

*Załącznik nr 1 do SWZ - postępowanie SSE/2/3.1/KOP/2026*

## **OPIS PRZEDMIOTU ZAMÓWIENIA**

**“Działania zwiększające poziom cyberbezpieczeństwa szpitala”**

## Spis treści

Spis treści.....	2
1. Część 1 - Zakup i dostawa urządzeń sieciowych .....	3
1.1. Zakres dostawy.....	3
2. Część 2 - Przedłużenie licencji użytkownika związanych z cyberbezpieczeństwem .....	8
2.1. Oprogramowanie antywirusowe klasy XDR .....	8
3. Część 3 - Wymiana stacji roboczych użytkowników .....	25
3.1. Wymagania.....	25
4. Część 4 - Wdrożenie wirtualnych stanowisk pracy .....	42
4.1. Zakres wdrożenia .....	42

## 1. Część 1 - Zakup i dostawa urządzeń sieciowych

Przedmiotem zamówienia jest zakup i dostawa urządzeń sieciowych w postaci przełączników dostępowych 8p (ilość: 10 szt.) w celu poprawienia bezpieczeństwa i wydajność infrastruktury IT.

W ramach zamówienia zostanie zapewniona instalacja, konfiguracja, uruchomienie nowych urządzeń aktywnych, ich podłączenie w infrastrukturze Zamawiającego oraz testy powdrożeniowe.

### 1.1. Zakres dostawy

W ramach realizacji zamówienia Wykonawca zobowiązany jest do:

- Dostarczenia **10 szt.** (słownie: dziesięciu) **przełączników dostępowych 8p** z wyszczególnioną poniżej przez Zamawiającego specyfikacją techniczną.
- Instalacji i konfiguracji przełączników - przypisanie adresów IP, konfiguracja VLAN, interfejsów w trybie trunk lub równoważnym w zakresie tryb pracy portu przełącznika, routingu statycznego/dynamicznego, wykonanie integracji z kontrolerami i punktami dostępowymi, zapewnienie odpowiedniego routingu, priorytetyzacji ruchu i obsługi VLAN.
- Uruchomienia, podłączenia w infrastrukturze Zamawiającego i testów powdrożeniowych – weryfikacja poprawności działania redundancji, synchronizacji kontrolerów oraz ich zdolności do przejęcia obsługi w przypadku awarii, w tym weryfikacja zasięgu i przepustowości sieci WiFi, przepustowości i stabilności przełączników oraz działania mechanizmów bezpieczeństwa,
- Montażu urządzeń w szafach Rack w wraz z podłączeniem do systemu zasilania i istniejącej infrastruktury sieciowej.
- Ustawienia interfejsów sieciowych, konfiguracji routingu statycznego i/lub dynamicznego, VLAN oraz polityk dostępowych.
- Uruchomienia mechanizmów IPS, ochrony przed złośliwym oprogramowaniem (Advanced Malware Protection), kontroli aplikacji, filtrowania URL/DNS, ochrony poczty (antyspam) oraz systemu filtrowania treści.
- Włączenie do centralnego systemu monitoringu i logowania, integracja z usługami katalogowymi (AD/RADIUS/LDAP), wdrożenie polityk QoS oraz reguł bezpieczeństwa.
- Przeprowadzenia testów powdrożeniowych w tym do weryfikacja poprawności konfiguracji, skuteczności działania usług ochronnych, przepustowości, stabilności oraz prawidłowego logowania zdarzeń bezpieczeństwa.
- Przygotowania i przekazania dokumentacji powdrożeniowej zawierającej opis wdrożonej konfiguracji, uruchomionych funkcji bezpieczeństwa oraz procedur odtworzeniowych.

W trakcie realizacji prac i dostaw wchodzących w zakres przedmiotu zamówienia Wykonawca będzie zobowiązany do ścisłej współpracy z Zamawiającym, a w szczególności będzie zobowiązany do uzgadniania prowadzonych prac z wyznaczonym koordynatorem Zamawiającego, który będzie nadzorował realizację umowy, w szczególności w zakresie zgodności prac i dostaw z istniejącą u Zamawiającego architekturą i specyfikacją techniczną, wymaganiami bezpieczeństwa i obowiązującą polityką organizacyjną.

#### Przełącznik dostępowy 8p – ilość: 10 szt.

	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. Przełącznik musi zawierać system operacyjny (firmware) dostarczony przez producenta urządzenia.
--	--

1.	<p>Wymagane parametry fizyczne:</p> <ul style="list-style-type: none"> <li>a) możliwość montażu w stelażu/szafie 19"</li> <li>b) wysokość maksymalna 1U</li> <li>c) minimum jeden wewnętrzny zasilacz 230V AC</li> <li>d) zakres temperatur pracy ciągłej co najmniej od -5 °C do +50 °C</li> <li>e) zakres wilgotności pracy co najmniej 5% - 95%</li> <li>f) głębokość urządzenia maksymalnie 24 cm (z racji ograniczonego miejsca w szafach teleinformatycznych Zamawiający nie dopuszcza urządzenia o większej głębokości niż 24 cm)</li> </ul>
2.	<p>Przetątnik musi posiadać minimum:</p> <ul style="list-style-type: none"> <li>a) 8 portów 10/100/1000BASE-T</li> <li>b) 4 porty 1GE SFP z obsługą modułów 1G-SX, 1G-LX</li> <li>c) Port konsoli RS232/RJ45</li> <li>d) Z racji ograniczonego miejsca w szafach teleinformatycznych nie ma fizycznego dostępu do „tyłu” urządzenia, dlatego wszystkie powyższe porty muszą być dostępne od frontu urządzenia</li> </ul>
3.	Maksymalny pobór mocy przez przetątnik: 22W
4.	Układ przetątniający o wydajności min. 24 Gbps
5.	Obsługa min. 32 000 adresów MAC
6.	Wbudowana pamięć RAM min. 2GB
7.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 1GB
8.	Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
9.	Możliwość skonfigurowania min. 1023 interfejsów vlan interface SVI działających równocześnie
10.	Obsługa ramek jumbo o wielkości min. 9200 bajtów
11.	Obsługa mechanizmów ERPS: G.8032 v1 G.8032 v2
12.	Obsługa protokołu BFD
13.	<p>Obsługa protokołu LACP</p> <p>Możliwość utworzenia min. 64 grup LAG (ang. link aggregation groups)</p> <p>Możliwość dodania 8 portów do grupy LAG</p>
14.	Obsługa protokołu HSRP IPv4 i IPv6 lub VRRP IPv4 i IPv6
15.	<p>Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP). Wymagane wsparcie dla min. 63 instancji protokołu MSTP. Wsparcie dla mechanizmu PVST lub równoważnego (innego niż wymagany standard STP/RSTP/MSTP)</p>

16.	Obsługa mechanizmu wykrywania jednokierunkowych połączeń Ethernet (unidirectional link detection) z możliwością automatycznej reakcji ochronnej
17.	Obsługa protokołu pozwalającego na centralne zarządzanie konfiguracją vlanów w sieci (VTP lub odpowiednik)
18.	Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
19.	Obsługa min. 4 000 tras dla routingu IPv4
20.	Obsługa min. 1 000 tras dla routingu IPv6
21.	Obsługa protokołów związanych z obsługą ruchu typu multicast: <ul style="list-style-type: none"> <li>a) IGMP v1, v2 i v3</li> <li>b) IGMP Snooping v1, v2 i v3</li> <li>c) PIM-SM, PIM-DM, PIM-SSM</li> </ul>
22.	Minimalny rozmiar tablicy ARP 2 048 wpisów
23.	Obsługa wirtualnych tablic routingu-forwardingu (VRF) minimum 60
24.	Obsługa protokołów LLDP i LLDP-MED
25.	Przetątnik musi obsługiwać mechanizm Energy Efficient Ethernet zgodny z IEEE 802.3az, zapewniający redukcję zużycia energii na nieaktywnych portach
26.	Przetątnik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
27.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: <ul style="list-style-type: none"> <li>a) min. 4 poziomy dostęp administracyjny poprzez konsolę</li> <li>b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydzielenia VLANu oraz dynamicznego przypisania listy ACL</li> <li>c) obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 2000 reguł ACL</li> <li>d) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC</li> <li>e) zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 i SSHv2</li> <li>f) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP</li> <li>g) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard</li> <li>h) obsługa mechanizmów związanych z ochroną protokołu STP: BPDU Protection, Root Protection, Loop Protection</li> <li>i) możliwość synchronizacji czasu zgodnie z NTP IPv4 i IPv6</li> <li>j) możliwość uwierzytelnienia wielu użytkowników na jednym porcie z możliwością przydzielenia różnych VLANów dla każdego użytkownika z osobna</li> </ul>
28.	Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:

	<ul style="list-style-type: none"> <li>• klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP</li> <li>• wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR</li> </ul>
29.	<p>Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania</p>
30.	<p>Wymagane opcje zarządzania:</p> <ol style="list-style-type: none"> <li>a) możliwość lokalnej obserwacji ruchu na określonym porcie</li> <li>b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)</li> <li>c) możliwość zarządzania urządzeniem z wykorzystaniem protokołu Netconf/Yang lub RESTCONF</li> <li>d) wsparcie dla skryptów Python uruchamianych na urządzeniu</li> <li>e) wsparcie dla RMON</li> </ol>
31.	<p>Przetącznik musi mieć opcję szybkiego przywrócenie konfiguracji do poprzedniej wersji (tzw. funkcjonalność rollback). Przywrócenie konfiguracji do poprzedniej wersji nie może wymagać restartu urządzenia (całego bądź częściowego) bądź ręcznego odwoływania konfiguracji. Administrator systemu musi mieć możliwość utworzenia znacznika/etykiety dla danej konfiguracji tak, aby podczas wykonywania procesu przywrócenia można było wskazać ustawiony wcześniej znacznik/etyketę jako punkt, do którego ma zostać przywrócona konfiguracja.</p>
32.	<p>Wraz z urządzeniami muszą zostać dostarczone:</p> <ol style="list-style-type: none"> <li>a) pełna dokumentacja w języku polskim lub angielskim. Zamawiający również zaakceptuje udzielenie dostępu do dokumentacji umieszczonej w zasobach producenta</li> <li>b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana</li> </ol>
33.	<p>Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 12 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy</p>

34.	<p>Oferowane urządzenia muszą być oryginalne, wolne od wad prawnych, dopuszczone do obrotu na terenie UE oraz objęte gwarancją obowiązująca na terytorium RP. Korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.</p> <p>Wykonawca zobowiązany jest zapewnić realizację gwarancji producenta na terytorium Rzeczypospolitej Polskiej, bez dodatkowych kosztów dla Zamawiającego.</p>
35.	<p>Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń</p>
36.	<p>Zamawiający wymaga, aby przetłaczarki posiadały 36-miesięczny serwis gwarancyjny świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).</p> <p>W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.</p>
37.	<p>Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta.</p>
38.	<p>Zamówienie będzie zgodne z zasadą DNSH „niewyrządzania znaczącej szkody środowisku” (DNSH – „do no significant harm”) w rozumieniu art. 17 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2020/852 z dnia 18 czerwca 2020 r. w sprawie ustanowienia ram ułatwiających zrównoważone inwestycje, zmieniającego rozporządzenie (UE) 2019/2088 (Dz. U. UE. L. z 2020 r. Nr 198, str.13 z późn. zm.), czego potwierdzeniem będzie m.in.:</p> <ul style="list-style-type: none"> <li>a) w odniesieniu do zasady: Łagodzenie zmian klimatu           <ul style="list-style-type: none"> <li>- przetłaczarki nie generują wysokiego zużycia energii m.in. dzięki inteligentnemu zarządzaniu PoE np. automatycznemu wyłączeniu nieaktywnych portów</li> </ul> </li> <li>b) odniesieniu do zasady: Przejście na gospodarkę o obiegu zamkniętym:           <ul style="list-style-type: none"> <li>- konstrukcja przetłaczarek umożliwia łatwą konserwację, wymianę i naprawę zamiast ich całkowitej wymiany</li> <li>- przetłaczarki zbudowane z elementów wielokrotnego użytku, zapobiegając w ten sposób ograniczeniu powstawaniu odpadów</li> <li>- dostawa zostanie zrealizowana przy jak najmniejszej liczbie opakowań w celu ograniczenia ilości odpadów</li> </ul> </li> </ul> <p>w trakcie instalacji punktów dostępu oraz przetłaczarek zapewnione zostaną rozwiązania ograniczające ryzyko powstania nadmiernej liczby odpadów, w tym niepodlegających recyklingowi</p>

## 2. Część 2 - Przedłużenie licencji użytkownika związanych z cyberbezpieczeństwem

Przedmiotem zamówienia jest dostawa licencji dla zintegrowanego rozwiązania podnoszącego poziom bezpieczeństwa teleinformatycznego Zamawiającego. W ramach realizacji zamówienia zostanie zapewnione wdrożenie oraz aktywacja licencji. Celem realizacji zamówienia jest zapewnienie zaawansowanej ochrony przed zagrożeniami pochodzącymi z cyberataków zgodnie z obowiązującymi standardami bezpieczeństwa oraz wymaganiami Zamawiającego.

