Cyberbezpieczne Wodociągi

Załącznik nr 2 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Dotyczy: „Zwiększenie cyberodporności i ciągłości działania Przedsiębiorstwa Wodno-Kanalizacyjnego Wołów Sp. z o.o. poprzez wdrożenie nowoczesnych rozwiązań, modernizację infrastruktury oraz podniesienie kompetencji personelu”.

Postępowanie nr IN/261/2/2026

Część 1 – Dostawa sprzętu IT

1. Serwer – 2 sztuki.

Nazwa elementu, parametru lub cechy	Opis wymagań Serwerów
Obudowa	Do instalacji w szafie Rack 19”, wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość instalacji ramienia do zarządzania kablami.
Procesor	Architektura x86, maksymalny TDP dla procesora – maksymalnie 150W. Wymagana ilość rdzeni dla procesora – 16. Minimalna częstotliwość pracy procesora 2.3GHz. Minimalna ilość kanałów procesora – 8. Ilość kości pamięci na kanał – 2. Wynik wydajności procesora nie powinien być niższy niż 373 punkty baseline w teście SPECrate 2017 Integer w konfiguracji dwuprocesorowej, opublikowanym przez SPEC.org (www.spec.org), dla serwera oferowanego producenta.
Liczba zainstalowanych procesorów	1
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów Intel Xeon wykonujących 64-bitowe instrukcje
Pamięć operacyjna	Zainstalowane minimum 128GB pamięci RAM o częstotliwości 6400MHz. Pamięć zainstalowana w kościach 32GB

	Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM.
Zabezpieczenie pamięci	Memory mirroring, ECC, SDDC, ADDDC
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.
Rozbudowa dysków	W chwili dostawy serwer musi posiadać zainstalowane minimum: • 2 sztuki dysków SSD SATA o pojemności min. 480GB każdy. Wymagana możliwość instalacji minimum dysków M.2 zabezpieczonych sprzętowym raid . Nie dopuszcza się rozwiązania, w którym dyski M.2 ani obsługujący je kontroler zajmują którykolwiek ze slotów PCIe. Wymagany jest wewnętrzny slot na kartę Micro SD.
Kontroler dyskowy	Zainstalowany sprzętowy kontroler SAS 12Gb. Kontroler musi posiadać 4GB pamięci Flash. Kontroler musi obsługiwać poziomy RAID - 0/1/10/5/50/6/60.
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 1300W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	Zainstalowana czteroportowa karta 1Gb. Karta nie może zajmować żadnego ze slotów PCIe. Zainstalowane dwuportowa karta 10/25Gb SFP28. Karta musi obsługiwać RoCE oraz

	iWARP. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
Sloty I/O	Serwer w momencie dostawy powinien posiadać 2 sloty PCIe Gen5 z czego 1 slot x16, 2 sloty OCP Gen5 (z czego jeden aktywny) oraz jeden slot PCIe wewnątrz obudowy serwera dedykowany pod kontroler dyskowy. Możliwość rozbudowy do 10 slotów PCIe Gen5 z czego: • 4 sloty x8 Low Profile • 2 sloty x8 High Profile • 4 sloty x16 High Profile
Dodatkowe porty	• z przodu obudowy: możliwość instalacji 2x USB 3 (z czego jeden z możliwością zarządzania serwerem) , zewnętrzny dedykowany port diagnostyczny, możliwość instalacji portu Mini DisplayPort • z tyłu obudowy: 2x USB 3, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9. • wewnątrz obudowy: Możliwość instalacji portu USB 3 wewnątrz obudowy. Wszystkie tylne porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port na kartę Micro SD powinny być umieszczone na osobnej dedykowanej płytce I/O, którą łączy się bezpośrednio z płytą główną serwera.
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1. Serwer w obecnej konfiguracji musi być przystosowany, aby mógł pracować w temperaturze otoczenia 30 stopni Celsjusza, wykorzystując pełne możliwości (bez Throttlingu).
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna • Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej,

	utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediów z wykorzystaniem Java client • Przekierowanie konsoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Kontroler zarządzania musi posiadać 100Mb wewnętrznej pamięci Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. Możliwość rozszerzenia tej przestrzeni d 4Gb poprzez zastosowanie karty microSD • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. • Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.
Funkcje zabezpieczeń	Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT (umieszczony na dedykowanej płytce I/O wspomnianej w sekcji Dodatkowe porty) wspierający TPM2.0 oraz Platform Firmware Resiliency (PFR)., Możliwość zainstalowania przedniego panelu zamykanego na klucz. Wbudowany w BIOS

	mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.
Urządzenia hot swap	Dyski twarde, zasilacze, wentylatory.
Obsługa	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu powinno odbywać się poprzez dedykowany port USB na froncie serwera. Wymaga się aby serwer posiadał diody sygnalizacyjne awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
Gwarancja	36 miesięcy gwarancji producenta z oknem serwisowym 24x7, z reakcją NBD. Uszkodzone nośniki danych pozostają własnością zamawiającego. Możliwość wykupienia dodatkowego wsparcia, świadczonego przez producenta, z gwarantowanym czasem naprawy w ciągu 6 godzin. Wsparcie musi być obsługiwane w języku Polskim z pojedynczym punktem kontaktu. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera..

2. Macierz dyskowa z dyskami – 1 sztuka.

L.p.	Parametr	Charakterystyka (wymagania minimalne)
1	Obudowa	Macierz musi mieć możliwość zainstalowania w standardowej szafie rack 19". Rozmiar jednostki sterującej macierzą nie może przekraczać 2U. W momencie dostawy macierz musi mieć możliwość zainstalowania do 12 dysków 3,5”. Dodawanie kolejnych półek lub dysków musi odbywać się bezprzerwowo.
2	Kontrolery	Wymagane dwa moduły sterujące macierzą pracujące w trybie active-active. W przypadku wystąpienia awarii sprawny moduł musi automatycznie przejąć obsługę wszystkich zasobów prezentowanych przez macierz.
3	Dostepne porty	Oferowana macierz musi posiadać w chwili dostawy minimum: • Po 2 porty 10/25Gb na kontroler (w sumie 4 porty na macierz). Oferowana macierz musi mieć możliwość rozszerzenia o porty (poprzez dołożenie kart rozszerzeń) na: - 2 karty posiadające 4 porty SAS 12Gb każda - 2 karty posiadające 4 porty 10Gb Base-T każda - 2 karty posiadające 4 porty 16/32Gb FC każda - 2 karty posiadające 4 porty 10/25Gb iSCSI każda
	Okablowanie	Do macierzy należy dostarczyć 4 kable DAC SFP+ o długości min. 3m Wraz z macierzą należy dostarczyć kabel USB-A --> USB-C służący do połączenia z portem szeregowym.
4	Cache	Każdy z modułów sterujących musi być wyposażony w min 32GB pamięci cache zabezpieczonej mechanizmem mirroringu. Pamięć podręczna musi być zabezpieczona przed utratą danych w przypadku zaniku zasilania. Rozwiązania wykorzystujące do tego celu tylko i wyłącznie tzw. podtrzymanie cache za pomocą baterii nie są akceptowalne. Bateria może być użyta tylko i wyłącznie na czas zrzutu danych z cache na pamięć nieulotną. Ponadto macierz musi umożliwiać utworzenie dedykowanej przestrzeni SSD stanowiącej pamięć cache pośredniczącą w operacjach odczytów danych z macierzy. Wymaga się możliwości utworzenia takiej przestrzeni o wielkości 5TB.
5	Dyski	Macierz musi obsługiwać dyski SSD, SSD FIPS, SAS, NL-SAS, NL-SAS FIPS, SAS FIPS. Macierz w momencie dostarczenia musi być wyposażona w minimum 12 dysków dysków pojemnoości minimum 4TB każdy.
6	Funkcjonalnosc	Macierz musi obsługiwać typy protekcji RAID 0,1,3,5,6,10 oraz powinna posiadać funkcjonalność zarzadzania informacjami o parzystości oraz dyskami spare w całej puli dysków utworzonej ze wszystkich dysków które mogą zastać zainstalowane w macierzy. W przypadki awarii dysku, do jego obudowy musi być używany każdy dysk z takiej puli. Macierz musi umożliwiać zwiększanie i zmniejszanie online pojemności poszczególnych wolumenów logicznych oraz dynamiczne alokowanie przestrzeni dyskowej (tzw. „*thin provisioning*”).

		Macierz musi posiadać funkcjonalność sprawdzania integralności zapisywanych danych poprzez odczyt sumy kontrolnej z karty HBA podłączonego serwera. Macierz musi mieć możliwość wykonywania minimum 512 kopii migawkowych typu copy-on-write (jeśli funkcjonalność wymaga licencji, nie jest wymagana w momencie dostawy). Macierz musi posiadać funkcjonalność klonowania danych. Wymagana możliwość definiowania maksymalnej ilości kopii migawkowych. W przypadku osiągniecia zdefiniowanej ilości kopii system musi automatyczne kasować kopie najstarsze. Ponadto macierz powinna posiadać funkcjonalność tworzenia konsystentnych kopii migawkowych ze wskazanych przestrzeni dyskowych. Macierz musi mieć możliwość replikacji danych po FC w trybie asynchronicznym. Nie wymaga się funkcjonalności replikacji w momencie dostawy. Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 512 partycji. Wymagana możliwość definiowania globalnych dysków hot-spare. Wymagana możliwość logicznej zamiany dysków z wykorzystaniem dysków nieprzypisanych. Macierz musi posiadać automatyczny monitoring z możliwością informowania o awariach poprzez protokół smtp oraz snmp oraz możliwość wysyłania powiadomień awarii do wskazanych odbiorców. Wysyłane powiadomienia musza zawierać nazwę macierzy, informacje o typie zdarzenia, datę i czas wystąpienia zdarzenia oraz krótki opis zdarzenia. Macierz musi mieć możliwość definiowania poziomu zajętości miejsca, po osiągnieciu którego nastąpi wysłanie powiadomienia pod wskazane adresy email. System zarzadzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego automatycznie w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień oraz braku wykrycia jakichkolwiek zadań wykonywanych na macierzy. Macierz musi mieć funkcjonalność automatycznej detekcji podłączonych hostów (nazwa hosta oraz typ systemu operacyjnego). Musi być możliwość edycji hostów dodanych w sposób automatyczny. Wymagana jest funkcjonalność automatycznego tworzenia przestrzeni dyskowych zoptymalizowanych pod katem używanych na nich aplikacji jak SQL Server, Exchange oraz Vmware vmfs. Wymagana jest możliwość automatycznego logicznego grupowania dysków macierzy (dodawanie dysków do istniejącej grupy oraz tworzenie nowej grupy z dodanych dysków). Macierz musi mieć możliwość definiowania priorytetu operacji wprowadzanych zmian konfiguracji w odniesieniu do obciążenia generowanego przez podłączone hosty. Wymagana jest możliwość sprawdzenia aktualnych zadań macierzy. Macierz musi umożliwiać szyfrowanie zapisywanych na niej danych poprzez zastosowanie dysków samoszyfrujących.

		Macierz musi posiadać możliwość fizycznej identyfikacji (dioda LED) aktywowanej z interfejsu zarzadzania oraz funkcjonalność fizycznego identyfikowania dysków (dioda LED) należących do jednej przestrzeni logicznej. Macierz musi mieć możliwość przypisania wolumenu danych tylko do wybranego hosta należącego do zdefiniowanego klastra.
7	Wydajność	Wymaga się możliwości rozbudowania macierzy do poziomu wydajności przynajmniej 299 000 operacji wejścia wyjścia dla losowego odczytu oraz przynajmniej 108 000 operacji wejścia wyjścia dla losowego zapisu. Wymagana pojemność dla wolumenów z dynamiczna alokacja przestrzeni to przynajmniej 256 TB
8	Zarzadzanie macierzą	Dostępne dwa porty 1Gbe Base-T w trybie primary/redundant. Dodatkowo po dwa porty Serial na kontroler (1x RJ-45 oraz 1x USB-C). Zarzadzanie macierzą powinno być możliwe za pomocą graficznego interfejsu użytkownika dostępnego poprzez protokół https, oraz za pomocą linii komend cli osiągalnej poprzez protokół ssh. Interfejs zarzadzania powinien wylogować sesje po maksymalnie 15 minutach bezczynności. Maksymalna ilość prób podania hasła administratora nie może być większa niż 5 do momentu zablokowania dostępu. Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control. Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy: - storage admin – pełen dostęp wyłączeniem ustawień bezpieczeństwa - security admin – dostęp do ustawień bezpieczeństwa - support admin – pełen dostęp serwisowy - monitor – możliwość odczytu konfiguracji Producent powinien udostępniać konsolę umożliwiająca dodawanie do domeny zarzadzania wielu macierzy jednocześnie. Wymaga się możliwości importu konfiguracji z jednej macierzy na inne.
9	Inne	Wymagana jest bezprzerwowa wymiana następujących elementów macierzy: kontrolery, moduły I/O, dyski, zasilacze oraz moduły SFP+. Obsługa systemów operacyjnych hosta: Microsoft Windows Server; Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES); VMware vSphere,
10	Gwarancja	36 miesięcy gwarancji producenta on-site z oknem serwisowym 24x7, z czasem reakcji NBD. Uszkodzone nośniki danych pozostają własnością zamawiającego.

		Możliwość wykupienia dodatkowego wsparcia z gwarantowanym czasem naprawy w ciągu 6 godzin. Serwis świadczony przez producenta macierzy lub przez autoryzowanego partnera serwisowego. Wymaga się aby serwis posiadał tylko jedną linie wsparcia, to znaczy że cały proces zgłaszania oraz procesowania zgłoszenia serwisowego odbywał się u jednego agenta dedykowanego do zgłoszenia.

3. Serwer do wykonywania kopii zapasowych typ 1 – 1 sztuka.

Nazwa elementu, parametru lub cechy	**Opis wymagań Serwerów**
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
Procesor	Architektura x86, maksymalny TDP dla procesora – 55W. Minimalna ilość rdzeni dla procesora – 4, taktowanie procesora nie niższe niż 3.5GHz. Wynik wydajności procesora instalowanego w oferowanym serwerze nie powinien być niższy niż 58 punków base w teście SPECspeed 2017 Floating Point, opublikowanym przez SPEC.org (www.spec.org). Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org
Liczba zainstalowanych procesorów	1
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera wykonujących 64-bitowe instrukcje

Pamięć operacyjna	Zainstalowane minimum 16GB pamięci RAM o częstotliwości minimum 5600MHz. Zainstalowana pamięć powinna być sygnowana i zoptymalizowana do użycia przez producenta serwera. Minimum 4 sloty na pamięć. Możliwość rozbudowy do 128GB RAM.
Zabezpieczenie pamięci	Minimum ECC
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu serwera. Wymagana możliwość instalacji portu VGA na panelu przednim.
Rozbudowa dysków	W chwili dostawy serwer musi posiadać możliwość instalacji do 4 dysków 3,5” Hot Swap. Serwer powinien posiadać zainstalowane: • Dysk SAS o pojemności minimum 8TB Możliwość instalacji adaptera posiadającego dwa dyski M.2 SSD zabezpieczonych sprzętowym kontrolerem RAID.

Kontroler dyskowy	Zainstalowany sprzętowy kontroler dyskowy 12Gb z 4GB Flash. Kontroler musi obsługiwać poziomy RAID – 0/1/10/5. Zainstalowana jedna dwuportowa karta HBA SAS 12Gb ze złączami SFF-8644.
Zasilacz	Jeden zasilacz o mocy minimum 800W z certyfikatem minimum Titanium wraz z kablem zasilającym C13-C14 minimum 2.8m długości. Możliwość rozbudowy o drugi redundantny zasilacz.
Interfejsy sieciowe	Zintegrowane na płycie 2 porty 1Gbs Base-T. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
Dodatkowe sloty I/O	Serwer powinien posiadać 2 sloty PCIe generacji 4. Dodatkowo serwer musi posiadać wewnętrzny slot PCIe na potrzeby kontrolera dyskowego.
Dodatkowe porty	• z przodu obudowy: 1x USB 3.2, 1x USB 2.0, Możliwość instalacji portu VGA. • z tyłu obudowy: 2x USB 3.2, , 1x port VGA , DB9
Chłodzenie	Przynajmniej cztery wentylatory.
Zarządzanie	Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania: • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna • Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O, lokalizacja • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie

	minimum 250 zdarzeń. • Wysylanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediów z wykorzystaniem Java client • Przekierowanie kosnoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. • Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.
Funkcje zabezpieczeń	Hasło włączania, hasło administratora, moduł TPM 2.0, Wymagana możliwość zainstalowania przedniego panelu zabezpieczającego zamykanego na klucz.
Urządzenia hot swap	Dyski twarde, zasilacze.
Diagnostyka	Możliwość przewidywania awarii dla pamięci, dysków wewnętrznych. Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji

	i włączenia/wyłączenia serwera.
Wymiary	Maksymalna długość obudowy – 561mm
Gwarancja	36 miesięcy gwarancji producenta z oknem serwisowym 24x7, z czasem reakcji NBD. Uszkodzone nośniki danych pozostają własnością zamawiającego. Możliwość wykupienia dodatkowego wsparcia z gwarantowanym czasem naprawy w ciągu 6 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.

