokalnego na profil domenowy

W procesie dołączania stacji roboczych do domeny konieczne jest przeprowadzenie migracji danych z profilu lokalnego każdego użytkownika na jego nowy profil domenowy. Migracja ma na celu zachowanie specyficznych ustawień lokalnych kont użytkowników (między innymi zachowanie ustawień aplikacji oraz poczty elektronicznej). Po zalogowaniu się na konto domenowe, użytkownik powinien mieć zachowaną tapetę oraz ustawienia pulpitu, dotychczas działające aplikacje powinny działać jak wcześniej bez potrzeby ponownej konfiguracji.

5. Dostawa i wdrożenie serwera do przechowywania kopii zapasowych (serwer backupowy)

Minimalne wymagania dla serwera przeznaczonego do przechowywania kopii zapasowych:

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1.	Obudowa	Obudowa o wysokości max. 2U dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji do min. 12 dysków 3,5” oraz opcjonalnego montażu dwóch dodatkowych dysków 2,5” hot-swap.
2.	Procesory	Zainstalowany min. jeden procesor o taktowaniu min. 2,9Ghz i maksymalnej liczbie rdzeni 16 oraz wyniku wydajności w teście SPECrate®2017 Integer Rates Baseline nie niższym niż 150 pkt. dla testowanej konfiguracji. Moc cieplna (TDP) procesora nie może przekraczać 160W.
3.	Pamięć RAM	Zainstalowane min. 256 GB pamięci ECC w nie więcej niż ośmiu modułach. Możliwość rozbudowy pamięci do min. 4TB.
4.	Płyta główna	Dedykowana do pracy w oferowanym serwerze.
5.	Złącza PCIe	Wymagane nie mniej niż trzy wolne (nieobsadzone) złącza PCIe Gen4, z czego nie mniej niż jedno pracujące z prędkością x16. Wymagane min. 2 wolne złącza PCIe Gen4 pracujące z prędkością x8.

6.	Dysk twardy	Zainstalowanych min. 8 dysków SATA Hot-Swap o pojemności min. 16TB każdy, dyski muszą być przeznaczone do pracy w serwerach, do pracy ciągłej.
7.	Karta sieciowa	Zainstalowana karta min. 2 portowa SFP+ 10 Gbit wraz z modułami SFP+
8.	Karta graficzna	Zintegrowana z układem zdalnego zarządzania karta graficzna.
9.	Porty	Min. 1 port Ethernet RJ-45 dedykowany dla interfejsu zdalnego zarządzania, Min. 4 porty USB 3.1, w tym min. 1 port z przodu obudowy oraz min. 1 port na płycie głównej. Min. 1 port VGA (15-pin video), Możliwość instalacji portu szeregowego podłączonego do płyty głównej bez użycia jakichkolwiek adapterów do innych portów.
10.	Kontroler dyskowy	Min. Jeden kontroler SAS 12G RAID 0,1,5,6,10,50,60 z min. 4GB pamięci cache obsługujący wszystkie 8 zatok dyskowych, kontroler musi być wyposażony w moduł ochrony danych pamięci podręcznej RAID. Zainstalowany dodatkowy kontroler RAID 0,1 z dwoma dyskami SSD min. 480GB każdy.
11.	Karta FC	Zainstalowana karta min. 1 portowa Fibre Channel min. 8Gbit do podłączenia biblioteki taśmowej.
12.	Zasilanie	Zainstalowane min. dwa redundantne zasilacze hot-plug, każdy o mocy maximum 1000W i posiadające certyfikat efektywności energetycznej min. Titanium.
13.	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.
14.	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 i 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)
15.	Wsparcie dla systemów	Microsoft Windows Server min. 2022, 2025 Red Hat Enterprise Linux (RHEL) 8.0 SUSE Linux Enterprise Server (SLES) min. 15 VMware ESXi min. 8.0
16.	Gwarancja	Minimum 3-letnia gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2 godzinnym czasem reakcji, w godzinach 8:00-17:00, z czasem rozpoczęcia naprawy w następnym dniu roboczym (NBD) w miejscu instalacji. Uszkodzone dyski staja się własnością Zamawiającego. Usługa wsparcia technicznego musi być świadczona przez autoryzowany serwis producenta oferowanych urządzeń. Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy 6 godzin i pozostawieniem uszkodzonych dysków u zamawiającego.

6. Dostawa i wdrożenie biblioteki taśmowej wraz z taśmami LTO-8

Minimalne wymagania dla biblioteki taśmowej:

Właściwość	Parametry minimalne
Obudowa	Obudowa typu Rack o wysokości max. 2U
Obsługiwane napędy	Min. LTO-7, LT-8, LTO-9
Obsługiwane interfejsy napędów	Min. 8 Gb Fibre Channel, 12 Gb/sec SAS (LTO-9), 6 Gb/sec SAS (LTO-8, LTO-7)
Typ zainstalowanych napędów LTO	Min. LTO-8
Ilość napędów	Min. 1
Technologie obsługiwanych taśm	Min. LTO-7, LT-8, LTO-9
Interfejs komunikacyjny napędu	Fibre Channel min. 8Gbps
Maksymalna, możliwa pojemność danych	Min. 280 TB natywnie oraz min. 700TB z użyciem kompresji danych
Maksymalny transfer danych	Min. 2.14 TB na godzinę dla konfiguracji z dwoma napędami LTO-8
Ilość slotów na taśmy	Min. 24
Panel diagnostyczny	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie urządzenia
Możliwość szyfrowania danych	Min. Kluczem AES256
Złącza	Min. 1 x RJ45 oraz min. 1x USB
Zarządzanie	- komunikacja poprzez interfejs RJ45 - wbudowana diagnostyka - wsparcie dla IPv4 i Ipv6 - sterowniki do Windows Serwer 2008/2012 R2/2016/2019 /2022/2025
Wyposażenie	Wraz z urządzeniem należy dostarczyć: 14 taśm LTO-8 RW, 7 taśm LTO-9 WORM, taśmę czyszczącą, etykiety dla taśm, kable zasilające oraz przewody połączeniowe (danych).
Wsparcie techniczne	Minimum 3-letnia gwarancja producenta na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2 godzinnym czasem reakcji na zgłoszenie. Rozpoczęcie naprawy w miejscu instalacji w następnym dniu roboczym. Usługi gwarancji oraz wsparcia technicznego muszą być świadczone przez autoryzowany serwis producenta oferowanych urządzeń. Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy do 6 godzin w miejscu instalacji.
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. Oferowany napęd LTO musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla

	systemów Windows Server. Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

7. Dostawa i wdrożenie oprogramowania do tworzenia kopii zapasowych, opracowanie i wdrożenie polityki backup 3-2-1.

Zadanie Backup 3-2-1 będzie składało się z 7 części:

