Załącznik nr 7 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Wymagania ogólne

1. Niniejszy załącznik stanowi szczegółowy opis przedmiotu zamówienia. Zaoferowane przez Wykonawcę rozwiązania muszą spełniać minimalne wymagania postawione w niniejszym załączniku w kolumnie „Wymagane minimalne parametry techniczne" oraz zostać dostarczony na warunkach określonych poniżej.

2. Zamówienie obejmuje kompleksową dostawę, wdrożenie oraz konfigurację wszystkich elementów infrastruktury objętych niniejszym zamówieniem. Wymagane jest, aby wszystkie elementy programowe stanowiły spójny, w pełni kompatybilny ekosystem technologiczny, umożliwiający ich wzajemną integrację oraz centralne zarządzanie. Wykonawca zobowiązany będzie do zapewnienia pełnego wdrożenia wszystkich systemów, ich uruchomienia oraz weryfikacji poprawności działania zgodnie z opisem przedmiotu zamówienia. W ramach realizacji przedmiotu zamówienia Wykonawca zapewni także wsparcie powdrożeniowe oraz przeprowadzi szkolenie dla Administratora IT wyznaczonych przez Zamawiającego, w sposób umożliwiający im samodzielną i efektywną obsługę oraz zarządzanie wdrożonymi systemami.

3. W ramach ceny zakupu systemów Wykonawca zapewnia gwarancję jakości obejmującą: usuwanie usterek i awarii, prawo do aktualizacji i poprawek bezpieczeństwa, dostęp do pomocy technicznej producenta lub autoryzowanego partnera (telefonicznej, mailowej, zdalnej), konsultacje techniczne niezbędne dla prawidłowego działania systemu, dostarczanie nowych wersji oprogramowania (upgrade/patch), jeśli zostaną wydane w okresie gwarancji.

4. Wszelkie dostarczane w ramach zamówienia oprogramowanie musi być fabrycznie nowe, nieużywane oraz nieaktywowane wcześniej na żadnym urządzeniu. Wykonawca zobowiązany jest dostarczyć je w najnowszej stabilnej wersji, dostępnej na dzień składania ofert, pochodzącej wyłącznie z oficjalnego kanału dystrybucyjnego producenta. Oprogramowanie nie może być obciążone żadnymi prawami osób trzecich, a jego nośniki – o ile występują – muszą być wolne od wad fizycznych i prawnych.

5. Wszystkie dostarczone w ramach zamówienia systemy muszą być objęte gwarancją producenta lub autoryzowanego partnera serwisowego, realizowaną na terenie Polski. Gwarancja obejmuje w szczególności: usuwanie usterek i awarii, prawo do aktualizacji i poprawek bezpieczeństwa, dostęp do pomocy technicznej w języku polskim (telefonicznej, mailowej, zdalnej), a także świadczenie usług serwisowych przez certyfikowany personel.

6. Wszystkie szkolenia w ramach zamówienia muszą być skierowane do administratora IT zatrudnionego w Urzędzie Gminy. Zamawiający dopuszcza realizację szkoleń w formie stacjonarnej lub zdalnej online. Szkolenia mogą być prowadzone równolegle z procesem wdrożenia dostarczanych systemów i urządzeń. Wszystkie szkolenia muszą być prowadzone przez osobę posiadającą odpowiednią wiedzę, doświadczenie i kwalifikacje potwierdzające kompetencje w zakresie danej tematyki.

7. Przy wyborze oferty Zamawiający będzie kierował się dwoma kryteriami: ceną (waga 60%) oraz okresem wsparcia powdrożeniowego i poszkoleniowego (waga 40%). Kryterium ceny pozwala na wybór rozwiązania najbardziej korzystnego ekonomicznie, natomiast kryterium wsparcia powdrożeniowego i poszkoleniowego zostało przyjęte z uwagi na konieczność zapewnienia nieprzerwanego i bezpiecznego funkcjonowania wdrożonych systemów oraz trwałości efektów szkoleniowych.

8. Pod pojęciem „okresu wsparcia powdrożeniowego i poszkoleniowego" Zamawiający rozumie czas, w którym Wykonawca zapewnia swoją dostępność w celu dokonania niezbędnych poprawek konfiguracyjnych mogących wystąpić w pierwszym okresie po wdrożeniu, a także udziela wsparcia w zakresie utrwalania wiedzy zdobytej podczas szkoleń oraz dodatkowych konsultacji związanych z prawidłowym użytkowaniem dostarczonych rozwiązań. Kryterium to nie dotyczy podstawowych świadczeń serwisowych w ramach gwarancji (które Wykonawca i tak jest zobowiązany zapewnić zgodnie z ofertą), lecz właśnie dostępności Wykonawcy w zakresie doradztwa, korekt i utrwalenia wiedzy, które mają kluczowe znaczenie dla pełnego i skutecznego wykorzystania rezultatów projektu „Cyberbezpieczny Samorząd". Szczegółowy zakres wsparcia poszkoleniowego i powdrożeniowego znajduje się na końcu OPZ.

Spis treści

1. Oprogramowanie do ochrony przed wyciekiem danych (DLP) - 75 użytkowników

Komponent	Wymagane minimalne parametry techniczne – Oprogramowanie DLP
System zabezpieczenia danych przed wyciekiem informacji	**1.** Wymaga się dostawy kompletnego rozwiązania do ochrony stacji roboczych Windows przed wyciekiem danych, pochodzącego od jednego producenta, o minimalnej funkcjonalności opisanej poniżej. Wymagane jest, aby cała funkcjonalność była dostępna w ramach jednej, jednolitej instalacji oferowanego systemu ochrony danych przed wyciekiem ze zintegrowanym systemem kontroli portów i szyfrowaniem – całość realizowana w ramach jednego agenta na stacjach roboczych.
Wymagania ogólne	**2.** Rozwiązanie ma chronić dane na stacjach roboczych Windows przed wyciekiem, poprzez kontrolę portów fizycznych i podłączanych do nich nośników zewnętrznych oraz przez szyfrowanie danych na dyskach lokalnych i nośnikach zewnętrznych. **3.** Rozwiązanie powinno działać w oparciu o definiowanie polityk bezpieczeństwa i integrować się z Active Directory przez wiązanie polityk bezpieczeństwa z obiektami Active Directory. Wymaga się, aby polityka mogła być powiązania z różnymi rodzajami obiektów AD: **3.1.** Domena **3.2.** Jednostka Organizacyjna (OU) **3.3.** Grupa **3.4.** Użytkownik **3.5.** Komputer **4.** Rozwiązanie nie może w żaden sposób modyfikować, usuwać ani tworzyć obiektów w drzewie AD. **5.** Rozwiązanie powinno składać się z pojedynczego serwera zarządzającego, oferującego konsolę administracyjną do zarządzania politykami bezpieczeństwa, konfigurowania i monitorowania pracy systemu oraz z agenta, instalowanego na stacjach roboczych, który egzekwuje polityki bezpieczeństwa przypisane do komputera bądź użytkownika. **6.** Dystrybucja polityk bezpieczeństwa i ich odświeżanie na stacjach roboczych muszą zachodzić automatycznie i cyklicznie z częstotliwością definiowaną przez administratora, ale również z możliwością wymuszonego odświeżenia na żądanie z poziomu konsoli administracyjnej oraz ze stacji roboczej. **7.** Wymaga się, aby polityki bezpieczeństwa były egzekwowane również w trybie „offline", czyli gdy stacja robocza nie ma kontaktu z serwerem zarządzającym (np. laptop poza firmą). **8.** Wymagane jest dostarczenie pliku instalacyjnego agenta w postaci pakietu MSI, z możliwością dystrybucji tego pakietu co najmniej przez Active Directory GPO lub inne systemy dystrybucji centralnej oprogramowania. **9.** Agent musi być wspierany dla stacji roboczych z biznesową wersją Windows 10/11.
Kontrola portów fizycznych i nośników zewnętrznych	**10.** Produkt musi umożliwiać całkowite blokowanie użycia portów fizycznych: **10.1.** USB **10.2.** Firewire **10.3.** PCMCIA **10.4.** Secure Digital **10.5.** Serial **10.6.** Paralel **10.7.** Porty wewnętrzne **10.8.** Wi-Fi