4. Serwer do wykonywania kopii zapasowych typ 2 – 1 sztuka.

Lp.	Elementy	Wymagane parametry i właściwości urządzenia
1.	Wykorzystana technologia	LTO-8 Ultrium wspierające technologię partycjonowania nośników. Urządzenie musi mieć możliwość instalowania w tej samej obudowie i w tym samym czasie także napędów LTO innych generacji
2.	Wbudowane napędy	Minimum jeden napęd LTO-8 wyposażony w złącze z interfejsem dual SAS 6GB. Urządzenie powinno mieć możliwość instalowania w tej samej obudowie także napędów LTO z interfejsem dual FC 8Gb oraz wspierać technologię LTFS (Linear Tape File System) kompatybilną z systemami Linux, MAC OS i Microsoft. Prędkość zapisu pojedynczego napędu LTO-8 bez kompresji – do 300 MB/sek. Zainstalowany napęd powinien mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching) oraz stosować szyfrowanie danych metodą AES 256-bit W komplecie: • kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m • 8x taśma LTO8 WORM • Oznaczenia dla taśm LTO8, numery: 1-200 • Oznaczenia dla taśm LTO8 WORM, numery: 1-200 • 1x Taśma czyszcząca
3.	Ilość slotów i magazynki	Minimum 8 kieszeni na taśmy (urządzenie musi być dostarczone z kompletem

		magazynków). Jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów i magazynków zainstalowanych w urządzeniu. Wymagana ilość mail slot (I/E): min. 1. Wymiana taśm przez MailSlot powinna odbywać się bez konieczności wysuwania całego magazynka.
4.	Pojemność	Pojemność bez kompresji – minimum 96TB
5.	Obudowa	Typu rack 19”. Wszystkie elementy do montażu winny być dostarczone wraz z urządzeniem, wysokość maksymalnie 1U
6.	Zarządzanie	Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia oraz zdalne przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu FastEthernet. Wymagane wsparcie SNTP, protokołów SSL/TLS i IPv6 oraz definiowanie minimum 3 poziomów zarządzania urządzeniem i dostępem do niego. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówna poprzez web GUI jak i poprzez panel kontrolny urządzenia. Wymagana możliwość zdalnego wysuwania magazynków, restartowania biblioteki oraz wyłączania zasilania napędów poprzez webGUI. Aktualizacja firmware robota biblioteki oraz napędu musi być możliwa poprzez web GUI oraz USB (panel operatora).
7.	Dodatkowe interfejsy	Biblioteka musi być wyposażone w interfejs sieciowy, interfejs USB oraz interfejs ADI
8.	Obsługa urządzenia	Wymagana możliwość wymiany napędu, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Zarówno napęd jak i moduł portów zarządzania powinny być wyposażone w lampki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki.
9.	Partycjonowanie	Wymagana jest możliwość stworzenia 1 logicznej partycji na urządzeniu – jeżeli do tej operacji konieczna jest dodatkowa licencja, należy ją dostarczyć wraz z urządzeniem.
10.	Wyposażenie	Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, zestaw kabli koniecznych do podłączenia do odpowiedniego kontrolera serwera umożliwiającego komunikację z urządzeniem – długość kabli min. 2m. Wraz z urządzeniem należy dostarczyć także zestaw nośników danych określonych w punkcie 2, przy czym wszystkie dostarczone nośniki muszą być kompatybilne i dedykowane do współpracy z oferowanym urządzeniem. Instrukcja instalacji - w języku polskim lub angielskim.
11.	Gwarancja i oświadczenia	36 miesięcy w miejscu instalacji urządzenia z czasem reakcji na zgłoszenia do następnego dnia roboczego. Czas przyjmowania zgłoszeń serwisowych w trybie 5x9. Przystąpienie do fizycznej naprawy najpóźniej w następnym dniu roboczym od zdiagnozowania awarii z terminem naprawy najpóźniej do 48 godzin od rozpoczęcia naprawy. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 72 miesięcy. Wsparcie i gwarancja muszą obejmować zarówna samo urządzenie jak i wszystkie zainstalowane w nim napędy oraz dostarczone nośniki. Zgłaszanie awarii wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany serwis producenta – kontakt z serwisem wyłącznie w języku polskim.

5. Zarządzalne urządzenie sieciowe – 2 sztuki.

Lp.	Minimalne wymagania Zamawiającego	
I.	CECHY ZARZĄDZANIA	
1.	Typ przełącznika	Zarządzany
2.	Przełącznik wielowarstwowy	L2/L3
3.	Obsługa jakość serwisu (QoS)	Tak
4.	Zarządzany w chmurze	Tak
5.	Zarządzanie przez stronę www	Tak
6.	Inspekcja ARP	Tak
7.	Konfigurowanie ustawień lokalizacji (CLI)	Tak
8.	Obsługa MIB	Y
II.	OCHRONA	
9.	Funkcje DHCP	DHCP relay, DHCP server, DHCPv6 client
10.	Lista kontrolna dostępu (ACL)	Tak
11.	Zasady Listy Kontroli Dostępu (ACL)	1024
12.	IGMP snooping	Tak
13.	Ochrona hasłem	Tak
14.	obsługuje SSH/SSL	Tak
15.	Filtrowanie adresów MAC	Tak
16.	Szyfrowanie / bezpieczeństwo	HTTPS, SSH, SSL/TLS
III.	PORTY I INTERFEJSY	
17.	Podstawowe przełączanie RJ-45 Liczba portów Ethernet	48
18.	Podstawowe przełączania Ethernet RJ-45 porty typ	Gigabit Ethernet (10/100/1000)
19.	Ilość slotów Modułu SFP+	4
20.	Liczba portów USB 2.0	1
IV.	SIEĆ	
21.	Standardy komunikacyjne	IEEE 802.1D, IEEE 802.1w, IEEE 802.1s, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ad
22.	Obsługa 10G	Tak
23.	Dublowanie portów	Tak
24.	Protokół drzewa rozpinającego	Tak
25.	Blokowanie head-of-line (HOL)	Tak
26.	Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s
27.	Kontrola wzrostu natężenia ruchu	Tak
28.	Automatyczne MDI/MDI-X	Tak
29.	Podpora kontroli przepływu	Tak
30.	Agregator połączenia	Tak
31.	Obsługa sieci VLAN	Tak
32.	Liczba VLANs	4094
V.	PRZESYŁANIE DANYCH	

33.	Wielkość tabeli adresów	16000 wejścia
34.	Zgodny z Jumbo Frames	Tak
35.	Rozszerzenie Jumbo Frames	9000
VI.	FUNKCJE MULTICAST	
36.	Obsługa Multicast	Tak
VII.	PROTOKOŁY	
37.	Protokoły zarządzające	SNMP
VIII.	KONSTRUKCJA	
38.	Możliwości montowania w stelażu	Tak
39.	Przycisk reset	Tak
40.	Diody LED	Tak
IX.	WYDAJNOŚĆ	
41.	Procesor wbudowany	Tak
42.	Taktowanie procesora	800 MHz
43.	Pojemność pamięci wewnętrznej	512 MB
44.	Wielkość pamięci flash	256 MB
45.	Aktualizacje oprogramowania urządzenia	Tak
X.	MOC	
46.	Zasilacz dołączony	Tak
XI.	WARUNKI PRACY	
47.	Zakres temperatur (eksploatacja)	-5 - 50 °C
48.	Zakres temperatur (przechowywanie)	-25 - 70 °C
49.	Zakres wilgotności względnej	10 - 90%
50.	Dopuszczalna wilgotność względna	10 - 90%

6. UTM – 2 sztuki.

Lp.	Minimalne wymagania Zamawiającego
1	Urządzenie musi posiadać interfejs WWW, z poziomu którego administrator może wykonać wszystkie czynności administracyjne.
2	Urządzenie musi posiadać możliwość podłączenia do systemu centralnego zarządzania oraz zarządzania nim poprzez dedykowaną aplikację dostępną na urządzenia mobilne z systemem Android oraz iOS.
3	Urządzenie musi posiadać możliwość zarządzania z poziomu chmurowego portalu centralnego zarządzania. Dostęp do portalu chmurowego musi być dostarczony w ramach podstawowej licencji, bez dodatkowych opłat.
4	Z poziomu interfejsu WWW administrator musi mieć możliwość szybkiego przeglądu stanu urządzenia, widząc

Lp.	Minimalne wymagania Zamawiającego
	na pierwszej stronie minimum następujące informacje: – wersja oprogramowania układowego, – nazwa urządzenia, – adres sprzętowy urządzenia, – czas pracy urządzenia od ostatniego restartu, – status połączenia z siecią Internet, – status sieci bezprzewodowej, – ostatnio wykryte urządzenia w sieci wraz z alertami, – aktywność sieci zawierająca wykres liczby pakietów oraz ilości danych przepływających w czasie rzeczywistym przez urządzenie.
5	Urządzenie musi umożliwiać wyświetlenie wszystkich aktywnych urządzeń pracujących w sieci w postaci listy dostępnej bezpośrednio z interfejsu WWW. Lista musi zawierać minimum: – nazwę urządzenia, – adres IP urządzenia, – adres MAC urządzenia, – typ urządzenia.
6	Urządzenie musi umożliwiać generowanie raportów ogólnych zawierających status urządzenia, minimum w odstępach: – ostatnia godzina, – ostatni dzień.
7	Urządzenie musi umożliwiać generowanie raportów z aktywności użytkowników i komputerów, minimum w odstępach: – ostatnia godzina, – ostatni dzień, – ostatni tydzień, – ostatni miesiąc.
8	Urządzenie musi umożliwiać wydruk raportów z aktywności użytkowników bezpośrednio z poziomu interfejsu WWW.
9	Urządzenie musi umożliwiać przegląd i wyszukiwanie logów sieciowych bezpośrednio z interfejsu WWW.
10	Urządzenie musi umożliwiać przegląd i wyszukiwanie logów systemowych bezpośrednio z interfejsu WWW.

Lp.	Minimalne wymagania Zamawiającego
11	Urządzenie musi umożliwiać wyświetlenie bezpośrednio z poziomu interfejsu WWW: – stanu zasobów sprzętowych, – tablicy routingu, – stanu połączenia z usługami chmurowymi.
12	Urządzenie musi posiadać funkcje pozwalające na wykonanie testów działania sieci, dostępne bezpośrednio z interfejsu WWW, obejmujące minimum narzędzia: – ping, – traceroute, – DNS lookup, – tcpdump.
13	Urządzenie musi umożliwiać wygenerowanie plików diagnostycznych z działania systemu urządzenia bezpośrednio z interfejsu WWW.
14	Interfejs WWW musi umożliwiać jednoczesne zalogowanie się wielu administratorom.
15	Urządzenie musi umożliwiać zarządzanie z poziomu dedykowanego serwera zarządzania oraz z poziomu usługi zarządzania w modelu chmurowym, bez konieczności wymiany urządzenia.

Funkcjonalność

Lp.	Minimalne wymagania Zamawiającego
1	Urządzenie musi pracować jako sonda współpracująca, raportująca do systemów klasy wykrywania i inwentaryzacji urządzeń medycznych oraz OT/IoT, minimum następujących producentów: Armis, Claroty, Medigate.
2	Urządzenie musi mieć możliwość pracy zarówno w trybie monitorowania (warstwa 2, transparentnym), jak i w trybie inline (routing, warstwa 3).
3	Urządzenie musi być minimalnie wyposażone w następujące moduły funkcjonalne: – Firewall, – Kontrola aplikacji i URL Filtering, – Rozpoznawanie użytkowników, – QoS, – IPS, – Anti-Virus, – Anti-Bot,

Lp.	Minimalne wymagania Zamawiającego
	– Emulacja zagrożeń (sandboxing), – Antyspam, – VPN Site-to-Site, – VPN Client-to-Site.
4	Urządzenie musi mieć możliwość monitorowania dostępu do sieci Internet poprzez weryfikację wskazanych przez administratora hostów, z monitorowaniem minimum następujących parametrów sieciowych: – utrata pakietów, – średnie opóźnienie, – minimalne opóźnienie, – maksymalne opóźnienie, – jitter.
5	Urządzenie musi umożliwiać pełną rekonfigurację interfejsów wewnętrznych, wspierając minimum: – utworzenie wirtualnego przełącznika z interfejsów, – utworzenie interfejsów typu bridge, – agregację interfejsów zgodną z IEEE 802.3ad (LACP), w trybie pasywnym i aktywnym.
6	Urządzenie musi mieć możliwość filtrowania ruchu sieciowego poprzez filtrowanie adresów MAC.
7	Urządzenie musi posiadać mechanizm DNS Proxy.
8	Urządzenie musi posiadać możliwość ograniczenia dostępu administracyjnego wyłącznie z konkretnych podsieci oraz wyłącznie z konkretnych stref bezpieczeństwa.
9	Urządzenie musi mieć możliwość synchronizacji czasu poprzez protokół NTP.
10	Urządzenie musi mieć możliwość uruchomienia serwera NTP bezpośrednio na urządzeniu.
11	Urządzenie musi wspierać serwisy DDNS, minimum: – DynDNS, – no-ip.org.
12	Urządzenie musi posiadać funkcję pozwalającą na zarządzanie urządzeniem z sieci Internet, również gdy znajduje się za NAT. Funkcja ta nie może wymagać od administratora uruchomienia tunelu VPN do sieci wewnętrznej i musi zostać dostarczona w ramach podstawowej licencji.
13	Urządzenie musi mieć możliwość działania w klastrze wysokiej dostępności (High Availability), minimum w trybie active–passive.
14	Urządzenie musi posiadać predefiniowane profile pracy modułów: Firewall, Kontrola aplikacji, URL Filtering oraz IPS.
15	Urządzenie musi umożliwiać ręczne definiowanie reguł działających na:

Lp.	Minimalne wymagania Zamawiającego
	– firewallu, – module kontroli aplikacji i URL Filtering, – module IPS.
16	Urządzenie musi umożliwiać logowanie każdej sesji sieciowej dopuszczonej lub zablokowanej na poziomie urządzenia.
17	Urządzenie musi posiadać dwa osobne zestawy reguł: jeden dla połączeń wychodzących do sieci Internet, drugi dla obsługi połączeń wewnętrznych.
18	Urządzenie musi posiadać predefiniowaną politykę translacji adresów (NAT), pozwalającą na jej zastosowanie przy połączeniach wychodzących do sieci Internet.
19	Urządzenie musi wspierać filtrowanie protokołów VoIP oraz pozwalać na konfigurację filtrowania tego ruchu za pomocą kreatora konfiguracji.
20	Urządzenie musi mieć możliwość integracji z usługami katalogowymi, minimum Microsoft Active Directory, w zakresie rozpoznawania tożsamości użytkowników.
21	Urządzenie musi mieć możliwość inspekcji ruchu SSL/TLS.
22	Urządzenie musi mieć możliwość kategoryzowania stron HTTPS bez inspekcji ruchu SSL/TLS.
23	Urządzenie musi posiadać interfejs, w którym administrator może zidentyfikować wszystkie zainfekowane urządzenia w sieci.
24	Urządzenie musi mieć możliwość całkowitego wyłączenia modułu IPS oraz uruchomienia go wyłącznie w trybie IDS (bez blokowania ruchu).
25	Urządzenie musi umożliwiać zestawianie tuneli VPN typu client-to-site minimum w formie: – dedykowanego klienta VPN dostarczanego przez producenta rozwiązania, – mobilnego klienta VPN dostarczanego przez producenta rozwiązania, – portalu SSL VPN, – klienta VPN wbudowanego w system operacyjny Windows.
26	Urządzenie musi posiadać moduł kontroli aplikacji rozpoznający nie mniej niż 9 300 różnych aplikacji.
27	Urządzenie musi posiadać funkcjonalność tzw. Virtual Patchingu, pozwalającą na blokowanie ataków kierowanych na podatne urządzenia, które z przyczyn technicznych nie mogą zostać zaktualizowane przez administratora.
28	Lista aplikacji wspieranych przez moduł kontroli aplikacji musi być publicznie dostępna i umożliwiać przeszukiwanie z wykorzystaniem różnych filtrów.
29	Urządzenie musi wspierać protokoły routingu dynamicznego, minimum: – OSPFv2, – BGPv4 oraz BGP4++,

Lp.	Minimalne wymagania Zamawiającego
	– RIP, – PIM (SM, DM, SSM), – IGMP.
30	Urządzenie musi wspierać protokół IPv6 w zakresie połączeń sieci lokalnej i Internetu, pracy w trybie dual stack, tunelowania IPv4 w IPv6, delegacji prefiksów oraz translacji NAT66.
31	Urządzenie musi posiadać wbudowaną funkcjonalność optymalizacji i redundancji łączy WAN (SD-WAN), dostarczoną w ramach podstawowej licencji.
32	Urządzenie musi obsługiwać nie mniej niż 1 024 interfejsy fizyczne i wirtualne (VLAN) zgodne z IEEE 802.1Q na pojedynczą bramę.
33	Urządzenie musi wspierać mechanizm redundancji bramy domyślnej zgodny z VRRPv3.

Wydajność i parametry sprzętowe

Lp.	Minimalne wymagania Zamawiającego
1	Urządzenie musi być przystosowane do pracy w temperaturze od 0 °C do 40 °C, przy wilgotności względnej 5–95% bez kondensacji. Dopuszczalna temperatura przechowywania: od -45 °C do 60 °C.
2	Urządzenie musi posiadać następujące certyfikacje w zakresie bezpieczeństwa: CB IEC 62368-1, CE LVD EN 62368-1, UL 62368-1, AS/NZS 62368.1.
3	Urządzenie musi spełniać wymagania w zakresie kompatybilności elektromagnetycznej potwierdzone oznakowaniem CE oraz wymagania środowiskowe: RoHS, REACH, WEEE.
4	Urządzenie musi posiadać następujące porty: – LAN: 8 x 1GbE RJ45 oraz 2 x 10GbE SFP+, – WAN: 1 x 1GbE RJ45, – DMZ: 1 x 1GbE SFP, – gniazdo kart pamięci micro-SD, – port konsolowy USB Type-C, – port USB 3.0 Type-A.
5	Urządzenie musi umożliwiać przełączenie dowolnego portu LAN do pracy jako port WAN.
6	Wymagana przepustowość urządzenia dla: – ruchu NGTP (Firewall, Kontrola aplikacji, URL Filtering, IPS, Anti-Virus, Anti-Bot, emulacja zagrożeń, z

Lp.	Minimalne wymagania Zamawiającego
	logowaniem): 1 850 Mb/s, – ruchu NGFW (Firewall, Kontrola aplikacji, IPS, z logowaniem): 3 750 Mb/s, – ruchu IPS: 5 170 Mb/s, – ruchu Firewall: 6 750 Mb/s, – Firewall dla pakietów UDP o wielkości 1518 bajtów: 11 600 Mb/s, – VPN AES-GCM 1452B: 4 000 Mb/s, – liczba nowych połączeń na sekundę: 53 000, – liczba jednoczesnych połączeń: 2 000 000.
7	Średnie opóźnienie wprowadzane przez moduł Firewall nie może przekraczać 30 µs (pomiar zgodny z RFC 3511, 2544, 2647, 1242).
8	Urządzenie musi obsługiwać nie mniej niż 200 jednoczesnych użytkowników zdalnego dostępu VPN.
9	Urządzenie musi być zasilane napięciem przemiennym 100–240 V AC, 47–63 Hz. Wymagana możliwość zastosowania zasilania redundantnego (dwa niezależne zasilacze).
10	Maksymalny pobór mocy urządzenia nie może przekraczać 32 W.
11	Wymiary urządzenia nie większe niż 210 x 194 x 42,5 mm (szer. x gł. x wys.), masa nie większa niż 1,4 kg. Wymagana możliwość montażu w szafie teleinformatycznej 19" przy użyciu dedykowanych akcesoriów producenta.
12	Deklarowany przez producenta wskaźnik MTBF nie mniejszy niż 33 lata.
13	Urządzenie musi posiadać wbudowany moduł bezprzewodowy standardu IEEE 802.11be (Wi-Fi 7) w konfiguracji 4x4 MIMO, pracujący w pasmach 2,4 GHz, 5 GHz oraz 6 GHz.

Urządzenie musi zostać dostarczone licencjami na okres nie przekraczający 31.12.2026 r., z pełnym zakresem wsparcia od strony producenta rozwiązania. Wsparcie producenta musi być realizowane w trybie 24/7, tzn. przez 24 godziny na dobę przez 7 dni w tygodniu. Czas odpowiedzi na zgłoszenie suportowe to 30 minut. Wsparcie producenta musi zapewniać automatyczne krytyczne poprawki, pakiety serwisowe i aktualizacje oraz dostęp do narzędzi diagnostycznych i zasobów online

7. Tokeny sprzętowe – 50 sztuk.

Wymagania funkcjonalne i techniczne (minimalne)

1. Standardy: FIDO U2F oraz FIDO2 (WebAuthn/CTAP) – urządzenie FIDO® Certified; możliwość użycia w trybie MFA oraz logowania bezhasłowego (tam gdzie wspierane).