Zamawiający pracuje na następujących systemach:

- a) Microsoft Windows Server 2019
- b) Microsoft Windows Server 2022
- c) Microsoft Windows 10 Professional
- d) Microsoft Windows 11 Professional
- e) Linux Debian 11.x, 12.x, 13.x
- f) Linux Oracle 8.x, 9.
- g) Linux SUSE SLES 15.x, 16.x
- h) Linux Ubuntu Server 22.04.x LTS, 24.04.x LTS
- i) macOS 15.x, 26.x
- j) Android 14.x, 15.x
- k) iOS 18.x, 26.x

W zakres zamówienia wchodzi:

**System bezpieczeństwa klasy XDR** – odpowiedzialny za aktywną i wielowarstwową ochronę stacji roboczych, serwerów i urządzeń mobilnych przed oprogramowaniem złośliwym, exploitami, zagrożeniami typu APT oraz nieautoryzowaną aktywnością, z wykorzystaniem mechanizmów analityki zagrożeń i korelacji zdarzeń (ilość: **385 licencji**).

Na okres od 15.06.2026 do 31.05.2029, bez ograniczeń terytorialnych.

Dostarczane rozwiązanie musi:

- być zgodne z wymaganiami technicznymi opisanymi w podrozdziale 2.1,
- zapewniać centralne zarządzanie i pełną kontrolę administracyjną,
- gwarantować wysoką dostępność oraz skalowalność,
- wspierać obowiązujące standardy bezpieczeństwa i protokoły szyfrowania,
- pochodzić z autoryzowanych kanałów producenta i obejmować wsparcie techniczne.

### 2.1. Oprogramowanie antywirusowe klasy XDR

Zamawiający wymaga rozszerzenia obecnie używanego oprogramowania Cortex XDR Pro for 1 endpoint + Host Insights add-on for Cortex XDR + Extended Threat Hunting w ilości **385 licencji** lub dostarczenia rozwiązania równoważnego, które zapewnia funkcjonalności nie gorsze niż oferowane przez wskazane powyżej oprogramowanie, zgodnie z poniżej określonymi wymaganiami:

Opis techniczny
-----------------



1.	<p>Opis oprogramowania antywirusowego klasy EDR/XDR – główne założenia.</p> <ul style="list-style-type: none"> <li>a) aktywna ochrona endpointów (stacji końcowych i serwerów) przed działaniem złośliwego oprogramowania i innych technik stosowanych przez cyberprzestępców</li> <li>b) detekcja i triage'u zagrożeń z kategorii APT</li> <li>c) odpowiedź na wykryte zdarzenie</li> <li>d) realizacja threat hunting</li> </ul>
2.	System bezpieczeństwa EDR/XDR (dalej: system) musi być dostarczony w formie SaaS.
3.	Dokumentacja systemu musi być publikowana przez producenta na jego stronie internetowej co najmniej w języku angielskim, traktowanym jako język podstawowy w środowisku informatycznym.
4.	<p>System musi obsługiwać następujący rodzaj endpointów, używany obecnie u Zamawiającego w tym:</p> <ul style="list-style-type: none"> <li>a) stacje robocze windows 10/11 (w tym VDI)</li> <li>b) stacje robocze macOS</li> <li>c) serwery Linux</li> <li>d) serwery Microsoft Server</li> <li>e) urządzenia mobilne z Android</li> <li>f) urządzenia mobilne z iOS</li> </ul>
5.	System musi przechowywać informacje o alarmach i incydentach co najmniej przez 180 dni.
6.	System musi przechowywać szczegółowe dane telemetryczne z endpointów zabezpieczonych agentem przez co najmniej 30 dni.
7.	System musi szyfrować dane w trakcie transmisji i w trakcie przechowywania za pomocą protokołów i algorytmów kryptograficznych uznanych powszechnie za bezpieczne. Dane w trakcie przechowywania muszą być szyfrowane algorytmem AES-256.
8.	<p>System wg ewaluacji MITRE Engenuity: Mitre Attack (rok 2023) musi spełniać kryteria w następujących kategoriach:</p> <ul style="list-style-type: none"> <li>a) detekcji w oparciu o techniki (Technique Level Detections) - posiadać skuteczność na poziomie minimum 93%</li> <li>b) analityki zagrożeń (Analytics Detections/Coverage) - posiadać skuteczność na poziomie minimum 97%</li> </ul>
9.	System musi umożliwiać zarządzania przez pojedynczy webowy interfejs graficzny z wykorzystaniem graficznej przeglądarki internetowej oraz przez REST API. Oba dostępne po https (co najmniej TLS 1.2). Nie dopuszcza się, aby webowy interfejs graficzny korzystał z technologii flash, silverlight lub java.
10.	Wszystkie składniki systemu muszą być konfigurowalne i zarządzane przez jeden spójny interfejs. Nie dopuszcza się, aby składniki systemu posiadały oddzielne pulpity/konsole do zarządzania konkretnymi funkcjami bezpieczeństwa, a dostęp do nich realizowany jest przez pojedyncze logowanie (Single Sign-On).

11.	Wymagana jest ocena na poziomie min „A+” dla wszystkich serwisów, z których korzysta oferowane rozwiązanie. Ocena będzie weryfikowana przy pomocy ogólnodostępnego narzędzia <a href="https://www.ssllabs.com">https://www.ssllabs.com</a>
12.	System musi posiadać możliwość ograniczenia logowania do systemu tylko ze wskazanych publicznych adresów IP.
13.	System musi umożliwiać integrację z zewnętrznym katalogiem użytkowników z wykorzystaniem protokołu SAML 2.0 (z obsługą dowolnego dostawcy tożsamości zgodnego z SAML 2.0), a także posiadać możliwość definiowania lokalnych użytkowników, których logowanie jest zabezpieczone hasłem oraz dodatkowym czynnikiem uwierzytelniającym w formie tokenu. System, jako dodatkową metodę uwierzytelniania, musi wspierać co najmniej tokeny w formie jednorazowych kodów generowanych w aplikacji mobilnej, zgodnie z algorytmem jednorazowych haseł opartym na czasie (Time-based One-Time Password – TOTP), zgodnym z RFC 6238. Wymaga się wsparcia dla aplikacji mobilnych realizujących mechanizm TOTP, dostępnych na platformach Android oraz iOS.
14.	System dla lokalnych kont podczas tworzenia haseł dla kont administracyjnych musi żądać stosowania się do przyjętej polityki, która wymaga ustawienia hasła spełniającego następujące kryteria: co najmniej 11 znaków, musi zawierać małe i duże litery łacińskie, cyfry i znaki specjalne.
15.	System musi umożliwiać przypisywanie użytkowników do grup użytkowników. Dodatkowo w przypadku użytkowników uwierzytelnionych via SAML 2.0 musi istnieć możliwość zmapowania grup SAML do lokalnie zdefiniowanych grup.
16.	Każdy użytkownik systemu (administrator, operator, analityk) muszą posiadać indywidualne konta pozwalające na jego jednoznaczną identyfikację
17.	System musi umożliwiać określenie zakresu dostępu z wykorzystaniem ról i ich przypisanie do użytkownika lub do grupy użytkowników. Rola musi definiować dostęp do określonego obszaru administracyjnego systemu, jego rodzaju (tylko do odczytu, pełen dostęp) oraz jego zakresu (wszystkie lub wybrane endpointy).
18.	System w ramach roli musi umożliwiać określenie dostępu do co najmniej następujących obszarów: <ol style="list-style-type: none"> <li>Ustawienia systemu</li> <li>Zarządzanie endpointami</li> <li>Zarządzanie politykami</li> <li>Zarządzanie regułami detekcyjnymi</li> <li>Zarządzania wykluczeniami</li> <li>Zarządzanie incydentami</li> <li>Uruchamianie odpowiedzi na incydent</li> <li>Nawiązywanie połączenia do linii poleceń</li> <li>Uruchamianie skryptów w języku Python</li> <li>Zarządzanie kwerendami do danych</li> <li>Zarządzanie raportami</li> </ol>

	l) Zarządzenie dashboardami/kokpitami
19.	System musi posiadać możliwość definiowania własnych dopasowanych do potrzeb ról.
20.	System musi posiadać zestaw predefiniowanych dashboardów informujących co najmniej: <ul style="list-style-type: none"> <li>a) O liczbie i powadze incydentów</li> <li>b) O liczbie incydentów przypisanych do analityków</li> <li>c) O endpointach z największą liczbą incydentów</li> <li>d) O liczbie agentów z rozbiem na wersję agenta</li> <li>e) O liczbie agentów z rozbiem na agentów offline i online</li> <li>f) O liczbie agentów z rozbiem na wersję aktualizacji podsystemów bezpieczeństwa</li> <li>g) O liczbie agentów z rozbiem na status ochrony</li> </ul>
21.	System musi umożliwiać tworzenie własnych spersonalizowanych dashboardów z wykorzystaniem predefiniowanych kontrolkek/widgetów oraz kontrolkek definiowanych samodzielnie poprzez kwerendy do danych telemetrycznych.
22.	System musi umożliwiać skonfigurowanie okresu, po którym użytkownik zostanie automatycznie wylogowany z systemu oraz możliwość automatycznego zawieszania kont użytkowników, którzy nie logowali się dłużej niż określona liczba dni.
23.	System musi co najmniej przez 365 dni przechowywać logi audytowe dokumentujące wszystkie akcje podejmowane przez użytkowników zalogowanych do systemu oraz logi audytowe dotyczące funkcjonowania agentów.
24.	System musi posiadać możliwość eksportu wybranych logów audytowych via syslog po ssl/tls w formacie CEF. W dokumentacji systemu musi być wskazany adres IP lub zakres adresów IP, z których nawiązywane będzie połączenie syslog.
25.	System musi posiadać możliwość alarmowania o wskazanych zdarzeniach zapisanych w logach audytowych poprzez wysłanie emaila na wskazany adres skrzynki poczty elektronicznej.
26.	System musi posiadać możliwość integracji z Microsoft Active Directory (AD) używanym obecnie u Zamawiającego w zakresie synchronizacji struktury organizacyjnej katalogu AD zarówno z lokalnym AD jak również z Azure AD na potrzeby automatycznego wzbogacania informacji na temat endpointów i użytkowników oraz tworzenia dynamicznych grup endpointów celem różnicowania konfiguracji agentów.
27.	System musi posiadać funkcjonalność wykrywania niezarządzanych endpointów w sieci w oparciu o skanowanie obiektów kont komputerów Active Directory używanego obecnie u Zamawiającego
28.	System po integracji z Active Directory używanego obecnie u Zamawiającego, musi mieć możliwość wyświetlenia widoku wszystkich komputerów obsługiwanych przez Active Directory Zamawiającego z możliwością filtrowania per OU. Konsola zarządzająca oferowanego rozwiązania musi wykrywać serwery będące członkami domeny Active Directory, na których nie zainstalowano agenta Systemu EDR. Widok powinien być podzielony na maszyny chronione i niechronione przez agenta. System co najmniej raz na