Komponent	Wymagane minimalne parametry techniczne – Oprogramowanie DLP
	10.9. Bluetooth **11.** Wymagane jest, aby produkt identyfikował i raportował urządzenia podłączane do portów USB stacji roboczych, według typu, producenta, modelu i numeru seryjnego. Funkcja ta jest konieczna, by usprawnić proces definiowania polityk bezpieczeństwa, dotyczących kontroli nośników zewnętrznych. Niezbędna jest możliwość zdalnego przeskanowania stacji roboczych z poziomu konsoli zarządzającej w celu zidentyfikowania podłączanych do nich urządzeń zewnętrznych. **12.** Produkt musi umożliwiać blokowanie wybranych typów urządzeń podłączanych do portu USB, rozróżniając: **12.1.** Telefony komórkowe **12.2.** Urządzenia oparte o system Android **12.3.** Urządzenia oparte o system iOS **12.4.** Urządzenia PDA **12.5.** Smart Card **12.6.** Urządzenia drukujące **12.7.** Adaptery sieciowe **12.8.** Urządzenia audio/video **12.9.** Urządzenia interfejsu HID **12.10.** Urządzenia do przetwarzania obrazów **12.11.** Sprzętowe KeyLoggery **13.** Produkt musi posiadać funkcję definiowania "białych list", czyli urządzeń wyjątkowo dopuszczonych do podłączenia, identyfikowanych przez określenie producenta, modelu i numeru seryjnego urządzenia. **14.** Dla zewnętrznych urządzeń pamięci masowej typu: pendrive, napędy CD/DVD, zewnętrzne dyski twarde – musi być możliwość zdefiniowania w polityce bezpieczeństwa mechanizmów: **14.1.** Blokowanie urządzeń danego typu **14.2.** Korzystanie w trybie „tylko do odczytu" **14.3.** Wymuszenie szyfrowania danych na nośniku **14.4.** Blokowanie możliwości odczytu z nośnika plików określonego typu (np. plików wykonywalnych) **14.5.** Blokowanie możliwości zapisywania na nośniku plików określonego typu **14.6.** Rejestrowanie w logach wszystkich zapisów i odczytów z nośnika, również wtedy, gdy stacja pracuje „offline" **15.** Szyfrowanie danych na nośnikach zewnętrznych musi być przezroczyste dla użytkownika i nie wymagać żadnego zarządzania kluczami szyfrującymi. Musi być możliwość zapisania i odczytania danych z zaszyfrowanego nośnika na dowolnej stacji roboczej wyposażonej w agenta oferowanego rozwiązania.
Szyfrowanie dysku lokalnego	**16.** Wymaga się funkcjonalności szyfrowania danych na dysku lokalnym, inicjowanej tym samym jednolitym mechanizmem, co inne funkcjonalności, tj. przez przypisanie odpowiedniej polityki bezpieczeństwa do stacji roboczej. **17.** Wymagane jest, aby szyfrowaniem objęte były tylko dane użytkowników, bez szyfrowania sektora rozruchowego i plików systemowych Windows. Przypisanie polityki szyfrowania do stacji roboczej powinno spowodować zaszyfrowanie danych na dysku. **18.** Szyfrowanie danych na dyskach lokalnych musi być przezroczyste dla użytkownika i nie wymagać żadnego zarządzania kluczami szyfrującymi. Proces

Komponent	Wymagane minimalne parametry techniczne – Oprogramowanie DLP
	deszyfrowania/szyfrowania musi być realizowany w czasie rzeczywistym przy modyfikacji plików przez użytkownika. **19.** Obsługa szyfrowania musi być realizowana w całości przez agenta oferowanego rozwiązania, bez konieczności korzystania z rozwiązań zewnętrznych. **20.** Wymaga się, aby zaszyfrowane dane były dostępne dla każdego użytkownika, który na stacji roboczej poprawnie zaloguje się na swoje konto domenowe (w zakresie jego uprawnień na poziomie systemu plików). **21.** Wymaga się, aby żadne zaszyfrowane dane nie były dostępne, gdy na stacji roboczej zaloguje się pracownik Helpdesku. Umożliwi to udzielanie wsparcia użytkownikom w zakresie utrzymania systemu operacyjnego, bez ryzyka ujawnienia treści ich danych przechowywanych na stacji roboczej. **22.** Musi być dostępne narzędzie, pozwalające na odszyfrowanie danych z dysku w przypadku, gdy nie da się uruchomić stacji roboczej w normalnym trybie, np. na skutek uszkodzenia systemu operacyjnego. Skorzystanie z narzędzia musi wymagać akceptacji administratora systemu, np. poprzez wygenerowanie jednorazowego kodu/hasła.
Pozostałe wymagania	**23.** Wymaga się, by produkt zaopatrzony był w funkcje zabezpieczające przed próbami ingerencji użytkowników w działanie agenta: **23.1.** Odinstalowanie oprogramowania możliwe dzięki hasłu, które zna wyłącznie administrator IT **23.2.** Ochrona przed użytkownikami posiadającymi uprawnienia administratora, chcącymi usunąć bądź wyłączyć oprogramowanie **23.3.** Rejestrowanie wszelkich prób manipulacji przez użytkowników (łącznie z usuwaniem logów) **23.4.** Wszystkie pliki logów muszą być zaszyfrowane przed nieautoryzowanym dostępem i próbą skasowania **23.5.** Wszystkie połączenia między aplikacją agencką na stacji roboczej a serwerem zarządzającym muszą być zaszyfrowane przy użyciu protokołu SSL **24.** Musi istnieć możliwość czasowego wstrzymania (zawieszenia) ochrony na stacji roboczej, bez konieczności modyfikacji lub usuwania i ponownego przypisywania polityk bezpieczeństwa. Wstrzymanie ochrony musi wymagać akceptacji administratora systemu, np. przez wygenerowanie jednorazowego hasła. **25.** W czasie swojego działania agent na stacji roboczej nie może obciążać zasobów (CPU, RAM, dysk) w stopniu odczuwalnym przez użytkownika i utrudniającym normalną pracę. Dopuszczalne jest większe obciążenie stacji jedynie przy pierwszym szyfrowaniu dysku lokalnego. **26.** Powinna być możliwość zdefiniowania własnej treści komunikatów w języku polskim, wyświetlanych przez agenta na stacji roboczej. **27.** Wymagana jest możliwość instalacji agenta w trybie ukrytym, tj. bez widoczności żadnych ikonek i bez wyświetlania jakichkolwiek komunikatów na stacji roboczej. **28.** Rozwiązanie musi posiadać wbudowany mechanizm automatycznego wykonywania backupu swojej konfiguracji i zgromadzonych logów wg harmonogramu zdefiniowanego przez administratora. System musi umożliwiać całkowite odtworzenie serwera zarządzającego z takiego backupu na wypadek awarii, bez konieczności reinstalowania agentów. **29.** Proponowane rozwiązanie musi wspierać instalację na wirtualnej platformie VMware lub Hyper-V i być z nią kompatybilne. **30.** Rozwiązanie musi być uruchomione na wskazanych zasobach Zamawiającego i nie może wymagać żadnych dodatkowych zewnętrznych komponentów, np. zewnętrznych baz danych lub zewnętrznych programów szyfrujących.