2. Interfejs: USB 2.0 Type-A; praca bez baterii i bez sterowników (HID), kompatybilność z USB-C.
3. Obsługa systemowa i usług: co najmniej Windows 10/11, macOS, Linux; współpraca z popularnymi usługami wspierającymi FIDO (np. Google, Microsoft itp.).
4. Sygnalizacja działania: przycisk z diodą LED lub równoważny mechanizm aktywacji.
5. Parametry środowiskowe: temp. pracy co najmniej 0–70°C; przechowywanie co najmniej –20–70°C.
6. Bezpieczeństwo: klucze prywatne generowane i przechowywane wyłącznie w urządzeniu; brak możliwości odczytu/klonowania z zewnątrz.
7. Kompatybilność organizacyjna: możliwość rejestracji wielu kont/usług na jednym kluczu; brak konieczności instalacji dodatkowego oprogramowania klienckiego (poza ewentualnymi narzędziami administracyjnymi).

2. Wymagania gabarytowe (kompaktowy rozmiar – klasa „mini")

Ze względu na konieczność pracy w gniazdach USB umieszczonych gęsto obok siebie (laptopy, stacje dokujące) oraz minimalizację ryzyka uszkodzeń mechanicznych, Zamawiający wymaga, aby klucz posiadał kompaktowe wymiary nieprzekraczające wartości poniżej. Wymagania wynikają z potrzeb użytkowych i ergonomii stanowisk pracy.

- Długość całkowita urządzenia (L) ≤ 25 mm.
- Szerokość zewnętrznej obudowy w najszerszym miejscu (W) ≤ 13 mm (nie mniejsza niż standard wtyku USB-A).
- Grubość (T) ≤ 2,0 mm (mierzona poza metalową osłoną wtyku, w najszerszym miejscu obudowy).

Uwaga: Powyższe progi są podyktowane ograniczeniami przestrzennymi oraz mają na celu zapewnienie ergonomii i bezpieczeństwa użytkowania. Zamawiający dopuszcza rozwiązania równoważne.

3. Dostawa i wsparcie

- Urządzenia fabrycznie nowe; gwarancja min. 24 miesiące;
- W zestawie skrócona instrukcja użytkownika w jęz. PL lub EN (online lub druk);
- Wsparcie producenta/dystrybutora w zakresie aktualizacji oprogramowania sprzętowego, jeżeli dotyczy.

8. Stacja robocza z akcesoriami – 1 sztuka.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.
2.	Obudowa	Typu tower, umożliwiająca montaż minimum dwóch dysków SSD oraz jednego dysku HDD 3,5". Obudowa trwale oznaczona nazwą producenta i modelem komputera. Obudowa otwierana beznarzędziowo.
3.	Chipset	Dostosowany do zaoferowanego procesora
4.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w: - 3 sloty M.2

		- 4 sloty DIMM na pamięć RAM - 3 sloty PCIe min. 3.0 o niskim profilu - 2 sloty SATA
5.	Procesor	Procesor klasy x86, zaprojektowany do pracy w komputerach stacjonarnych o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core Ultra 5 225 na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na stronie http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
6.	Pamięć operacyjna	Min. 16GB DDR5 Możliwość rozbudowy pamięci do min. 128 GB
7.	Dysk twardy	Min. 512 GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość rozbudowy jednostki komputerowej o 2 dodatkowe dyski twarde.
8.	Karta graficzna	Zintegrowana z procesorem
9.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowany głośnik multimedialny o mocy 2W.
10.	Sieć	Karta sieciowa LAN obsługująca prędkości 10/100/1000
11.	Porty/złącza	Z przodu obudowy: - 1x USB 3.2 typu C z możliwością ładowania podłączonych urządzeń - 4x USB 3.2 typu A - złącze audio combo Z tyłu obudowy: - 4x USB 3.2 typu A - 1x HDMI 2.1 - 2x DisplayPort 1.4a - 1x RJ-45 - line out Obudowa komputera wyposażona w czytnik kart multimedialnych oraz napęd DVD-RW na jej przednim panelu. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp. Nie dopuszcza się stosowania zewnętrznych czytników kart multimedialnych i napędów optycznych, podłączanych do urządzenia za pomocą złącza USB.

12.	Klawiatura/mysz	Przewodowe USB: klawiatura w układzie US + mysz z rolką
13.	Zasilacz	Energooszczędny zasilacz o mocy min. 250W oraz sprawności na poziomie min. 90%.
14.	System operacyjny	System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na

		firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych.

		35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
15.	BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - modelu komputera, - numerze seryjnym, - wersji BIOS, - zainstalowanym procesorze wraz z taktowaniem, - zainstalowanej pamięci RAM wraz z taktowaniem, - adresie MAC karty sieciowej. Administrator z poziomu BIOS musi mieć możliwość: - wyłączenia portów USB - wyłączenia karty sieciowej

		- wyłączenia karty audio - wyłączenia funkcji Wake on LAN - wyłączenia wirtualizacji - ustawienia hasła: administratora, Power-On, dysku twardego - zdefiniowania sekwencji bootowania - załadowania optymalnych ustawień BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych
16.	System Diagnostyczny	Zaimplementowany w UEFI BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System obsługiwany za pomocą myszy lub klawiatury, umożliwiający wykonanie minimum następujących czynności diagnostycznych: 1. Wykonanie testu komponentów w zakresie przyspieszonym lub rozszerzonym z możliwością wyboru algorytmów testowania oraz liczby cykli testowych do przeprowadzenia. System diagnostyczny powinien umożliwiać wykonanie testu następujących komponentów: - pamięci ram, - procesora, - pamięci masowej, - płyty głównej 2. Identyfikację jednostki i jej komponentów w następującym zakresie: - urządzenie (producent, model, numer seryjny), - bios (wersja oraz data wydania), - procesor (nazwa, taktowanie, ilości pamięci L1, L2, L3, liczba rdzeni), - pamięć ram (ilość zainstalowanej pamięci ram, producent oraz numer seryjny), - dysk twardy (producent, model, numer seryjny, pojemność), - płyta główna (liczba złącz USB, liczba złącz PCI)
17.	Certyfikaty i standardy	Dla producenta sprzętu - ISO 9001 - ISO 14001 - ISO 50001

		Dla komputera: - Deklaracja zgodności CE - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki - EPEAT min. Silver - TCO
18.	Bezpieczeństwo	- Złącze typu Kensington Lock - Oczko na kłódkę, zabezpieczającą urządzenie przed nieautoryzowanym otwarciem - Sprzętowy moduł TPM 2.0 (dTPM 2.0) z certyfikacją TCG - Czujnik otwarcia obudowy
19.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.
20.	Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania użytkowego producenta, w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać ich zbiorczą instalację.
21.	Gwarancja i wsparcie techniczne producenta	Min. 36 miesięcy świadczona w miejscu użytkowania sprzętu (on-site). Firma serwisująca posiadająca certyfikat ISO 9001:2000 na świadczenie usług serwisowych. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta. Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej: - fabrycznej konfiguracji urządzenia, - rodzaju gwarancji, - dacie wygaśnięcia gwarancji, - aktualizacjach. Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Monitor	Monitor – **2 sztuki**, będzie wykorzystywany dla potrzeb aplikacji biurowych, obróbki zdjęć lub wideo. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację monitora
2.	Wielkość ekranu	Przekątna ekranu min. 27”
3.	Matryca	Powłoka matrycy o wykończeniu matowym typu IPS
4.	Nominalna rozdzielczość	Rozdzielczość nie mniejsza niż 2560x1440
5.	Kąty widzenia	Kąty widzenia min. 178 stopni w pionie i w poziomie
6.	Plamka	Wielkość plamki (pojedynczego piksela) nie większa niż 0.25mm
7.	Częstotliwość odświeżania	Nie mniejsza niż 90Hz
8.	Jasność	Nie mniejsza niż 350 nitów

9.	Czas reakcji matrycy	Nie większy niż 7 ms
10.	Zakres kolorów	Nie mniejszy niż 99% sRGB Obsługa min. 16,7 miliona kolorów
11.	Kontrast statyczny	Nie mniejszy niż: 1500:1
12.	Multimedia	Wbudowane głośniki o mocy minimum 2x 2W
13.	Porty/złącza	– 2x HDMI – 1x DisplayPort
14.	Waga	Nieprzekraczająca 6.5 kg z podstawą według karty katalogowej producenta
15.	Ergonomia	Możliwość regulacji ustawienia monitora w zakresie: – Przód / tył w zakresie min. -5 do 20 stopni – Lewo / prawo w zakresie 360 stopni – Pivot w zakresie min. -90 do 90 stopni – Wysokość do min. 150mm
16.	Obudowa	– musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej – Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA (100x100)

17.	Bezpieczeństwo	Złącze typu Kensington Lock
18.	Certyfikaty i standardy	Dla producenta sprzętu należy dostarczyć certyfikat: - ISO 9001 - ISO 14001 Dla urządzenia: – Energy Star – TCO min. 8.0 – EPEAT Gold dla kraju Polska według danych widocznych na stronie https://epeat.net/search-computers-and-displays
19.	Ukompletowanie	Kabel HDMI o długości min. 1,8m Kabel zasilający o długości min. 1,8m
20.	Gwarancja i wsparcie	Minimum 36 miesięcy

9. Access point – 1 sztuka.

Lp.	Parametr	Wymagane parametry minimalne	Parametry oferowane
I. Parametry radiowe			

Lp.	Parametr	Wymagane parametry minimalne	Parametry oferowane
1	**Standard transmisji**	Urządzenie zgodne ze standardem IEEE 802.11be (Wi-Fi 7), ze wsteczną zgodnością ze standardami IEEE 802.11a/b/g/n/ac/ax.	
2	**Architektura radiowa**	Trzy niezależne moduły radiowe pracujące jednocześnie w pasmach 2,4 GHz, 5 GHz oraz 6 GHz (tri-band).	
3	**Liczba strumieni przestrzennych**	Łącznie nie mniej niż 6 strumieni przestrzennych (po 2 strumienie w każdym z pasm).	
4	**MIMO**	2 x 2 MU-MIMO w kierunku downlink i uplink w każdym z pasm: 2,4 GHz, 5 GHz, 6 GHz.	
5	**Szerokość kanału**	Obsługa kanałów o szerokości co najmniej: – 320 MHz w paśmie 6 GHz, – 240 MHz w paśmie 5 GHz, – 40 MHz w paśmie 2,4 GHz.	
6	**Maksymalna przepływność radiowa (wg specyfikacji producenta)**	– pasmo 6 GHz: nie mniej niż 5,7 Gb/s, – pasmo 5 GHz: nie mniej niż 4,3 Gb/s, – pasmo 2,4 GHz: nie mniej niż 688 Mb/s.	
7	**Obsługiwane prędkości**	802.11be: od 7,3 Mb/s do co najmniej 5,7 Gb/s (MCS0–	

Lp.	Parametr	Wymagane parametry minimalne	Parametry oferowane
	transmisji	MCS13, NSS 1/2, EHT 20/40/80/160/240/320).	
8	**Mechanizmy transmisyjne**	Obsługa: MLO (Multi-Link Operation), OFDMA (DL/UL), modulacji 4096-QAM, BSS Coloring, TWT (Target Wake Time), agregacji ramek A-MPDU/A-MSDU.	
9	**Anteny**	Anteny wewnętrzne, dookólne, zintegrowane z obudową, o zysku energetycznym nie mniejszym niż: – 2,4 GHz: 4 dBi, – 5 GHz: 6 dBi, – 6 GHz: 5,8 dBi.	
10	**Maksymalna moc nadawania**	Moc nadawania (wartość przewodzona, wg specyfikacji producenta) nie mniejsza niż: – 2,4 GHz: 22 dBm, – 5 GHz: 26 dBm, – 6 GHz: 23 dBm. Urządzenie musi umożliwiać programową regulację mocy nadawania w celu zachowania limitów EIRP obowiązujących na terytorium RP.	
11	**Liczba identyfikatorów BSSID**	Nie mniej niż 8 BSSID na każdy moduł radiowy.	

Lp.	Parametr	Wymagane parametry minimalne	Parametry oferowane
12	**Pojemność**	Obsługa nie mniej niż 300 jednocześnie podłączonych urządzeń klienckich.	
13	**Zasięg**	Deklarowana przez producenta powierzchnia pokrycia nie mniejsza niż 140 m².	
II. Interfejsy, zasilanie i konstrukcja			
14	**Interfejs sieciowy**	Co najmniej 1 port RJ-45 obsługujący prędkości 1 Gb/s oraz 2,5 Gb/s (1/2,5 GbE) z autonegocjacją i funkcją Auto-MDI/MDI-X.	
15	**Metoda zasilania**	Zasilanie przez Ethernet zgodne ze standardem IEEE 802.3at (PoE+). Zakres napięcia zasilania co najmniej 44–57 V DC.	
16	**Pobór mocy**	Maksymalny pobór mocy nie większy niż 21 W.	
17	**Materiał obudowy**	Poliwęglan oraz metal. Uchwyt montażowy wykonany ze stali nierdzewnej (SUS304), płyta montażowa ze stali ocynkowanej (SGCC).	
18	**Wymiary**	Nie większe niż ⌀206 x 46 mm (urządzenie bez uchwytu montażowego).	
19	**Masa**	Nie większa niż 680 g (urządzenie bez uchwytu	

Lp.	Parametr	Wymagane parametry minimalne	Parametry oferowane
		montażowego).	
20	**Montaż**	Możliwość montażu sufitowego oraz naściennego. Komplet akcesoriów montażowych dostarczony wraz z urządzeniem.	
21	**Sygnalizacja i elementy sterujące**	Dioda LED sygnalizująca stan pracy urządzenia, z możliwością jej programowego wyłączenia. Sprzętowy przycisk przywracania ustawień fabrycznych.	
22	**Warunki pracy**	Zakres temperatur pracy obejmujący co najmniej przedział od 0 °C do +40 °C, wilgotność względna 5–95% bez kondensacji. Urządzenie przeznaczone do pracy wewnątrz budynków.	
III. Funkcjonalność sieciowa			
23	**Zarządzanie**	Zarządzanie przez interfejs Ethernet z poziomu kontrolera (lokalnego lub chmurowego) zapewniającego centralne zarządzanie wszystkimi oferowanymi punktami dostępowymi. Oprogramowanie zarządzające bez dodatkowych opłat licencyjnych i subskrypcyjnych przez cały okres eksploatacji urządzenia.	
24	**Sieci bezprzewodowe i VLAN**	Obsługa znaczników VLAN zgodnie z IEEE 802.1Q, przypisanie odrębnego identyfikatora VLAN do każdego SSID.	

Lp.	Parametr	Wymagane parametry minimalne	Parametry oferowane
25	**Roaming i optymalizacja**	Obsługa IEEE 802.11k/v/r (fast roaming), band steering, automatycznego doboru kanału i mocy nadawania, Passpoint (Hotspot 2.0), pracy w trybie mesh.	
26	**Sieć gościnna**	Izolacja sieci gościnnej, izolacja urządzeń klienckich, portal uwierzytelniający z możliwością własnej personalizacji graficznej, uwierzytelnianie: hasłem, kodami voucher, przez zewnętrzny serwer portalu, z możliwością autoryzacji płatnej.	
27	**Kontrola pasma**	Ograniczanie prędkości transmisji dla poszczególnych SSID lub klientów oraz harmonogramy czasowe działania sieci bezprzewodowych.	
IV. Bezpieczeństwo			
28	**Uwierzytelnianie i szyfrowanie**	Obsługa WPA2-Personal, WPA2-Enterprise, WPA3-Personal, WPA3-Enterprise oraz trybów przejściowych, uwierzytelnianie IEEE 802.1X.	
29	**Integracja z RADIUS**	Obsługa serwerów RADIUS, w tym RADIUS over TLS (RadSec) oraz dynamicznego przypisywania VLAN na podstawie atrybutów RADIUS.	
30	**Indywidualne klucze dostępu**	Obsługa mechanizmu indywidualnych, współdzielonych kluczy dostępu (private PSK) umożliwiającego przypisanie odrębnego hasła i VLAN w ramach jednego SSID.	

Lp.	Parametr	Wymagane parametry minimalne	Parametry oferowane
31	**Aktualizacje**	Możliwość aktualizacji oprogramowania układowego z poziomu systemu zarządzania. Producent zapewnia nieodpłatny dostęp do aktualizacji, w tym poprawek bezpieczeństwa, przez okres nie krótszy niż okres gwarancji.	
V. Wymagania formalne			
32	**Fabryczna nowość**	Urządzenia fabrycznie nowe, nieużywane, nieregenerowane, wyprodukowane nie wcześniej niż 12 miesięcy przed terminem dostawy, pochodzące z oficjalnego kanału dystrybucji producenta na terytorium Unii Europejskiej.	
33	**Zgodność z przepisami**	Oznakowanie CE oraz deklaracja zgodności UE. Zgodność z dyrektywą 2014/53/UE (RED) oraz 2011/65/UE (RoHS). Urządzenie dopuszczone do użytkowania na terytorium Rzeczypospolitej Polskiej w pasmach 2,4 GHz, 5 GHz i 6 GHz bez konieczności uzyskania pozwolenia radiowego.	
34	**Gwarancja**	Gwarancja producenta na okres nie krótszy niż 24 miesiące od daty podpisania protokołu odbioru, realizowana na terytorium Rzeczypospolitej Polskiej, obejmująca wymianę urządzenia wadliwego.	

10. Oprogramowanie serwerowe – 6 sztuk.

Wymagane minimalne parametry
Oprogramowanie Windows Server 2025 Standard lub równoważne.

Opis równoważności dla systemu Windows Server 2025 Standard:

1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.
2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 5 lat.
4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny będącego w pełni zgodnym z domeną wdrożoną u Zamawiającego domeną Active Directory pracującą w oparciu o system Windows Server 2016 musi także być dostarczona możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server
5. Licencja na system operacyjny musi być bez ograniczeń czasowych.
6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.
7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
8. System operacyjny musi posiadać graficzny interfejs użytkownika.
9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:

a. zarządzania użytkownikami,
b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
c. możliwości przydzielania praw dostępu do zasobów sieciowych,
d. instalacji zdalnej oprogramowania z pakietów msi,
e. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 7,8,8.1, 10,11.

10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Center.
12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.
13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
15. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra
16. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra
17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
19. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
22. System operacyjny musi posiadać obsługa PowerShell 5.1,
23. System operacyjny musi posiadać obsługa certyfikatów w Active Directory
24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

11. Oprogramowanie serwerowe – 4 sztuki (20 licencji).

Wymagana licencja typu Cal User OEM do systemu Windows Server 2025 (z niniejszego zamówienia) lub równoważne, jeśli oprogramowanie równoważne takich licencji wymaga.

Opis równoważności dla funkcjonalności dotyczące wymaganego przez Zamawiającego oprogramowania równoważnego do Windows Server 2025 na użytkownika:
Licencja dostępowa dla użytkownika umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2025 typu User Cal z wdrożoną rolą Active Directory

Część 2 – Dostawa i wdrożenie oprogramowania IT oraz szkolenia

1. Oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych – 20 sztuk.

Informacje Ogólne.