	dobę musi alarmować (co najmniej notyfikacja emailowa i via syslog), jeśli serwery w określonym OU nie są chronione przez agenta.
29.	System musi posiadać możliwość określenia strefy czasowej wykorzystywanej do reprezentowania znaczników czasowych w interfejsie zarządzania oraz formatu tego znacznika co najmniej w takim zakresie, aby uwidaczniał on strefę czasową.
30.	<p>System musi posiadać oprogramowanie agenta co najmniej dla następujących systemów operacyjnych obecnie używanych przez Zamawiającego:</p> <ul style="list-style-type: none"> <li>a) Windows 8, 10 i 11 (włącznie ze środowiskiem Persistent oraz Non-Persistent VDI)</li> <li>b) Windows Server 2012 R2, 2016 standard i core, 2019 standard i core oraz 2022,</li> <li>c) Linux               <ul style="list-style-type: none"> <li>a. Red Hat Enterprise Linux 7, 8 i 9</li> <li>b. Rocky Linux 8 i 9</li> <li>c. SUSE Linux Enterprise Server 11, 12 i 15</li> <li>d. Ubuntu 18.04 LTS, 20.04 LTS i 22.04 LTS</li> <li>e. Oracle Linux 6 i 7</li> <li>f. CentOS 6,7 i 8</li> <li>g. Debian 9, 10 i 11</li> </ul> </li> <li>d) macOS 11.x, 12.x i 13.x</li> <li>e) Kubernetes</li> <li>f) Android 10,11 i 12</li> <li>g) g. iOS 15.x i 16.x</li> </ul>
31.	<p>System musi umożliwiać wygenerowanie i pobranie pakietu instalacyjnego zgodnie z systemami używanymi u Zamawiającego:</p> <ul style="list-style-type: none"> <li>a) W formacie msi dla systemów Windows</li> <li>b) W formacie rpm, deb i sh dla systemów Linux</li> <li>c) W formacie dpkg dla systemów macOS</li> <li>d) W formacie helm dla klastrów kubernetes</li> </ul>
32.	<p>Pakiet instalacyjny agenta dla systemów Windows, macOS, Linux, które są obecnie używane u Zamawiającego i klastrów kubernetes musi posiadać możliwość:</p> <ul style="list-style-type: none"> <li>a) Przypisanie do endpointa nieusuwalnego znacznika, który może być wykorzystany do tworzenia dynamicznych grup endpointów i określenia zakresu dostępu jaki posiada rola użytkownika.</li> <li>b) Skonfigurowania komponentu pośredniczącego w komunikacji z systemem</li> <li>c) Wyłączenia opcji wykonywania skryptów python</li> <li>d) Wyłączenia opcji pobierania plików</li> <li>e) Wyłączenia opcji dostępu do linii poleceń</li> </ul>
33.	Pakiet instalacyjny agenta dla systemów Windows, na których pracuje Zamawiający, musi posiadać możliwość wskazania lokalnej kopii aktualizacji podsystemów bezpieczeństwa.

34.	Instalacja agenta i jego aktywacja w systemie nie może wymagać restartu systemu operacyjnego
35.	<p>Komunikacja pomiędzy agentem a systemem musi być zabezpieczona z wykorzystaniem https (co najmniej TLS 1.2) i w zależności od konfiguracji być realizowana w sposób bezpośredni lub pośredni via dedykowany komponent pośredniczący (dalej proxy) tego samego producenta, który:</p> <ul style="list-style-type: none"> <li>a) musi umożliwiać uruchomienie w formie maszyny wirtualnej</li> <li>b) musi obsługiwać funkcję proxy chaining dla http z uwierzytelnieniem</li> <li>c) musi umożliwiać cache'owanie aktualizacji oprogramowania agenta i aktualizacji podsystemów bezpieczeństwa agenta</li> </ul>
36.	Komunikacja pomiędzy proxy a systemem musi być zabezpieczona z wykorzystaniem https (co najmniej TLS 1.2). Proxy musi posiadać możliwość manualnej lub automatycznej aktualizacji. System musi umożliwiać centralne zarządzanie ustawieniami proxy.
37.	System musi obsługiwać co najmniej 3 proxy.
38.	W dokumentacji systemu muszą być wskazane publiczne adresy IP oraz adresy URL niezbędne do zapewnienia poprawnej komunikacji między agentami i systemem oraz pomiędzy proxy a systemem. Komunikacja musi być zawsze nawiązywana w kierunku od agenta/proxy do systemu.
39.	<p>System musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup endpointów. Polityka automatycznej konfiguracji agenta musi umożliwiać określenie:</p> <ul style="list-style-type: none"> <li>a) Dnia tygodnia i zakresu czasu, w którym wykonywana jest aktualizacja</li> <li>b) Maksymalnej liczby równolegle aktualizowanych agentów</li> <li>c) Zakresu: tylko minor release, tylko minor release w ramach wskazanego major release, najnowszy major.minor release, najnowszy przedostatni major.minor release</li> <li>d) Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowego release</li> <li>e) Źródła: bezpośrednio z systemu, z komponentu pośredniczącego, peer-to-peer</li> </ul>
40.	<p>System musi posiadać możliwość skonfigurowania manualnej i automatycznej różnicowej aktualizacji podsystemów bezpieczeństwa agenta dla wskazanych grup endpointów. Polityka automatycznej aktualizacji podsystemów bezpieczeństwa musi umożliwiać określenie:</p> <ul style="list-style-type: none"> <li>a) Zakresu: tylko major release, najnowszy major.minor release</li> <li>b) Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowego release</li> <li>c) Źródła: bezpośrednio z systemu, z komponentu pośredniczącego, peer-to-peer</li> <li>d) Globalnego limitu na wykorzystanie pasma przy bezpośrednim pobieraniu z systemu</li> </ul>

41.	System musi umożliwiać alarmowanie w przypadku, gdy: <ul style="list-style-type: none"> <li>a) Podsystemy bezpieczeństwa agenta nie będą funkcjonowały poprawnie</li> <li>b) Agent zostanie odinstalowany</li> <li>c) Agent nie zgłosi się do systemu a równocześnie endpoint zaloguje się w domenę Active Directory (dotyczy systemów Windows), na którym pracuje Zamawiający</li> </ul>
42.	System musi umożliwiać różnicowanie konfiguracji agenta i podsystemów bezpieczeństwa poprzez przypisanie różnych profili konfiguracyjnych do wybranych grup endpointów lub pojedynczych endpointów.
43.	System musi umożliwiać przetwarzanie i przechowywanie danych telemetrycznych i alarmów z urządzeń firewall.
44.	System musi umożliwiać przetwarzanie i przechowywanie danych telemetrycznych co najmniej z następujących systemów.
45.	System musi umożliwiać przetwarzanie i przechowywanie danych telemetrycznych w formacie co najmniej IPFIX.
46.	System musi umożliwiać przetwarzanie i przechowywanie danych telemetrycznych przesyłanych przez syslog w formacie CEF i LEEF a w przypadku nieustrukturyzowanych danych umożliwiać ich analizę i mapowanie.
47.	System musi umożliwiać przetwarzanie i przechowywanie danych telemetrycznych przesyłanych w ramach mechanizmu Windows Event Forwarding używanego obecnie u Zamawiającego.
48.	W ramach przechowywania danych telemetrycznych i alarmów z rozwiązań wymienionych w punktach 42-46 system musi zapewniać możliwość przetwarzania minimum 33GB danych dziennie i przechowywać je minimum 30 dni.
49.	Wszystkie dane telemetryczne muszą być przechowywane przez system w centralnym i przeszukiwalnym repozytorium danych.
50.	System musi umożliwiać przeszukiwanie danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem kwerend. Kwerendy muszą umożliwiać łączenie danych telemetrycznych z różnych źródeł, ich filtrowanie i przekształcanie wyników. Reguły tworzenia kwerend muszą być opisane w dokumentacji systemu.
51.	System musi umożliwiać zapisanie kwerendy do danych telemetrycznych do prywatnej biblioteki kwerend danego użytkownika lub do globalnej biblioteki kwerend dostępnej dla wszystkich innych użytkowników.
52.	System musi umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via REST API.
53.	System musi umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego.
54.	System musi umożliwiać uruchamianie kwerendy cyklicznie zgodnie z podanym harmonogramem lub jeden raz o określonym czasie.
55.	System musi umożliwiać wizualizację wyników kwerendy do danych telemetrycznych w formie tabelarycznej i w formie wykresu: liniowego, słupkowego i kołowego.

56.	System musi umożliwiać wykorzystanie wyników kwerendy do tworzenia periodycznie generowanych raportów.
57.	System musi umożliwiać wykorzystanie wyników kwerend do wizualizacji danych w dashboardach.
58.	System musi umożliwiać przekształcenie kwerendy do danych telemetrycznych w uruchamianą zgodnie z zadaniem harmonogramem regułę korelacyjną generującą alarmy, jeśli kwerenda zwróciła jakiekolwiek rekordy.
59.	System musi umożliwiać definiowanie atomowych wskaźników kompromitacji w formie: SHA256, nazwy domenowej, adresu IPv4, adresu IPv6, ścieżki, nazwy pliku. Musi istnieć możliwość dodania znacznika ręcznie, zaimportowania znaczników z pliku i via REST API oraz oznaczenia reputacji, wiarygodności i okresu wygaśnięcia znacznika.
60.	System musi umożliwiać definiowanie złożonych wskaźników kompromitacji opisujących zachowanie procesu co najmniej w zakresie: operacji plikowych, uruchamianych procesów i ich parametrów, operacji sieciowych i operacji na rejestrze. Funkcjonalność powinna być dostępna na system Windows, obecnie używany przez Zamawiającego.
61.	System dla każdego wprowadzonego atomowego i złożonego wskaźnika kompromitacji musi wygenerować alarm(-y): a) jeśli znacznik został odszukany w historycznych danych telemetrycznych (zgromadzonych przed dodaniem wskaźnika) b) jeśli znacznik zostanie odszukany w nowych danych telemetrycznych
62.	System musi umożliwiać przekształcanie złożonych wskaźników kompromitacji w reguły prewencyjne co najmniej dla agenta dla Windows, macOS i Linux używane obecnie u Zamawiającego.
63.	System musi umożliwiać integrację z VirusTotal lub równoważnym, umożliwiającym skanowanie poszczególnych plików i przedstawienie wyników pozwalających stwierdzić ewentualną infekcję szkodliwym oprogramowaniem.
64.	System musi umożliwiać globalne blokowanie uruchamiania/ładowania plików binarnych o określonych SHA256.
65.	System w ramach odpowiedzi na incydent musi umożliwiać: a) Remediację ze wskazaniem kroków, które mogą być podjęte automatycznie i kroków, które należy zrealizować manualnie. Musi istnieć możliwość wyboru kroków remediacyjnych, które zostaną wykonane automatycznie b) Uruchomienie skryptu w języku Python na endpointcie c) Nawiązanie interaktywnego połączenia do linii poleceń na endpointcie d) Wstrzymanie procesu na endpointcie e) Wyłączenie procesu na endpointcie f) Izolację sieciovą endpointa g) Dodanie adresu IP do listy publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi systemami bezpieczeństwa



	<ul style="list-style-type: none"> <li>h) Dodanie nazwy domenowej do publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi systemami bezpieczeństwa</li> <li>i) Zmianę w rejestrze (tylko w przypadku systemu Windows, na którym pracuje Zamawiający)</li> <li>j) Usunięcie pliku na endpointcie</li> <li>k) Przeniesienie pliku na endpointcie do kwarantanny</li> <li>l) Wyszukanie pliku na innych endpointach</li> <li>m) Zrzucenie pamięci procesu na endpointcie</li> </ul>
66.	System musi posiadać mechanizm wykrywania anomalii w ruchu sieciowym i w zachowaniu użytkownika i procesów.
67.	System musi obsługiwać co najmniej następujące poziomy powagi alarmów: informacyjny, niski, średni, wysoki i krytyczny.
68.	System musi automatycznie grupować powiązane alarmy w celu przyspieszenia i ułatwienia triażu i analizy incydentu.
69.	W ramach incydentu system musi grupować: <ul style="list-style-type: none"> <li>a) powiązanych z incydentem użytkowników</li> <li>b) Endpointy</li> <li>c) Pliki</li> <li>d) Domeny</li> <li>e) Adresy IP</li> </ul>
70.	System dla alarmów zgrupowanych w ramach incydentu musi automatycznie tworzyć łańcuchy przyczynowo skutkowe reprezentujące zależności pomiędzy procesami wykorzystywanymi w trakcie ataku i powiązane dane telemetryczne, tak aby analityk mógł w łatwy sposób przeanalizować wykorzystywane techniki, określić zakres ataku, ustalić potencjalny cel ataku i zweryfikować, czy cel został osiągnięty.
71.	System musi umożliwiać wgląd w raport z sandboxa dla plików powiązanych z incydentem i eksport raportu.
72.	System musi umożliwiać zarządzanie incydentami co najmniej w następującym zakresie: <ul style="list-style-type: none"> <li>a) Przypisanie incydentu do analityka</li> <li>b) Zmianę stanu incydentu: badany, false positive, true positive, duplikat, testy</li> <li>c) Dodawanie notatek Komunikacja z innymi analitykami</li> <li>d) Raportowanie czasu MTTR</li> </ul>
73.	System musi mapować alarmy do matrycy technik i taktyk MITRE ATT&CK.
74.	Nie może wykorzystywać Oracle Java JRE/JDK.
75.	Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa: <ul style="list-style-type: none"> <li>a) Bezpośrednio z systemu</li> <li>b) Z komponentu pośredniczącego</li> <li>c) Od innych endpointów w tej samej podsieci (peer-to-peer)</li> </ul>