Komponent	Wymagane minimalne parametry techniczne – Oprogramowanie DLP
	31. Rozwiązanie musi obsłużyć minimum 75 stacji roboczych. **32.** Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej z odnawianym corocznie supportem, zawierającym wsparcie techniczne producenta oraz dostęp do poprawek i nowych wersji. **33.** Wymaga się, aby funkcjonalność szyfrowania dysków lokalnych była licencjonowana osobno od funkcjonalności kontroli portów fizycznych i nośników zewnętrznych, pozwalając na elastyczność w doborze licencji do potrzeb. **34.** Wymaga się dostarczenia 75 licencji wieczystych z rocznym wsparciem technicznym dla funkcjonalności kontroli portów fizycznych i nośników zewnętrznych oraz 75 licencji wieczystych z rocznym wsparciem technicznym dla funkcjonalności szyfrowania dysków lokalnych.
Usługi	**35.** Wymaga się, aby dostawca zaoferował usługę zdalnego wdrożenia rozwiązania w infrastrukturze Zamawiającego, przeprowadzoną przez inżyniera certyfikowanego przez producenta rozwiązania, w zakresie: **35.1.** instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego **35.2.** szkolenie dla administratora rozwiązania **35.3.** wsparcie w języku polskim w trybie 8x5 w dni robocze **35.4.** kwartalny przegląd konfiguracji rozwiązania

2. Oprogramowanie do kontroli dostępu do sieci (NAC) - 200 adresów IP

Komponent	Wymagane minimalne parametry techniczne – Oprogramowanie NAC
Opis funkcjonalności rozwiązania	**1.** Wymagane jest dostarczenie rozwiązania typu NAC (Network Access Control), służącego do monitorowania sieci lokalnych w celu uwidocznienia pracujących w nich urządzeń oraz wykrywania nowych urządzeń pojawiających się w sieci, w czasie rzeczywistym. Rozwiązanie musi raportować aktualny stan każdego urządzenia, z uwzględnieniem takich atrybutów, jak adres MAC, adres IP, nazwa hosta, system operacyjny, itp., pozyskując te informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.). **2.** Rozwiązanie ma za zadanie zapewnić, aby tylko urządzenia, których aktualny stan spełnia zdefiniowaną przez administratora politykę bezpieczeństwa, mogły bez ograniczeń ze strony NAC pracować w sieci lokalnej. Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenia, których aktualny stan nie spełnia danych warunków polityki bezpieczeństwa (np. nowe, po raz pierwszy pojawiające się urządzenie lub stacja robocza z wyłączonym oprogramowaniem antywirusowym). Mechanizm kwarantanny powinien umożliwiać całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, jak również blokowanie częściowe, w zakresie definiowanym przez administratora (przez wskazanie adresów IP, z którymi urządzenie może się komunikować). Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej. **3.** Rozwiązanie musi posiadać funkcjonalność typu Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów.
Wymagania ogólne rozwiązania NAC	**4.** Ma zapewnić widoczność i monitorowanie wszystkich urządzeń pracujących w sieci lokalnej oraz powiadamiać o nowych urządzeniach pojawiających się w sieci. **5.** Musi zapewniać automatyczne blokowanie komunikacji sieciowej między nowym, niezaufanym urządzeniem a zaufanymi, zarządzanymi urządzeniami pracującymi w sieci. **6.** Musi umożliwiać sprawdzanie statusu aktualizacji oprogramowania antywirusowego i poprawek systemowych na zarządzanych stacjach roboczych Windows i w przypadku niespełniania określonych wymagań, automatycznie ograniczać tym stacjom roboczym możliwość pracy w sieci. **7.** Musi umożliwiać odbieranie komunikatów bezpieczeństwa z innych systemów bezpieczeństwa (np. firewalla) i automatyczne blokowanie na tej podstawie wskazanych urządzeń w sieci. **8.** Musi mieć funkcję wykrywania faktu skanowania urządzeń i portów wykonywanego przez urządzenie w sieci lokalnej i automatycznie blokować takie urządzenie, aby zapobiegać potencjalnemu szerzeniu się malware. **9.** Stosowany mechanizm blokowania musi wykorzystywać protokół ARP i działać całkowicie niezależnie od innych elementów infrastruktury sieciowej. **10.** Rozwiązanie musi działać bezagentowo, bez konieczności instalowania jakichkolwiek agentów na urządzeniach w sieci oraz bez konieczności dokonywania zmian w infrastrukturze sieciowej. **11.** Rozwiązanie musi umożliwiać wysyłanie alertów do administratora za pomocą e-maila oraz SMS **12.** Rozwiązanie musi być zarządzane przez interfejs webowy, obsługiwany przeglądarką internetową

Komponent	Wymagane minimalne parametry techniczne – Oprogramowanie NAC
	13. Wymaga się, aby rozwiązanie było dostarczone w postaci maszyny wirtualnej na platformę VMware oraz Hyper-V. System musi pozwalać na monitorowanie co najmniej 10 sieci VLAN i monitorowanie łącznie co najmniej 200 urządzeń. **14.** Wymaga się, aby rozwiązanie było licencjonowane w modelu licencji wieczystej i dostarczone z licencją pozwalającą na monitorowanie 200 urządzeń wraz ze wsparciem technicznym na okres 12 miesięcy.
Wymagania szczegółowe – monitorowanie podsieci	**15.** Rozwiązanie musi w czasie rzeczywistym raportować widoczność wszystkich urządzeń pracujących w monitorowanych podsieciach. **16.** Rozwiązanie musi wykrywać nowe nieznane urządzenie, dołączające się do sieci LAN lub WLAN, w czasie nie dłuższym, niż 5 sekund oraz wysyłać powiadomienie mailowe do administratora **17.** Rozwiązanie musi wykrywać przypadki skanowania urządzeń i portów w monitorowanych podsieciach i blokować urządzenie inicjujące takie skanowanie **18.** Rozwiązanie musi posiadać funkcję pułapki sieciowej (honeypot), symulującą w każdej monitorowanej podsieci standardowe usługi sieciowe, co najmniej: ssh, telnet, ftp i smb. Rozwiązanie musi rejestrować każdą próbę zalogowania się do takiej symulowanej usługi, zapisując użytą nazwę użytkownika, hasło użytkownika i źródłowy MAC/IP. **19.** Rozwiązanie musi określać aktualny stan każdego urządzenia, pozyskując informacje bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.) oraz odświeżać te informacje cyklicznie. Musi być możliwość wykorzystania pozyskanych informacji do definiowania polityk bezpieczeństwa. **20.** Rozwiązanie musi chronić przed podszywaniem się pod adres MAC (MAC spoofing), umożliwiając zdefiniowanie „odcisku palca" (fingerprint) dla każdego zaufanego urządzenia. Odcisk palca musi być kombinacją co najmniej: adresu MAC, adresu IP, nazwy hosta, nazwy systemu operacyjnego, otwartych portów TCP. Jeśli przeprowadzana cyklicznie weryfikacja odcisku palca wykaże jego zmianę, urządzenie powinno zostać zablokowane. **21.** Rozwiązanie musi obsługiwać VLANy, tj. umożliwiać monitorowanie przez jeden fizyczny interfejs sieciowy wielu podsieci, zdefiniowanych jako VLANy
Wymagania szczegółowe – polityka bezpieczeństwa	**22.** Rozwiązanie musi umożliwiać definiowanie polityki bezpieczeństwa, czyli określenie przez administratora, jakie warunki musi spełniać aktualny stan urządzenia, aby uzyskało ono określony dostęp do sieci. **23.** W definiowaniu polityki bezpieczeństwa musi być możliwość wykorzystania informacji o aktualnym stanie urządzenia, pozyskanych bezagentowo bezpośrednio od samych urządzeń oraz od usług zarządzania infrastrukturą sieciową (np. Active Directory, serwery DNS/DHCP, serwery AV, WMI, itp.), poprzez integrację z tymi systemami. **24.** Polityka bezpieczeństwa musi umożliwiać przypisanie do urządzenia jednego z trzech trybów dostępu do sieci: **24.1.** pełny dostęp **24.2.** blokowanie (całkowity brak dostępu) **24.3.** ograniczony dostęp **25.** Zakres ograniczonego dostępu powinien być definiowany przez administratora, np. w postaci list ACL, określających, do których adresów IP i portów urządzenie ma dostęp. Musi być możliwość zdefiniowania wielu różnych zakresów ograniczonego dostępu.