- Dostarczone licencje na oprogramowanie muszą być licencjami wieczystymi (bezterminowymi). Zamawiający nie dopuszcza licencji terminowych, subskrypcyjnych ani wynajmu licencji. Ewentualne wsparcie producenta i prawo do aktualizacji mogą być ograniczone czasowo, co nie może wpływać na bezterminowe prawo korzystania z dostarczonej wersji oprogramowania.
- Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
- Oprogramowanie współpracuje z serwerem SQL Server 2019, SQL Server 2017, SQL Server 2016 SP3, SQL Server 2014 SP3, Oracle 19c, Oracle 12c R2.
- Oprogramowanie serwera aplikacji umożliwia wysyłanie powiadomień mailowych.
- Oprogramowanie posiada system ról, dzięki któremu jest możliwe przypisywanie wybranych grup stanowisk do poszczególnych użytkowników konsoli.
- Wszelkie raporty, zestawienia oraz funkcje grupowe obejmują wtedy tylko w/w przypisane grupy stanowisk.
- Oprogramowanie realizuj zarządzanie wszystkimi modułami systemu z poziomu tej samej konsoli zarządzającej.
- Oprogramowanie agenta realizuje wszystkie wymagane funkcjonalności z poziomu jednej instancji usługi lub procesu bez wykorzystywania aplikacji oraz usług firm trzecich za wyjątkiem aplikacji oraz usług wbudowanych w system operacyjny na którym zainstalowany został Agent.
- Oprogramowanie pozwala export do Excel'a dowolnego widoku konsoli administracyjnej.
- Oprogramowanie pozwala zarządzać z jednej konsoli zarówno stacjami klienckimi, serwerami jak i urządzeniami mobilnymi z systemami operacyjnymi Android oraz iOS.
- Oprogramowanie, niezależnie od ilości funkcjonalności lub zarządzanych urządzeń końcowych działa w oparciu o 1 oprogramowanie typu Agent na urządzeniu końcowym.

- Oprogramowanie posiada architekturę trójwarstwową składającą się z Bazy Danych, Serwera Aplikacji oraz Agenta.
- Oprogramowanie działa na minimalnych wymaganiach sprzętowych:

  Wymagania sprzętowe:
  - procesor minimum 2 rdzenie;
  - 8 GB wolnej pamięci- rekomendowane 16 GB;
  - karta sieciowa min 1 Gigabit;
  - przestrzeń w celu instalacji: minimum 5 GB;

  Wymagane oprogramowanie dla Serwera:
  - Serwer OS - od Windows Server 2016 (64-Bit);
  - od 5 GB wolnej przestrzeni dyskowej na instalacje serwera;
  - Baza Danych - od SQL Server 2014 SP3;

  Wymagania dla stacji klienckiej:
  - od Intel Pentium IV procesor z 1GHz;
  - od 256 MB wolnej pamieci RAM;
  - od 200 MB wolnego miejsca na dysku twardym;

- Oprogramowanie musi posiadać procedurę uwierzytelnienia i autoryzacji Administratora w konsoli zarządzającej, który umożliwia jednoczesną prace wielu administratorom. Logowanie użytkowników konsoli zarządzającej powinno być zintegrowane z kontami Active Directory.
- Oprogramowanie umożliwia dystrybucję dowolnego oprogramowania, nie tylko paczek MSI, ale również takich jak InnoSetup, InstallShield i inne.
- Oprogramowanie umożliwia automatyzowanie instalatorów wraz z możliwością customizowania instalatorów w taki sposób, żeby można było nadpisywać pola opisowe, zmieniać dowolne wartości, w tym miejsce zapisu na dysku na urządzeniu końcowym.
- Oprogramowanie umożliwia administratorowi zautomatyzowanie procesu instalacji, w taki sposób, by nagrany został cały proces instalacji w taki sposób, by w momencie instalacji na urządzeniu końcowym nie było wymagane podanie jakichkolwiek opcji.
- Oprogramowanie musi umożliwiać zautomatyzowania zdalnej instalacji dowolnego oprogramowania w taki sposób, by oprogramowanie można było zainstalować zdalnie w trybie cichym (Silent Mode) lub graficznym.
- Oprogramowanie musi umożliwiać dodawanie takich opcji w instalatorach jak:
  - blokowanie klawiatury i myszki,
  - zmiany w ustawieniach w rejestracj na stacjach klienckich,
  - działania na plikach I folderach na stacji klienckiej,
  - dodanie skryptu np. w PowerShellu
  - zatrzymanie/wznowienie usług oraz procesów na stacji klienckiej"
- Zdalna dystrybucja oprogramowania musi wykorzystywać natywną inteligencję instalatora. Nie może wykorzystywać Snapshotingu.
- Zdalna dystrybucja oprogramowania musi mieć opcje schedullingu:
  - w zadanym przedziale czasowym;
  - wprowadzenie cykliczności (np. wybrany dzień tygodnia o wybranej godzinie);
  - połączenie dwóch powyższych;
  - na żądanie w danym momencie;
- Oprogramowanie musi umożliwiać wzbudzanie stacji klienckich metodą Wake-On-LAN.

- Oprogramowanie musi umożliwiać administratorowi podgląd co do Statusu danego taska per maszyna w czasie rzeczywistym, a w przypadku błędu w wykonaniu - zwrócić informację co było przyczyną błędu.
- W przypadku dokupienia nowych funkcjonalności/modułów oprogramowania, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera (wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
- W przypadku zwiększenia ilości zarządzanych maszyn w dowolnym momencie, nie wymagana będzie jakakolwiek reinstalacja po stronie serwera(wystarczy podmiana klucza licencji oraz umożliwia aktualizację licencji online, bez konieczności wymiany plikowej).
- Oprogramowanie musi umożliwiać zdalną dystrybucję oprogramowania z jednej konsoli zarówno na stacjach klienckich (jak PC I laptop/notebook) jak i urządzeniach mobilnych z systemem Android.
- Oprogramowanie dostarczy administratorowi informacji o dacie ostatniego uruchomienia aplikacji na stacji klienckiej PC per każda stacja kliencka.
- Dystrybucja agentów na stacjach klienckich musi być możliwa zarówno w sposób automatyczny jak i ręczny.
- Oprogramowanie umożliwia integrację z Active Directory oraz pobranie informacji z AD I automatyczne zarejestrowanie urządzeń z AD w serwerze.
- Zarówno w przypadku stacji klienckich PC jak I urządzeń mobilnych z systemem Android, oprogramowanie musi umożliwiać administratorowi dostarczenie użytkownikowi końcowemu interfejsu typu self-service, w którym będzie miał listę dostępnych instalatorów z możliwością ich dociągnięcia i zainstalowania; Musi istnieć możliwość automatycznej personalizacji takiej listy per grupa lub konkretne urządzenie końcowe.
- Oprogramowanie musi posiadać otwarte API do integracji z zewnętrznymi serwerami, np. poprzez Web Service'y.
- Oprogramowanie musi umożliwiać również tworzenie własnych skryptów, które następnie można automatycznie instalować na urządzeniach końcowych, typu stacja kliencka.
- W przypadku automatycznej zdalnej instalacji oprogramowania na stacjach klienckich, oprogramowanie musi dać opcje tworzenia listy oprogramowania zależnego, tzn. w przypadku gdy do poprawnego działania aplikacja X wymaga instalacji aplikacji Y, Oprogramowanie musi dawać opcję ustalenia listy takiego oprogramowania zależnego na poziomie konfiguracji aplikacji X z poziomu konsoli. W przypadku dystrybucji aplikacji X, gdy na stacji klienckiej nie będzie zainstalowana aplikacja Y, serwer automatycznie wypchnie na tą stację paczkę instalacyjną aplikacji Y .
- Oprogramowanie musi dawać administratorowi możliwość przypisywania wykonywania tasków zarówno na urządzeniach końcowych spełniających wybrane warunki dynamiczne (np. Wolne miejsce na dysku C, wersja systemu operacyjnego itp.), jak i urządzeniach przypisanych do konkretnych grup, jak w AD.
- Oprogramowanie musi posiadać środowisko skryptowe, umożliwiające tworzenie własnych skryptów i w łatwej dystrybucji skryptów z poziomu konsoli.
- Oprogramowanie musi posiadać możliwość automatycznego skanowania komputerów i serwerów pod kątem podatności i przestrzegania wytycznych dotyczących bezpieczeństwa i zgodności z wykorzystaniem standardowych zbiorów reguł, które są utrzymywane przez certyfikowane organizacje i firmy zajmujące się bezpieczeństwem cybernetycznym (proces wyszukiwania podatności musi bazować na minimum 25000 stale aktualizowanych reguł) oraz reguł definiowanych przez użytkownika.

Architektura Platformy.

- Oprogramowanie wspiera MsSQL-Server (również w wersji Express);
- Oprogramowanie posiada konsolę zarządzającą jako część oprogramowania (nie tylko interfejs webowy);
- Oprogramowanie posiada Agenta dla systemów klienckich Windows od Windows oraz Windows Server;

- Oprogramowanie wspiera więcej niż jeden serwer-repozytorium (DIP-Server) ;
- Oprogramowanie wspiera PXE-Relay;
- Oprogramowanie wspiera WakeUp-Points;
- Oprogramowanie posiada możliwość integracji z Active Directory;

Komunikacja (server-clients).

- Oprogramowanie obsługuje niewielką przepustowością łącza dla kontroli agentów i przesyłania informacji o statusach
- Oprogramowanie umożliwia indywidualną synchronizację pomiędzy pojedynczymi serwerami repozytorium (ograniczenie czasowe i przepustowości łącza)
- Oprogramowanie posiada dostęp read-only do AD, bez rozszerzeń schematu
- Oprogramowanie umożliwia wybudzanie stacji klienckich Wake-On-LAN
- Oprogramowanie wspiera zadania/Joby Push i Pull (łącznie z Shutdown)
- Oprogramowanie umożliwia komunikację bez konieczności zestawiania połączenia VPN z urządzeniami, które są poza siecią poprzez bramkę Proxy instalowaną w DMZ. Bramka Proxy musi stanowić integralną część Oprogramowania. Komunikacja pomiędzy bramką a agentem, jak i bramką a serwerem musi odbywać się poprzez HTTPS

Operacje wykonywane przez Oprogramowanie.

- Oprogramowanie umożliwia pracę wielu administratorów równocześnie na jednej konsoli
- Oprogramowanie posiada wsparcie dla LAN, zdalne i OFFLINE stanowiska pracy
- Oprogramowania umożliwia wyświetlenie informacji i stanu/statusów dostępnych w czasie rzeczywistym ze znacznikiem czasowym
- W przypadku zakończenia wykonania zadania na stacji z błędem, administrator widzi w konsoli administracyjnej szczegółowe przyczyny błędu, które spowodowały niewykonanie danego zadania
- Komunikaty o błędach są generowane natychmiast (wraz z informacją o docelowym systemie OS)
- Dowolnie definiowane dodatkowe pola (Variable/Zmienne) przechowywane w tej samej bazie danych (np. Informacje o gnieździe sieciowym, danych dotyczących wynajmu, informacje supportowe)
- Rozbudowane funkcjonalności dotyczące zarządzania uprawnieniami
- Wsparcie dla grup dynamicznych na potrzeby indywidualnych informacji/widoku
- Oprogramowanie musi zawierać opcję ukrywania danych osobowych użytkowników (takich jak imię, nazwisko, login) dla wybranych administratorów
- Oprogramowanie musi umożliwiać przyznawanie i blokowanie dostępu do wybranej części infrastruktury oraz wybranych części funkcjonalności oprogramowania wskazanym administratorom.

Minimum możliwości w zakresie zadań jakie powinno spełniać oprogramowanie.

- Oprogramowanie umożliwia wysyłanie polecenia w trybie "Push";
- Oprogramowanie umożliwia wysyłanie polecenia w trybie "Pull";
- Oprogramowanie umożliwia wysyłanie polecenia w trybie "shutdown".;
- Oprogramowanie pozwala na indywidualną interakcję użytkownika w trakcie wykonywania zadania uruchomionego przez administratora w trybach: opóźnienie, odmowa, przypomnienie o instalacji;
- Oprogramowanie umożliwia wysyłanie polecenia Wake-on LAN;
- Oprogramowanie umożliwia automatyczne generowanie i wysyłanie powtarzających się zadań (recurring Jobs);

- Oprogramowanie umożliwia uruchomienie zadania z poziomu użytkownika końcowego poprzez Kiosk samoobsługowy SelfService (dostępny przez Web);
- Zadania mogą być inicjowane z poziomu aplikacji selfservice - konsoli Webowej;
- Zawartość aplikacji SelfService (Kiosku) może być definiowana zarówno per User/Grupa Userów jak i per PC/Organisation Unit;

Instalacja Oprogramowania (uwagi i wymagania minimalne).

- Kreator do tworzenia pakietów, w skład których wchodzi różnorodne oprogramowanie;
- Detekcja oraz wsparcie kreatory dla wielu mechanizmów instalacji: MSI, InnoSetup, NullSoft, Wise-Installer i inne;
- Uzupełnienie instalacji oprogramowania na urządzeniu końcowym o dodatkowe kroki ze strony użytkownika końcowego (np.: deaktywacja okna powitalnego, itp);
- Integracja procedury odinstalowania;
- Natywna instalacja pakietów (a nie tylko wrap aplikacji w innym skrypcie instalacyjnym);
- Transparentna instalacja (w Logach znajduje się informacja dotycząca instalacji np.: msiexec.exe /i \\...\software-xyz.msi /qn /noreboot);
- Indywidualna konfiguracja zależności (np.:uprzednia instalacja .net (w przypadku, jeśli takowa nie miała jeszcze miejsca), następnie instalacja docelowego oprogramowania);
- Ustawianie zachowań w trakcie Reboot również dla oprogramowania;
- Możliwość użycia własnych skryptów, żeby np: customizować Linki, Rejestry, Working Directories, itd.;
- Użycie narzędzia do tworzenia własnych skryptów w celu tworzenia własnych pakietów instalacyjnych (np.: "kopiuj pliki z .. , stwórz ikonę Start");
- Dostarczenie narzędzia do nagrywania kroków instalacji oprogramowania, tak, by administrator mógł przejść wszystkie kroki instalatora i wypchnąć tak wyklikany instalator zdalne;
- Różnorodna weryfikacja instalacji (np.: jaka jest wartość zwrotna programu instalacyjnego, czy istnieje jakiś określony wpis do rejestru lub usługa);
- Ustawienie dowolnego kontekstu security/uprawnień z jakimi dana paczka ma zostać zainstalowana na urządzeniu końcowym;

Automatyczna dystrybucja poprawek dla systemów MS / Patch Management

- Oprogramowanie umożliwia dystrybucji patchy Windows bez WSUS;
- Oprogramowanie umożliwia triggerowanie z poziomu WSUS;
- Oprogramowanie umożliwia obsługę systemów operacyjne Microsoft — Windows Server 2008, Windows 7, Windows 8, Windows 10, Windows 11, Windows Server 2008R2, Windows Server 2012, Windows Server 2019 z natywną instalacją;
- Producent oprogramowania zapewnia stały dostęp do bazy danych z poprawkami Microsoft - baza jest dostępna dla Klienta z poziomu konsoli oprogramowania w dniu jej opublikowania przez Microsoft;
- Oprogramowanie umożliwia określenie ścisłych wymagań czasowych dla instalacji poprawek Microsoft i te wymagania kontrolować. Oprogramowanie nie wymaga ingerencji w reguły eksploatacji serwerów, a mimo to zapewnia ich odpowiednio szybkie zamknięcie w razie luk w zabezpieczeniach;
- Oprogramowanie pozwala administratorowi zarządzać aktualizacją systemów: możliwość sprawdzania tylko pod kątem brakujących poprawek i czy poprawki mają być od razu instalowane. Poprawki mogą być zatwierdzane automatycznie lub ręcznie. Oprogramowanie pozwala także ustalać reguły dla różnych grup w systemie IT;

- Oprogramowania pozwala by metodą drag and drop w środowisku zgodnym z MMC określać, w jakich systemach mają być instalowane poprawki. W taki sam sposób definiowane są również automatyczne instalacje i sytuacje, w których administrator ma być wcześniej pytany o zgodę. Oprogramowanie automatycznie pobiera wszystkie poprawki Microsoft i na żądanie automatycznie je rozprowadza w infrastrukturze Klienta zgodnie z wytycznymi administratora kreator skryptów, konfiguracji pakietów i autmatyzacja dowolnych procesów / Automate i Package Studio;
- Oprogramowanie pozwala na tworzenie plików transformacji (MST), które umożliwiają niezawodne dopasowanie do każdego MSI;
- Oprogramowanie pozwala na tworzenie kreatora instalacji dla dowolnej aplikacji - nie wymaga paczki MSI;
- Oprogramowanie pozwala tworzyć pakiety instalacyjne, gdzie w ramach procesu można zainstalować "n" aplikacji lub wykonać szereg dodatkowych funkcji związanych np. z inwentaryzacją;
- Oprogramowanie obsługuje wszystkie powszechnie dostępne na rynku systemy operacyjne Microsoft — Windows Vista i Server 2008, Windows 7, Windows 8, Windows10, Windows 11, Windows Server 2008R2, Windows Server 2012 i Windows 2019;
- Oprogramowanie umożliwia tworzenie plików sterujących (tansform);
- Oprogramowanie pozwala na automatyzacje niemal każdego procesu wykonywanego ręcznie na komputerze;
- Oprogramowania pozwala na proste tworzenie skryptów metodą drag and drop;
- Oprogramowanie zawiera standardowy zestaw poleceń;
- Oprogramowanie posiada możliwość sterowania również interfejsami niezgodnymi ze standardem (np. Java);
- Oprogramowanie posiada pomoc kontekstową;
- Oprogramowanie posiada tryb testowy step by step;

Moduły

- Identyfikacja urządzeń SNMP, takich jak drukarki, routery, przełączniki inne urządzenia sieciowe;
- Wizualizacja topologii sieci;
- Automatyczne skanowanie sieci firmowej;
- Identyfikacja stopnia wykorzystania oprogramowania;
- Automatyczna i natywna instalacja systemów operacyjnych;
- Bezpośrednie połączenie z urządzeniami końcowymi w sieci;
- Rejestracja zużycia energii na stanowiskach pracy;
- Kontrola przypisanych licencji do konta;
- Automatyczne skanowanie pod kątem podatności;
- Podniesienie poziomu bezpieczeństwa;

2. Oprogramowanie przeciwdziałające wyciekowi danych – 20 sztuk.

Dostarczone licencje muszą być licencjami wieczystymi (bezterminowymi), uprawniającymi Zamawiającego do korzystania z oprogramowania bez ograniczenia czasowego, również po wygaśnięciu wsparcia producenta i po dniu 31 grudnia 2026 r. Zamawiający nie dopuszcza licencji terminowych, subskrypcyjnych ani wynajmu licencji. Ewentualne wsparcie producenta i prawo do aktualizacji mogą być ograniczone czasowo, co nie może wpływać na bezterminowe prawo korzystania z dostarczonej wersji oprogramowania.

1. System operacyjny:
   a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi,
   b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi,
   c. MacOS 12 lub nowszy.