76.	Musi posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Wyłączenie podsystemów bezpieczeństwa i odinstalowanie agenta musi wymagać podania hasła, które może być skonfigurowane per grupa endpointów lub indywidualnie dla danego endpointa po stronie systemu. Nie dopuszcza się rozwiązań, w których hasło jest statyczne i podawane w trakcie uruchamiania instalatora. Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym systemu.
77.	Musi być procesem chronionym w trybie PPL dla oprogramowanie anty-malware'owego.
78.	Musi zapewniać mechanizm wczesnego uruchamiania (early launch), który umożliwia skanowanie i ocenę sterowników oraz innych komponentów systemowych przed ich pełnym załadowaniem.
79.	Musi umożliwiać: <ul style="list-style-type: none"> <li>a) Ukrycie ikony agenta w zasobniku systemowym</li> <li>b) Wyłączenie powiadomień o zablokowanych zagrożeniach</li> <li>c) Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej</li> <li>d) Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego</li> <li>e) Spolszczenie komunikatów powiadomień</li> <li>f) Zarządzanie host firewallem endpointa z wykorzystaniem Windows Filtering Platform, obecnie używanym przez Zamawiającego</li> <li>g) Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczania dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu</li> <li>h) Weryfikację stanu szyfrowania dysków</li> </ul>
80.	Musi posiadać możliwość zrzucenia pamięci wskazanego procesu
81.	Musi integrować się z Windows Security Center używanym obecnie przez Zamawiającego
82.	Musi posiadać możliwość blokowania uruchamiania programów z zewnętrznej pamięci masowej podłączonej na porcie USB i z napędów optycznych.
83.	Musi posiadać możliwość blokowania uruchamiania programów ze wskazanych lokalizacji w systemie plików.
84.	Musi posiadać możliwość blokowania uruchamiania programów z zasobów sieciowych poza wybranymi ścieżkami.
85.	Do kolekcji danych telemetrycznych musi używać sterownika lub sterowników (działać w jądrze systemu operacyjnego).
86.	Musi wykonywać: <ul style="list-style-type: none"> <li>a) monitoring zdarzeń w trybie kernela, aby uniemożliwić usunięcie hooków z poziomu programów działających w trybie użytkownika, co najmniej w następującym zakresie:               <ul style="list-style-type: none"> <li>a. Pobieranie informacji o procesach (tworzenie procesu i otwieranie handlerów)</li> <li>b. Pobieranie informacji o wątkach (tworzenie wątku i otwieranie handlerów)</li> <li>c. Pobieranie informacji o ładowaniu bibliotek dll</li> <li>d. Pobieranie informacji o próbach dostępu do rejestru</li> <li>e. Pobieranie informacji o operacjach na systemie plików.</li> </ul> </li> </ul>

	<p>b) monitoring co najmniej następujących funkcje NT API:</p> <ol style="list-style-type: none"> <li>VirtualAlloc i VirtualAllocEx</li> <li>VirtualProtect i VirtualProtectEx</li> <li>CreateThread, CreateRemoteThread i CreateRemoteThreadEx</li> <li>NtAllocateVirtualMemory i ZwAllocateVirtualMemory</li> <li>NtCreateThread, NtCreateThreadEx, ZwCreateThread i ZwCreateThreadEx</li> <li>NtProtectVirtualMemory i ZwProtectVirtualMemory</li> <li>NtSetInformationProcess i ZwSetInformationProcess</li> </ol> <p>Monitoring zdarzeń ETW-TI (Event Tracing for Windows - Threat Intelligence) poprzez subskrypcję na zdarzenia Microsoft-Windows-Threat-Intelligence używanego obecnie u Zamawiającego.</p>
87.	<p>Musi zbierać co najmniej następujące dane telemetryczne:</p> <ol style="list-style-type: none"> <li>Utworzenie nowego procesu i zakończenie procesu</li> <li>Wszystkie operacje na plikach: tworzenie, zapisywanie, kasowanie, zmiana nazwy, przesunięcie, modyfikacja, link symboliczny</li> <li>Ładowanie bibliotek DLL</li> <li>Wstrzykiwanie do procesu</li> <li>Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, create, listen, close, bind</li> <li>Statystyki połączeń sieciowych</li> <li>Praca z rejestrem: skasowanie wartości, ustawienie wartości, utworzenie klucza, kasowanie klucza, zmiana nazwy klucza</li> <li>Wywołania RPC (atributy: action_rpc_interface_uuid, action_rpc_interface_version_major, action_rpc_interface_version_minor / action_rpc_func_opnum / action_rpc_func_str_call_fields / action_rpc_func_int_call_fields / action_rpc_interface_name, action_rpc_func_name)</li> <li>Wywołania systemowe (atributy: action_syscall_string_params, action_syscall_int_params, action_syscall_target_instance_id / action_syscall_target_image_path / action_syscall_target_image_name / action_syscall_target_os_pid / Action_syscall_target_thread_id, address_mapping)</li> </ol>
88.	<p>Musi obsługiwać dziennik zdarzeń:</p> <ol style="list-style-type: none"> <li>Security: <ol style="list-style-type: none"> <li>Successful logon (4624), Failed logon (4625), Logoff (4634), User initiated logoff (4647), Logon attempted, explicit credentials (4648), Replay attack (4649), Special privileges attempted login (4672), Kerberos TGT request (4768), Kerberos service ticket requested (4769), Kerberos service ticket renewal (4770), Kerberos pre-authentication failed (4771), Domain controller validation attempt (4776), Session was reconnected to a Windows station (4778), Workstation locked (4800), Workstation unlocked (4801), Screensaver was invoked (4802), Screensaver was dismissed (4803), A user account was created (4720), A user account was enabled (4722), An attempt was made to change an account's password (4723), An attempt was made to reset an account's</li> </ol> </li> </ol>

	<p>password (4724), A user account was disabled (4725), A user account was deleted (4726), Group creations (4727, 4731, 4754), Group member additions (4728, 4732, 4756), Group member removals (4729, 4733, 4757), Group changes (4735, 4737, 4755, 4764), A user account was changed (4738), A user account was locked out (4740), A computer account was created (4741), A computer account was changed (4742), A computer account was deleted (4743), SID history (4765, 4766), A user account was unlocked (4767), ACL set on accounts (4780), Group membership enumeration (4799), System time was changed (4616), Kerberos service ticket was denied (4821), NTLM authentication failed (4822, 4823), Kerberos pre-authentication failed (4824), User denied access to Remote Desktop (4825), Key file operation (5058), Key migration operation (5059), A scheduled task was created (4698), A scheduled task was updated (4702), Certificate Services received a certificate request (4886), Certificate Services approved a certificate request (4887), A Certificate Services template was updated (4899), Certificate Services template security was updated (4900), A network share object was accessed (5140), Security Log cleared events (1102), CA Service Stopped (4880), CA Service Started (4881), CA DB row(s) deleted (4896), CA Template loaded (4898), Kerberos policy was changed (4713)</p> <p>b) Microsoft-Windows-DNS-Client/Operational używanego obecnie u Zamawiającego: DNS Query Completed (3008) without local machine name resolution events and without empty name resolution events</p> <p>c) Microsoft-Windows-PowerShell/Operational używanego obecnie u Zamawiającego: PowerShell executes block activity (4103), Remote Command (4104), Start Command (4105), Stop Command (4106)</p>
89.	<p>Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploatacji:</p> <ul style="list-style-type: none"> <li>a) Przekierowanie APC</li> <li>b) Obejście Data Execution Prevention</li> <li>c) DLL Hijacking</li> <li>d) Exploit Kit Fingerprinting</li> <li>e) JIT</li> <li>f) Null Dereference</li> <li>g) ROP</li> <li>h) Structures exception handler hijackings</li> <li>i) Heap Spray</li> <li>j) Kernel Privilege Escalation</li> </ul>
90.	<p>Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi umożliwiając skonfigurowanie co najmniej następujących mechanizmów:</p> <ul style="list-style-type: none"> <li>a) Weryfikacja sha256 w bazie threat intelligence producenta systemu</li> <li>b) Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym endpointzie)</li> <li>c) Lokalna analiza statyczna</li> </ul>

	d) Weryfikacja podpisu pliku binarnego e) Przeniesienie pliku binarnego do kwarantanny f) Zablokowanie uruchomienia/załadowania złośliwego pliku binarnego g) Zablokowanie uruchomienia pliku z przenośnej pamięci masowej USB h) Zablokowanie uruchomienia pliku z innych lokalizacji sieciowych niż wskazane i) Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego j) Wykrywanie shellcodu'u ładowanego do pamięci Wykrycie i przerwanie próby szyfrowania plików na dysku (ochrona przeciw ransomware).
91.	Musi wykrywać i blokować próbę wyłączenia Volume Shadow Copy Service (VSS) lub równoważnego w zakresie tworzenia kopii zapasowych.
92.	Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami co najmniej w plikach Microsoft Word i Microsoft Excel umożliwiając skonfigurowanie co najmniej następujące mechanizmy: <ul style="list-style-type: none"> <li>a) Weryfikacja sha256 w bazie threat intelligence producenta systemu</li> <li>b) Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym endpointzie)</li> <li>c) Lokalna analiza statyczna</li> </ul>
93.	Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.
94.	Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do systemu.
95.	Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każdy endpoint musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.
96.	Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa: <ul style="list-style-type: none"> <li>a) Bezpośrednio z systemu</li> <li>b) Z komponentu pośredniczącego</li> </ul> Od innych endpointów w tej samej podsieci (peer-to-peer)
97.	Musi posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Wyłączenie podsystemów bezpieczeństwa i odinstalowanie agenta musi wymagać podania hasła, które może być skonfigurowane per grupa endpointów lub indywidualnie dla danego endpointa po stronie systemu. Nie dopuszcza się rozwiązań, w których hasło jest statyczne i podawana w trakcie uruchamiania instalatora. Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym systemu.