Komponent	Wymagane minimalne parametry techniczne – Oprogramowanie NAC
	26. Rozwiązanie powinno automatycznie sprawdzać, które warunki polityki bezpieczeństwa spełnia urządzenie i na tej podstawie przypisywać do urządzenia właściwy zakres dostępu. **27.** Zakres dostępu, wynikający ze spełnienia przez urządzenie danych warunków polityki bezpieczeństwa powinien być egzekwowany przez mechanizm kwarantanny. **28.** Musi być możliwość łatwego, manualnego tworzenie białej listy adresów MAC, czyli listy urządzeń mogących bez żadnych ograniczeń ze strony NAC pracować w sieci.
Wymagania szczegółowe – mechanizm kwarantanny	**29.** Rozwiązanie musi być wyposażone w mechanizm kwarantanny, nakładanej przez NAC automatycznie na urządzenie, aby wyegzekwować ograniczenia dostępu do sieci, wynikające z polityki bezpieczeństwa **30.** Mechanizm kwarantanny powinien umożliwiać: **30.1.** całkowite blokowanie komunikacji urządzenia z otoczeniem sieciowym, **30.2.** częściowe blokowanie komunikacji urządzenia z otoczeniem sieciowym, w zakresie definiowanym przez administratora przez wskazanie adresów IP i portów, z którymi urządzenie może się komunikować **31.** Mechanizm kwarantanny powinien blokować komunikację urządzenia w czasie nie dłuższym niż 5 sekund od zaistnienia warunku, powodującego nałożenie kwarantanny **32.** Dla urządzeń zaufanych, czyli w polityce bezpieczeństwa spełniających kryteria pełnego dostępu do sieci, rozwiązanie nie powinno w żaden sposób przekierowywać ani blokować komunikacji wychodzącej z tych urządzeń **33.** Kwarantanna powinna być zdejmowana z urządzenia automatycznie, gdy spełni ono kryteria polityki bezpieczeństwa, pozwalające na pełny dostęp **34.** Mechanizm kwarantanny musi działać bezagentowo, wykorzystując protokół ARP, bez konieczności dokonywania jakichkolwiek zmian w konfiguracji infrastruktury sieciowej, musi być niezależny od stosowanych w sieci przełączników, zarządzalnych bądź niezarządzalnych **35.** Awaria rozwiązania nie może powodować blokady komunikacji w sieci, tj. w przypadku awarii rozwiązania wszystkie urządzenia mają mieć pełny dostęp do sieci **36.** Rozwiązanie musi umożliwiać włączenie i wyłączenie mechanizmu kwarantanny (blokowania komunikacji) w każdej monitorowanej podsieci osobno
Wymagania szczegółowe – integracja z systemami zewnętrznymi	**37.** Rozwiązanie musi umieć sprawdzić, czy urządzenia z systemem Windows są dołączone do domeny AD **38.** Rozwiązanie powinno umożliwiać sprawdzanie statusu oprogramowania antywirusowego, poprawek systemowych i firewalla bezpośrednio na zarządzanych stacjach roboczych Windows w domenie AD, w sposób bezagentowy, przy użyciu WMI. **39.** Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym poprawkami Windows i sprawdzanie statusu zainstalowanych poprawek na zarządzanych urządzeniach z systemem Windows. Wymagana jest możliwość integracji co najmniej z systemami: Microsoft WSUS. **40.** Rozwiązanie musi umożliwiać bezagentową integrację z serwerem zarządzającym agentami antywirusowymi i sprawdzanie statusu agentów AV zainstalowanych na zarządzanych urządzeniach (co najmniej, czy agent jest zainstalowany, aktywny i ma aktualne sygnatury wirusów). Wymagana jest możliwość integracji co najmniej z systemami: Bitdefender, Carbon Black, CrowdStrike, Cybereason, Eset, FireEye, McAfee, SentinelOne, Sophos, Symantec, TrendMicro, Webroot.

Komponent	Wymagane minimalne parametry techniczne – Oprogramowanie NAC
	41. Rozwiązanie musi umożliwiać wykorzystanie pozyskanych informacji, wymienionych w poprzedzających punktach 1-4, do definiowania polityki bezpieczeństwa. **42.** Rozwiązanie musi umieć odbierać alerty przysyłane za pomocą e-mail lub syslog z innych urządzeń bezpieczeństwa (np. firewalla) i na podstawie zawartych w nich informacji blokować wskazane podejrzane urządzenie
Wymagania szczegółowe – rejestracja urządzeń zewnętrznych: pracowników, gości i konsultantów (Captive Portal)	**43.** Rozwiązanie musi posiadać wbudowaną funkcję Captive Portal, służącą do rejestrowania i kontrolowania dostępu do sieci dla niezarządzanych urządzeń zewnętrznych, podłączanych przez pracowników (BYOD), gości i zewnętrznych konsultantów. NAC musi przekierowywać ruch HTTP/S od nieznanych urządzeń do tego portalu. **44.** Captive Portal musi umożliwiać pracownikom rejestrowanie urządzeń prywatnych (BYOD) i wnioskowanie o dostęp do sieci w ograniczonym zakresie, zdefiniowanym przez administratora. **45.** Przy rejestracji przez pracowników ich prywatnych urządzeń, Captive Portal powinien umożliwiać użycie ich kont Active Directory **46.** Powinna istnieć możliwość ograniczenia ilości i rodzaju rejestrowanych przez pracownika prywatnych urządzeń **47.** Powinna być możliwość przypisania ograniczonego dostępu dla zarejestrowanych urządzeń prywatnych **48.** Captive Portal musi umożliwiać osobom niebędącym pracownikami (gościom lub konsultantom) wnioskowanie o ograniczony dostęp do sieci **49.** W przypadku rejestracji urządzeń gości powinna być możliwość rejestracji samodzielnie przez gościa oraz przez uprawnionego pracownika firmy **50.** Zarejestrowane urządzenia gości powinny automatycznie tracić przydzielony dostęp po upływie zdefiniowanego czasu **51.** Powinna istnieć możliwość ograniczenia ilości urządzeń rejestrowanych przez gościa **52.** Dla zarejestrowanych urządzeń gości powinna być możliwość ograniczenia, w jakich przedziałach czasu i z jakich podsieci będą one miały dostęp do sieci **53.** Dla urządzeń gości powinna być możliwość przypisania dostępu ograniczonego tylko do dostępu do Internetu **54.** Dla urządzeń konsultantów powinna być możliwość przypisania dostępu ograniczonego do wybranych zasobów lokalnych **55.** Rozwiązanie musi umożliwiać zatwierdzenie dostępu dla zarejestrowanego urządzenia gościa i konsultanta drogą mailową. Osoba zatwierdzająca powinna otrzymać z systemu e-mail z wnioskiem o dostęp i udzielić go, odpowiadając na maila lub klikając przygotowany link w treści maila. **56.** Rozwiązanie musi przechowywać historyczne raporty dostępu do sieci użytkowników typu gość i konsultant **57.** Wygląd Captive Portal musi być edytowalny w zakresie co najmniej zmiany firmowego logo i kolorów oraz informacji, jakie we wniosku rejestracyjnym musi podać gość lub konsultant
Pozostałe wymagania	**58.** Rozwiązanie powinno oferować uwierzytelnianie administratora za pomocą dodatkowego faktora, oprócz hasła (2FA). **59.** Rozwiązanie powinno oferować możliwość zainstalowania opcjonalnego agenta na zarządzanych stacjach roboczych (wymagane wsparcie dla Windows, Linux i MacOS), który przesyła do serwera zarządzającego NAC szczegółowe informacje na temat stacji roboczej, umożliwiając definiowanie na bazie tych informacji precyzyjnych polityk bezpieczeństwa.