1. Konfiguracja serwera kopii zapasowych, biblioteki taśmowej wraz z taśmami, licencji systemu do tworzenia kopii zapasowych, doposażenie serwerów produkcyjnych Zamawiającego w karty sieciowe dwuportowe z portami SFP+
2. Montaż sprzętu w wskazanej szafie rack, konfiguracja, uruchomienie; instalacja, konfiguracja dostarczonego oprogramowania do backupu
3. Opracowanie polityki backupu 3-2-1 w oparciu o dostarczony sprzęt, oprogramowanie oraz sprzęt Zamawiającego, opracowanie Harmonogramu, utworzenia zadań backupowych
4. Min. tygodniowy (7 dniowy) nadzór nad systemem tworzenia kopii wg Harmonogramu
5. Przeprowadzenie testów odtworzeniowych z tworzonych kopii zapasowych wraz z administratorami Zamawiającego
6. Przeprowadzenie instruktażu z obsługi wdrożonego rozwiązania dla administratorów Zamawiającego
7. Opracowanie dokumentacji powykonawczej

System backup wdrożony zostanie w taki sposób, aby był zgodny z zasadą 3-2-1. Jest to to strategia tworzenia kopii zapasowych danych zaprojektowana w celu zapewnienia możliwości szybkiego odzyskania i przywrócenia danych w przypadku incydentu utraty danych. W szczególności ta strategia tworzenia kopii zapasowych musi zapewniać posiadanie trzech niezależnych kopii danych:

- Pierwsza kopia będzie przechowywana lokalnie na wewnętrznych dyskach twardych serwera backupowego,
- Druga kopia będzie przechowywana na taśmach LTO umieszczonych w bibliotece LTO,
- Trzecia kopia danych będzie przechowywana na taśmach LTO (zarówno wielokrotnego zapisu RW jak jednokrotnego zapisu WORM), przy czym taśmy będą umieszczane w bezpiecznym miejscu poza budynkiem Gminy (kopia wyniesiona)

Celem wdrożenia strategii tworzenia kopii zapasowych 3-2-1 jest zmniejszenie potencjalnego wpływu „pojedynczego punktu podatności na awarię". Oznacza to, że jeśli jedno z urządzeń ulegnie awarii i znajdująca się na nim kopia danych zostanie utracona, do dyspozycji są jeszcze pozostałe dwie kopie danych. Wyniesienie taśm z kompletną kopia zapasową poza budynek Gminy umożliwia natomiast odzyskanie kluczowych danych Zamawiającego w przypadku awarii dużych rozmiarów bądź fizycznego zniszczenia siedziby Zamawiającego (pożar, wybuch, działania terrorystyczne, klęski żywiołowe).

Kluczowym elementem wdrożenia jest opracowanie polityki backupowej, w której opisane zostaną wszystkie zasady, według których będą tworzone kopie zapasowe z wyszczególnieniem kto je wykonuje, kiedy, gdzie przenoszone będą nośniki danych oraz kto będzie odpowiedzialny za poszczególne etapy wykonywania czynności, kto będzie odpowiedzialny za monitoring i weryfikację tworzonych kopii zapasowych.
Polityka backup oraz uruchomione środowisko backup misi być również zgodne z rekomendacją dotycząca wykonywania kopii zapasowych opublikowaną przez Ministerstwo, która dostępna jest pod adresem:
https://www.gov.pl/web/baza-wiedzy/tworzenie-zapasowych-kopii-danych

Wymagany zakres prac do wykonania w ramach zadania Backup 3-2-1:

1. Dostawa serwera przeznaczonego do przechowywania kopii zapasowych (serwer backupowy); biblioteki taśmowej LTO wraz z taśmami; niezbędnych licencji oprogramowania do tworzenia kopii zapasowych z wsparciem technicznym oraz dostępem do aktualizacji przez okres min. 24 miesięcy,

2. Montaż serwera oraz biblioteki w wskazanej szafie rack; podłączenie biblioteki do serwera poprzez interfejs Fibre Channel, konfiguracja serwera do pracy w infrastrukturze Zamawiającego, uruchomienie; instalacja taśm LTO w bibliotece, konfiguracja biblioteki; aktualizacja firmware serwera oraz biblioteki LTO; instalacja hypervizora na serwerze backupowym na potrzeby dostarczonego oprogramowania; konfiguracja maszyny wirtualnej dla systemu backupu; instalacja serwera/konsoli zarządzającej kopiami zapasowymi;
3. Opracowanie polityki backupu 3-2-1 w oparciu o:
   - dostarczony sprzęt, oprogramowanie,
   - sprzęt Zamawiającego
   - przeprowadzoną analizę środowiska Zamawiającego (liczba maszyn wirtualnych, krytyczność systemu, wielkość maszyny wirtualnych czy ilość danych na serwerach fizycznych