2. Serwer administracyjny musi obsługiwać instalację na systemach:
    a. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych:
    a. MS SQL Server 2016 lub nowsze,
    b. MS SQL Express,
    c. AzureSQL S3 lub nowsze.
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. System musi posiadać mechanizm usuwający najstarsze informacje, gdy rozmiar bazy osiągnie domyślny limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości e- mail oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20.Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać możliwość połączenia z serwerem SMTP udostępnianym przez producenta.
24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak
i nowo powstałych na bazie już skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Administrator musi mieć możliwość tworzenia kategorii danych dla plików zaszyfrowanych lub dla takich gdzie zawartość pliku jest niemożliwa do odczytania.
27. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
28. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików
w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, numer REGON, NIP, wyrażenia regularne, określone ciągi znaków i numer IBAN.
29. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.

30. Administrator musi mieć możliwość wyszukiwania danych wrażliwych
w zasobach lokalnych 31 Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
32.Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
33. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego
oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
34. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
35. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików
w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
36. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach.
37. System musi umożliwiać synchronizacji grup bezpieczeństwa z Active Directory na potrzeby logowania do konsoli zarządzającej.
38.System musi umożliwiać administratorowi nadanie użytkownikowi uprzywilejowanego dostępu, przez co nie będzie obejmowany politykami przez określony czas – 1 godzinę, 6 godzin lub do końca dnia.
39. System musi posiadać możliwość tworzenia polityk dynamicznych, pozwalających na dostosowywanie się akcji (takich jak zapisywanie logu, powiadomienie użytkownika, blokowanie lub blokowanie z możliwością zastąpienia przez użytkownika) w zależności od profilu pracy użytkownika wykonującego daną czynność, gdzie akcja dobierana jest w zależności od wyniku systemu uczenia maszynowego.
40. System musi umożliwiać dostosowanie polityk dynamicznych do dwóch trybów: standardowy oraz łagodny. Możliwość taka musi istnieć per użytkownik.
41. System musi umożliwiać tworzenie raportów na podstawie logów zebranych
w układach danych z możliwością dostosowania filtrów, użytkowników oraz zakresu czasu objętych raportowaniem.
42. System musi umożliwiać utworzenie raportu, który będzie zawierał podsumowanie stanu zabezpieczenia danych wraz z rekomendacjami w formie cyklicznej.
43. System musi zbierać informacje na temat podłączanych urządzeń do komputera, odwiedzanych domen internetowych, ścieżek sieciowych, drukarek lokalnych oraz sieciowych, umożliwiając jednocześnie przypisanie takowych wpisów do bezpiecznych lub niezaufanych lokalizacji bez potrzeby manualnego wpisywania ścieżek lub numerów seryjnych urządzeń.
44. Dla każdej z wyżej wymienionych lokalizacji system powinien umożliwiać przypisanie indywidualnej polityki dostępu – np. umożliwiając przesyłanie danych do lokalizacji oznaczonej jako bezpieczna, jednocześnie blokując wysyłkę do lokalizacji oznaczonej jako niezaufana lub nieprzypisana.
45. System musi umożliwiać audyt operacji wykonywanych przez administratora
w obszarze konsoli DLP.
46. System musi umożliwiać podłączenie archiwa logów w formacie plików

3. Oprogramowanie typu XDR – 55 sztuk.

Oprogramowanie musi zostać dostarczone na okres nie przekraczający 31.12.2026 r.
Minimalne wymagania Zamawiającego:
Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami
2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.
3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi
4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog.
5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
6. Wbudowana technologia do ochrony przed rootkitami.

7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Możliwość dodawania wykluczeń na podstawie

a. Plik
b. Folder
c. Rozszerzenie
d. Proces
e. Hash pliku
f. Hash certyfikatu
g. Nazwa zagrożenia
h. Wiersz poleceń
i. IP/maska

13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.
14. Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
20. Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.
21. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
22. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.
23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie" możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.
24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
25. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia.
26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
28. Praca programu musi być niezauważalna dla użytkownika.
29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.
30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
32. Możliwość odblokowania ustawień programu po wpisaniu hasła.

33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu.
34. Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie).
35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu.
36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.
37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora.
38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
40. Wbudowany IDS
41. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego.
42. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji.
43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego.
44. Możliwość tworzenia list sieci zaufanych.
45. Możliwość dezaktywacji funkcji zapory sieciowej.
46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
48. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji.
49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa)
50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups
51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.
52. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:

a. Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:

-Ochrony przeglądarki internetowej
-Sieć i poświadczenia
-Błędna konfiguracja systemu operacyjnego

System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

b. System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.
c. System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.
d. System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.
e. System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.
f. System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie

53. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
a. Możliwość wymuszenia funkcji DEP systemu Windows
b. Możliwość wymuszenia relokacji modułów (ASLR)

Uwaga: Ta warstwa zabezpieczeń dotyczy systemów opartych na systemie Windows.

54. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:
- Wczesny dostęp
- Dostęp do poświadczeń
- Wykrycie
- Crimeware

55. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji.

Formaty plików jakie mogą być odzyskane:
3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini|jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx|png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml|

Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.

56. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:
a. Ukierunkowane ataki
b. Podejrzane pliki i ruch w sieci
c. Exploity
d. Ransomware
e. Grayware
57. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego
58. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na:
a. Tolerancyjny
b. Normalny
c. Agresywny
59. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku
a. Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora
b. Możliwość przesłania archiwum zabezpieczonego hasłem
c. Możliwość przesłania adresu URL
d. W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
60. Wbudowany sandbox musi działać w trybie monitorowania i blokowania
61. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny
62. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.
63. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
64. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB
65. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB.

66. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).
67. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń, wskaźniki te obejmują:

Maszyny Wirtualne

1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu).
2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem.
4. Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera.
5. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
6. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta.
7. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
8. Możliwość wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych.

Stacje robocze i serwery Windows

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
6. Skanowanie plików spakowanych i skompresowanych.
7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu.
9. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę.
10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych.
11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.
13. Program musi mieć wbudowany skaner wyszukiwania rootkitów
14. Możliwość odblokowania ustawień programu po wpisaniu hasła
15. Możliwość uruchomienia zadania skanowania z niskim priorytetem
16. Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego.
17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej.
18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem
19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym.
20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

Ochrona Exchange

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w przeciągu ostatnich kilku godzin / dni.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania.
4. Możliwość wykluczenia potencjalnie niechcianych aplikacji (PUA) z filtrowania antymalware.

5. Możliwość skanowania w poszukiwania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowania maila do konkretnej skrzynki pocztowej.
11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

Konsola zdalnej administracji

1. Dwa typy konsoli administracyjnej:

- Konsola Cloud – serwer administracyjny po stronie producenta
- Konsola On-premise – lokalny serwer administracyjny

2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
3. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
4. Możliwość integracji Domeny Active Directory w obu typach konsoli.
5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
7. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
11. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv.
14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
15. Możliwość generowania raportu co godzinę.
16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
17. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
18. Możliwość dodania etykiety do stacji roboczej.

19. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
20. Możliwość przechowywania kwarantanny maksymalnie 180 dni
21. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
22. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
23. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
24. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.[2]
25. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.
26. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
27. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie

-Zakres adresów IP/IP
-Adres bramy
-Adres serwera WINS
-Adres serwera DNS
-Połączenie DHCP sufiksów DNS
-Punkt końcowy może rozwiązać hosta
-Typ sieci
-Nazwa hosta

28. Integracja z serwerem Syslog.
29. Uwierzytelnienie dwuskładnikowe realizowane wyłącznie przez aplikację Google Authenticator.
30. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
31. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
32. Funkcja pojedynczego logowania – Single Sign-on (SSO).
33. Możliwość naprawy instalacji z poziomu konsoli.
34. Raport streszczający - Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak:

- Zarządzane punkty końcowe
- Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne
- Pięć najczęściej blokowanych zagrożeń
- Podział zagrożeń na urządzenia takie jak stacje robocze i serwery
- Status incydentów bezpieczeństwa które wystąpiły
- Stan modułów punktów końcowych
- Ocena ryzyka firmy
- Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
- Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware

35. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak:

a. Pakiety
b. Sieć
c. Kwarantanna
d. Licencjonowanie
e. Integracje
f. Polityki
g. Raporty
h. Konta
i. Firmy

36. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na określenie godziny kiedy te maszyny będą usuwane
37. Możliwość określenia własnego serwera NTP.
38. Integracja z vCenter Server.
39. Integracja z Xen Server.
40. Integracja z nutanix Prism Element.
41. Możliwość integracji z Amazon EC2.
42. Intergracja z Azure.
43. Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach konfiguracyjnych, komputery fizyczne, Urządzenia mobilne.
44. Serwer centralnej administracji musi posiadać funkcje przełączenia się miedzy widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych.
45. Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych.
46. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
47. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.
48. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej.
49. Pion firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej, dostępne muszą być opcje takie jak:

a. Lotnictwo
b. Rolnictwo
c. Automotive
d. Usługi komercyjne
e. Doradztwo
f. Energia
g. Usługi finansowe
h. Rząd
i. Opieka zdrowotna
j. Technologie
k. Transport
l. Non-profit
m. Górnictwo
n. Media

50. Funkcja kontroli aplikacji która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów.
51. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym.
52. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.
53. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
54. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
55. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS.
56. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
57. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
58. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
59. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1.
60. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.

61. Możliwość skanowania SSL dla połączeń RDP.
62. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.
63. Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Program wczesnego dostępu powinien umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.
64. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych.
65. Oprogramowanie musi umożliwiać przypisywanie znaczników ręcznie lub automatycznie.
66. Oprogramowanie musi umożliwiać filtrowanie punktów końcowych na podstawie wybranych znaczników, musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
67. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.

EDR-Endpoint Detection and Response

Produkt musi zapewnić szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze
Wspierane systemy operacyjne

A. Systemy desktopowe

- Windows 11 (initial)
- Windows 10 November 2021 Update (21H2)
- Windows 10 May 2021 Update (21H1)
- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10 (initial)
- Windows 8.1
- Windows 8
- Windows 7 SP1

B. Systemy operacyjne dla serwerów:

- Windows Server 2022
- Windows Server 2019 Core
- Windows Server 2019
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

C. MacOS:

- macOS Monterey (12.x)
- macOS Big Sur (11.x)

- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)

D. Linux

- RHEL 7.x & 8.x ; 3.10.0-957 - 4.18.0
- RHEL 9x 5.14.x
- Oracle Linux 7.x (UEK +RHCK) ; 3.10.0-957 - 4.18.0
- Oracle Linux 8.x (UEK +RHCK) ; 3.10.0-957 - 4.18.0
- CentOS 7.x ; 3.10.0-957 - 4.18.0
- CentOS 8.x ; 3.10.0-957 - 4.18.0
- Debian 10 ; 4.19
- Debian 11 ; 5.10
- Ubuntu 16.04.x ; 4.8 / 4.10 / 4.13 / 4.15
- Ubuntu 18.04.x ; 5.0 / 5.3 / 5.4
- Ubuntu 20.04.x ; 5.4 / 5.8 / 5.11 / 5.13
- Ubuntu 22.04.x ; 5.15
- SLES 12 SP4 ; 4.12.14-x
- SLES 12 SP5 ; 4.12.14-x
- SLES 15 SP1 ; 4.12.14-x
- SLES 15 SP2 ; 5.3.18-x
- SLES 15 SP3 ; 5.3.18-x
- openSUSE Leap 15.2 ; 5.3.18
- AWS Bottlerocket 2020.03 ; 5.4.x, 5.10.x
- Amazon Linux v2 ; 4.14.x / 4.19.x
- Google COS Milestones 77, 81, 85 ; 4.19.112 / 5.4.49
- Fedora 31 – 36 ; Wspierane do wygaśnięcia.
- AlmaLinux 8.x ; 4.18.0
- Rocky Linux 8.x ; 4.18.0
- CloudLinux 8.x ; 4.18.0
- CloudLinux 7.x ; 3.10
- Pardus 21 ; 5.10
- Linux Mit 20.3 ; 5.4.0

Komponenty EDR

Główne elementy:

1. Czujnik EDR, który gromadzi i przetwarza dane w celu raportowania danych dotyczących punktu końcowego i zachowania aplikacji.
2. Security Analytics, komponent służący do interpretacji metadanych gromadzonych przez czujnik EDR.
3. Możliwość instalacji dodatkowego, lekkiego agenta z czujnikiem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną ochronę. Agent posiada też ochronę urządzenia i ruchu sieciowego oraz filtr stron internetowych.

Wykrywanie podejrzanej aktywności

1. Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności.
2. Bazowanie na systemach bazujących na wskaźnikach ataku MITRE i własnej inteligencji.
3. Zgłaszanie wszystkich naruszeń jako incydent w module EDR.

Badanie incydentów i wizualizacja

1. Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym przedziale czasu.
2. Produkt integruje się z bazą wiedzy ATT & CK firmy MITRE i odpowiednio oznacza zdarzenia bezpieczeństwa
3. Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi informacjami lub działaniami z następującymi informacjami:

a. Karta Podsumowanie zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia.
b. Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej.
c. Działania naprawcze gromadzą informacje o działaniach blokujących automatycznie podejmowanych przez produkt w związku z bieżącym zdarzeniem bezpieczeństwa.

<u>Incydenty</u>

1. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość:

a. Filtrowania zdarzeń
b. Blokowania procesów
c. Dodawanie procesów do czarnej listy
d. Dodawanie procesów do białej listy
e. Izolacja hosta
f. Aktualizacja oprogramowania firm trzecich na hoście (wymagany add-on)
g. Przesłanie pliku do Sandbox
h. Sprawdzenie informacji o pliku w Google
i. Sprawdzenie informacji o pliku w VirusTotal

2. Filtrowanie zdarzeń odbywa się na podstawie:

a. Ocena zagrożenia od 10 do 100 punktów
b. Data wykrycia
c. Status
d. ID
e. Nazwa punktu końcowego
f. Typ ataku

- Ransomware
- Potencjalnie niechciana aplikacja
- Malware
- Exploit
- Fileless
- Password stealer
- Downloader
- Inne
- Zdefiniowane przez użytkownika

3. Wyszukiwanie zdarzeń może odbywać się na podstawie:

a. Nazwa alertu
b. IP punktu końcowego
c. Hash MD5
d. Hash SHA256
e. Nazwa użytkownika

4. Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem.
5. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.
6. Możliwość wyświetlenia zablokowanych hashy plików.
7. Możliwość dodania własnych hashy MD5 oraz SHA256
8. Możliwość importu hashy z pliku CSV

9. Możliwość filtrowania dodanych hashy na podstawie:
a. Typu hashu
b. Wartości hash
c. Źródło dodania
d. Informacje o źródle
e. Nazwa pliku
f. Firma której dotyczy wpis
g. Możliwość wyświetlenia 10,20,30,50,100 wpisów na jednej stronie.

4. Oprogramowanie do wykonywania kopii zapasowych – 2 sztuki.

Dostarczone licencje muszą być licencjami wieczystymi (bezterminowymi), uprawniającymi Zamawiającego do korzystania z oprogramowania bez ograniczenia czasowego, również po wygaśnięciu wsparcia producenta i po dniu 31 grudnia 2026 r. Zamawiający nie dopuszcza licencji terminowych, subskrypcyjnych ani wynajmu licencji. Ewentualne wsparcie producenta i prawo do aktualizacji mogą być ograniczone czasowo, co nie może wpływać na bezterminowe prawo korzystania z dostarczonej wersji oprogramowania.

Lp.	Minimalne wymagania Zamawiającego
I. **Wymagania ogólne**	
1.	Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie: - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
2.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
3.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
II. **Całkowite koszty posiadania**	
1.	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
2.	Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3.	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
4.	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
5.	Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.

6.	Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
7.	Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
8.	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9.	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
10.	Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
11.	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
12.	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
13.	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
14.	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
15.	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
16.	Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej

5. Testy socjotechniczne.

1. Przygotowanie kampanii socjotechnicznej;
   a. wybór i zakup przez Wykonawcę domeny (łudząco podobnej do domeny Zamawiającego), która zostanie wykorzystana do kampanii socjotechnicznej;
   b. opracowanie bazy mailingowej pracowników objętych kampanią socjotechniczną oraz spreparowanego dokumentu zbliżonego wyglądem do dokumentów Zamawiającego, zawierającego dodatkowy niezłośliwy kod pozwalający na mierzenie efektów kampanii;
   c. wyznaczenie osób wtajemniczonych w fakt przeprowadzania testów (np. najwyższe kierownictwo, dział informatyczny lub wyłącznie szef tego działu, inspektor ochrony danych lub inna osoba odpowiedzialna za bezpieczeństwo w organizacji);
   d. wsparcie w zakresie dodania domeny wybranej do przeprowadzenia kampanii socjotechnicznej do tzw. białej/zaufanej listy w celu pominięcia filtrów antyspamowych (celem testu jest dostarczenie spreparowanej wiadomości na wszystkie skrzynki pracowników i weryfikacja ich podatności na prawdziwe kampanie cyberprzestępców).
2. Przygotowanie spreparowanych zasobów służących wyłudzaniu informacji:
   a. serwer strony www z bazą danych powiązany z domeną, która została zakupiona w celu przeprowadzenia kampanii socjotechnicznej;
   b. wygenerowanie niezbędnych certyfikatów SSL;

c. przygotowanie spreparowanego aktywnego dokumentu PDF, wyposażonego w autorski, niezłośliwy skrypt, którego celem jest zebranie informacji o użytkownikach, którzy dokonali otwarcia pliku PDF i uruchomienia niezłośliwego skryptu (w prawdziwej kampanii byłoby to złośliwe oprogramowanie);

d. utworzenie nowej podstrony, na której umieszczony zostanie spreparowany plik PDF;

e. przygotowanie konta mailowego, którego celem jest podszycie się pod jedną z osób wtajemniczonych w prowadzone testy phishingowe;

f. przygotowanie treści wiadomości e-mail i wyposażenie jej w mechanizmy pozwalające na przeprowadzenie tzw. detekcji umiejscowienia (uzyskanie adresu IP potencjalnej „ofiary").

3. Przeprowadzenie kampanii socjotechnicznej (wysłanie przygotowanej uprzednio wiadomości e-mail do pracowników wskazanych w bazie mailingowej).
4. Wykonanie raportu z testu socjotechnicznego w języku polskim.

6. Szkolenie z cyberbezpieczeństwa dla pracowników.

Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników administracyjnych.

Szkolenie stacjonarne lub online z zakresu cyberbezpieczeństwa skierowane do pracowników administracyjnych, obejmujące co najmniej następujące obszary:

a) wprowadzenie do cyberbezpieczeństwa:
   - czym jest cyberbezpieczeństwo;
   - dlaczego cyberbezpieczeństwo jest ważne;
   - kluczowe zagadnienia związane z cyberbezpieczeństwem;
   - przegląd statystyk i trendów w cyberbezpieczeństwie.

b) typy zagrożeń w cyberprzestrzeni:
   - malware (wirusy, trojany, robaki itp.);
   - ataki typu phishing i spear phishing;
   - ataki DDoS;
   - ataki ransomware;
   - zagrożenia związane z sieciami społecznościowymi.

c) zasady bezpieczeństwa i praktyki:
   - zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
   - zasady bezpieczeństwa e-mail;
   - bezpieczeństwo w sieciach bezprzewodowych;
   - bezpieczne przeglądanie internetu;

- backup i odzyskiwanie danych.

d) reagowanie na incydenty i planowanie awaryjne:

- jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;
- zasady reagowania na incydenty;
- planowanie awaryjne i kontynuacja działalności;
- Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione.