Komponent	Wymagane minimalne parametry techniczne – Oprogramowanie NAC
	60. Rozwiązanie nie powinno pogarszać wydajności pracy przełączników i routerów, nie może wymagać współpracy z przełącznikami przez port mirroring czy port spanning. **61.** Rozwiązanie nie powinno pogarszać wydajność łącz WAN **62.** Rozwiązanie nie powinno pogarszać wydajności pracy monitorowanych urządzeń w sieci
Wdrożenie	**63.** Wymaga się, aby dostawca zaoferował usługę wdrożenia rozwiązania w infrastrukturze Zamawiającego, w wymienionym poniżej zakresie, przeprowadzoną przez wykwalikowanego inżyniera, certyfikowanego przez producenta rozwiązania: **63.1.** instalacja i konfiguracja rozwiązania w maszynie wirtualnej na platformie Zamawiającego **63.2.** szkolenie dla administratora rozwiązania **63.3.** wsparcie w języku polskim w trybie 8x5 w dni robocze **63.4.** kwartalny przegląd konfiguracji rozwiązania **64.** Wymaga się, aby dostawca przedstawił: **64.1.** oświadczenie producenta o posiadaniu przez dostawcę kwalifikacji technicznych, niezbędnych do wykonania wdrożenia oferowanego rozwiązania i szkolenia **64.2.** osobowy certyfikat inżynierski pracownika, która będzie wykonywał wdrożenie

3. Oprogramowanie do wykonywania kopii zapasowych

Wymagane minimalne parametry techniczne – Oprogramowanie do backupu
1. Możliwość backupu 75 stacji roboczych, 2 serwerów, 3 hostów wirtualizacji
2. Oprogramowanie działające w architekturze klient-serwer w oparciu o protokół TCP/IP, z centralnym modułem sterowania wykonywaniem kopii zapasowych z dysków komputerów klienckich
3. Program serwerowy kompatybilny z systemami: Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2003, 2008, 2012, 2016, 2019, 2022, 2025, Linux, BSD, Mac OS X, QNAP, Synology
4. Program kliencki kompatybilny z systemami: Microsoft Windows 2000, XP, Vista, Windows 7, Windows 8, Windows 10; Windows 11; Microsoft Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, 2025, Linux, BSD, Mac OS X, QNAP, Synology
5. Możliwość archiwizacji pełnej, przyrostowej/różnicowej i delta (różnica na poziomie fragmentów plików)
6. Możliwość archiwizacji otwartych i zablokowanych plików bez korzystania z usługi Volume Shadow Copy Service (VSS)
7. Automatyczny backup przy wyłączaniu komputera
8. Możliwość wybrania do archiwizacji lub wykluczenia z archiwizacji określonych woluminów, katalogów, plików za pomocą symboli wieloznacznych * i?
9. Backup całego systemu operacyjnego i zainstalowanych programów (tylko Windows)
10. Backup baz danych i plików poczty w trybie online i offline
11. Kopie rotacyjne (wersjonowanie)
12. Zapis archiwów w otwartym formacie (ZIP 64-bit)
13. Backup i odzyskiwanie maszyn wirtualnych Microsoft Hyper-V oraz VMWare ESX/ESXi
14. Odzyskiwanie systemu operacyjnego na czystym dysku twardym bez konieczności ponownej instalacji (bare metal restore)
15. Bezpośrednie odzyskiwanie plików do lokalizacji oryginalnej
16. Odzyskiwanie z kopii różnicowych i delta tak jak z kopii pełnych
17. Szyfrowanie archiwów i transferu zapewniających bezpieczeństwo sieci i informacji wymaganych przez RODO
18. Kompresja po stronie stacji roboczej
19. Replikacja archiwów na dodatkowy dysk twardy, NAS, serwer FTP,
20. Centralne sterowanie całym Systemem z jednego miejsca
21. Transparentna archiwizacja wykonywana w tle, która nie jest odczuwalna przez pracowników
22. Możliwość równoległej archiwizacji wszystkich komputerów podłączonych do sieci LAN/WAN
23. Wysyłanie Alertów administracyjnych na e-mail
24. Możliwość uruchamiania zewnętrznych programów, skryptów i plików wsadowych na serwerze backupu i na komputerach zdalnych
25. Raporty podsumowujące przebieg archiwizacji, zawierające informacje na temat zaległych zadań archiwizacji oraz statystyki
26. Automatyczna aktualizacja oprogramowania na komputerach zdalnych
27. Bezterminowa licencja - licencja nie może być ograniczona czasowo
28. Interfejs, instrukcja i pomoc techniczna w języku polskim

4. Usługa wykonania segmentacji sieci

Komponent	Wymagane minimalne parametry techniczne – segmentacja sieci
Etap analizy i planowania	**1.** Audyt infrastruktury sieciowej **1.1.** Przeprowadzenie szczegółowego audytu istniejącej infrastruktury IT, w tym topologii sieci, urządzeń końcowych, serwerów, drukarek i innych urządzeń sieciowych. **1.2.** Identyfikacja krytycznych zasobów, przepływów danych oraz potencjalnych punktów awarii lub luk w bezpieczeństwie. **2.** Opracowanie projektu segmentacji **2.1.** Stworzenie logicznej struktury segmentacji sieci opartej na potrzebach urzędu, np. podział na VLAN-y dla wydziałów (np. Administracja, Finanse, IT, Obsługa interesantów) oraz usług (np. Internet, drukarki, monitoring). **2.2.** Zdefiniowanie reguł dostępu między segmentami sieci zgodnie z zasadą minimalnych uprawnień (Least Privilege). **3.** Uwzględnienie przyszłych potrzeb skalowalności w projekcie.
Etap instalacji i konfiguracji sprzętu	**4.** Przygotowanie urządzeń sieciowych **4.1.** Aktualizacja oprogramowania firmware przełączników do najnowszej wersji w celu zapewnienia pełnej funkcjonalności i bezpieczeństwa. **4.2.** Konfiguracja podstawowych parametrów przełączników, takich jak adresy IP, nazwy urządzeń, połączenia uplinkowe i redundancja.
Etap konfiguracji sieci VLAN	**5.** Tworzenie VLAN-ów **5.1.** Wprowadzenie VLAN-ów w celu oddzielenia ruchu między różnymi działami urzędu (np. VLAN dla finansów, administracji, IT, obsługi interesantów). **5.2.** Utworzenie VLAN-ów dla zasobów wspólnych, takich jak drukarki sieciowe, kamery monitoringu oraz Internet. **6.** Przypisywanie portów do VLAN-ów **6.1.** Przypisanie portów przełączników do odpowiednich VLAN-ów w zależności od przynależności urządzeń do danego działu lub funkcji. **6.2.** Konfiguracja trunków VLAN na portach uplink w celu zapewnienia komunikacji między przełącznikami i urządzeniami zarządzającymi siecią. **7.** Zastosowanie routingu między VLAN-ami **7.1.** Skonfigurowanie routingu warstwy 3 na przełącznikach w celu umożliwienia komunikacji między VLAN-ami zgodnie z określonymi zasadami bezpieczeństwa. **8.** Wdrożenie polityk trasowania i priorytetów (QoS) w celu optymalizacji ruchu sieciowego.
Etap konfiguracji zabezpieczeń	**9.** Listy kontroli dostępu (ACL) **9.1.** Zdefiniowanie list kontroli dostępu dla każdego VLAN-u w celu ograniczenia ruchu tylko do autoryzowanych urządzeń i użytkowników. **9.2.** Przykłady reguł ACL: **9.3.** Użytkownicy w VLAN administracyjnym mają dostęp do zasobów finansowych tylko przez określone aplikacje. **9.4.** Blokowanie dostępu do Internetu dla urządzeń monitoringu. **10.** Implementacja zabezpieczeń na poziomie warstwy 2