   Na podstawie zebranych danych oraz wymagania Zamawiającego, Wykonawca opracuje Harmonogram tworzenia kopii zapasowych z podziałem na maszyny fizyczne/wirtualne; określeniem: częstotliwości tworzenia kopii pełnych, częstotliwości tworzenia kopii przyrostowych, częstotliwości tworzenia kopii na taśmach WORM, częstotliwości weryfikacji poprawności tworzonych kopii zapasowych, częstotliwości i zakresu przeprowadzania testów odtworzeniowych. Na podstawie Harmonogramu Wykonawca skonfiguruje zadania backupowe na dostarczonym oprogramowaniu. Uruchomi tworzenie kopii zapasowych na serwerze backupowym oraz na taśmach LTO. Na żądanie Zamawiającego Wykonawca skonfiguruje dodatkowo tworzenie kopii zapasowych na wskazanych przez Zamawiającego zasobach dyskowych lub chmurowych.
4. Począwszy od dnia uruchomienia tworzenia kopii zapasowych, Wykonawca będzie zobowiązany do monitorowania pracy systemu backupowego przez min. 7 dni. Nadzór będzie miał na celu potwierdzenie prawidłowości wykonywanych kopii na serwerze oraz taśmach LTO; potwierdzenie tworzenia kopii zgodnie z Harmonogramem.
5. Po zakończeniu pełnego cyklu tygodniowego tworzenia kopii zapasowych zgodnie z Harmonogramem, Wykonawca odtworzy wszystkie serwery fizyczne/maszyny wirtualne z kopii zapasowych na serwerze backupowym. Testy odtworzeniowe będą przeprowadzone przy udziale administratora Zamawiającego
6. Po okresie monitorowania, na podstawie potwierdzenia przez Zamawiającego zgodności wykonywanych kopii zgodnie z Harmonogramem oraz na podstawie zakończonych sukcesem testów odtworzeniowych, Wykonawca przeprowadzi instruktaż z zakresu:
   - bieżącej obsługi systemu, podstaw administracji,
   - modyfikacji Harmonogramu i zadań backupowych,
   - czynności sprawdzania prawidłowości wykonywanych kopii zapasowych na serwerze oraz taśmach LTO,
   - procedury i czynności przeprowadzania testów odtworzeniowych,
7. Ostatnim etapem wdrażania systemu backupu 3-2-1 jest opracowanie dokumentacji powykonawczej, która będzie zawierać opis wszystkich wykonanych prac, niezbędne dane konfiguracyjne, opis polityki backupowej wraz z harmonogramem oraz instrukcjami umożliwiającymi samodzielne użytkowanie, administrowanie wdrożonym środowiskiem przez Zamawiającego.

7.1 Minimalne wymagania dla oprogramowania do tworzenia kopii zapasowej:

W ramach realizacji zadania Wykonawca dostarczy licencje bezterminowe z wsparciem technicznym przez okres min. 24 miesięcy dla 4 procesorów serwerów fizycznych Zamawiającego, spełniające poniższe wymagania minimalne:

1. Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji

a. Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
b. Vmware vSphere min. w wersjach v5.5-7.0.3
c. Nutanix AHV 5.15, 5.20 (LTS)
d. Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012
e. Microsoft 365 (Exchange online, One Drive for Business, Sharepoint, Teams)

2. Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V

3. Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
   a. na serwerze Windows lub Linux
   b. jako maszyna wirtualna Vmware
   c. jako maszyna wirtualna Amazon
   d. na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital

4. Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS

5. Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania

6. Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).

7. Oprogramowanie ma umożliwiać wdrożenie schematu backupu według zasady 3-2-1

8. Oprogramowanie ma umożliwiać zapewnienie niezmienności kopii chroniąc przed oprogramowaniem ransomware z zastosowaniem niezmiennych kopii zapasowych (worm lub chmura) oraz ze szczeliną powietrzną (rozłączane taśmy, as)

9. Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności

10. W ramach dostawy wymagane jest dostarczenie licencji na ochronę min. 6 gniazd procesorów w hostach Vmware lub Hyper-V

11. Dostarczona wersja oprogramowania i licencji, powinna mieć możliwość rozbudowy ilości chronionych zasobów w przyszłości

12. W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie minimum 36 miesięcy wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania

13. Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska

14. Oprogramowanie musi posiadać funkcje backupu i replikacji:
   a. Backup maszyn wirtualnych Vmware
   b. Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
   c. Backup maszyn wirtualnych Hyper-V
   d. Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu

e. Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
f. Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
g. Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
h. Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
i. Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych
j. Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
k. Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
l. Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji

15. Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
    a. Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
    b. Kompresja backupu, w tym konfigurowalny stopień kompresji
    c. Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne

16. Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
    a. Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
    b. Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
    c. Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji: Microsoft Exchange 2013, 2016, 2019
    d. Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
    e. Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki

17. Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V

18. Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania

19. Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji

20. Oprogramowanie musi posiadać poniższe funkcje:
    a. Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
    b. Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
    c. Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
    d. Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
    e. Microsoft Exchange, MS Active Directory, MS SQL

f. Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.

21. Oprogramowanie do backupu musi pozwalać na:
    a. Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
    b. Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
    c. Backup z pominięciem sieci LAN dzięki opcjom dostępu bezpośredniego w sieciach SAN
    d. Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
    e. Wsparcie dla urządzeń oferujących dodatkową deduplikację danych

22. Oprogramowanie musi pozwalać na następujące formy zarządzania:
    a. Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
    b. Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
    c. Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania
    d. wielu harmonogramów dla pojedynczego zadania
    e. Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków, do których będzie robiony eksport.
    f. Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
    g. Oprogramowanie musi umożliwiać integrację z oferowaną usługą katalogową z zadania nr 3.

7.2 Instalacja, konfiguracja systemu do tworzenia kopii zapasowej

Wykonawca dokona konfiguracji dostarczonego systemu kopii bezpieczeństwa, która będzie obejmować:

1. instalacji i konfiguracji dostarczonego systemu kopii bezpieczeństwa na dostarczonym serwerze backupowym
2. skonfigurowanie przestrzeni dla kopii bezpieczeństwa na dostarczonym serwerze backupowym
3. konfigurację miejsc przechowywania, w tym biblioteki taśmowej
4. konfigurację polityki składowania oraz harmonogramów
5. konfigurację zabezpieczeń wewnętrznych, w tym kopii ratunkowej (ang. disaster recovery) systemu kopii bezpieczeństwa
6. instalację i konfigurację dodatkowych maszyn wirtualnych klientów, jeśli są wymagane, w środowisku Zamawiającego
7. konfigurację kopii zapasowych maszyn wirtualnych Zamawiającego dla dwóch repozytoriów: serwera backupowego dyskowej i biblioteki taśmowej
8. sposób wymiany nośników LTO w dostarczonej bibliotece taśmowej;
9. instalację niezbędnych agentów dla środowiska bazodanowego Zamawiającego i konfigurację kopii zapasowych do 2 baz danych
10. konfigurację automatycznej weryfikacji kopii bezpieczeństwa maszyn wirtualnych Zamawiającego.
11. konfigurację powiadomień i codziennych raportów
12. Oferowany system tworzenia kopii zapasowych musi umożliwiać wysyłanie zaszyfrowanych kopi zapasowych do zasobów chmurowych.