Przewiduje się, że szkolenie potrwa łącznie minimum 8 godzin roboczych, rozłożonych na co najmniej 1 dzień. Zajęcia będą organizowane w dwóch grupach szkoleniowych, gdzie każda grupa będzie miała 4 godziny zajęć dziennie. Dodatkowo, każda sesja będzie obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

7. Szkolenie z cyberbezpieczeństwa dla menedżerów.

Przekazanie menedżerom zaawansowanej wiedzy i narzędzi niezbędnych do efektywnej ochrony przed rosnącymi zagrożeniami cybernetycznymi, poprzez pogłębione rozumienie ryzyk, strategii obronnych, regulacji prawnych oraz najnowszych trendów w cyberbezpieczeństwie.

Struktura programu szkoleniowego:
Szkolenie powinno być kompleksowym procesem, który umożliwia uczestnikom zdobycie dogłębnej wiedzy na temat wybranych zagadnień. Powinno ono nie tylko dostarczyć podstawowej informacji, ale także omówić zaawansowane aspekty danej tematyki, aby uczestnicy mieli pełniejsze zrozumienie tematu i byli w stanie zastosować zdobytą wiedzę w praktyce. Przekazywanie wiedzy powinno być interaktywne i angażujące, wykorzystując różnorodne metody nauczania, takie jak prezentacje, dyskusje, studia przypadków czy praktyczne ćwiczenia, co pozwoli uczestnikom efektywniej przyswoić omawiany materiał.

W ramach przeprowadzonego szkolenia wykonawca

1. Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa:
- Podstawy i definicje: zapewnienie uczestnikom solidnych podstaw w dziedzinie cyberbezpieczeństwa poprzez omówienie kluczowych pojęć i zasad. Ponadto, zostanie przedstawiona rola menedżera w formowaniu bezpiecznego środowiska cyfrowego, co pozwoli zrozumieć jak ważne jest aktywne zaangażowanie kierownictwa w procesy zapewnienia bezpieczeństwa informacji. W ten sposób uczestnicy będą mieć pełniejsze zrozumienie zarówno teoretycznych, jak i praktycznych aspektów cyberbezpieczeństwa oraz będą lepiej przygotowani do podejmowania decyzji w tym obszarze.
- Statystyki i trendy: skoncentrowanie się na przekazaniu uczestnikom szczegółowej analizy globalnych i lokalnych danych dotyczących cyberataków. Poprzez omówienie ewolucji tych ataków oraz ich metodologii, uczestnicy zyskają wgląd w aktualne trendy i sposoby działania cyberprzestępców. Ponadto, zostaną przedstawione skutki, jakie cyberatak może mieć dla biznesu, co pozwoli uczestnikom lepiej zrozumieć znaczenie inwestycji w bezpieczeństwo informacji oraz skuteczne zarządzanie ryzykiem cybernetycznym dla organizacji. Dzięki temu będą mogli podejmować bardziej świadome decyzje w zakresie ochrony swoich danych i infrastruktury cyfrowej.

2. Omówienie światowych standardów i norm w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji:

- Normy ISO/IEC: Szczegółowe omówienie serii norm: ISO/IEC 27000: (zarysowuje leksykon oraz globalne zasady nadrzędne systemu zarządzania bezpieczeństwem informacji, kreśląc fundament pod szersze zrozumienie oraz efektywniejsze stosowanie pozostałych norm z rodziny 27000), ISO/IEC 27001 (stanowi kanon dotyczący wymagań dla systemów zarządzania bezpieczeństwem informacji, umożliwiając organizacjom zabezpieczenie informacji pod kątem ich poufności, integralności oraz dostępności przez implementację adekwatnych procedur zarządczych), ISO/IEC 27002 (oferuje referencyjny zbiór praktyk dla organizacji dążących do identyfikacji, wdrażania, utrzymania oraz doskonalenia swoich mechanizmów ochrony informacji w kontekście SZBI), ISO/IEC 27004 (dostarcza metodykę do monitorowania, przeglądu, oceny oraz doskonalenia efektywności systemu zarządzania bezpieczeństwem informacji, akcentując znaczenie mierzalnych wskaźników), ISO/IEC 27005 (zawiera wytyczne dotyczące zarządzania ryzykiem w kontekście bezpieczeństwa informacji, nakreślając proces identyfikacji, oceny oraz zarządzania ryzykiem informacyjnym), ISO/IEC 27006 (określa wymogi dla organizacji świadczących usługi certyfikacji systemów zarządzania bezpieczeństwem informacji, wyznaczając ramy dla procesu audytu i certyfikacji), ISO/IEC 27013 (podaje wytyczne integrujące system zarządzania bezpieczeństwem informacji z systemem zarządzania usługami IT, promując koherentną i efektywną infrastrukturę zarządzania), ISO/IEC 27017 (koncentruje się na bezpieczeństwie informacji w chmurze, proponując kontrole oraz wytyczne dla dostawców i użytkowników usług przetwarzania w chmurze), ISO/IEC 27018 (ustanawia kodeks praktyk dla ochrony informacji osobowych w chmurze, zgodnie z wymaganiami prywatności i ochrony danych), ISO/IEC 22301 (specyfikuje wymogi dla systemów zarządzania ciągłością działania, umożliwiając organizacjom przygotowanie na incydenty zakłócające normalne funkcjonowanie), ISO/IEC 24762 (zawiera wytyczne dla usług odzyskiwania po awariach w centrach danych i innych środowiskach IT, podkreślając kluczowe elementy potrzebne do przywrócenia operacji IT po katastrofie, ISO/IEC 27036 (skupia się na zarządzaniu bezpieczeństwem informacji w relacjach między organizacjami, oferując wytyczne dotyczące bezpieczeństwa w outsourcingu i partnerstwach biznesowych), ISO/IEC 31000 (dostarcza wytyczne dotyczące zarządzania ryzykiem ogólnym, promując model zarządzania ryzykiem, który można dostosować do różnych typów organizacji i kontekstów), 13501-2 (norma ta przeprowadza proces kategoryzacji reakcji na ogień wyrobów używanych w budownictwie oraz elementów konstrukcyjnych budowli, określając ich parametry odporności na pożary i zachowanie w ekstremalnych warunkach termicznych), norma 1627 (stanowi kryteria odporne na nieautoryzowany dostęp przez systemy zamykające, jak okna, drzwi oraz osłony, hierarchizując je zgodnie z ich zdolnością do stawiania oporu przy próbach sforsowania), norma 12209-04 (wytycza wymagania techniczne oraz procedury badawcze dla mechanizmów blokujących w obszarze budowlanym, takich jak zamki mechaniczne wraz z ich komponentami, oceniając ich funkcjonalność oraz niezawodność.), norma 50131-1 (określa specyfikacje dla systemów alarmowych przeznaczonych do sygnalizacji prób włamania czy napadu, wyznaczając standardy dotyczące ich skuteczności oraz metodyki testowania).

- Omówienie znaczenia powyższych norm i ich w zapewnianiu wysokiego poziomu bezpieczeństwa informacji oraz praktycznego zastosowania w organizacjach.
- Inne standardy: Przedstawienie i dyskusja na temat innych standardów:
    - ramy dotyczące zarządzania ryzykiem cyberbezpieczeństwa - NIST Cybersecurity Framework;
    - ramy dotyczące wdrażania, rozwoju i doskonalenia polityki IT – COBIT;
    - zbiór praktyk dotyczący zarządzania usługami IT – ITIL;
    - akceptowalna polityka szyfrowania SANS;
    - techniki kryptograficzne - ENISA ;
    - ramy ochrony informacji i zasobów federalnych agencji rządowych USA - 800-53 rev3.
- Rola powyższych zagranicznych standardów w kształtowaniu efektywnych polityk bezpieczeństwa w organizacjach.

3. Omówienie zaawansowanych strategii ochrony organizacji:

- Zarządzanie ryzykiem: Metody identyfikacji, oceny, mitygacji i monitorowania ryzyka cybernetycznego. Wykorzystanie narzędzi i technologii do analizy ryzyka.
- Wprowadzenie do zarządzania incydentami, zdefiniowanie incydentów i wektorów ataku: atak przeprowadzony z nośnika wymiennego lub urządzenia peryferyjnego, atak wykorzystujący metody brute-force w celu złamania, degradacji lub zniszczenia systemów, sieci lub usług, ataki wykonane z poziomu witryny internetowej lub aplikacji internetowej, atak przeprowadzony za pośrednictwem wiadomości e-mail lub załącznika, naruszenia zasad dopuszczalnego użytkowania organizacji przez autoryzowanego użytkownika, z wyłączeniem powyższych

kategorii, utrata lub kradzież urządzenia komputerowego lub nośnika używanego przez organizację, na przykład laptopa lub urządzenia typu smartfon.

- Szczegółowy opis i kroki zarządzania incydentami:
  - wykrywanie: inicjacja procesu inicjującego, mającego na celu detekcję niestandardowych aktywności lub zdarzeń infrastrukturalnych, które mogą sygnalizować potencjalne zagrożenia w obszarze cybernetycznym;
  - rejestrowanie: operacja dokumentacyjna, polegająca na chronologicznym zapisie zaobserwowanych dysfunkcji w dedykowanych bazach danych, by zapewnić dokumentację dowodową dla późniejszych faz postępowania;
  - analizowanie: metodyczne badanie zgromadzonych artefaktów zdarzeń w celu zrozumienia ich genezy, dynamiki oraz wpływu na ekosystem informacyjny;
  - klasyfikowanie: systematyzacja incydentów według ustalonego kodu klasyfikacyjnego, uwzględniająca ich naturę, zasięg oraz potencjalne konsekwencje dla organizacji.
  - priorytetyzowanie: alokacja zasobów reakcyjnych na bazie oceny krytyczności, która koresponduje z możliwymi konsekwencjami incydentu dla misji instytucji;
  - podejmowanie działań naprawczych: inicjowanie interwencji korygujących mających na celu restytucję funkcji systemowych i prewencję przed podobnymi naruszeniami w przyszłości;
  - ograniczanie skutków incydentu: implementacja taktyk zaradczych, które mają za zadanie minimalizację negatywnych rezultatów incydentu oraz odbudowę stanu równowagi operacyjnej.
- Priorytetyzacja incydentów na 3 kategorie: krytyczny, wysoki, średni na podstawie poniższych opisów:
  - Priorytet krytyczny - Incydent wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT. Procesy wewnętrzne są sparaliżowane lub zakłócone w znaczącym stopniu. Istnieje wysokie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
  - Priorytet wysoki - Incydent wymaga szybkiego działania oraz zgłoszenia do właściwego CSIRT w ciągu 24 godzin. Procesy wewnętrzne są częściowo zakłócone lub sparaliżowane. Istnieje niskie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
  - Priorytet średni - Incydent prawdopodobnie nie wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT ze względu na brak symptomów działania z zewnątrz. Procesy wewnętrzne nie są sparaliżowane lub zakłócone w żadnym stopniu. Ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji nie występuje.
- Budowanie zespołów ds. bezpieczeństwa: Definicja ról, odpowiedzialności, umiejętności oraz ścieżek rozwoju dla członków zespołu bezpieczeństwa.
- Lista omówionych kompetencji w szkoleniu:
  - Szef działu bezpieczeństwa (kierownik, dyrektor);
  - Pełnomocnik ds. Bezpieczeństwa Informacji;
  - Specjalista ds. Zarządzania Ryzykiem;
  - Specjalista ds. Zgodności;
  - Specjalista ds. Bezpieczeństwa Fizycznego;
  - Architekt Systemów Bezpieczeństwa;
  - Koordynator Programu Bezpieczeństwa;
  - Analityk Bezpieczeństwa (II linia wsparcia);
  - Inżynier ds. Bezpieczeństwa (II linia wsparcia);
  - Administrator Systemów Bezpieczeństwa (II linia wsparcia);
  - Specjalista ds. Odpowiedzi na Incydenty (III linia wsparcia);
  - Specjalista ds. Testów Penetracyjnych (III linia wsparcia);
  - Specjalista ds. Testów Socjotechnicznych (III linia wsparcia).

4. Regulacje prawne i compliance:

- Zharmonizowanie działalności Podmiotu z imperatywami Ustawy o Krajowym Systemie Cyberbezpieczeństwa, z naciskiem na implementację procedur i protokołów zapewniających wytrzymałość infrastruktury informatycznej na potencjalne zagrożenia cyfrowe.
- Inicjacja, adaptacja, perpetuacja oraz ewolucja Systemu Zarządzania Bezpieczeństwem Informacji, skonstruowanego na fundamencie czterech norm określonych w paragrafie 20 Krajowego Ramienia Interoperacyjności, stanowiących kamień węgielny dla ochrony danych.
- Egzekwowanie procedury tworzenia redundancji danych dziennikowych poprzez generowanie kopii zapasowych, które będą przechowywane przez okres minimalny dwóch lat, zgodnie z dyrektywą zawartą w paragrafie 21 Krajowego Ramienia Interoperacyjności.
- Implementacja kompleksowej agregacji logów (rejestrowanych zdarzeń) pochodzących z heterogenicznej gamy urządzeń, maszyn i aplikacji działających w ramach infrastruktury teleinformatycznej Podmiotu, umożliwiająca szczegółową analizę i audyt bezpieczeństwa.
- Integracja z zaawansowanym systemem zarządzania cyberbezpieczeństwem S46 (S46-react), celem optymalizacji procesów detekcji, reagowania i prewencji w zakresie incydentów bezpieczeństwa cyfrowego.
- Kodyfikacja programu regularnych audytów wewnętrznych i zewnętrznych, obejmujących spektrum standardów i regulacji (KRI, KSC, ISO, RODO), wraz z przeprowadzaniem testów penetracyjnych i socjotechnicznych, mających na celu weryfikację skuteczności implementowanych środków ochrony.
- Monitorowanie zdarzeń systemowych w trybie ciągłym, poprzez wykorzystanie mechanizmów korelacji zdarzeń, umożliwiających identyfikację i interpretację wzorców aktywności sugerujących potencjalne scenariusze ataków cybernetycznych.
- Dostosowanie się do rozszerzonego zakresu wymagań wynikających z implementacji Dyrektywy NIS2, która wprowadza nowe, zaostrzone standardy w zakresie cyberbezpieczeństwa, wymagające od organizacji ponownej oceny i ulepszenia istniejących strategii ochrony danych.
- Wyznaczenie dedykowanego Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji, którego rola nie będzie interferować ani generować konfliktów interesów z innymi kluczowymi funkcjami w organizacji (np. Inspektorem Ochrony Danych, Informatykiem, Dyrektorem).
- Rekonfiguracja systemów informatycznych oraz protokołów pracy zdalnej w zgodzie ze zmienionymi standardami bezpieczeństwa, uwzględniającymi nowelizację Kodeksu Pracy, w celu zabezpieczenia integralności danych korporacyjnych w rozproszonym środowisku pracy.
- Realizacja oczekiwań organów nadzorczych w kontekście konstruowania oraz utrzymywania zaawansowanych systemów cyberbezpieczeństwa, zdolnych do przeciwdziałania współczesnym zagrożeniom w przestrzeni cyfrowej.
- Implementacja rygorystycznych protokołów ochrony danych osobowych, mających na celu eliminację ryzyka wycieków informacji, spowodowanych przez nieświadome bądź intencjonalne działania personelu organizacji.
- Automatyzacja procesów aktualizacji oprogramowania w celu zapewnienia najwyższego poziom

5. Zarządzanie bezpieczeństwem w praktyce:
- Zrozumienie znaczenia typów licencji względem konieczności ich testowania:

  - Licencje niewyłączne, w których udzielający licencji może zezwolić na korzystanie z utworu wielu osobom równocześnie, które nie muszą mieć formy pisemnej.
  - Licencje wyłączne, spotykane głównie w przypadku oprogramowania pisanego na zamówienie (np. strona www), w tym przypadku zwykle umowa licencyjna wynika z umowy o dzieło, na podstawie której firma wykonująca oprogramowanie wykonuje zamówioną aplikację, umowa taka wymaga formy pisemnej pod rygorem nieważności.
  - Sublicencja, w której licencjobiorca może udzielić dalszej licencji, pod warunkiem wszakże takiego upoważnienia w jego umowie licencyjnej.
  - OEM, to programy sprzedawane wraz ze sprzętem komputerowym (przypisane do konkretnego komputera), po wymianie sprzętu na nowszy, nie można ich przenieść na nowy komputer tylko trzeba ponownie je zakupić.
  - BOX, to programy, które można przenosić na kolejne komputery jednak pod warunkiem, że zawsze zainstalowany jest tylko na jednym komputerze. Legalny jest tylko program ostatnio zainstalowany.

- Open Source (otwarte oprogramowanie) to alternatywa dla Freeware (wolne oprogramowanie), którego celem jest istnienie swobodnego dostępu do oprogramowania dla wszystkich jego uczestników. Zapewnia swoim użytkownikom prawo do legalnego oraz darmowego korzystania z zasobów.

- Techniki hardeningu: Wzmocnienie infrastruktury IT oraz zarządzanie patchami bezpieczeństwa.
- Testy penetracyjne i socjotechniczne: Organizacja i przeprowadzanie testów w celu oceny gotowości organizacji

Szkolenie powinno odbyć się w czasie nie krótszym niż 4 godziny robocze w ciągu jednego dnia z uwzględnieniem conajmniej 4 przerw po 15 minut. Po szkoleniu przewidziano 30 minut na pytania i odpowiedzi uczestników.

8. Wdrożenie oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych.

Usługi wdrożeniowe oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej.

A. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.

B. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.

C. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.

D. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.

E. Wykonawca zainstaluje oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania do zarządzania i aktualizacji systemów operacyjnych na stacjach roboczych, serwerach, urządzeniach sieciowych oraz monitorowania infrastruktury informatycznej, na wskazanym serwerze lokalnym lub w chmurze i skonfiguruje je zgodnie z wymaganiami i najlepszymi praktykami.

F. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.

G. Wykonawca przeprowadzi konfigurację strefy DMZ dla wymaganych usług.

H. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.

I. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze.

J. Wykonawca przeprowadzi testy zarządzania urządzeniami, w tym możliwość dodawania, usuwania i zarządzania urządzeniami w konsoli administracyjnej oprogramowania oraz poprawność wykonywania instalacji, aktualizacji i usuwania oprogramowania. Wykonawca przetestuje, że konfiguracje mogą być efektywnie stosowane na wybranych urządzeniach.