Komponent	Wymagane minimalne parametry techniczne – segmentacja sieci
	10.1. Wdrożenie mechanizmów ochrony, takich jak DHCP Snooping, ARP Inspection i Port Security, aby zapobiegać atakom wewnętrznym, np. spoofingowi. **11.** Włączenie logowania i monitorowania **11.1.** Skonfigurowanie centralnego systemu logowania dla przełączników w celu rejestrowania zdarzeń, takich jak nieautoryzowane próby dostępu. **12.** Wdrożenie narzędzi monitorujących (np. SNMP, Syslog) do bieżącej analizy wydajności i bezpieczeństwa sieci.
Etap testowania	**13.** Testy wydajnościowe i funkcjonalne **13.1.** Sprawdzenie przepustowości sieci oraz poprawności konfiguracji VLAN-ów. **13.2.** Symulacja różnych scenariuszy ruchu, takich jak przesyłanie danych między VLAN-ami czy dostęp do usług wspólnych. **14.** Testy awaryjne **14.1.** Symulacja awarii jednego z przełączników i sprawdzenie poprawności działania mechanizmów redundancji. **15.** Testowanie zachowania sieci w przypadku naruszenia polityk bezpieczeństwa.
Szkolenie i dokumentacja	**16.** Szkolenie administratorów IT **16.1.** Szkolenie z zakresu zarządzania nową infrastrukturą, w tym konfiguracji VLAN-ów, routingu oraz mechanizmów bezpieczeństwa. **16.2.** Przekazanie procedur diagnostycznych i rozwiązywania problemów. **17.** Przygotowanie dokumentacji **17.1.** Opracowanie pełnej dokumentacji technicznej, obejmującej topologię sieci, konfiguracje przełączników oraz reguły ACL. **18.** Przekazanie procedur awaryjnych i harmonogramu przeglądów.
Dobre praktyki uwzględnione w wdrożeniu	**19.** Zasada minimalnych uprawnień: Dostęp do zasobów przydzielany wyłącznie na podstawie faktycznych potrzeb. **20.** Redundancja: Konfiguracja portów uplink i zastosowanie dwóch przełączników dla kluczowych połączeń w celu zapewnienia ciągłości działania. **21.** Regularne aktualizacje: Utrzymywanie aktualnego oprogramowania przełączników w celu minimalizacji ryzyka podatności. **22.** Monitorowanie i audyt: Stały nadzór nad działaniem sieci i okresowe przeglądy polityk bezpieczeństwa.
Efekty wdrożenia	**23.** Zwiększenie bezpieczeństwa dzięki izolacji segmentów sieci. **24.** Optymalizacja wydajności i przepływów danych. **25.** Poprawa zarządzania siecią i skalowalność na przyszłość. **26.** Gotowość infrastruktury do obsługi nowych usług i wymagań urzędu.

5. Wdrożenie i konfiguracja oprogramowania klasy SIEM typu open source

Komponent	Wymagane minimalne parametry techniczne – SIEM
Cel wdrożenia	**1.** Celem zamówienia jest wdrożenie i konfiguracja oprogramowania open source klasy SIEM, przeznaczonego do centralnego monitorowania bezpieczeństwa teleinformatycznego, obejmującego zbieranie, korelację i analizę zdarzeń bezpieczeństwa, wykrywanie incydentów, monitorowanie integralności systemów oraz wsparcie procesów reagowania na incydenty i raportowania. **2.** Rozwiązanie ma umożliwiać bieżący nadzór nad bezpieczeństwem systemów informatycznych Zamawiającego, zwiększenie zdolności detekcyjnych oraz spełnienie wymagań organizacyjnych i prawnych w zakresie monitorowania i zarządzania incydentami bezpieczeństwa informacji.
Architektura rozwiązania	**3.** Wykonawca wdroży rozwiązanie o architekturze scentralizowanej, opartej na komponentach typu open source, obejmującej co najmniej: **3.1.** centralny komponent zarządzający (serwer/menedżer), **3.2.** komponent odpowiedzialny za gromadzenie, indeksowanie i przechowywanie danych zdarzeniowych, **3.3.** interfejs użytkownika (panel zarządczy / dashboard), **3.4.** agentów instalowanych na monitorowanych systemach końcowych. **4.** Rozwiązanie musi umożliwiać skalowanie (pionowe lub poziome) oraz pracę w architekturze jedno- lub wielowęzłowej, w zależności od potrzeb Zamawiającego.
Zakres prac wdrożeniowych	**5.** Analiza przedwdrożeniowa. Wykonawca przeprowadzi analizę środowiska Zamawiającego oraz uzgodni: **5.1.** zakres monitorowanych systemów i usług, **5.2.** docelową architekturę rozwiązania, **5.3.** sposób instalacji (np. instalacja natywna lub konteneryzacja), **5.4.** polityki bezpieczeństwa, retencji danych oraz kopii zapasowych, **5.5.** role i zakresy uprawnień użytkowników. **6.** Instalacja i uruchomienie komponentów centralnych **6.1.** Wykonawca zainstaluje i skonfiguruje wszystkie niezbędne komponenty centralne rozwiązania open source, zapewniając ich prawidłową integrację, komunikację oraz gotowość do pracy w środowisku produkcyjnym Zamawiającego. **6.2.** Instalacja zostanie wykonana w infrastrukturze Zamawiającego, na dostarczonym lub posiadanym sprzęcie i systemach, z uwzględnieniem zasad bezpieczeństwa, separacji usług oraz odporności na awarie. **7.** Instalacja i konfiguracja agentów **7.1.** Wykonawca zainstaluje i skonfiguruje agenty na wskazanych przez Zamawiającego systemach końcowych (w szczególności serwerach i stacjach roboczych), zapewniając: **7.1.1.** bezpieczną komunikację z komponentem centralnym, **7.1.2.** przypisanie agentów do logicznych grup/polityk, **7.1.3.** centralne zarządzanie konfiguracją agentów.
Konfiguracja funkcjonalna systemu	**8.** Zbieranie i analiza zdarzeń. Wykonawca skonfiguruje mechanizmy zbierania i analizy zdarzeń bezpieczeństwa, obejmujące co najmniej: **8.1.** logi systemowe i bezpieczeństwa systemów operacyjnych, **8.2.** zdarzenia aplikacyjne i usługowe (w zakresie uzgodnionym z Zamawiającym), **8.3.** podstawową korelację zdarzeń i generowanie alertów bezpieczeństwa.

Komponent	Wymagane minimalne parametry techniczne – SIEM
	9. Monitorowanie integralności. Wykonawca skonfiguruje funkcję monitorowania integralności plików i konfiguracji systemowych, umożliwiającą wykrywanie nieautoryzowanych zmian w określonych lokalizacjach systemowych i aplikacyjnych oraz generowanie powiadomień o wykrytych naruszeniach. **10.** Automatyzacja reakcji. Wykonawca skonfiguruje mechanizmy reakcji na incydenty bezpieczeństwa, umożliwiające automatyczne lub półautomatyczne wykonywanie zdefiniowanych akcji po wystąpieniu określonych zdarzeń lub alertów, z zachowaniem mechanizmów kontroli i ograniczenia ryzyka fałszywych alarmów. **11.** Wizualizacja i raportowanie. Wykonawca skonfiguruje interfejs użytkownika umożliwiający: **11.1.** wizualizację zdarzeń i alertów bezpieczeństwa, **11.2.** przegląd stanu monitorowanych systemów, **11.3.** analizę zdarzeń historycznych, **11.4.** generowanie zestawień i raportów na potrzeby zarządcze i audytowe.
Zarządzanie dostępem i bezpieczeństwo rozwiązania	**12.** Wykonawca skonfiguruje mechanizmy zarządzania dostępem, obejmujące: **12.1.** role użytkowników i zakresy uprawnień, **12.2.** zasadę minimalnych uprawnień, **12.3.** rejestrowanie działań administracyjnych. **13.** Komunikacja pomiędzy komponentami systemu oraz agentami musi być zabezpieczona kryptograficznie, a wdrożenie wykonane zgodnie z zasadami „hardeningu" oraz dobrymi praktykami bezpieczeństwa.
Retencja danych i kopie zapasowe	**14.** Wykonawca zaprojektuje i wdroży: **14.1.** politykę retencji danych zdarzeniowych, **14.2.** mechanizmy rotacji i archiwizacji danych, **14.3.** procedury wykonywania kopii zapasowych konfiguracji systemu oraz danych niezbędnych do jego odtworzenia po awarii.
Testy	**15.** Wykonawca przeprowadzi testy poprawności działania systemu, obejmujące w szczególności: **15.1.** weryfikację poprawnej komunikacji pomiędzy agentami a komponentem centralnym, **15.2.** generowanie i obsługę alertów bezpieczeństwa, **15.3.** poprawność działania mechanizmów uprawnień i wizualizacji.