Wykonawca opracuje i przedstawi Zamawiającemu dokumentację powykonawczą zawierającą:

1. podstawowe procedury obsługowe
2. opis skonfigurowanych polityk i harmonogramów
3. opis odtworzenia maszyn wirtualnych
4. opis odtworzenia pojedynczego pliku
5. opis odtworzenia bazy danych Zamawiającego
6. opis wymiany nośników LTO w dostarczonej bibliotece
7. opis sposobu aktualizacji systemu

Wykonawca przeprowadzi jednodniowy instruktaż stacjonarny w siedzibie Zamawiającego w czasie do 21 dni kalendarzowych od daty zakończenia wdrożenia dla 2 pracowników Zamawiającego, który obejmie co najmniej:

1. podstawową wiedzę dotycząca systemu
2. dodawania i usuwanie z systemu maszyn wirtualnych
3. dodawanie i usuwanie z systemu fizycznych urządzeń
4. zagadnienia dotyczące zmian platform wirtualizacji
5. możliwości dodawania, zmiany i usuwania kolejnych miejsc przechowywania kopii zapasowych
6. procedurę aktualizacji systemu
7. procedurę odtworzenia konfiguracji po awarii dysków głównego serwera backupu, np. po ponownej instalacji hypervizora, systemu operacyjnego serwera

8. Dostawa i wdrożenie przełączników sieci LAN, wdrożenie systemu NAC.

Obecnie używane przez Zamawiającego przełączniki tworzące sieć LAN są przestarzałe, nie ma wydzielonych przełączników do rdzenia sieci, brak możliwości instalacji nowego oprogramowania wewnętrznego. Przedmiotem zadania jest dostawa 2 nowych przełączników umożliwiających utworzenia rdzenia sieci LAN. Ponadto należy dostarczyć 4 nowe przełączniki dostępowe. Wraz z przełącznikami należy dostarczyć wszystkie niezbędne moduły SFP+ oraz przewody połączeniowe umożliwiające uruchomienie nowej sieci LAN. Następnie należy dostarczyć oraz wdrożyć system klasy NAC (Network Access Control) zgodnie z zaakceptowanym przez Zamawiającego projektem wdrożenia.

8.1 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	Min. 24 miesiące gwarancji w miejscu instalacji

8.2 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 stosu przełączników
- 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

8.3 Przełącznik sieciowy, zarządzalny dostępowy – 4 sztuki

Element konfiguracji	Wymagania minimalne
Fizyczne	Wysokość w szafie 19” – 1U, głębokość nie większa niż 150mm, możliwość montażu w szafie rack
Techniczne	Minimum 1 port ethernet 10/000BaseT Minimum 24 gigabitowe porty Ethernet, Minimum 2 porty SFP+ pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP) Minimum 1 port konsoli: RJ45
Wydajność	Pojemość matrycy przełączania: minimum 75Gbps Wydajność przełączania: minimum 35Gbps Tablica adresów MAC o wielkości minimum 16k pozycji
Procesor	Min. 1 procesor 800Mhz
Pamięć RAM	Min. 512 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	Min. 24 miesiące gwarancji w miejscu instalacji

8.4 Zakres wdrożenia przełączników dostępowych sieci LAN:

Wykonawca dostarczy nowe urządzenia, przedstawi projekt topologii sieci i wdrożenia przełączników dostępowych z uwzględnieniem połączeń do rdzenia sieci LAN Zamawiającego. Na podstawie zaakceptowanego projektu zainstaluje przełączniki w wskazanych przez Zamawiającego lokalizacjach i wykona przełączenia urządzeń podłączonych do starych przełączników na nowe. 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 przełączników na podstawie obecnej infrastruktury
- konfiguracja agregacji połączeń z przełącznikami rdzeniowymi
- konfiguracja syslog dla przełączników
- konfiguracja protokołu SNMP zgodnie z obecnym systemem monitoringu
- konfiguracja użytkowników administracyjnych przełączników zgodnie z wytycznymi bezpieczeństwa

8.5 Doposażenie serwerów produkcyjnych Zamawiającego w karty sieciowe z dwoma portami SFP+ 10Gbit

Wymiana przełączników sieci LAN i utworzenie nowego rdzenia sieci w oparciu o przełączniki sieciowe z portami 10Gbit umożliwiające utworzenie bardzo wydajnych połączeń pomiędzy kluczowymi zasobami Zamawiającego pozwala na znaczące skrócenie czasu tworzenia kopii zapasowych z serwerów produkcyjnych Zamawiającego. Podłączenie serwerów do rdzenia sieci LAN wymaga doposażenia tychże serwerów w karty sieciowe z portami SFP+. Zamawiający wymaga dostarczenia 3 kart sieciowych z wbudowanymi 2 portami SFP+ 10gbit wraz modułami 10Gbit oraz niezbędnymi przewodami połączeniowymi. Wykonawca dostarczy i zamontuje karty w serwerach, podłączy redundantnie do nowego rdzenia sieci, skonfiguruje karty do pracy w sieci LAN Zamawiającego. Wszystkie prace muszą się odbywać w oknie serwisowym: niedziela od godz. 20:00 do 5:00.

8.6 Dostawa, wdrożenie systemu NAC (Network Access Control).

Zamawiający wymaga dostarczenia systemu zabezpieczającego przed nieautoryzowanym dostępem do sieci LAN klasy NAC (Network Access Control) wraz z wsparciem technicznym gwarantującym dostępem do najnowszych wersji i poprawek przez okres min. 24 miesięcy. Zamawiający wymaga wdrożenia oferowanego systemu w taki sposób, aby możliwe było używanie systemu z wymaganą poniżej funkcjonalnością. W ramach wdrożenia Wykonawca musi skonfigurować wszystkie urządzenia Zamawiającego do prawidłowej współpracy z wdrażanym systemem. System kontroli dostępu musi charakteryzować się następującymi cechami:

- Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
- System musi odsługiwać minimum 150 urządzeń klienckich (w tym gości) w trybie HA – klaster dwóch maszyn wirtualnych pracujących w trybie wysokiej dostępności (redundancja). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia
- Musi posiadać wbudowany serwer Radius
- Musi wspierać RADIUS VSA co najmniej niżej wymienionych producentów, w tym:
    - Cisco Systems
    - D-Link
    - Alcatel-lucent
    - AlliedTelesis
    - HPE Aruba / ProCurve
    - Huawei Networks
    - Fortinet
    - PaloAlto Networks