K. Wykonawca przeprowadzi testy zdalnego zarządzania poprzez zdalne sterowanie komputerem oraz zdalne wsparcie ekranowe. Wykonawca w ramach tego zadania zweryfikuje dodatkowo czy można efektywnie udzielać pomocy technicznej użytkownikom poprzez konsolę oprogramowania.
L. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje na temat stanu infrastruktury IT oraz czy możliwość monitorowania wydajności urządzeń i systemów za pomocą narzędzi dostępnych w oprogramowaniu działa prawidłowo, zgodnie z założeniami prawidłowego działania oprogramowania.
M. Wykonawca przeprowadzi testy zabezpieczeń, weryfikując czy zastosowane zabezpieczenia, takie jak zasady bezpieczeństwa i ochrona antywirusowa, są skutecznie wdrażane na urządzeniach.
N. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.
O. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

9. Wdrożenie oprogramowania przeciwdziałającego wyciekowi danych.

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym pod kontrolą systemu Windows Server co najmniej w wersji 2016 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

A. Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.
B. Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.
C. Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.
D. Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.
E. Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.
F. Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.
G. Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.
H. Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.
I. Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.
J. Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:

- Numery kart kredytowych

- Numery IBAN
- Numery dowodów osobistych
- Polski numer paszportu
- Numer PESEL

K. Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.
L. Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.
M. Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.
N. Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.
O. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.
P. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.
Q. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

10. Wdrożenie klastra serwerów.

Krok 1: Planowanie i Przygotowanie:

- Określenie wymagań dotyczących infrastruktury, w tym sprzętu, sieci i przechowywania.
- Wybranie serwerów, które zostaną użyte jako węzły klastra. Upewnij się, że są one zgodne z wymaganiami wybranego oprogramowania.
- Skonfigurowanie łącza sieciowego i przestrzeni dyskowej, aby zapewnić odpowiednią przepustowość i pojemność.
- Zainstalowanie systemu operacyjnego na każdym węźle klastra.

Krok 2: Instalacja roli oprogramowania do wirtualizacji:

- Instalacja odpowiedniej roli za pomocą menedżera serwerów lub PowerShell.
- Konfiguracja ustawień sieciowych i przechowywania na węzłach klastra, tak aby były zgodne z wymaganiami projektu.

Krok 3: Konfiguracja klastra:

- Uruchomienie kreatora konfiguracji klastra w menedżerze serwerów na jednym z węzłów.
- Dodanie pozostałych węzłów klastra do konfiguracji.
- Konfiguracja ustawień klastra, takie jak nazwa klastra, adresy IP i konfiguracja przechowywania współdzielonego.

Krok 4: Konfiguracja wysokiej dostępności klastra:

- Włączenie funkcji wysokiej dostępności dla maszyn wirtualnych na klastrze.
- Konfiguracja ustawień zapasowych dla klastra, aby zapewnić ochronę przed awariami węzłów.

Krok 5: Tworzenie i Zarządzanie Maszynami Wirtualnymi:

- Utworzenie nowych maszyn wirtualnych na klastrze z wykorzystaniem oprogramowania do wirtualizacji.
- Konfiguracja ustawień maszyn wirtualnych, takich jak liczba procesorów, ilość pamięci i przypisywanie zasobów sieciowych.
- Zarządzanie maszynami wirtualnymi, monitorowanie ich wydajności i wykonywanie niezbędnych operacji konserwacyjnych jest kluczowe w zapewnieniu prawidłowo funkcjonującego środowiska wirtualnego uruchomionego w klastrze.

Krok 6: Testowanie i Monitorowanie:

- Testowanie działania klastra, w tym jego zdolność do migracji wirtualnej i przywracania po awariach.
- Konfiguracja narzędzi monitorujących, w celu śledzenia wydajności i dostępności klastra oraz maszyn wirtualnych.
- Regularnie przeglądanie logów i raportów, w celu szybkiego reagowania na ewentualne problemy.

11. Wdrożenie kontrolera domeny.

Etap 1: Analiza Wstępna i Planowanie Wdrożenia

1.1. Analiza Stanu Obecnego:

- Ocena istniejącej infrastruktury IT, w tym systemów operacyjnych, sieci, aplikacji i baz danych.
- Identyfikacja istniejących rozwiązań zarządzania tożsamościami i bezpieczeństwem oraz ich ewentualnych ograniczeń.

1.2. Wymagania Organizacyjne i Techniczne:

- Konsultacje z interesariuszami w celu zrozumienia potrzeb biznesowych i oczekiwań dotyczących infrastruktury IT.
- Identyfikacja wymagań dotyczących zarządzania tożsamościami użytkowników, zasobami sieciowymi i politykami bezpieczeństwa.

1.3. Opracowanie Planu Wdrożenia:

- Sporządzenie szczegółowego planu projektowego uwzględniającego harmonogram, zadania, zasoby i odpowiedzialności.
- Określenie struktury domen, schematu nazewnictwa i strategii replikacji dla środowiska Active Directory.

Etap 2: Instalacja i Konfiguracja Środowiska Active Directory

2.1. Instalacja Roli AD DS:

- Konfiguracja serwera Windows Server jako kontrolera domeny, włączając rolę Active Directory Domain Services.

2.2. Konfiguracja DNS:

- Ustawienie serwera DNS zgodnie z wymaganiami Active Directory.
- Konfiguracja strefy forward i reverse DNS dla domeny.

2.3. Tworzenie Dominy lub Integracja:

- Utworzenie nowej domeny Active Directory lub integracja z istniejącymi domenami w środowisku.

2.4. Konfiguracja Zasad Replikacji:

- Określenie i skonfigurowanie zasad replikacji między kontrolerami domeny w różnych lokalizacjach.

Etap 3: Strukturyzacja i Organizacja Domeny

3.1. Projektowanie Struktury Organizacyjnej:

- Tworzenie jednostek organizacyjnych (OU) odpowiadających strukturze organizacyjnej firmy.
- Utworzenie kont użytkowników, grup i zasobów oraz ich odpowiednie uporządkowanie w hierarchii.

3.2. Konfiguracja Polityk Grupowych (GPO):

- Ustanowienie zasad dostępu, konfiguracji użytkowników i komputerów za pomocą GPO.
- Implementacja polityk bezpieczeństwa dotyczących haseł, dostępu i innych ustawień

Etap 4: Zabezpieczenie Active Directory

4.1. Wdrożenie Zaawansowanych Mechanizmów Zabezpieczeń:

- Konfiguracja zasad kont haseł, polityk blokowania kont, kontroli dostępu.
- Implementacja szyfrowania komunikacji i audytu zdarzeń w AD.

4.2. Konfiguracja Środków Obronnych:

- Wdrożenie mechanizmów zabezpieczeń przed atakami, w tym monitorowanie logów, wykrywanie zagrożeń i zapobieganie atakom.

Etap 5: Walidacja i Optymalizacja Konfiguracji

5.1. Testowanie Funkcjonalności i Bezpieczeństwa:

- Przeprowadzenie testów weryfikujących działanie i bezpieczeństwo środowiska AD.
- Identyfikacja i rozwiązywanie ewentualnych problemów lub luk w zabezpieczeniach.

5.2. Optymalizacja Wydajności:

- Optymalizacja konfiguracji AD w celu zapewnienia efektywności i wydajności działania.
- Integracja z istniejącymi systemami i aplikacjami w celu zapewnienia spójności działań.

Etap 6: Dokumentacja Techniczna

6.1. Sporządzenie Dokumentacji:

- Przygotowanie szczegółowej dokumentacji technicznej, zawierającej opisy konfiguracji, ustawień polityk, procedur bezpieczeństwa i architektury systemu.
- Dokumentacja będzie służyć jako punkt odniesienia dla administratorów IT i personelu technicznego.

Cel Końcowy Usługi

Finalizacja usługi zapewni pełne wdrożenie systemu Active Directory, skonfigurowane zgodnie z najlepszymi praktykami branżowymi, gotowe do efektywnego zarządzania środowiskiem IT. System będzie przygotowany do zapewnienia wysokiego poziomu bezpieczeństwa, stabilności operacyjnej i skalowalności, odpowiadając na bieżące oraz przyszłe potrzeby organizacji.

12. Wdrożenie kluczy U2F.

1. Cel zamówienia

Celem zamówienia jest podniesienie poziomu bezpieczeństwa infrastruktury teleinformatycznej Zamawiającego poprzez wdrożenie silnego uwierzytelniania (MFA) w oparciu o klucze sprzętowe U2F. Realizacja obejmuje zaprojektowanie i wdrożenie hierarchicznej infrastruktury klucza publicznego (PKI), integrację z usługą katalogową Active Directory oraz konfigurację stacji końcowych.

2. Zakres prac (Etapy realizacji)

Etap 1: Analiza przedwdrożeniowa i Projekt

Wykonawca zobowiązany jest do przeprowadzenia audytu środowiska i przygotowania projektu technicznego.

- Analiza infrastruktury: Ocena obecnego stanu Active Directory, poziomu funkcjonalności domeny i lasu oraz usług DNS pod kątem wdrożenia PKI.
- Wymagania organizacyjne: Uzgodnienie z Zamawiającym polityk bezpieczeństwa dotyczących cyklu życia certyfikatów oraz procedur wydawania i unieważniania kluczy U2F.
- Projekt architektury PKI: Opracowanie schematu dwustopniowego urzędu certyfikacji (Offline Root CA oraz Enterprise Sub CA) zgodnie z najlepszymi praktykami bezpieczeństwa Microsoft.

Etap 2: Budowa i konfiguracja infrastruktury PKI

Zgodnie z wymaganiami technicznymi, Wykonawca przeprowadzi instalację ról serwerowych niezbędnych do obsługi logowania kartą inteligentną/kluczem U2F.

2.1. Główne Centrum Certyfikacji (Root CA):

- Instalacja systemu operacyjnego i przygotowanie dedykowanej maszyny (lub maszyny wirtualnej) dla roli Root CA.
- Instalacja i konfiguracja roli Active Directory Certificate Services (AD CS) w trybie Standalone Root CA.
- Wygenerowanie głównego certyfikatu Root CA o odpowiedniej długości klucza i algorytmie (min. RSA 4096-bit lub ECDSA).
- Konfiguracja punktów dystrybucji list CRL (CDP) oraz dostępu do informacji o urzędach (AIA).

2.2. Dystrybucja zaufania w domenie:

- Opublikowanie certyfikatu Root CA w kontenerze konfiguracji Active Directory.
- Konfiguracja GPO w celu automatycznej dystrybucji certyfikatu Root CA do magazynu „Zaufane główne urzędy certyfikacji” na wszystkich stacjach roboczych i serwerach w domenie.

2.3. Podrzędne Centrum Certyfikacji (Sub CA - Issuing CA):

- Instalacja i konfiguracja serwera w roli Enterprise Subordinate CA.
- Wygenerowanie żądania certyfikatu i podpisanie go przez Root CA.
- Konfiguracja usług sieciowych (Web Enrollment, OCSP - jeśli wymagane) dla obsługi żądań użytkowników.

Etap 3: Konfiguracja Active Directory i szablonów certyfikatów

Wykonawca dokona integracji infrastruktury PKI z mechanizmami uwierzytelniania domeny.

- Szablony certyfikatów: Utworzenie i konfiguracja dedykowanych szablonów certyfikatów (Certificate Templates) dla logowania kartą inteligentną/kluczem FIDO2, uwzględniając wymagania kluczy U2F.
- Uprawnienia: Nadanie odpowiednich uprawnień (Read, Enroll) dla grup użytkowników i komputerów upoważnionych do korzystania z kluczy.
- Konfiguracja Kontrolerów Domeny: Wystawienie i dystrybucja certyfikatów "Domain Controller Authentication" (lub Kerberos Authentication) dla wszystkich kontrolerów domeny, aby umożliwić obsługę logowania certyfikatem.
- Mapowanie certyfikatów: Konfiguracja usługi *name mapping* (jeśli wymagana) w celu poprawnego przypisywania certyfikatów z kluczy U2F do kont użytkowników w AD.

Etap 4: Wdrożenie polityk (GPO) i konfiguracja klientów

- Opracowanie i wdrożenie obiektów GPO wymuszających lub umożliwiających logowanie za pomocą klucza sprzętowego na stacjach roboczych.
- Wsparcie w konfiguracji stacji roboczych do obsługi minidriverów lub sterowników niezbędnych dla kluczy U2F (jeśli dotyczy).
- Wsparcie w konfiguracji wygaszacza ekranu i blokady stacji po wyjęciu klucza (opcjonalnie, zgodnie z ustaleniami z Etapu 1).

Etap 5: Testy i Walidacja

Wykonawca przeprowadzi szczegółowe testy wdrożonego rozwiązania w środowisku testowym, a następnie produkcyjnym.

- Testy propagacji: Weryfikacja, czy certyfikaty Root CA i Sub CA są poprawnie widoczne na stacjach końcowych.
- Testy logowania: Przeprowadzenie prób logowania do systemu Windows za pomocą klucza U2F na różnych typach stacji roboczych.
- Testy dostępu do zasobów: Weryfikacja dostępu do zasobów sieciowych (pliki, aplikacje intranetowe) po zalogowaniu kluczem, w celu potwierdzenia poprawnego działania Kerberos.
- Scenariusze awaryjne: Test zachowania systemu w przypadku niedostępności serwera Sub CA lub CRL (sprawdzenie *cache'owania* poświadczeń).

Etap 6: Dokumentacja i Szkolenia

- Dokumentacja powykonawcza: Dostarczenie dokumentacji technicznej zawierającej opis konfiguracji PKI, parametry szablonów certyfikatów, konfigurację GPO oraz procedury awaryjne (Backup/Restore CA).
- Instrukcja dla użytkownika: Opracowanie skróconej instrukcji dla użytkownika końcowego dotyczącej rejestracji i użycia klucza.
- Szkolenie administratorów: Przeprowadzenie warsztatu (min. 4 godziny) dla zespołu IT Zamawiającego obejmującego zarządzanie cyklem życia certyfikatów, obsługę konsoli PKI i rozwiązywanie problemów z logowaniem.

3. Wymagania dotyczące Wykonawcy

- Wykonawca zapewni wsparcie techniczne (gwarancję) na wdrożoną konfigurację przez okres 12 miesięcy od daty podpisu protokołu odbioru.

4. Terminy i Odbiór

- Odbiór prac nastąpi na podstawie protokołu zdawczo-odbiorczego po pomyślnym przeprowadzeniu testów akceptacyjnych opisanych w Etapie 5.

13. Wdrożenie oprogramowania do wykonywania kopii zapasowych.

1. Planowanie i Przygotowanie:

- Określenie wymagań dotyczących backupu i replikacji, w tym ilość danych do przechowywania, czas przywracania, dostępność i inne czynniki.

- Weryfikacja posiadania odpowiedniej ilości przestrzeni dyskowej i zasobów sieciowych do przechowywania kopii zapasowych.
- Pobranie niezbędnego oprogramowania do wykonywania kopii zapasowych i przeczytanie jego dokumentacji.

2. Instalacja i Konfiguracja:

- Uruchomienie instalatora wybranego oprogramowania do wykonywania kopii zapasowych na wybranym serwerze.
- Postępuj zgodnie z kreatorami instalacji, akceptując licencję, wybierając komponenty do zainstalowania i konfigurując ustawienia.
- Konfiguracja połączenia ze swoim środowiskiem wirtualizacji.

3. Konfiguracja Backupu:

- Konfiguracja planów backupu, określając harmonogramy, miejsca przechowywania i inne parametry.
- Wybranie, które maszyny wirtualne lub inne zasoby będą chronione za pomocą kopii zapasowych.
- Ustawienie retencji danych i polityki przechowywania, aby dostosować je do wymagań firmy.

4. Konfiguracja Replikacji (opcjonalnie):

- Konfiguracje odpowiedniego zadania replikacji, określając maszyny wirtualne źródłowe i docelowe, harmonogramy i inne parametry.
- Weryfikacja dostępności docelowego środowiska na przyjęcie replikowanych maszyn wirtualnych.

5. Testowanie i Wdrażanie:

- Przetestowanie planów backupu i replikacji, aby upewnić się, że są one zgodne z oczekiwaniami i spełniają wymagania czasu przywracania.
- Wdrożenie skonfigurowanych i przetestowanych planów na produkcji, monitorując ich wydajność i skuteczność.

6. Monitorowanie i Administracja:

- Regularne monitorowanie wykonywanych kopii zapasowych i replikacji, w celu weryfikacji ich poprawności i zgodności z planem.
- Weryfikacja raportów i dzienników zdarzeń oprogramowania do wykonywania kopii zapasowych, aby szybko reagować na jakiekolwiek problemy.

14. Segmentacja sieci IT/OT.

Usługa kompleksowej segmentacji sieci teleinformatycznej (IT/OT)

1. CEL ZAMÓWIENIA

Przedmiotem zamówienia jest przeprowadzenie kompleksowej segmentacji infrastruktury sieciowej Zamawiającego obejmującej środowiska IT oraz OT, w celu:

- zwiększenia poziomu bezpieczeństwa systemów informatycznych i przemysłowych,
- zapewnienia kontroli dostępu między strefami IT i OT,
- ograniczenia ryzyka propagacji zagrożeń (w tym ransomware) pomiędzy segmentami,
- spełnienia dobrych praktyk (m.in. ISA/IEC 62443, NIST SP 800-82),
- zapewnienia ciągłości działania systemów przemysłowych.