98.	<p>Musi umożliwiać:</p> <ul style="list-style-type: none"> <li>a) Ukrycie ikony agenta w zasobniku systemowym</li> <li>b) Wyłączenie powiadomień o zablokowanych zagrożeniach</li> <li>c) Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej</li> <li>d) Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego</li> <li>e) Spolszczenie komunikatów powiadomień</li> <li>f) Zarządzanie host firewallem endpointa</li> <li>g) Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu</li> <li>h) Weryfikację stanu szyfrowania dysków</li> </ul>
99.	<p>Musi posiadać wbudowany runtime python 3.7 lub nowszy i możliwość uruchamiania wbudowanych i własnych skryptów python z wykorzystaniem co najmniej następujących bibliotek: argparse, base64, certifi, contextlib, csv, ctypes, datetime, enum, fnmatch, functools, glob, globmatch, gzip, hashlib, importlib, io, json, LnkParse3, locale, logging, multiprocessing, netifaces, os, pathlib, pefile, platform, pprint, protobuf, psutil, pysftp, pytest, python_hosts, pythoncom, pytsk3, pywin32, pywintypes, queue, random, re, Registry, requests, runpy, setuptools, shlex, shutil, signal, socket, sqlite_utils, sqlite3, ssl, stat, struct, subprocess, sys, threading, time, traceback, types, unicodedata, websocket, win32api, win32com, win32con, win32evtlog, win32evtlogutil, win32file, win32net, win32netcon, win32process, win32security, win32service, win32serviceutil, win32timezone, winerror, winreg, wmi, xml, xmljson, yara, zipfile, zlib.</p>
100.	<p>Musi posiadać możliwość wyszukania plików we wskazanej ścieżce przy pomocy filtrów yara lub równoważnych w zakresie identyfikacji i klasyfikacji złośliwego oprogramowania na podstawie wzorców.</p>
101.	<p>Musi posiadać możliwość zrzucenia pamięci wskazanego procesu</p>
102.	<p>Musi zbierać co najmniej następujące dane telemetryczne:</p> <ul style="list-style-type: none"> <li>a) Utworzenie nowego procesu i zakończenie procesu</li> <li>b) Wszystkie operacje na plikach: tworzenie, zapisywanie, kasowanie, zmiana nazwy, przesunięcie, otwarcie</li> <li>c) Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, connect failure, disconnect, listen</li> <li>d) Statystyki połączeń sieciowych</li> <li>e) Zdarzenia z event logu dotyczącego uwierzytelnienia</li> </ul>
103.	<p>Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technik eksploatacji:</p> <ul style="list-style-type: none"> <li>a) Dylib Hijacking</li> <li>b) JIT</li> <li>c) ROP</li> </ul>
104.	<p>Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:</p>

	<ul style="list-style-type: none"> <li>a) Weryfikacja sha256 w bazie threat intelligence producenta systemu</li> <li>b) Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym endpointcie)</li> <li>c) Lokalna analiza statyczna</li> <li>d) Weryfikacja podpisu pliku binarnego</li> <li>e) Przeniesienie pliku binarnego do kwarantanny</li> <li>f) Weryfikacja i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego.</li> </ul>
105.	<p>Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:</p> <ul style="list-style-type: none"> <li>a) Weryfikacja sha256 w bazie threat intelligence producenta systemu</li> <li>b) Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym endpointcie)</li> <li>c) Lokalna analiza statyczna</li> <li>d) Weryfikacja podpisu pliku binarnego</li> <li>e) Przeniesienie pliku binarnego do kwarantanny</li> <li>f) Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego</li> <li>g) Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.</li> </ul>
106.	<p>Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:</p> <ul style="list-style-type: none"> <li>a) Weryfikacja sha256 w bazie threat intelligence producenta systemu</li> <li>b) Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym endpointcie)</li> <li>c) Lokalna analiza statyczna</li> <li>d) Weryfikacja podpisu pliku binarnego</li> <li>e) Przeniesienie pliku binarnego do kwarantanny</li> <li>f) Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego</li> <li>g) Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.</li> <li>h) Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacja sieciowa) poza połączeniem do systemu.</li> </ul>
107.	<p>Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utraci łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każdy endpoint musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.</p>

108.	<p>Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa:</p> <ul style="list-style-type: none"> <li>a) Bezpośrednio z systemu</li> <li>b) Z komponentu pośredniczącego</li> </ul> <p>Od innych endpointów w tej samej podsieci (peer-to-peer)</p>
109.	Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym systemu.
110.	Musi posiadać wsparcie dla rozszerzenia eBPF.
111.	<p>Musi wysyłać zgromadzone dane telemetryczne do systemu nie rzadziej niż co 5 minut, przy czym wymagane jest, aby agent posiadał możliwość wymuszenia wystania danych telemetrycznych na żądanie. Jeśli z powodu braku łączności sieciowej agent nie może wysłać danych telemetrycznych, to dane telemetryczne muszą zostać lokalnie przechowane (zcache'owane) i wysłane do systemu po przywróceniu łączności sieciowej.</p>
112.	<p>Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technik eksploatacji:</p> <ul style="list-style-type: none"> <li>a) Java Deserialization</li> <li>b) SO Hijacking</li> <li>c) Heap spray</li> <li>d) ROP</li> <li>e) Kernel Privilege Escalation</li> </ul>
113.	<p>Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:</p> <ul style="list-style-type: none"> <li>a) Weryfikacja sha256 w bazie threat intelligence producenta systemu</li> <li>b) Analiza dynamiczna w sandboxie chmurowym producenta systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym endpointcie)</li> <li>c) Lokalna analiza statyczna</li> <li>d) Przeniesienie pliku binarnego do kwarantanny</li> <li>e) Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego</li> <li>f) Wykrywanie webshelli</li> </ul>
114.	Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.
115.	Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do systemu.
116.	<p>Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utraci łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każdy endpoint musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać</p>



	agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.
117.	Musi umożliwiać automatyczną instalację via system MDM i manualną.
118.	Operacja deinstalacji agenta musi zostać zapisana w dzienniku audytowym systemu i wygenerować alarm.
119.	Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi aplikacjami wykorzystując co najmniej następujące mechanizmy: a) Weryfikacja sha256 w bazie threat intelligence producenta systemu b) Analiza dynamiczna w sandboxie chmurowym producenta systemu
120.	Operacja deinstalacji agenta musi zostać zapisana w dzienniku audytowym systemu i wygenerować alarm.
121.	Musi weryfikować i raportować integralność systemu operacyjnego (tzw. jail break).
122.	Musi zapewniać ochronę przed groźnymi wiadomościami tekstowymi przez weryfikację linków url (ochrona przeciw smishingowa).
123.	Musi zapewniać ochronę przed groźnymi połączeniami głosowymi (ochrona przeciw vishingowa).
124.	Musi umożliwiać użytkownikowi raportowanie podejrzanych wiadomości tekstowych.
125.	Musi mieć opcję okresowego przypominania o konieczności restartu telefonu.
126.	Wymaga się, aby dane były przechowywane i przetwarzane na terenie Polski
127.	System musi posiadać możliwość analizy dynamicznej plików wykonywalnych Windows, Linux i MacOS, używane obecnie u Zamawiającego w systemie sandbox tego samego producenta co producent oferowanego systemu i obsługiwać pliki o rozmiarze co najmniej 100MB. System musi umożliwiać pobranie raportu z analizy dynamicznej, Wymaga się, aby system analizy typu sandbox był realizowany na terenie Polski
128.	Moduł ochrony anty-exploitowej bazujący na wykrywaniu technik exploitacji musi być wspierany na systemach Windows, MacOS i Linux, używane obecnie u Zamawiającego oraz system musi umożliwiać zdefiniowanie listy chronionych procesów, tak aby możliwa była ochrona aplikacji dziedzinowych a nie tylko tych wyspecyfikowanych przez producenta
129.	Agent musi posiadać opcję dystrybucji aktualizacji agenta w trybie peer-to-peer celem zmniejszenia obciążenia łączu WAN i Internet.
130.	System musi posiadać możliwość publikowania indykatorów (co najmniej adresy IP i nazwy domenowy) oznaczonych przez analityka jako groźne w formie płaskiego pliku tekstowego publikowanego po uwierzytelnionym https, celem umożliwienia bezpośredniej integracji z firewallami następnej generacji i przyspieszenia aktywnego procesu odpowiedzi na incydent.
131.	Musi wykrywać podatności zidentyfikowane na stacji końcowej.
132.	Musi wykrywać aplikacje zainstalowane na stacji końcowej.



### 3. Część 3 - Wymiana stacji roboczych użytkowników

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja, uruchomienie oraz wdrożenie nowych stacji roboczych zgodnych z wymaganiami technicznymi określonymi przez Zamawiającego, na które składają się:

- Laptopy – ilość: 40 szt.
- Komputery stacjonarne – ilość: 130 szt.
- Monitory – ilość: 130 szt.

przeznaczonych do pracy w infrastrukturze Zamawiającego.

W ramach realizacji zamówienia Wykonawca zobowiązany jest również do dostarczenia niezbędnych akcesoriów (klawiatur bezprzewodowych USB z układzie polski programista w ilości 130 sztuk, myszek bezprzewodowych USB z klawiszami oraz rolką scroll w ilości 170 sztuk).

Dzięki wymianie stacji roboczych zwiększy się bezpieczeństwo, ergonomia pracy, skróci się czas reakcji systemów oraz zostanie zapewnione lepsze wsparcie dla cyfrowych usług klinicznych. Zmodernizowany sprzęt umożliwi sprawną obsługę nowych narzędzi, w tym systemów HIS, EDM i platform opartych na AI. Rozwiązanie ma zapewnić niezawodne, wydajne i bezpieczne środowisko pracy użytkowników, a także pełną kompatybilność z istniejącą infrastrukturą teleinformatyczną i domeną Zamawiającego, zgodnie z wyszczególnioną specyfikacją techniczną.

#### 3.1. Wymagania

- Stacje robocze muszą być fabrycznie nowe, oryginalne, wolne od wad prawnych, dopuszczone do obrotu na terenie UE oraz objęte gwarancją obowiązująca na terytorium RP. Korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Wykonawca zobowiązany jest zapewnić realizację gwarancji producenta na terytorium Rzeczypospolitej Polskiej, bez dodatkowych kosztów dla Zamawiającego.
- Każda stacja robocza musi być objęta gwarancją przez okres nie krótszy niż 36 miesięcy.

#### Laptop – ilość: 40 szt.

Nazwa	Wymagane parametry techniczne
Typ	Laptop – komputer mobilny
Zastosowanie	Komputer mobilny będzie wykorzystywany do działań służących zwiększeniu efektywności udzielania świadczeń medycznych, w tym także do dostępu do Internetu oraz poczty elektronicznej.
Matryca	14" FHD+ (1920 x 1200), matryca IPS, powłoka przeciwoodbleskowa, jasność minimalna 300 cd/m2.
Procesor	Procesor musi być wyposażony w jednostki przetwarzania neuronowego (NPU) o wydajności co najmniej 12 TOPS. Ponadto, procesor musi osiągać w teście PassMark Performance Test, co najmniej 17400 punktów w kategorii Average CPU Mark. Wynik dostępny na stronie: <a href="https://www.cpubenchmark.net/cpu_list.php">https://www.cpubenchmark.net/cpu_list.php</a>
Pamięć RAM	Minimum 16GB DDR5 5200 MT/s, jeden slot wolny.
Pamięć masowa	Minimum 256GB NVMe SSD M.2

<b>Karta graficzna</b>	Zintegrowana karta graficzna.
<b>Klawiatura urządzenie wskazujące</b>	<p>Klawiatura z wbudowanym podświetleniem w układzie US – QWERTY. Wszystkie klawisze funkcyjne typu: mute, regulacja głośności, print screen dostępne w ciągu klawiszy F1-F12. Dedykowany klawisz do obsługi asystenta AI.</p> <p>Touchpad lub clickpad z obsługą gestów, umożliwiający kontrolowanie kursora na ekranie w systemie diagnostycznym oraz podczas instalacji systemu operacyjnego.</p>
<b>Multimedia</b>	<p>Wbudowane dwa głośniki o mocy nie mniejszej niż 2W każdy.</p> <p>Dwa kierunkowe, cyfrowe mikrofony z funkcją redukcji szumów i poprawy mowy.</p> <p>Kamera internetowa działająca w rozdzielczości FHD, trwale zainstalowana w obudowie matrycy opatrzona we wbudowaną mechaniczną przystonę.</p>
<b>Łączność bezprzewodowa</b>	Karta Wi-Fi min. 6E AX z Bluetooth 5.3.
<b>Bateria i zasilanie</b>	<p>Bateria o pojemności min. 55WH.</p> <p>Ładowanie baterii do poziomu 80% w czasie nie dłuższym niż 1 godzina.</p> <p>Bateria objęta nie krótszą niż 36 miesięczną gwarancją producenta komputera.</p> <p>Zasilacz o mocy min. 60W ze złączem Typu – C</p>
<b>Waga</b>	Katalogowa waga startowa nie większa niż 1.4kg wg. oficjalnej dokumentacji producenta.
<b>Obudowa</b>	<p>Kąt otwarcia minimum 180 stopni.</p> <p>Komputer spełniający normy MIL-STD-810H.</p>
<b>Ochrona oprogramowania układowego</b>	Komputer wyposażony w mechanizm weryfikacji i ochrony BIOS/UEFI, działający automatycznie przy każdym uruchomieniu komputera poza warstwą systemu operacyjnego oraz w samym środowisku systemu operacyjnego. Mechanizm musi umożliwiać ochronę oprogramowania układowego poprzez weryfikację integralności BIOS/UEFI pod kątem próby jego modyfikacji oraz ataku w trakcie rozruchu komputera (również podczas uruchamiania systemu operacyjnego). Weryfikacja poprawności BIOS/UEFI musi odbywać się poza hostem.
<b>BIOS/UEFI</b>	<p>Możliwość odczytania z BIOS informacji o:</p> <ul style="list-style-type: none"> <li>a) Wersji BIOS</li> <li>b) Numerze seryjnym komputera</li> <li>c) Numerze inwentarzowym</li> <li>d) Typie (modelu) procesora, ilości rdzeni.</li> <li>e) Ilości pamięci RAM i jej prędkości.</li> <li>f) Pojemności i modelu zainstalowanego dysku.</li> <li>g) MAC adresie zintegrowanej karty sieciowej lub adresie MAC Address Pass Through (tzw. MAPT)</li> <li>h) Mocy podpiętego zasilacza</li> </ul>