    - Mikrotik
    - Juniper
    - Netgear
- System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN.
- System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.
- Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
- Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych
    - Microsoft Active Directory
    - Radius
    - LDAP
    - Google Workspace
    - Azure Active Directory
    - OAuth 2
    - SAML
    - Eduroam
- Musi obsługiwać metody profilowania (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie):
    - DHCP
    - TCP
    - MAC OUI
    - SNMP
- Wspierać min poniższe protokoły:
    - Radius, Radius CoA, web authentication, SAML
    - EAP-FAST (EAP-MSCHAPv2, EAP-TLS)
    - PEAP (EAP-MSCHAPv2, EAP-TLS, EAP-PEAP)
    - EAP-TLS
    - 802.1X
    - NAC
    - Windows machine authentication
    - MAC Auth
    - WPA2-Enterprise
    - OCSP (Online Certificate Status Protocol)
    - SNMP (BRIDGE-MIB, Q-BRIDGE-MIB, IF-MIB, IEEE8021-PAE-MIB
- Funkcja integracji z systemem monitorowania sieci oraz analizy zdarzeń bezpieczeństwa w celu śledzenie ewentualnych niezgodności oraz naruszeń bezpieczeństwa (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie)
- Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:
    - Co najmniej ESXi 7.0
    - Co najmniej Windows 2016 i 2019 z Hyper-V
    - Co najmniej KVM on CentOS 7.7. Ubuntu 18.04, and Ubuntu 20.04
    - Co najmniej Amazon AWS (EC2)
    - Co najmniej Microsoft Azure

Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (150). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.
System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności

- Samodzielna rejestracja klientów gościnnych w oparciu o:
    - Adres e-mail

- Numer telefonu (wiadomość SMS)
  - Logowanie w oparciu o portale społecznościowe (Google, Facebook, Github, LinkedIn)
  - Funkcja integracji z systemami trzecimi poprzez API
  - Wspieranie rozwiązań mobilnych poprzez skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
  - Funkcja personalizacji strony gościnnej

Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

- System musi wspierać obsługę następujących systemów operacyjnych
  - MS Windows
  - Mac OS X
  - iOS
  - Android
  - Chromebook
  - Ubuntu
- Umożliwienie klientowi samorejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
- Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
- Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID
- Funkcja dostępu sponsorowanego opartego na rejestracji klienta oraz przesłanie odpowiedniego formularza do administratora systemu celem weryfikacji i zaakceptowania podanego żądania.

Wbudowane mechanizmy natywnej integracji oferowanego systemu NAC z oferowanym systemem SIEM (funkcjonalność opcjonalna, dodatkowo punktowana).

Na dostarczony system NAC należy udzielić Zamawiającemu 24 miesiące gwarancji. Gwarancja musi zapewniać dostęp do poprawek oprogramowania oraz wsparcia technicznego w trybie 8x5 na wszystkie elementy systemu. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta lub jego partnera. Zamawiający musi mieć możliwość tworzenia zgłoszeń serwisowych na dedykowanym portalu oraz poprzez dedykowaną polskojęzyczną infolinię zgłoszeniową.

Do oferowanego rozwiązania musi być dostępna dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.
Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji oferowanego oprogramowania, wymaganych w niniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłuższym niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.

9. Dostawa, wdrożenie systemu SIEM (Security Information and Event Management) z usługą zewnętrznego SOC - Centrum Operacji Bezpieczeństwa (Security Operations Center) oraz 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. 6 miesięcy (parametr punktowany dodatkowo).

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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)	Do 2
Windows Server	Do 15
Linux Server	Do 10
DNS, DHCP	Do 2
Systemy bezpieczeństwa np.: serwer systemu antywirusowego, web application firewall, inne	Program antywirusowy
Centralny Firewall / UTM	1
Pomocniczy Firewall / UTM	1
IPS / IDS	2
VPN	2
Przełączniki sieci LAN, punkty dostępowe WiFi	Do 10

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

9.8 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. 4 500

b) Zarządzanie logami: min. 2 lata

c) Liczba obsługiwanych urządzeń min. 200

d) Liczba zapisu zdarzeń na dobę: min 9000 MB

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

9.9 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) Licencja na zakup i serwis oprogramowania musi bazować na ilości aktywnie występujących w ruchu sieciowym adresów IP. Ilość adresów, objętych monitorowaniem: 150.
h) Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce
i) 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.
j) Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia oraz musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).
k) Konsola musi umożliwiać grupowanie takich samych zdarzeń w ramach jednego wpisu oraz podawać liczbę wystąpień identycznego zdarzenia
l) Konsola musi umożliwiać utworzenie zgłoszenia z dowolnego zdarzenia
m) Konsola musi posiadać dedykowany widok dla utworzonych zgłoszeń
n) Z poziomu konsoli musi być dostępna opcja zmiany statusu zgłoszenia
o) 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.

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

q) Serwer dedykowany musi posiadać opisane poniżej parametry minimalne:

L.p.	Element konfiguracji	Wymagane minimalne parametry techniczne
1.	Obudowa	Obudowa o wysokości max. 2U dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji do min. 12 dysków 3,5” oraz możliwość opcjonalnego montażu dwóch dodatkowych dysków 2,5” hot-swap.
2.	Procesory	Zainstalowany min. jeden procesor o taktowaniu min. 2,9Ghz i maksymalnej liczbie rdzeni 16 oraz wyniku wydajności w teście SPECrate®2017 Integer Rates Baseline nie niższym niż 150 pkt. dla testowanej konfiguracji. Moc cieplna (TDP) procesora nie może przekraczać 160W.
3.	Pamięć RAM	Zainstalowane min. 256 GB pamięci ECC w nie więcej niż ośmiu modułach. Możliwość rozbudowy pamięci do min. 4TB.
4.	Płyta główna	Dedykowana do pracy w oferowanym serwerze.
5.	Złącza PCIe	Wymagane nie mniej niż trzy wolne (nieobsadzone) złącza PCIe Gen4, z czego nie mniej niż jedno pracujące z prędkością x16. Wymagane min. 2 wolne złącza PCIe Gen4 pracujące z prędkością x8.
6.	Dysk twardy	Zainstalowane min. 3 dysk SATA Hot-Swap o pojemności min. 20TB każdy, dyski muszą być przeznaczone do pracy w serwerach, do pracy ciągłej. Zainstalowane min. 3 dyski SSD o pojemności 3,84TB
7.	Karta sieciowa	Zainstalowane min dwie karty sieciowe, każda wyposażona w min. 2 porty SFP+ 10Gbit wraz z modułami SFP+
8.	Karta graficzna	Zintegrowana z układem zdalnego zarządzania karta graficzna.
9.	Porty	Min. 1 port Ethernet RJ-45 dedykowany dla interfejsu zdalnego zarządzania, Min. 4 porty USB 3.1, w tym min. 1 port z przodu obudowy oraz min. 1 port na płycie głównej. Min. 1 port VGA (15-pin video), Możliwość instalacji portu szeregowego podłączonego do płyty głównej bez użycia jakichkolwiek adapterów do innych portów.
10.	Kontroler dyskowy	Min. Jeden kontroler SAS 12G RAID 0,1,5,6,10,50,60 z min. 4GB pamięci cache obsługujący wszystkie 8 zatok dyskowych, kontroler musi być wyposażony w moduł ochrony danych pamięci podręcznej RAID.
11.	Zasilanie	Zainstalowane min. dwa redundantne zasilacze hot-plug, każdy o mocy maximum 1000W i posiadające certyfikat efektywności energetycznej min. Titanium.
12.	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 o 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.
13.	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 i 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)
14.	Wsparcie dla systemów	Microsoft Windows Server min. 2022, 2025 Red Hat Enterprise Linux (RHEL) 8.0 SUSE Linux Enterprise Server (SLES) min. 15 VMware ESXi min. 8.0
15.	Gwarancja	Minimum 3-letnia gwarancja na części, robociznę i naprawę w miejscu instalacji typu On-Site z 2 godzinnym czasem reakcji, w godzinach 8:00-17:00, 7 dni w tygodniu, z czasem wykonania naprawy w następnym dniu roboczym (NBD) w miejscu instalacji. Możliwość rozszerzenia usługi gwarancyjnej do 5 lat realizowanej przez serwis producenta serwera z gwarantowanym czasem naprawy 6 godzin i pozostawieniem uszkodzonych dysków u zamawiającego.

9.10 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.

9.11 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,

9.12 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.

9.13 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 8:00 a 17:00.
<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>180 min</td><td>6 h</td></tr><tr><td>Wysoki</td><td>240 min</td><td>8 h</td></tr><tr><td>Średni</td><td>360 min</td><td>12 h</td></tr><tr><td>Niski</td><td>8 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 8:00 a 17:00.
<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>
<tr><td>Scenariusz użycia systemu bezpieczeństwa</td><td>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.</td></tr>
</table>

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; • 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; • 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

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;
	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; • 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.

9.14 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

9.15 Zespół SOC

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

1. Operatorzy I linii SOC – 3 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

9.16 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.

6.17 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 150 urządzeń wraz z wsparciem technicznym na okres min. 24 miesięcy. 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.

6.18 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 150 adresów IP wraz z wsparciem technicznym na okres min. 24 miesięcy. 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

6.19 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 – do 5 sztuk – maszyna wirtualna Windows / Linux – do 25 sztuk – serwer AD - 2 sztuki – Macierze / NASy – do 3 sztuk – Przełącznik rdzeniowy – 2 sztuki – Przełącznik dostępowy (LAN) – do 8 sztuk – Zasilacz awaryjny (UPS) – do 2 sztuk – Serwer bazodanowy - 1 sztuka – Serwer wirtualizacji (Host, hypervizor) – do 4 sztuk – Serwer Backupu - 1 sztuka

10. Aktualizacja polityki Zarządzania Bezpieczeństwem Informacji dla Gminy.

Przygotowanie aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwa Informacji zgodnie z wymaganiami normy PN–EN ISO/IEC 27001:2023 musi obejmować weryfikację i przebudowę dokumentacji wymaganej przez normę PN–EN ISO/IEC 27001:2023, a w szczególności:

- Politykę bezpieczeństwa informacji (jednostronicowy dokument – wymóg punktu 5.2 normy)
- Procedury systemowe wraz z wzorami formularzy, tj.:
  a) Identyfikację ryzyk i szans,
  b) Nadzór nad udokumentowanymi informacjami,
  c) Postępowanie z nośnikami,
  d) Kontrola dostępu,
  e) Zabezpieczenie i dostęp do infrastruktury,
  f) Czyste biurko i ekran,
  g) Kopie zapasowe,
  h) Komunikacja teleinformatyczna,
  i) Zarządzanie incydentami,
  j) Administrowanie i monitoring systemów informatycznych,
  k) Działania na wypadek dysfunkcji systemu - zarządzanie ciągłością działania,
  l) Audyt wewnętrzny,
  m) Niezgodności i działania korygujące,
  n) Zarządzanie dostawcami,
- Deklarację stosowania zabezpieczeń,
- Przewodnik po SZBI,
- Wzór Protokołu z przeglądu zarządzania.

Proces aktualizacji dokumentacji rozpocznie się w chwili zakończenia wdrażania systemów informatycznych z niniejszego postępowania.

11. Szkolenia z zakresu Cyberbezpieczeństwa dla administratorów.

Przedmiotem zadania jest pakiet dwóch 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 6 miesięcy licząc od dnia wystawienia i dostarczenia do Zamawiającego. Wymagane jest ustalenie z Zamawiającym terminu wystawienia każdego vouchera.

11.1 Szkolenie z zakresu administrowania systemem Windows Serwer – 2 vouchery na szkolenie ważne przez okres min. 6 miesięcy

W ramach postępowania Wykonawca dostarczy 2 Vouchery na szkolenie z używanego w Urzędzie systemu Windows Server 2022 ważne przez minimum 6 miesięcy. Szkolenie zostanie przeprowadzone w formie stacjonarnej w siedzibie wyznaczonej przez Wykonawcę jednak odległość między siedzibą Zamawiającego a miejscem przeprowadzenia szkolenia nie będzie większa niż 60 km. W przypadku gdy odległość między siedzibą Zamawiającego a miejscem wykonania szkolenia będzie wynosić więcej niż 60 km Wykonawca pokryje koszty

dojazdu, zakwaterowania i pełnego wyżywienia (śniadanie, obiad, kolacja). Zakwaterowanie w hotelu (co najmniej trzygwiazdkowym) nie może być oddalone od miejsca szkolenia więcej niż 15 minut pieszo. Wymagany czas trwania szkolenia wynosi 5 dni – łącznie 40 godzin lekcyjnych (jedna godzina lekcyjna trwa 45 minut). Celem szkolenia jest zdobycie wiedzy z zakresu: zarządzania tożsamością, siecią, pamięcią masową i obliczeniami przy użyciu systemu Windows Server oraz wiedzy na temat: scenariuszy, wymagań oraz opcji dostępnych w systemie Windows Serwer. Minimalny, przykładowy zakres szkolenia przedstawiono poniżej:

Moduł 1: Wprowadzenie do administracji systemu Windows Server

a. Wprowadzenie do systemu Windows Server
b. Wprowadzenie do systemu Windows Server Core
c. Wprowadzenie do zasad i narzędzi administracyjnych systemu Windows Server
d. **Ćwiczenie:** Wdrażanie i konfiguracja systemu Windows Server
   - Wdrażanie i konfiguracja systemu Server Core
   - Wdrażanie i stosowanie zdalnej administracji serwerami

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać system Windows Server, a także techniki wdrażania, serwisowania i aktywacji,
- Opisać system Windows Server Core, przedstawić jego specyfikę i sposoby administrowania nim.

Moduł 2: Usługi zarządzania tożsamością w systemie Windows Server

a. Wprowadzenie do AD DS
b. Wdrażanie kontrolerów domeny Windows Server
c. Wprowadzenie do usługi Azure AD
d. Wdrażanie zasad grupy
e. Wprowadzenie do usług certyfikatów Active Directory
f. **Ćwiczenie:** Wdrażanie usług zarządzania tożsamością i zasad grupy
   - Wdrażanie nowego kontrolera domeny w systemie Server Core
   - Konfigurowanie zasad grupy
   - Wdrażanie i korzystanie z usług certyfikatów
   - Wyjaśnienie podstaw zasad grupy i konfiguracja GPO w środowisku domenowym
   - Opis roli usług certyfikatów Active Directory i korzystanie z certyfikatów

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać AD DS w środowisku systemu Windows Server,
- Wdrażać kontrolery domeny w AD DS,
- Opisać Azure AD i korzyści płynące z integracji Azure AD z AD DS.

Moduł 3: Usługi infrastruktury sieciowej w systemie Windows Server

a. Wdrażanie i zarządzanie protokołem DHCP
b. Wdrażanie i zarządzanie systemem DNS
c. Wdrażanie i zarządzanie systemem IPAM
d. Usługi dostępu zdalnego w systemie Windows Server
e. **Ćwiczenie:** Wdrażanie i konfiguracja usług infrastruktury sieciowej w systemie Windows Server
   - Wdrażanie i konfiguracja protokołu DHCP
   - Wdrażanie i konfiguracja systemu DNS
   - Wdrażanie serwera proxy aplikacji sieci WWW

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać, wdrożyć i skonfigurować usługę DHCP,
- Wdrażać, konfigurować i zarządzać systemem DNS,
- Opisać, wdrożyć i zarządzać systemem IPAM.

Moduł 4: Serwery plików i zarządzanie pamięcią masową w systemie Windows Server

a. Woluminy i systemy plików w systemie Windows Server
b. Wdrażanie udostępniania w systemie Windows Server
c. Wdrażanie rozwiązania Storage Spaces (przestrzeni dyskowych) w systemie Windows Server
d. Wdrażanie deduplikacji danych

e. Wdrażanie interfejsu iSCSI
f. Wdrażanie rozproszonego systemu plików
g. **Ćwiczenie:** Wdrażanie rozwiązań pamięci masowej w systemie Windows Server
   - Wdrażanie deduplikacji danych
   - Konfiguracja magazynu iSCSI
   - Konfiguracja nadmiarowych przestrzeni dyskowych
   - Wdrażanie Storage Spaces Direct

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Wdrażać udostępnianie w systemie Windows Server,
- Wdrożyć technologię Storage Spaces,
- Wdrażać funkcję deduplikacji danych,
- Wdrażać pamięć masową opartą na iSCSI,
- Wdrożyć i zarządzać rozproszonym systemem plików (DFS - Distributed File System).

Moduł 5: Wirtualizacja Hyper-V i kontenery w systemie Windows Server

a. Hyper-V w systemie Windows Server
b. Konfiguracja maszyn wirtualnych /li>
c. Zabezpieczanie wirtualizacji w systemie Windows Server
d. Kontenery w systemie Windows Server
e. Wprowadzenie do platformy Kubernetes
f. **Ćwiczenie:** Wdrażanie i konfiguracja wirtualizacji w systemie Windows Server
   - Tworzenie i konfigurowanie maszyn wirtualnych
   - Instalacja i konfiguracja kontenerów

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać kluczowe cechy Hyper-V w systemie Windows Server,
- Opisać ustawienia maszyn wirtualnych oraz wdrożyć i skonfigurować maszyny wirtualne w Hyper-V,
- Wyjaśnić zastosowanie technologii bezpieczeństwa w wirtualizacji,
- Opisać i wdrożyć kontenery w systemie Windows Server,
- Wyjaśnić zastosowanie platformy Kubernetes w systemie Windows.

Moduł 6: Wysoka dostępność w systemie Windows Server

a. Planowanie wdrożenia klastra pracy awaryjnej
b. Tworzenie i konfiguracja klastra pracy awaryjnej
c. Wprowadzenie do rozciągniętych klastrów
d. Planowanie rozwiązań w zakresie wysokiej dostępności i odzyskiwania danych po awarii z wykorzystaniem maszyn wirtualnych funkcji Hyper-V
e. **Ćwiczenie:** Wdrażanie klastra pracy awaryjnej
   - Konfiguracja pamięci masowej i tworzenie klastra
   - Wdrażanie i konfiguracja serwera plików o wysokiej dostępności
   - Sprawdzanie poprawności wdrożenia serwera plików o wysokiej dostępności

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać klaster pracy awaryjnej i warunki jego wdrożenia,
- Tworzyć i konfigurować klastry pracy awaryjnej,
- Opisać klastry rozciągnięte,
- Opisać opcje osiągania wysokiej dostępności za pomocą maszyn wirtualnych Hyper-V.

Moduł 7: Odzyskiwanie danych po awarii w systemie Windows Server

a. Funkcja Hyper-V Replica
b. Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server
c. **Ćwiczenie:** Wdrażanie funkcji Hyper-V Replica i Windows Server Backup
   - Wdrażanie funkcji Hyper-V Replica
   - Wdrażanie tworzenia kopii zapasowych i przywracania za pomocą narzędzia Windows Server Backup

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać i wdrożyć funkcję Hyper-V Replica,
- Opisać usługę Azure Site Recovery,
- Opisać i wdrożyć narzędzie Windows Server Backup,
- Opisać usługę Azure Backup.