2. ZAKRES USŁUGI

2.1. Analiza infrastruktury sieciowej (IT/OT)

Wykonawca przeprowadzi szczegółową inwentaryzację i analizę obejmującą:

Środowisko IT:

- Identyfikację urządzeń aktywnych i pasywnych
- Analizę przepływów sieciowych i wzorców ruchu
- Ocenę aktualnego stanu segmentacji i mechanizmów bezpieczeństwa

- Pomiar przepustowości i wydajności kluczowych łączy

Środowisko OT:

- Identyfikację systemów przemysłowych (SCADA, DCS, PLC, HMI, RTU, systemy telemetryczne)
- Mapowanie komunikacji przemysłowej (np. Modbus, Profinet, OPC, DNP3)
- Identyfikację zależności między systemami OT a IT
- Ocenę istniejących mechanizmów izolacji (jeśli występują)
- Analizę wymagań dostępności i deterministyczności systemów OT

2.2. Klasyfikacja zasobów i analiza ryzyka (IT/OT)

Wykonawca dokona klasyfikacji zasobów oraz analizy ryzyka:

- Otrzymanie od Zamawiającego zidentyfikowanych i skategoryzowanych zasobów krytycznych
- Otrzymanie klasyfikacji zasobów wg metodyki CIA (poufność, integralność, dostępność)
- Klasyfikacja danych, systemów IT i OT według poziomów wrażliwości

Dodatkowo dla OT:

- Klasyfikacja systemów pod kątem krytyczności operacyjnej (bezpieczeństwo procesów, wpływ na produkcję)
- Analiza ryzyka dla systemów ICS (uwzględniająca zagrożenia specyficzne dla OT)
- Identyfikacja punktów styku IT/OT (tzw. conduits)

2.3. Projekt architektury segmentacji (IT/OT)

Wykonawca opracuje szczegółowy projekt segmentacji obejmujący:

Model segmentacji IT:

- Definicję stref bezpieczeństwa (minimum):
  - DMZ
  - sieć produkcyjna IT
  - sieć biurowa
  - sieć zarządzania
  - sieć gości
  - sieć IoT

Model segmentacji OT (zgodny z ISA/IEC 62443):

- Podział na poziomy (Purdue Model), w tym:
  - Level 0/1 – urządzenia polowe
  - Level 2 – sterowanie (PLC, HMI)
  - Level 3 – systemy operacyjne (SCADA/MES)
  - Level 3.5 – Industrial DMZ (IDMZ)
  - integracja z IT (Level 4/5)
- Definicja stref i kanałów komunikacyjnych (zones & conduits)
- Zaprojektowanie Industrial DMZ (IDMZ) pomiędzy IT i OT

Wspólne elementy:

- Polityki kontroli dostępu (IT/OT)
- Reguły firewall i ACL (w tym firewalle przemysłowe)
- Segmentacja logiczna (VLAN, VRF, mikrosegmentacja)
- Rekomendacje technologii (NGFW, NAC, IDS/IPS, rozwiązania OT-aware)
- Plan adresacji IP dla wszystkich segmentów
- Strategia mikrosegmentacji dla zasobów krytycznych (IT i OT)
- Mechanizmy monitoringu ruchu IT/OT

2.4. Wdrożenie i konfiguracja (IT/OT)

Wykonawca przeprowadzi wdrożenie zaprojektowanej segmentacji:

- Konfiguracja urządzeń sieciowych i bezpieczeństwa
- Wdrożenie polityk bezpieczeństwa i reguł filtracji ruchu

- Segmentacja ruchu IT/OT zgodnie z zasadą least privilege
- Implementacja IDMZ oraz separacji IT/OT
- Integracja z istniejącymi systemami zarządzania i monitoringu

Dla OT:

- Wdrożenie z uwzględnieniem ciągłości procesów przemysłowych
- Prace realizowane w oknach serwisowych lub trybie bezprzerwowym (jeśli wymagane)
- Minimalizacja wpływu na systemy sterowania i produkcję

2.5. Testowanie i weryfikacja (IT/OT)

Wykonawca przeprowadzi kompleksowe testy:

- Testy komunikacji między segmentami (IT i OT)
- Weryfikacja reguł filtracji i kontroli dostępu
- Testy izolacji między strefami (w tym IT ↔ OT)
- Walidacja poprawności działania systemów OT po segmentacji

Dodatkowo dla OT:

- Testy bezpieczeństwa komunikacji przemysłowej
- Weryfikacja braku wpływu na deterministykę i opóźnienia systemów sterowania
- Testy scenariuszy awaryjnych i redundancji

3. DODATKOWE WYMAGANIA (NOWA SEKCJA – REKOMENDOWANA)

- Zgodność z normami:
  - ISA/IEC 62443
  - NIST SP 800-82
  - ISO 27001 (dla IT)
- Uwzględnienie:
  - systemów legacy w OT
  - ograniczeń patchowania w OT
  - monitoringu pasywnego (np. NDR dla OT)
- Dokumentacja powdrożeniowa obejmująca:
  - mapę segmentacji IT/OT
  - listę reguł firewall
  - diagramy stref i przepływów
  - procedury zarządzania zmianą

4. REZULTATY USŁUGI

- Wdrożona segmentacja IT i OT
- Oddzielenie i kontrola komunikacji IT ↔ OT
- Zmniejszenie powierzchni ataku
- Zwiększona odporność na incydenty cyberbezpieczeństwa
- Pełna dokumentacja architektury

15. Wsparcie lokalne przy wdrożeniach.

W ramach wsparcia lokalnego przewiduje się realizację prac wdrożeniowych związanych z podłączeniem sprzętu informatycznego na warstwie fizycznej oraz instalacją oprogramowania. Prace te będą prowadzone w trybie hybrydowym – częściowo w siedzibie Zamawiającego, a częściowo zdalnie, przy wykorzystaniu połączenia z systemami Zamawiającego.

Wsparcie lokalne dotyczy wyłącznie czynności realizowanych na warstwie fizycznej, w szczególności podłączenia, montażu i uruchomienia sprzętu, i powinno być zapewnione przez minimum 3 dni robocze lub do momentu zakończenia podłączania całego sprzętu dostarczonego w ramach zamówienia – w zależności od tego, które z tych zdarzeń nastąpi wcześniej.

16. Dostawa i wdrożenie SIEM.

Zamawiający na potrzeby instalacji i wdrożenia udostępni infrastrukturę na serwerach zwirtualizowanych, wg. specyfikacji uzgodnionych z Wykonawcą. Czynności związane z wdrożeniem systemu będącego przedmiotem umowy będzie wykonywał Wykonawca. Instalacja systemu przez Wykonawcę odbywać się będzie z wykorzystaniem środków komunikacji elektronicznej. Wykonawca zobowiązuje się do dostarczenia kompleksowego oprogramowania typu Security Information and Event Management (SIEM) oraz EDR (Endpoint Detection and Response), które będzie spełniało poniższe wymagania funkcjonalne i techniczne.

1. Funkcjonalności systemu.

- Monitorowanie zdarzeń (logów) w trybie ciągłym.
- Zbieranie zdarzeń z serwerów wirtualnych, fizycznych, Active Directory, przełączników oraz innych urządzeń w infrastrukturze Zamawiającego.
- Agregacja i korelacja logów.
- Wykrywanie ataków typu brute force i innych złośliwych działań.
- Analiza logów w oparciu o wbudowane reguły bezpieczeństwa.
- Możliwość tworzenia własnych reguł korelacji.
- Konfigurowanie alertów o wysokim priorytecie w przypadku wykrycia podejrzanych zdarzeń.
- Panel do wyszukiwania i analizy zdarzeń.
- Możliwość integracji z innymi systemami bezpieczeństwa.
- Przechowywanie logów z kluczowych zasobów przez okres 24 miesięcy.
- Monitorowanie i ochrona punktów końcowych (np. komputerów, laptopów, serwerów).
- Wykrywanie i blokowanie złośliwego oprogramowania.
- Zapobieganie atakom typu ransomware.
- Automatyczne reagowanie na incydenty bezpieczeństwa.
- Dostęp do szczegółowych informacji o zdarzeniach na punktach końcowych.

1. Wdrożenie systemu.

   Wykonawca będzie odpowiedzialny za instalację i konfigurację oraz optymalizację środowiska systemu w infrastrukturze Zamawiającego oraz opiekę serwisową i wsparcie techniczne przez okres 30 dni.

3. Wykonawca przeprowadzi instruktaż stanowiskowy dla Administratorów (zarządzających systemem), co najmniej w n/w zakresie:

- Przedstawienie architektury systemu.
- Omówienie procedur obsługi administracyjnej systemu;
- Omówienie możliwości funkcjonalnych, zakresu dostępnych funkcji oraz ograniczeń systemu;
- Przekazanie informacji na temat konfiguracji i zarządzania systemem;
- Instruktaż stanowiskowy musi obejmować część teoretyczną i praktyczną.

Część 3 – Dostawa i wdrożenie systemu monitorowania sieci przemysłowej (OT)

1. Dostawa i wdrożenie systemu monitorowania sieci przemysłowej.

Przedmiotem zamówienia jest:

1. wdrożenie systemu monitorowania sieci przemysłowej służącego do monitorowania sieci przemysłowej, składającego się z sond sprzętowych oraz oprogramowania do zarządzania i analizy ruchu sieciowego (system IDS),
2. dostawa licencji oraz sond sprzętowych,
3. udzielenie wsparcia dla administratorów Zamawiającego,
4. organizacja i realizacja szkoleń dla administratorów Zamawiającego.

1. Funkcjonalność i specyfikacja.

1. Oprogramowanie musi być w 100% niezależne od dostawców automatyki oraz zawierać wsparcie dla urządzeń przemysłowych wykorzystywanych przez Zamawiającego.
2. Przetwarzane dane w systemie nie mogą być przesyłane poza infrastrukturę Zamawiającego.
3. Całość rozwiązania, tj. system IDS wraz z silnikiem analitycznym oraz wszystkie sondy systemowe – zarówno sondy fizyczne, jak i wirtualne – muszą pochodzić od jednego producenta. Producent systemu IDS musi być jednocześnie producentem sond, a rozwiązanie powinno stanowić spójny, zintegrowany produkt, zaprojektowany i rozwijany jako całość.
4. System IDS musi posiadać interfejs graficzny min. w języku polskim i angielskim, który ma być dostępny przez przeglądarkę internetową. Dostęp do interfejsu musi być zabezpieczony protokołem szyfrowania TLS. Zamawiający musi mieć możliwość importu własnego certyfikatu.
5. System IDS nie może ograniczać wielkości przestrzeni dla przechowywanych logów i archiwalnego ruchu sieciowego. Musi umożliwiać ustawienie czasu przechowywania informacji o anomaliach i archiwum ruchu sieciowego.
6. System IDS musi umożliwiać konfigurowanie poziomów dostępu dla użytkowników.
7. System IDS musi umożliwiać aktualizację bazy danych, oprogramowania, podatności w trybie offline.
8. System IDS musi umożliwiać synchronizację czasu przy użyciu protokołu NTP.
9. System IDS musi zapewniać:
   a. pasywne monitorowanie sieci przemysłowej Zamawiającego,
   b. automatyczne tworzenie graficznej mapy rządzeń min.: PLC, HMI, RTU, IED, stacje operatorskie SCADA, wraz z możliwością filtrowania po urządzeniach, protokołach, portach.
   c. szczegółową inwentaryzację urządzeń,
   d. automatyczne odzwierciedlenie połączeń komunikacyjnych,
   e. informowanie o zmianach min.: utrata urządzenia, pojawienie się nowego urządzenia, zmiana komunikacji,
   f. wykrywanie podatności urządzeń i oprogramowania w sieci przemysłowej wykorzystując powszechnie znane podatności CVE na podstawie bazy MITRE i/lub NIST,
   g. budowę mapy topologii sieci przemysłowej wraz z informacją o sposobie komunikacji,
   h. obsługę LLDP, CDP, CIP, SSDP.
10. System IDS musi posiadać mechanizmy alarmujące, które będą działać w trakcie budowania modelu sieci przemysłowej w celu wykrywania zagrożeń w procesie nauki.
11. System IDS musi posiadać zaimplementowane mechanizmy wsparcia i rozumienia komend dla głównych protokołów OT i IT.
12. System IDS musi mieć możliwość dodawania nowego typu protokołu.
13. System IDS musi działać na kopii ruchu oraz musi być w 100% pasywny. Nie może generować żadnego dodatkowego ruchu w monitorowanej sieci ani mieć wpływu na komunikację w sieci przemysłowej.

14. Kopia ruchu sieciowego musi się odbywać na bazie kopii dostarczanej ze SPAN/mirror portów przełączników, lub w trybie „pass-through / in-line" przy wpięciu do linii.
15. System IDS musi umożliwiać analizę ruchu sieciowego: Packet Capture (pliki PCAP).
16. System IDS musi monitorować i klasyfikować cyberincydenty oraz zdarzenia operacyjne.
17. System IDS powinno być oparte na technologii uczenia maszynowego i umożliwiać modelowanie sieci w czasie maksymalnie 5 dni.
18. System IDS musi umożliwiać generowanie potencjalnych wektorów ataku, bazując na analizie ruchu sieciowego oraz rekomendować sposoby zwiększenia bezpieczeństwa.
19. System IDS musi umożliwiać integrację z systemami typu SIEM (np. poprzez Syslog)
20. System IDS musi zapewniać w trybie ciągłym monitoring online sieci przemysłowej z alarmowaniem w czasie rzeczywistym wykorzystując metody /techniki behawioralne.
21. System IDS musi umożliwiać sortowanie alarmów zgodnie z min.: stopniem, ważności, typie, czasie wystąpienia.
22. System IDS musi umożliwiać wysyłanie wiadomości e-mail w razie wystąpienia alarmów.
23. System IDS musi gromadzić informacje o zaistniałych alarmach min.: opis techniczny alarmu, stopień oraz ważność, rekomendacje, plik z ruchem sieciowym.
24. System IDS musi pozwalać na głęboką analizę pakietów (DPI) dla min. protokołów: MODBUS RTU, DNP3.
25. System IDS musi wspierać analizę ML/AI dla protokołów min.: Profinet, Profibus, Powerlink, Modbus RTU, Modbus TCP/IP, TASE2, DNP3, OPC UA, OPC, EtherCAT, GE EGD, EtherNet/IP, BUSZ, CIP, IEC- 61850, SRTP, BACnet.
26. System IDS musi identyfikować anomalie w ruchu sieciowym oraz incydenty w tej sieci.
27. System IDS musi obsługiwać incydenty w zakresie min.: wykrywania, rejestrowania, analizy, ustawienia priorytetu, ustawienia statusu, podejmowanie działań naprawczych, rekomendacji.
28. System IDS musi wykrywać zagrożenia min.:

a. malware/"zero-day",
b. atak DOS/DDOS,
c. atak typu ATP,
d. spyware, skanowanie sieci,
e. zagrożenia Man-in-the-Middle,
f. anomalie min.: rozpoznawanie częstotliwości komunikacji urządzeń, niezgodność, komend, skanowanie PLC, skanowanie urządzeń sterujących,
g. wykrywanie połączeń do innej sieci LAN/internet,
h. wykrywanie połączeń do kluczowych urządzeń wraz z prezentacją sposobu komunikacji.

29. System IDS musi pozwalać na generowanie raportów w zakresie analizy danych.
30. System IDS musi umożliwiać instalację sond programowych w środowisku Linux.
31. System IDS musi umożliwiać szyfrowaną komunikację z sondami sprzętowymi.
32. System IDS musi umożliwiać zapamiętywanie widoków graficznych skonfigurowanych przez użytkownika.
33. System IDS musi zapewniać funkcjonalność budowy oraz utrzymania Software Bill of Materials (SBOM) dla monitorowanej infrastruktury przemysłowej, realizowaną w sposób pasywny, bez ingerencji w pracę urządzeń końcowych.
34. System IDS musi mieć możliwość ukrywania urządzeń typu MULTICAST/BORADCAST.
35. System IDS musi mieć możliwość wykrywania producenta urządzenia min. pod adresie MAC.
36. System IDS musi umożliwiać eksport listy urządzeń do pliku CSV i/lub PDF z podziałem na podsieć.
37. System IDS musi umożliwiać eksport protokołów do pliku CSV i/lub PDF z informacją w której podsieci zostały one wykryte.
38. System IDS musi mieć możliwość eksportu co najmniej do pliku PCAP wybranych pakietów.
39. System IDS musi mieć możliwość zdalnej zmiany konfiguracji oraz firmware sond sprzętowych.
40. Sondy sprzętowe muszą posiadać możliwość przechowywania danych na karcie pamięci w formie zaszyfrowanej

min. AES128.

41. Sonda sprzętowa musi mieć możliwość instalacji na szynie DIN.
42. Sonda sprzętowa musi być zasilana napięciem 24 VDC z podtrzymaniem bateryjnym do 30 minut przy zaniku zasilania z sieci.
43. Sonda sprzętowa musi wspierać: DHCP, stały adres IP.
44. Sonda sprzętowa musi być zabezpieczona przed ingerencją tzn.: dane muszą zostać skasowane przy próbie odczytu pamięci FLASH.
45. Sonda sprzętowa musi generować alarm w systemie IDS podczas próby otwarcia obudowy.
46. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS485.
47. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS422.
48. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący RS232.
49. Sonda sprzętowa musi posiadać pasywny interfejs monitorujący CAN.
50. Sonda sprzętowa musi posiadać min. jeden interfejs monitorujący RJ45 10/100Mbps pracujący w trybie Span-port. Interfejs monitorujący RJ45 nie może identyfikować się w sieci poprzez adres MAC oraz musi być pozbawiony funkcji Tx.
51. Sonda sprzętowa musi umożliwiać przekazywanie do systemu IDS wskazaną część ruchu sieciowego min.: dla wybranych urządzeń logicznych, protokołu.
52. Sonda sprzętowa musi umożliwiać przekazywać do systemu IDS strumień sieciowy w formacie IPFIX.

2. Dostawa, wdrożenie.

1. Wykonawca dostarczy:

a. sondy sprzętowe w liczbie 3 szt. do monitorowania sieci przemysłowej,
b. licencję wieczystą na system IDS dla nielimitowanej liczby monitorowanych urządzeń,
c. usługi wsparcia serwisowego producenta systemu IDS na okres nie przekraczając 31.12.2026 r.
serwis producenta systemu IDS ma obejmować:

- Dostęp do dokumentacji technicznej i instrukcji systemu IDS w języku polskim.
- Dostęp do nowych wersji systemu IDS.
- Dostęp do aktualizacji i poprawek systemu IDS.
- Dostęp do aktualizacji oprogramowania sond sprzętowych.
- Wymianę uszkodzonych sond sprzętowych w razie awarii.
- Przekazanie danych kontaktowych do działu technicznego producenta systemu IDS.
- Wsparcie administratorów Zamawiającego w zakresie obsługi systemu IDS podczas wdrożenia i późniejszej eksploatacji.
- Wsparcie administratorów Zamawiającego przy identyfikacji problemów a także ich rozwiązywaniu lub zastosowaniu obejścia.

2. Wykonawca zainstaluje i zalicencjonuje oraz skonfiguruje system IDS w środowisku serwerowym wskazanym przez Zamawiającego.
3. Licencje systemowe oraz sprzęt serwerowy zapewni Zamawiający.
4. Wykonawca przeprowadzi instalację sond sprzętowych w miejscach wskazanych przez Zamawiającego. Miejsce w szafach zapewni Zamawiający a Wykonawca wykona wszystkie niezbędne połączenia pomiędzy dostarczonym sprzętem a istniejącą infrastrukturą oraz zapewni wymagane okablowanie. Instalacja sond sprzętowych nie może powodować przerw działania sieci ani wprowadzać zakłóceń do sieci.
5. Wykonawca przeprowadzi pełną konfigurację i wdrożenia systemu u Zamawiającego (konfiguracja serwera, oprogramowania, konfiguracja switchy itp.), zapewniając pełną funkcjonalność i sprawność systemu pod nadzorem Zamawiającego.
6. Wykonawca przekaże Zamawiającemu wszelkie hasła, użyte w oprogramowaniu wraz z opisem ich funkcji i uprawnień w systemie.

7. Dla całego powyższego zakresu dot. instalacji, konfiguracji i parametryzacji Wykonawca przeprowadzi testy sprawdzające prawidłowość jego wykonania i działania.
8. Wszystkie powyższe prace mają być zrealizowane w siedzibie i pod nadzorem Zamawiającego.
9. Wykonawca przeprowadzi szkolenie dla administratorów Zamawiającego z konfiguracji i administracji systemem IDS. Zamawiający dopuszcza realizację szkolenia zdalnie. Termin szkolenia zostanie uzgodniony w późniejszym terminie pomiędzy Zamawiającym a Wykonawcą.
10. Wykonawca przygotuje dokumentację powykonawczą opisującą wszystkie prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni kalendarzowych od dnia zrealizowania całego powyższego zakresu. Zakończenie wdrożenia i jego odbiór nastąpi po odebraniu dokumentacji powykonawczej.