	<ul style="list-style-type: none"> <li>i) Poziomie naładowania baterii</li> <li>j) Dacie produkcji komputera</li> <li>k) Maksymalnej prędkości procesora</li> <li>l) Kontrolerze audio (producent lub oznaczenie)</li> </ul> <p>BIOS musi zapewniać możliwość zarządzania:</p> <ul style="list-style-type: none"> <li>a) Kamerą</li> <li>b) Mikrofonem oraz głośnikami</li> <li>c) Portami USB</li> <li>d) Kontrolerem NVMe</li> <li>e) Zintegrowaną kartą sieciową (o ile występuje)</li> <li>f) Kartą sieci bezprzewodowej i bluetooth (o ile występuje)</li> <li>g) Podświetleniem klawiatury</li> <li>h) Jasnością matrycy oddzielnie dla zasilania bateryjnego i sieciowego</li> <li>i) Trybami ładowania baterii w min. 4 predefiniowanych trybach</li> <li>j) Zarządzanie funkcją Power Delivery dla portu typu – C</li> <li>k) Trybem pracy układu chłodzenia wg. Min. trzech predefiniowanych scenariuszu (zoptymalizowany, cicha praca, maksymalna wydajność)</li> <li>l) Funkcją odpowiedzialną za zarządzanie podświetleniem klawiatury umożliwiającą wybór predefiniowanego trybu podświetlenia wg. sposobu lub czasu lub stopnia podświetlenia</li> </ul> <p>Powyższe funkcjonalności muszą być realizowane wyłącznie przez BIOS. Nie dopuszcza się realizacji poprzez dodatkowe oprogramowanie oraz przez system diagnostyczny.</p>
<b>BIOS/UEFI bezpieczeństwo</b>	<p>- W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych organizacji, BIOS/UEFI musi umożliwiać:</p> <ul style="list-style-type: none"> <li>a) Nadanie hasła administratora</li> <li>b) Ustawienie hasła dla zainstalowanego dysku</li> <li>c) Ustawienie portów USB w trybie „No BOOT”</li> <li>d) Zarządzanie funkcją Wake on Lan oraz PXE Boot zintegrowanej karty sieciowej (o ile występuje)</li> <li>e) Zarządzanie funkcją Secure Boot</li> <li>f) Zarządzanie układem TPM</li> <li>g) Zarządzania funkcją tworzenia recovery BIOS</li> <li>h) Zarządzania funkcją downgrade BIOS</li> <li>i) Zarządzanie czujnikiem otwarcia obudowy (dolnej pokrywy)</li> <li>j) Zapisywanie incydentów w formacie tzw. logów z możliwością ich przejrzenia</li> <li>k) Bezpieczne usuwanie danych z zainstalowanego dysku zgodnie z wytycznymi NIST 800-88r1</li> </ul>

	<p>l) Nadanie numeru inwentarzowego bezpośrednio w BIOS bez użycia dodatkowego oprogramowania. Nadany numer nie może być edytowalny w BIOS ani nie może ulec skasowaniu po jego aktualizacji</p> <p>m) Możliwość nadania hasła uniemożliwiającego rozruch systemu operacyjnego, możliwość zmiany tego hasła w BIOS musi być zachowana także po nadaniu hasła administratora.</p> <p>n) Możliwość blokowania upgrade BIOS przez system operacyjny.</p> <p>Powyższe funkcjonalności muszą być realizowane wyłącznie przez BIOS. Nie dopuszcza się realizacji poprzez dodatkowe oprogramowanie oraz przez system diagnostyczny.</p>
<b>Certyfikaty</b>	<ol style="list-style-type: none"> <li>1. Certyfikat ISO 9001 dla producenta sprzętu lub równoważny w zakresie jakości</li> <li>2. Certyfikat ISO 14001 dla producenta sprzętu lub równoważny w zakresie zarządzania środowiskiem</li> <li>3. Certyfikat ISO 50001 dla producenta sprzętu lub równoważny w zakresie zarządzania energią</li> </ol>
<b>Ergonomia</b>	<p>Głośność jednostki centralnej może wynosić maksymalnie 25dB według oficjalnego dokumentu producenta. Głośność musi być zmierzona zgodnie z normą ISO 7779 lub równoważną w zakresie pomiaru hałasu emitowanego przez sprzęt informatyczny oraz wykazana zgodnie z normą ISO 9296 lub równoważną w zakresie ustalania wartości emisji hałasu dla sprzętu informatycznego, w pozycji obserwatora w trybie pracy dysku twardego (IDLE).</p>
<b>Oprogramowanie diagnostyczne</b>	<p>System diagnostyczny z graficznym interfejsem użytkownika, działający poza środowiskiem systemu operacyjnego, dostępny z poziomu BIOS lub szybkiego menu boot'owania.</p> <p>System umożliwiający przetestowanie komponentów bez konieczności uruchamiania systemu operacyjnego. Pełna obsługa systemu diagnostycznego za pomocą klawiatury i myszy jak i samej myszy.</p>
<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>• Dedykowany układ sprzętowy TPM min. 2.0 zgodny z certyfikacją TCG lub równoważną w zakresie standardów bezpieczeństwa, przechowujący klucze kryptograficzne i certyfikaty.</li> <li>• Wbudowany czujnik otwarcia obudowy (dolnej pokrywy).</li> <li>• Wbudowana w obudowę matrycy kamera IR umożliwiająca autentykację na poziomie oferowanego systemu operacyjnego</li> <li>• Wbudowany czytnik linii papilarnych</li> </ul>
<b>Zarządzanie zdalne</b>	<p>Wbudowana w płytę główną technologia zdalnego monitorowania i zarządzania komputerem na poziomie sprzętowym (out-of-band) działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC. Technologia ta powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (<a href="http://www.dmtf.org/standards/wsman">http://www.dmtf.org/standards/wsman</a>) oraz DASH 1.2.0</p>

	<p>(<a href="http://www.dmtf.org/standards/mgmt/dash">http://www.dmtf.org/standards/mgmt/dash</a>) oraz musi obsługiwać łącznie wszystkie następujące funkcje:</p> <ol style="list-style-type: none"> <li>Zdalny odczyt konfiguracji komponentów komputera – model komputera i jego nr seryjny, model procesora, ilość, rodzaj i nr seryjne modułów pamięci RAM, model i nr seryjny dysku HDD/SSD, wersja BIOS FW płyty głównej, nr seryjny płyty głównej, dla laptopów model, znamionowa pojemność, numer seryjny i data produkcji baterii</li> <li>Zdalną konfigurację ustawień komputera przez interfejs BIOS setup w trybie graficznym lub tekstowym (ASCII)</li> <li>Zdalne przejście konsoli tekstowej systemu – tzw. Text Console Redirection lub Serial over LAN z możliwością jej wykorzystania do zdalnej zmiany ustawień BIOS Setup oraz odblokowania MS BitLocker Recovery, używane obecnie u Zamawiającego</li> <li>Zdalne przejście pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) na poziomie sprzętowym bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 2560×1600 (WQXGA) włącznie zgodnie z profilem DSP1076 standardu DASH <a href="https://www.dmtf.org/sites/default/files/standards/documents/DSP1076_1.0.1.pdf">https://www.dmtf.org/sites/default/files/standards/documents/DSP1076_1.0.1.pdf</a></li> </ol> <p>Funkcja przekierowania konsoli graficznej musi przechwytywać każdy rodzaj wyświetlanego na fizycznym lokalnym ekranie obrazu włącznie z procesem uruchamiania komputera (POST), odblokowania systemu szyfracji dysku, ładowania OS z dowolnego nośnika, zamykania OS oraz błędów ww. procesów: POST, ładowania OS (np. brak nośnika uruchamiającego, uszkodzenia OS BSOD (Blue Screen of Death) bez potrzeby modyfikacji tzw. loadera OS.</p>
<b>System operacyjny</b>	<p>Zainstalowany system operacyjny typu Windows 11 Pro (używany obecnie u Zamawiającego) lub równoważny, klucz licencyjny zapisany trwale w BIOS, musi umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. Za system równoważny Zamawiający nie uznaje systemu Linux.</p>
<b>Oprogramowanie dodatkowe</b>	<p>Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające:</p> <ul style="list-style-type: none"> <li>- upgrade i instalacje wszystkich sterowników, dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,</li> <li>- możliwość przed instalacją sprawdzenia każdego sterownika, BIOS'u bezpośrednio na stronie producenta lub Wykonawcy przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji:</li> </ul> <ol style="list-style-type: none"> <li>poprawkach i usprawnieniach dotyczących aktualizacji</li> <li>dacie wydania ostatniej aktualizacji</li> </ol>

	<p>c) priorytecie aktualizacji</p> <p>d) zgodność z systemami operacyjnymi</p> <p>e) jakiego komponentu sprzętu dotyczy aktualizacja</p> <p>f) wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.</p> <ul style="list-style-type: none"> <li>- wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne</li> <li>- możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji, która tego wymaga.</li> <li>- rozpoznanie modelu oferowanego komputera, numeru seryjnego komputera, informacji, kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)</li> <li>- sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)</li> <li>- dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml</li> <li>- raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.</li> </ul> <p>Oprogramowanie umożliwiające aktualizację BIOS bezpośrednio z serwera producenta komputera przy wykorzystaniu bezpiecznego, szyfrowanego połączenia bez konieczności uruchamiania systemu operacyjnego oraz wykorzystywania zewnętrznych nośników pamięci masowej.</p> <p>Oprogramowanie musi automatycznie rozpoznawać model urządzenia i bieżącą wersję BIOS.</p> <p>Oprogramowanie posiadające bezterminową licencję.</p> <p>Możliwość zabezpieczenia dostępu do oprogramowania hasłem administratora.</p> <p>Oprogramowanie umożliwiające przywrócenie obrazu systemu operacyjnego bezpośrednio z serwera producenta komputera przy wykorzystaniu bezpiecznego, szyfrowanego połączenia bez konieczności uruchamiania systemu operacyjnego.</p> <p>W przypadku wystąpienia awarii oprogramowanie automatycznie uruchomi się i zapewni możliwość naprawy systemu operacyjnego lub przywrócenie go do stanu fabrycznego z możliwością dokonania kopii zapasowej plików przed uruchomieniem procesu.</p>
--	--

	<p>Dodatkową funkcją oprogramowania jest możliwość wykonania kopii dysku (tzw. klonowania) wraz z plikami, ustawieniami aplikacji, systemem operacyjnym i jego ustawieniami.</p> <p>Licencja pozwalająca na bezpłatne korzystanie z oprogramowania przez cały okres gwarancji komputera, jednak nie krócej niż 36 miesięcy</p>
<b>Porty i złącza</b>	<p>Wbudowane porty i złącza: min. 1 x HDMI 2.1, 2 x USB 3.2 typ A, 1 x USB typ C, 1 x Thunderbolt 4, port audio combo, 1 x RJ – 45, gniazdo linki zabezpieczającej.</p>
<b>Warunki gwarancyjne, wsparcie techniczne</b>	<p>Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.</p> <p>Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta lub dystrybutora (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).</p> <p>Nie krótsza niż 36-miesięczna gwarancja producenta świadczona na miejscu u klienta.</p> <p>Czas reakcji serwisu – najpóźniej do końca następnego dnia roboczego od dnia zgłoszenia.</p> <p>W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.</p>
<b>Dostępność dla osób z niepełnosprawnościami</b>	<p>Laptopy muszą dysponować następującymi funkcjonalnościami, dzięki którym będą dostępne osób z niepełnosprawnością:</p> <ul style="list-style-type: none"> <li>a) możliwość podłączenia dodatkowego monitora w celu powiększenia obrazu lub lepszego kontrastu</li> <li>b) możliwość podłączenia słuchawek z redukcją hałasu</li> <li>c) możliwość podłączenia zewnętrznej klawiatury</li> </ul>
<b>Zasada DNSH</b>	<p>Zamówienie będzie zgodne z zasadą DNSH „niewyrządzania znaczącej szkody środowisku” (DNSH – „do no significant harm”) w rozumieniu art. 17 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2020/852 z dnia 18 czerwca 2020 r. w sprawie ustanowienia ram ułatwiających zrównoważone inwestycje, zmieniającego rozporządzenie (UE) 2019/2088 (Dz. U. UE. L. z 2020 r. Nr 198, str.13 z późn. zm.), czego potwierdzeniem będzie m.in.:</p> <ul style="list-style-type: none"> <li>a) w odniesieniu do zasady: Przejście na gospodarkę o obiegu zamkniętym:             <ul style="list-style-type: none"> <li>- dostawa zostanie zrealizowana przy jak najmniejszej liczbie opakowań w celu ograniczenia ilości odpadów,</li> <li>- opakowania (tam, gdzie to możliwe) będą wykonane z materiałów podlegających powtórnemu przetworzeniu</li> <li>- w trakcie instalacji laptopów zapewnione zostaną rozwiązania ograniczające ryzyko powstania nadmiernej liczby odpadów, w tym niepodlegających recyklingowi</li> </ul> </li> </ul>