Moduł 8: Bezpieczeństwo systemu Windows Server

a. Ochrona danych uwierzytelniających i dostępu uprzywilejowanego
b. Hardening systemu Windows Server
c. JEA w systemie Windows Server
d. Zabezpieczanie i analiza ruchu w SMB
e. Zarządzanie aktualizacjami w systemie Windows Server
f. **Ćwiczenie:** Konfiguracja zabezpieczeń w systemie Windows Server
   - Konfiguracja funkcji Windows Defender Credential Guard
   - Lokalizowanie problematycznych kont
   - Wdrażanie rozwiązania LAPS

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać dane uwierzytelniające wykorzystywane w systemie Windows Server,
- Wyjaśnić, jak wdrożyć zabezpieczenia dostępu uprzywilejowanego,
- Opisać metody i technologie hardeningu zabezpieczeń w systemie Windows Server,
- Opisać i skonfigurować usługę Just Enough Administration (JEA),
- Zabezpieczyć ruch SMB w systemie Windows Server,
- Opisać usługę Windows Update oraz jej opcje wdrażania i zarządzania.

Moduł 9: RDS (usługi pulpitu zdalnego) w systemie Windows Server

a. Wprowadzenie do RDS
b. Konfiguracja wdrażania pulpitu opartego na sesji
c. Wprowadzenie do osobistych i połączonych pulpitów wirtualnych
d. **Ćwiczenie:** Wdrażanie RDS w systemie Windows Server
   - Wdrażanie RDS
   - Konfigurowanie ustawień kolekcji sesji i wykorzystywanie RDC
   - Konfiguracja szablonu pulpitu wirtualnego

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać usługi Remote Desktop Services (RDS - usługi pulpitu zdalnego) w systemie Windows Server,
- Opisać i wdrożyć pulpity oparte na sesji,
- Opisać osobiste i połączone pulpity wirtualne.

Moduł 10: Dostęp zdalny i usługi internetowe w systemie Windows Server

a. Wdrażanie sieci VPN
b. Wdrażanie usługi Always On VPN
c. Wdrażanie systemu NPS
d. Wdrażanie serwera WWW w systemie Windows Server
e. **Ćwiczenie:** Wdrażanie obciążeń sieciowych
   - Wdrażanie sieci VPN w systemie Windows Server
   - Wdrażanie i konfiguracja serwera WWW

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać opcje sieci VPN w systemie Windows Server,
- Opisać funkcję Always On VPN,
- Opisać i skonfigurować NPS,
- Opisać i skonfigurować serwer WWW (IIS).

Moduł 11: Monitorowanie serwera i wydajności w systemie Windows Server

a. Wprowadzenie do narzędzi do monitorowania systemu Windows Server

b. Korzystanie z monitora wydajności
c. Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów
d. **Ćwiczenie:** Monitorowanie i rozwiązywanie problemów z systemem Windows Server
   - Ustanowienie bazowego poziomu wydajności
   - Identyfikacja źródła problemu z wydajnością

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać narzędzia monitorujące w systemie Windows Server,
- Opisać monitorowanie wydajności i wykorzystać je w systemie Windows Server,
- Opisać rejestrowanie zdarzeń i monitorować rejestrowanie zdarzeń dla celów rozwiązywania problemów.

Moduł 12: Aktualizacja i migracja w systemie Windows Server

a. Migracja AD DS
b. Usługa migracji pamięci masowej
c. Narzędzia do migracji systemu Windows Server
d. **Ćwiczenie:** Migracja obciążeń serwera
   - Wdrażanie usługi migracji pamięci masowej

Po ukończeniu tego modułu uczestnicy będą w stanie:

- Opisać narzędzia, których należy użyć do migracji AD DS,
- Opisać usługę migracji pamięci masowej,
- Opisać narzędzia do migracji Windows Server i scenariusze ich użycia.

11.2 Szkolenie z zakresu zarządzania usługą Active Directory w środowisku Microsoft Windows Server 2022 – 2 vouchery na szkolenie ważne przez okres min. 6 miesięcy

W ramach postępowania Wykonawca dostarczy 2 Vouchery na szkolenie z używanego w Urzędzie systemu Windows Server 2022 na poziomie odpowiadającym Identity with Windows Server ważne przez minimum 6 miesięcy. Szkolenie zostanie przeprowadzone w formie stacjonarnej w siedzibie wyznaczonej przez Wykonawcę jednak odległość między siedzibą Zamawiającego a miejscem przeprowadzenia szkolenia nie będzie większa niż 60 km. W przypadku gdy odległość między siedzibą Zamawiającego a miejscem wykonania szkolenia będzie wynosić więcej niż 60 km Wykonawca pokryje koszty dojazdu, zakwaterowania i pełnego wyżywienia (śniadanie, obiad, kolacja). Zakwaterowanie w hotelu (co najmniej trzygwiazdkowym) nie może być oddalone od miejsca szkolenia więcej niż 15 minut pieszo. Wymagany czas trwania szkolenia wynosi 2 dni – łącznie 16 godzin lekcyjnych (jedna godzina lekcyjna trwa 45 minut). Celem szkolenia jest zdobycie wiedzy z zakresu: zarządzania tożsamościami użytkowników m.in. za pomocą usług i kontrolerów domeny usług Active Directory Domain Services (ADDS), wykorzystanie Group Policy Object (GPO) oraz automatyzacji zarządzania użytkownikami np. za pomocą zasad grupy. Minimalny, przykładowy zakres szkolenia przedstawiono poniżej:

Moduł 1: 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

Moduł 2: 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

Moduł 3: Zarządzanie zaawansowaną infrastrukturą AD DS

- Wprowadzenie do zaawansowanych wdrożeń AD DS
- Wdrożenie rozproszonego środowiska AD DS

- Konfiguracja relacji zaufania AD DS

Moduł 4: 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

Moduł 5: 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

Moduł 6: Zarządzanie ustawieniami użytkowników za pomocą zasad grupy

- Wdrażanie szablonów administracyjnych
- Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów
- Konfiguracja preferencji zasad grupowych