6. Wdrożenie i konfiguracja systemu do monitorowania infrastruktury informatycznej

Komponent	Wymagane minimalne parametry techniczne – SIEM
Wymagania ogólne	**1.** Przedmiotem zamówienia jest konfiguracja i wdrożenie aktualnie posiadanego oprogramowania do monitorowania infrastruktury IT typy open-source, zwanego dalej System. **2.** Opis posiadanego Systemu, spis funkcjonalności: **2.1.** przystosowane do monitorowania złożonych środowisk IT **2.2.** monitoring sieci, serwerów, chmury, aplikacji i usług w jednym systemie **2.3.** możliwość zdefiniowania inteligentnych progów problemowych, proaktywnego reagowania i przewidywania trendów, możliwość wykorzystywania machine learning **2.4.** możliwość wysyłania wielokanałowo customizowanych powiadomień o problemach przy pomocy: min. sms, email, slack, telegram, VictorOPS, SIGNL4 **2.5.** możliwość prezentacji danych poprzez tworzenie wizualizacji, wykresów, map, map infrastruktury, raportów **2.6.** maksymalnie jeden interfejs do całej infrastruktury **2.7.** możliwość śledzenia wybranych KPI
Zakres wdrożenia Systemu	**3.** Instalacja i konfiguracja serwera systemu w najnowszej dostępnej na dzień wdrożenia wersji LTS wraz z bazą danych oraz interfejsem Web **4.** Przygotowanie instrukcji instalacji oraz konfiguracji Agenta na urządzeniach z systemami rodziny Windows oraz Linux **5.** Utworzenie akcji automatycznego dodawania hostów do monitoringu z zainstalowanym Agentem z podziałem na rodzinę systemów operacyjnych Linux oraz Windows **6.** Wykreowanie monitoringu podstawowych parametrów maszyn z systemami operacyjnymi rodziny Windows oraz Linux takich jak dostępność urządzenia, zajętość dysków, obciążenie CPU, obciążenia kart sieciowych, działanie poszczególnych usług **7.** Wykreowanie monitoringu parametrów macierzy dyskowej takich jak dostępność urządzenia, temperatura dysków, zajętość puli dyskowej, prędkość wolumenów, obciążenie CPU i stan komponentów z wykorzystaniem protokołu HTTP oraz konfiguracja macierzy **8.** Wykreowanie monitoringu podstawowych parametrów 3 modeli urządzeń sieciowych firmy CISCO takich jak dostępność urządzenia, czas pracy, status działania oraz prędkość interfejsów sieciowych z wykorzystaniem protokołu SNMP **9.** Wykreowanie monitoringu parametrów do 3 wskazanych przez Klienta stron internetowych takich jak data wygaśnięcia certyfikatów, dostępność oraz czas ładowania strony **10.** Wykreowanie monitoringu parametrów systemu wirtualizacji VMware VCenter takich jak wystąpień błędów w eventlogu, stan zdrowia klastra, opóźnienia odczytu i zapisu oraz ilości wolnego miejsca wszystkich datastore'ów, stanu zdrowia, zużycia CPU, miejsca wszystkich hypervisor'ów **11.** Wykreowanie monitoringu parametrów blade'ów firmy HP takich jak stan działania poszczególnych komponentów oraz dostępność urządzeń z wykorzystaniem protokołu IPMI **12.** Wykreowanie monitoringu statusów wykonywanych jobów oraz sesji systemu Backup z wykorzystaniem interfejsu REST API

Komponent	Wymagane minimalne parametry techniczne – SIEM
	13. Wykreowanie i konfiguracja monitoringu parametrów takich jak zużycie miejsca, prędkość zapisu i odczytu, ilość napotkanych błędów i blokad baz danych opartych o silnik MSSQL z wykorzystaniem sterownika ODBC **14.** Wykreowanie i konfiguracja monitoringu parametrów takich zużycie miejsca, pamięci podręcznej, prędkość zapisu oraz odczytu, ilość błędów i stan baz danych opartych o silnik Oracle z wykorzystaniem sterownika ODBC **15.** Wytworzenie integracji powiadamiania mailowego oraz wytworzenie do 5 różnych akcji powiadamiania w przypadku problemu na hoście bądź grupie hostów **16.** Szkolenie powdrożeniowe w zakresie przedstawienia działania wytworzonych rozwiązań monitoringu oraz podstawowej obsługi Systemu **17.** Wytworzenie dokumentacji powdrożeniowej **18.** Wytworzenie rozszerzonego monitoringu pojedynczej strony internetowej przy wykorzystaniu zewnętrznego skryptu automatyzującego przemieszczania się po stronie według scenariusza przygotowanego przez Klienta i weryfikowania konkretnego kodu błędu

7. Szkolenia dla Administratora IT

Komponent	Wymagane minimalne parametry techniczne – Szkolenia
Szkolenie z dostarczonego systemu DLP	**1.** Wykonawca przeprowadzi szkolenie z obsługi i administracji dostarczonego systemu klasy DLP (Data Loss Prevention), przeznaczone dla administratorów oraz osób odpowiedzialnych za bezpieczeństwo informacji u Zamawiającego. **2.** Zakres szkolenia musi obejmować co najmniej: **2.1.** omówienie architektury wdrożonego systemu oraz jego roli w systemie bezpieczeństwa Zamawiającego, **2.2.** zasady klasyfikacji danych i polityk ochrony informacji, **2.3.** konfigurację reguł zapobiegania utracie danych oraz mechanizmów wykrywania naruszeń, **2.4.** obsługę alertów i incydentów związanych z nieautoryzowanym przetwarzaniem lub wyciekiem danych, **2.5.** raportowanie zdarzeń oraz analizę incydentów, **2.6.** podstawowe czynności administracyjne i utrzymaniowe. **3.** Szkolenie powinno umożliwiać samodzielną, bezpieczną eksploatację systemu oraz świadome reagowanie na zdarzenia związane z ochroną danych.
Szkolenie z dostarczonego systemu NAC	**4.** Wykonawca przeprowadzi szkolenie z obsługi i administracji dostarczonego systemu klasy NAC (Network Access Control), przeznaczone dla administratorów infrastruktury IT oraz personelu odpowiedzialnego za bezpieczeństwo sieci. **5.** Zakres szkolenia musi obejmować co najmniej: **5.1.** omówienie zasad działania i architektury wdrożonego systemu, **5.2.** konfigurację polityk dostępu do sieci przewodowej i bezprzewodowej, **5.3.** identyfikację i autoryzację urządzeń końcowych oraz użytkowników, **5.4.** zarządzanie profilami urządzeń i regułami dostępu, **5.5.** obsługę zdarzeń naruszeń polityk dostępu i reagowanie na nieautoryzowane próby podłączenia, **5.6.** monitorowanie stanu sieci oraz interpretację komunikatów i raportów systemowych. **6.** Szkolenie powinno zapewnić uczestnikom wiedzę umożliwiającą bieżące zarządzanie dostępem do sieci oraz ograniczanie ryzyk bezpieczeństwa.
Szkolenie z dostarczonego systemu do backupu	**7.** Wykonawca przeprowadzi szkolenie z obsługi i administracji wdrożonego systemu do tworzenia kopii zapasowych, przeznaczone dla administratorów systemów i infrastruktury IT. **8.** Zakres szkolenia musi obejmować co najmniej: **8.1.** omówienie architektury wdrożonego rozwiązania oraz zakresu objętego backupem, **8.2.** konfigurację harmonogramów kopii zapasowych oraz polityk retencji danych, **8.3.** zarządzanie repozytoriami danych i nośnikami kopii zapasowych, **8.4.** procedury odtwarzania danych (restore) na poziomie plików, systemów oraz usług, **8.5.** monitorowanie poprawności wykonywania kopii zapasowych i analiza błędów, **8.6.** dobre praktyki w zakresie bezpieczeństwa danych i testów odtwarzania. **9.** Szkolenie powinno przygotować uczestników do samodzielnego zarządzania procesem backupu i odtwarzania danych.