	<p>b) w odniesieniu do zasady: ochrona i odbudowa bioróżnorodności i ekosystemów:</p> <ul style="list-style-type: none"><li>- elementy składające się na laptopy nie posiadają cech szkodliwych dla stanu zachowania siedlisk i gatunków, w tym siedlisk i gatunków objętych zakresem zainteresowania Unii Europejskiej.</li></ul>
--	--



**Komputer stacjonarny – ilość: 130 szt.**

Nazwa komponentu	Wymagane parametry techniczne komputerów
<b>Typ</b>	Komputer stacjonarny
<b>Zastosowanie</b>	Komputer będzie wykorzystywany do działań służących zwiększeniu efektywności udzielania świadczeń medycznych, w tym także do dostępu do Internetu oraz poczty elektronicznej.
<b>Obudowa</b>	<p>Małogabarytowa typu Small Form Factor z obsługą kart PCI Express wyłącznie o niskim profilu, umożliwiającą montaż wewnątrz obudowy napędu optycznego w dedykowanej zewnętrznej wnęce 5.25” typu Slim.</p> <p>Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy.</p> <p>Obudowa jednostki centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych).</p> <p>Moduł konstrukcji obudowy komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycie wkrętów, śrub motylkowych).</p> <p>Suma wymiarów obudowy mierzona po krawędziach obudowy nie może przekraczać 700 mm.</p>
<b>Płyta główna</b>	<p>Płyta główna musi być wyposażona w sloty i złącza min.:</p> <ul style="list-style-type: none"> <li>a) 2 złącza DIMM z obsługą do 64GB pamięci RAM DDR5</li> <li>b) 1 złącze M.2 dedykowane dla dysku SSD</li> <li>c) 1 złącze M.2 WLAN</li> <li>d) 1 złącze PCIe x16 Gen 3.0</li> <li>e) 2 złącza PCIe x1 Gen 3.0</li> <li>f) 2 złącza SATA 3.0.</li> </ul>
<b>Procesor</b>	<p>Procesor musi być wyposażony w jednostki przetwarzania neuronowego (NPU) o wydajności co najmniej 12 TOPS.</p> <p>Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 39000 pkt. według wyników opublikowanych na stronie <a href="http://www.cpubenchmark.net/cpu_list.php">http://www.cpubenchmark.net/cpu_list.php</a>.</p>
<b>Pamięć RAM</b>	Minimum 16GB DDR5 4800 MT/s, slot wolny.
<b>Pamięć masowa</b>	Dysk M.2 SSD 256GB PCIe NVMe.
<b>Wydajność grafiki</b>	Zintegrowana karta graficzna.
<b>Komunikacja</b>	<p>Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika),</p> <p>Karta Wi-Fi min. 6E AX z Bluetooth 5.3</p>
<b>Wypożenie multimedialne</b>	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu (combo).

<b>Porty</b>	<p>Porty wlutowane w płytę główną i wyprowadzone bezpośrednio bez stosowania przejściówek, adapterów, rozgałęziaczy itp.:</p> <p>Panel przedni min.:</p> <ul style="list-style-type: none"> <li>a) 1 x Universal audio jack (słuchawki i mikrofon)</li> <li>b) 1 x USB 3.2 Gen 1 typu A</li> <li>c) 1 x USB 3.2 Gen 1 typu C</li> </ul> <p>Panel tylny min.:</p> <ul style="list-style-type: none"> <li>a) 1 x DisplayPort 1.4a</li> <li>b) 1 x HDMI 2.1</li> <li>c) 2 x USB 3.2 Gen 1 typ A</li> <li>d) 2 x USB 2.0</li> <li>e) 1 x RJ45 10/100/1000</li> </ul> <p>Dodatkowy port wyprowadzony z płyty głównej zamontowany na tylnym panelu I/O bez zajmowania slotów dla kart rozszerzeń:</p> <ul style="list-style-type: none"> <li>a) 1x HDMI 2.1.</li> </ul>
<b>Bezpieczeństwo</b>	<p>Dedykowany układ sprzętowy TPM min. 2.0.</p> <p>Komputer musi być wyposażony w czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzającym – diagnostycznym.</p> <p>Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (wbudowane w obudowę gniazdo blokady Kensington lub równoważnej w zakresie wytrzymałości) oraz kłódki (oczko w obudowie do założenia kłódki).</p>
<b>Ochrona oprogramowania układowego</b>	<p>Komputer wyposażony w mechanizm weryfikacji i ochrony BIOS/UEFI, działający automatycznie przy każdym uruchomieniu komputera poza warstwą systemu operacyjnego oraz w samym środowisku systemu operacyjnego. Mechanizm musi umożliwiać ochronę oprogramowania układowego poprzez weryfikację integralności BIOS/UEFI pod kątem próby jego modyfikacji oraz ataku w trakcie rozruchu komputera (również podczas uruchamiania systemu operacyjnego). Weryfikacja poprawności BIOS/UEFI musi odbywać się poza hostem.</p>
<b>BIOS/UEFI</b>	<p>Możliwość odczytania z BIOS informacji o:</p> <ul style="list-style-type: none"> <li>a) Wersji BIOS</li> <li>b) Numerze seryjnym komputera</li> <li>c) Numerze inwentarzowym</li> <li>d) Typie (modelu) procesora</li> <li>e) Ilości rdzeni</li> <li>f) Ilości pamięci RAM, jej prędkości oraz obsadzeniu w slotach</li> <li>g) Pojemności i modelu zainstalowanego dysku</li> <li>h) MAC adresie zintegrowanej karty sieciowej</li> <li>i) Technologii zdalnego zarządzania (o ile występuje)</li> </ul> <p>BIOS musi umożliwiać:</p> <ul style="list-style-type: none"> <li>a) Włączenie/wyłączenie zintegrowanej karty sieciowej</li> </ul>

	<ul style="list-style-type: none"> <li>b) Włączenie/wyłączenie karty sieci bezprzewodowej oraz Bluetooth (o ile występuje)</li> <li>c) Włączenie/wyłączenie karty audio</li> <li>d) Włączenie/wyłączenie poszczególnych portów USB</li> </ul> <p>Powyższa funkcjonalność musi być realizowana wyłącznie poprzez BIOS. Nie dopuszcza się realizacji poprzez dodatkowe oprogramowanie, takie jak np. System diagnostyczny.</p>
<b>BIOS/UEFI bezpieczeństwo</b>	<p>W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa danych organizacji, BIOS/UEFI musi umożliwiać:</p> <ul style="list-style-type: none"> <li>a) Nadanie hasła administratora</li> <li>b) Ustawienie hasła dla zainstalowanego dysku</li> <li>c) Ustawienie portów USB w trybie „No BOOT”</li> <li>d) Zarządzanie funkcją Wake on Lan oraz PXE Boot zintegrowanej karty sieciowej</li> <li>e) Zarządzanie funkcją Secure Boot</li> <li>f) Zarządzanie układem TPM</li> <li>g) Zarządzanie funkcją tworzenia recovery BIOS</li> <li>h) Zarządzanie funkcją downgrade BIOS</li> <li>i) Zarządzanie czujnikiem otwarcia obudowy</li> <li>j) Zapisywanie incydentów w formacie tzw. logów z możliwością ich przejrzenia</li> <li>k) Bezpieczne usuwanie danych z zainstalowanego dysku zgodnie z wytycznymi NIST 800-88r1</li> <li>l) Nadanie numeru inwentarzowego bezpośrednio w BIOS bez użycia dodatkowego oprogramowania. Nadany numer nie może być edytowalny w BIOS ani nie może ulec skasowaniu po jego aktualizacji.</li> <li>m) Możliwość nadania hasła uniemożliwiającego rozruch systemu operacyjnego, możliwość zmiany tego hasła w BIOS musi być zachowana także po nadaniu hasła administratora</li> <li>n) Możliwość blokowania upgrade BIOS przez system operacyjny</li> <li>o) Blokowanie downgrade BIOS w celu zapewnienia kompatybilności z poprawkami systemu operacyjnego.</li> </ul> <p>Powyższa funkcjonalność musi być realizowana wyłącznie poprzez BIOS. Nie dopuszcza się realizacji poprzez dodatkowe oprogramowanie, takie jak np. System diagnostyczny.</p>
<b>Oprogramowanie diagnostyczne</b>	<p>System diagnostyczny z graficznym interfejsem użytkownika, działający poza środowiskiem systemu operacyjnego, dostępny z poziomu BIOS lub szybkiego menu boot'owania.</p> <p>System umożliwiający przetestowanie komponentów bez konieczności uruchamiania systemu operacyjnego. Pełna obsługa systemu diagnostycznego za pomocą klawiatury i myszy jak i samej myszy.</p>

<b>Zintegrowany wizualny system diagnostyczny</b>	<p>Wbudowany wizualny system diagnostyczny usytuowany na przednim panelu obudowy, działający w oparciu o sygnalizację LED wbudowaną np. w przycisk włącznika komputera.</p> <p>System służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami poprzez zmianę statusów wyświetlania diody (miganie w określonej sekwencji oraz zmiana barw wyświetlania).</p> <p>System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS'u, awarię procesora.</p> <p>Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wewnątrz zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji, a które nie są dedykowane dla systemu diagnostycznego.</p>
<b>Zasilacz</b>	<p>Zasilacz o mocy min. 180W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%.</p>
<b>Zdalne zarządzanie</b>	<p>Wbudowana w płytę główną technologia zdalnego monitorowania i zarządzania komputerem na poziomie sprzętowym (out-of-band) działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC. Wymagana jest obsługa funkcji zdalnego zarządzania przez wbudowane w komputer porty zarówno sieci przewodowej LAN, jak i bezprzewodowej WLAN, z wykorzystaniem protokołów TCP/IP w tym IPv6 wraz z szyfracją komunikacji zarządzania z silnym protokołem minimum TLS 1.2 i zestawami silnych szyfrów TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384; TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 &amp; TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 lub silniejszymi/nowocześniejszymi.</p> <p>Technologia ta powinna być zgodna z otwartymi standardami DMTF WS-MAN 1.0.0 (<a href="http://www.dmtf.org/standards/wsman">http://www.dmtf.org/standards/wsman</a>) oraz DASH 1.2.0 (<a href="http://www.dmtf.org/standards/mgmt/dash">http://www.dmtf.org/standards/mgmt/dash</a>) oraz musi obsługiwać łącznie wszystkie następujące funkcje:</p> <ol style="list-style-type: none"> <li>Zdalny odczyt konfiguracji komponentów komputera – model komputera i jego nr seryjny, model procesora, ilość, rodzaj i nr seryjne modułów pamięci RAM, model i nr seryjny dysku HDD/SSD, wersja BIOS FW płyty głównej, nr seryjny płyty głównej, dla laptopów, model, znamionowa pojemność, numer seryjny i data produkcji baterii.</li> <li>Kontrolę stanu zasilania komputera pozwalającą na sprawdzenie aktualnego stanu zasilania komputera (stany ACPI S0/S3/S4/S5) oraz zdalne włączenie komputera ze stanu pełnego wyłączenia, hibernacji, uśpienia i tzw. Modern Standby (Connected Standby) lub równoważnego w zakresie uruchamiania komputera oraz zdalne wyłączenie/reset bez udziału systemu operacyjnego.</li> </ol>