Komponent	Wymagane minimalne parametry techniczne – Szkolenia
Szkolenie z obsługi wdrożonego systemu SIEM	**10.** Wykonawca przeprowadzi szkolenie z obsługi i eksploatacji wdrożonego systemu klasy SIEM, przeznaczone dla administratorów, personelu IT oraz osób odpowiedzialnych za monitoring bezpieczeństwa. **11.** Zakres szkolenia musi obejmować co najmniej: **11.1.** omówienie architektury wdrożonego systemu oraz źródeł zbieranych danych, **11.2.** obsługę interfejsu użytkownika i paneli wizualizacyjnych, **11.3.** analizę zdarzeń bezpieczeństwa i interpretację alertów, **11.4.** podstawy korelacji zdarzeń oraz identyfikacji incydentów, **11.5.** obsługę mechanizmów reagowania na incydenty (manualnych lub automatycznych), **11.6.** generowanie raportów oraz zestawień na potrzeby operacyjne i audytowe. **12.** Szkolenie powinno umożliwiać samodzielny monitoring bezpieczeństwa środowiska IT Zamawiającego.
Szkolenie z obsługi wdrożonego systemu do monitorowania infrastruktury IT	**13.** Wykonawca przeprowadzi szkolenie z obsługi i administracji wdrożonego systemu monitorowania infrastruktury IT, przeznaczone dla administratorów systemów i sieci. **14.** Zakres szkolenia musi obejmować co najmniej: **14.1.** omówienie architektury i zakresu monitorowanej infrastruktury, **14.2.** konfigurację monitoringu zasobów sprzętowych, systemowych i usługowych, **14.3.** definiowanie progów alarmowych i powiadomień, **14.4.** analizę stanu infrastruktury oraz identyfikację problemów wydajnościowych, **14.5.** interpretację alertów i raportów, **14.6.** podstawowe czynności administracyjne i utrzymaniowe systemu. **15.** Szkolenie powinno przygotować uczestników do bieżącego nadzoru nad infrastrukturą IT oraz wczesnego wykrywania awarii i nieprawidłowości.

8. Rozwiązania równoważne

1. Zamawiający dopuszcza oferowanie rozwiązań równoważnych w stosunku do wymagań opisanych w OPZ, o ile oferowane rozwiązania będą spełniały minimalne wymagania określone przez Zamawiającego oraz zapewniały uzyskanie parametrów technicznych i funkcjonalnych nie gorszych niż wskazane w dokumentacji zamówienia.
2. Wszelkie nazwy własne, znaki towarowe, certyfikaty, normy, standardy, technologie, typy urządzeń lub oprogramowania przywołane w OPZ należy traktować jako przykładowe. Zamawiający dopuszcza rozwiązania równoważne, rozumiane jako takie, które zapewniają co najmniej:
   - **2.1.** tę samą funkcjonalność,
   - **2.2.** parametry techniczne nie gorsze niż określone w OPZ,
   - **2.3.** zgodność z istniejącą infrastrukturą Zamawiającego,
   - **2.4.** poziom bezpieczeństwa i niezawodności nie gorszy niż określony w OPZ,
   - **2.5.** zgodność z wymaganymi normami prawnymi, branżowymi i standardami interoperacyjności.
3. Ocena równoważności będzie dokonywana przez Zamawiającego na podstawie analizy dokumentów i oświadczeń złożonych przez Wykonawcę.
4. W celu wykazania równoważności, Wykonawca jest zobowiązany do przedłożenia wraz z ofertą:
   - **4.1.** szczegółowego opisu technicznego oferowanego rozwiązania,
   - **4.2.** kart katalogowych, specyfikacji producenta lub innych dokumentów potwierdzających spełnianie wymagań OPZ,
   - **4.3.** w zakresie wymagań bezpieczeństwa – stosownych certyfikatów lub deklaracji zgodności,
   - **4.4.** oświadczenia Wykonawcy o równoważności oferowanego rozwiązania.
5. W przypadku, gdy Wykonawca nie wykaże równoważności zaoferowanego rozwiązania, oferta zostanie odrzucona na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp jako niezgodna z treścią SWZ.

9. Zakres wsparcia powdrożeniowego i poszkoleniowego

1. Pod pojęciem „okresu wsparcia powdrożeniowego i poszkoleniowego" Zamawiający rozumie czas, w którym Wykonawca, poza świadczeniem podstawowej gwarancji, zapewnia swoją dostępność w zakresie:
2. Wsparcia technicznego, obejmującego:
   - **2.1.** diagnozę i usuwanie błędów konfiguracyjnych,
   - **2.2.** wsparcie w zakresie optymalizacji działania systemów wdrożonych w ramach zamówienia,
   - **2.3.** doradztwo w zakresie dalszego dostosowywania parametrów rozwiązań do potrzeb użytkownika.
3. Wsparcia merytorycznego, obejmującego:
   - **3.1.** konsultacje w zakresie prawidłowego korzystania z funkcjonalności systemu,
   - **3.2.** odpowiedzi na pytania związane z eksploatacją wdrożonych rozwiązań,
   - **3.3.** wsparcie w tworzeniu i weryfikacji wewnętrznych procedur użytkownika dotyczących wdrożonych rozwiązań.
4. Wsparcia poszkoleniowego, obejmującego:
   - **4.1.** dodatkowe wyjaśnienia, powtórzenia i uzupełnienia treści szkoleń przeprowadzonych w ramach realizacji zamówienia,
   - **4.2.** utrwalanie wiedzy przekazanej pracownikom Zamawiającego,
   - **4.3.** udostępnienie materiałów szkoleniowych oraz odpowiedzi na pytania zgłaszane po szkoleniach.
5. Zasady świadczenia wsparcia:
   - **5.1.** Wykonawca zobowiązany jest zapewnić wsparcie powdrożeniowe i poszkoleniowe przez minimum 14 dni kalendarzowych od daty podpisania protokołu odbioru końcowego. Za zaoferowanie dłuższego okresu wsparcia Zamawiający przyzna dodatkowe punkty zgodnie z opisem kryteriów oceny ofert w SWZ.
   - **5.2.** Czas reakcji Wykonawcy:
     - **5.2.1.** dla zgłoszeń zwykłych – odpowiedź Wykonawcy w terminie do 1 dnia roboczego,
     - **5.2.2.** dla zgłoszeń krytycznych (tj. uniemożliwiających korzystanie z podstawowych funkcji systemu) – odpowiedź w ciągu 4 godzin roboczych.
   - **5.3.** Dostępność wsparcia:
     - **5.3.1.** od poniedziałku do piątku w godzinach pracy urzędu, tj. od 7:00 do 15:00 (z wyłączeniem dni ustawowo wolnych od pracy),
     - **5.3.2.** w ramach zaoferowanego okresu wsparcia Wykonawca pozostaje dostępny minimum przez 5 godzin tygodniowo.
   - **5.4.** Możliwe formy kontaktu ze wsparciem:
     - **5.4.1.** telefon kontaktowy,
     - **5.4.2.** adres e-mail dedykowany dla Zamawiającego,
     - **5.4.3.** opcjonalnie: panel zgłoszeń online lub inny system ticketowy (jeśli jest dostępny po stronie Wykonawcy).
   - **5.5.** Sposób dokumentowania:
     - **5.5.1.** Wykonawca prowadzi rejestr zgłoszeń Zamawiającego, który przekazuje Zamawiającemu w formie zestawienia po zakończeniu okresu wsparcia.