	<p>c) Zdalną konfigurację ustawień komputera przez interfejs BIOS setup w trybie graficznym lub tekstowym (ASCII).</p> <p>d) Zdalne przejście konsoli tekstowej systemu – tzw. Text Console Redirection lub Serial over LAN z możliwością jej wykorzystania do zdalnej zmiany ustawień BIOS Setup oraz odblokowania MS BitLocker Recovery używanego obecnie u Zamawiającego.</p> <p>e) Zdalne przejście pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse), na poziomie sprzętowym bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego do rozdzielczości 2560×1600 (WQXGA) włącznie zgodnie z profilem DSP1076 standardu DASH</p> <p>Funkcja przekierowania konsoli graficznej musi przechwytywać każdy rodzaj wyświetlanego na fizycznym lokalnym ekranie obrazu, włącznie z procesem uruchamiania komputera (POST), odblokowania systemu szyfracji dysku, ładowania OS z dowolnego nośnika, zamykania OS oraz błędów ww. procesów: POST, ładowania OS (np. brak nośnika uruchamiającego, uszkodzenia OS BSOD (Blue Screen of Death) bez potrzeby modyfikacji tzw. loadera OS.</p>
<b>Wirtualizacja</b>	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
<b>System operacyjny</b>	Zainstalowany system operacyjny typu Windows 11 Pro (używany obecnie u Zamawiającego), lub równoważny, klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać reinstalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego. Za system równoważny Zamawiający nie uznaje systemu Linux.
<b>Certyfikaty standardy</b>	i <ol style="list-style-type: none"> <li>1. Certyfikat ISO 9001 dla producenta komputera lub równoważny w zakresie jakości</li> <li>2. Certyfikat ISO 14001 dla producenta komputera lub równoważny w zakresie zarządzania środowiskiem</li> <li>3. Certyfikat ISO 50001 dla producenta komputera lub równoważny w zakresie zarządzania energią</li> </ol>
<b>Ergonomia</b>	<p>Głośność jednostki centralnej może wynosić maksymalnie 25dB według oficjalnego dokumentu producenta. Głośność musi być zmierzona zgodnie z:</p> <ul style="list-style-type: none"> <li>• normą ISO 7779 lub równoważną w zakresie pomiaru hałasu emitowanego przez sprzęt informatyczny oraz</li> <li>• wykazaną zgodnie z normą ISO 9296 lub równoważną w zakresie ustalania wartości emisji hałasu dla sprzętu informatycznego, w pozycji obserwatora w trybie pracy dysku twardego (IDLE).</li> </ul>
<b>Wymagania dodatkowe</b>	<p>Napęd optyczny DVD +/-RW o prędkości min. 8x zamontowany w dedykowanej wnęce zewnętrznej 5.25” typu slim.</p> <p>Dołączony nośnik ze sterownikami</p>

	<p>Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie oraz musi być wpisany na stałe w BIOS.</p>
<b>Warunki gwarancji</b>	<p>Dedykowany portal techniczny producenta lub Wykonawcy, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.</p> <p>Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta lub Wykonawcę (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego)</p> <p>Nie krótsza niż 36-miesięczna gwarancja producenta świadczona na miejscu u klienta. Czas reakcji serwisu - nie później niż do końca następnego dnia roboczego.</p> <p>W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.</p>
<b>Dodatkowe oprogramowanie</b>	<p>Dołączone do oferowanego komputera oprogramowanie z nieograniczoną licencją czasowo na użytkowanie umożliwiające:</p> <ul style="list-style-type: none"> <li>• upgrade i instalacje wszystkich sterowników, dostarczonych w obrazie systemu operacyjnego producenta, BIOS'u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,</li> <li>• możliwość przed instalacją sprawdzenia każdego sterownika, BIOS'u bezpośrednio na stronie producenta lub Wykonawcy przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji o:             <ol style="list-style-type: none"> <li>a. poprawkach i usprawnieniach dotyczących aktualizacji</li> <li>b. dacie wydania ostatniej aktualizacji</li> <li>c. priorytecie aktualizacji</li> <li>d. zgodności z systemami operacyjnymi</li> <li>e. jakiego komponentu sprzętu dotyczy aktualizacja</li> <li>f. wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.</li> </ol> </li> <li>• wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne</li> <li>• możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji, która tego wymaga.</li> <li>• rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informacji, kiedy dokonany został ostatnio upgrade, w szczególności z uwzględnieniem daty (dd-mm-rrrr)</li> <li>• sprawdzenia historii upgrade'u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją (rewizja wydania)</li> </ul>

	<ul style="list-style-type: none"> <li>dokładny wykaz wymaganych sterowników, aplikacji, BIOS'u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu *.xml</li> <li>raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach, zainstalowanych aktualizacjach z dokładnym rozbiem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku *.xml. Raport musi zawierać z dokładną datą (dd-mm-rrrr) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku.</li> </ul> <p>Oprogramowanie umożliwiające aktualizację BIOS bezpośrednio z serwera producenta komputera lub Wykonawcy przy wykorzystaniu bezpiecznego, szyfrowanego połączenia bez konieczności uruchamiania systemu operacyjnego oraz wykorzystywania zewnętrznych nośników pamięci masowej.</p> <p>Oprogramowanie musi automatycznie rozpoznawać model urządzenia i bieżącą wersję BIOS.</p> <p>Oprogramowanie posiadające bezterminową licencję.</p> <p>Możliwość zabezpieczenia dostępu do oprogramowania hasłem administratora.</p> <p>Oprogramowanie umożliwiające przywrócenie obrazu systemu operacyjnego bezpośrednio z serwera producenta komputera przy wykorzystaniu bezpiecznego, szyfrowanego połączenia bez konieczności uruchamiania systemu operacyjnego.</p> <p>W przypadku wystąpienia awarii oprogramowanie automatycznie uruchomi się i zapewni możliwość naprawy systemu operacyjnego lub przywrócenie go do stanu fabrycznego z możliwością dokonania kopii zapasowej plików przed uruchomieniem procesu.</p> <p>Dodatkową funkcją oprogramowania jest możliwość wykonania kopii dysku (tzw. klonowania) wraz z plikami, ustawieniami aplikacji, systemem operacyjnym i jego ustawieniami.</p> <p>Licencja pozwalająca na bezpłatne korzystanie z oprogramowania przez cały okres gwarancji komputera, jednak nie krótszą niż 36 miesięcy.</p>
<b>Dostępność dla osób z niepełnosprawnościami</b>	<p>Komputery stacjonarne muszą dysponować następującymi funkcjonalnościami, dzięki którym będą dostępne osobom z niepełnosprawnościami:</p> <ol style="list-style-type: none"> <li>Ergonomiczna i dostępna obudowa – łatwy dostęp do portów (USB) umieszczonych z przodu obudowy, możliwość ustawienia jednostki centralnej na biurku lub pod nim</li> <li>Wsparcie dla urządzeń wspomagających – możliwość podłączenia np. specjalistycznych klawiatur, myszy ergonomicznych</li> <li>Wsparcie systemowe i aktualizacje – system operacyjny z regularnymi aktualizacjami oraz wbudowanymi funkcjami dostępności (np. narracja, rozpoznawanie mowy)</li> </ol>



<b>Zasada DNSH</b>	<p>Zamówienie będzie zgodne z zasadą DNSH „niewyrządzania znaczącej szkody środowisku” (DNSH – „do no significant harm”) w rozumieniu art. 17 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2020/852 z dnia 18 czerwca 2020 r. w sprawie ustanowienia ram ułatwiających zrównoważone inwestycje, zmieniającego rozporządzenie (UE) 2019/2088 (Dz. U. UE. L. z 2020 r. Nr 198, str.13 z późn. zm.), czego potwierdzeniem będzie m.in.:</p> <ul style="list-style-type: none"> <li>a) w odniesieniu do zasady: Łagodzenie zmian klimatu</li> <li>b) w odniesieniu do zasady: Przejście na gospodarkę o obiegu zamkniętym: <ul style="list-style-type: none"> <li>a. dostawa zostanie zrealizowana przy jak najmniejszej liczbie opakowań w celu ograniczenia ilości odpadów,</li> <li>b. opakowania (tam, gdzie to możliwe) będą wykonane z materiałów podlegających powtórnemu przetworzeniu</li> </ul> </li> <li>c) w trakcie instalacji komputerów stacjonarnych zapewnione zostaną rozwiązania ograniczające ryzyko powstania nadmiernej liczby odpadów, w tym niepodlegających recyklingowi</li> <li>d) elementy składające się na komputery stacjonarne nie posiadają cech szkodliwych dla stanu zachowania siedlisk i gatunków, w tym siedlisk i gatunków objętych zakresem zainteresowania Unii Europejskiej.</li> </ul>
--------------------	--

**Monitor – ilość: 130 szt.**

Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
<b>Typ ekranu</b>	Ekran ciekłokrystaliczny z aktywną matrycą IPS o przekątnej min. 26.95”
<b>Rozmiar plamki (maksymalnie)</b>	0,312 mm x 0,312 mm
<b>Jasność</b>	Minimum 300 cd/m2
<b>Kontrast statyczny</b>	1500:1
<b>Kąty widzenia (pion/poziom)</b>	Minimum 178/178 stopni
<b>Czas reakcji matrycy (maksymalnie)</b>	8ms (gray to gray)
<b>Rozdzielczość maksymalna</b>	1920 x 1080 przy 100Hz (dotyczy cyfrowych portów wideo)
<b>Gama koloru</b>	sRGB 99%
<b>Pochylenie monitora</b>	W zakresie 26 stopni
<b>Wydłużenie w pionie</b>	Tak, min. 150 mm
<b>PIVOT</b>	Tak
<b>Obrót lewo/prawo</b>	W zakresie min. (-45/+45) stopni
<b>Powłoka powierzchni ekranu</b>	Antyodblaskowa
<b>Podświetlenie</b>	System podświetlenia LED
<b>Zużycie energii</b>	Całkowite zużycie energii (kWh/rok): maks. 45 kWh rocznie



	Dane zużycia do zweryfikowania na stronie Energy Star: <a href="https://www.energystar.gov/productfinder/">https://www.energystar.gov/productfinder/</a>
<b>Bezpieczeństwo</b>	Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą
<b>Złącze (min.)</b>	<ul style="list-style-type: none"> <li>• x HDMI 1.4,</li> <li>• x DisplayPort 1.2,</li> <li>• x VGA,</li> <li>• x USB 3.2 Gen 1 typu A</li> <li>• x USB 3.2 Gen 1 typu C</li> <li>• 1 x USB 3.2 Gen 1 typu B</li> </ul>
<b>Gwarancja</b>	<p>Czas trwania gwarancji - min. 36 miesięcy.</p> <p>Czas reakcji serwisu - nie później niż do końca następnego dnia roboczego</p> <p>Wykonawca lub firma, któremu będzie zlecona usługa serwisowania musi posiadać spełniać wymagania normy ISO 9001 lub równoważnej w zakresie standardów świadczenia usług serwisowych. Czas naprawy nie może przekraczać 60 dni.</p>
<b>Certyfikaty</b>	<ol style="list-style-type: none"> <li>1. Certyfikat ISO 9001 dla producenta monitora lub równoważny w zakresie jakości</li> <li>2. Certyfikat ISO 14001 dla producenta monitora lub równoważny w zakresie zarządzania środowiskiem</li> <li>3. Deklaracja zgodności CE</li> </ol>
<b>Inne</b>	Odtaczany stand bez użycia narzędzi VESA 100mm.
<b>Dodatkowe oprogramowanie</b>	<p>Dołączone oprogramowanie producenta monitora z bezterminową licencją na użytkowanie, umożliwiające zarządzanie oferowanym monitorem bezpośrednio z poziomu systemu operacyjnego podłączonego komputera w zakresie:</p> <ol style="list-style-type: none"> <li>a) Konfiguracji ustawień wyświetlania obrazu, w tym min:             <ol style="list-style-type: none"> <li>a. jasność i kontrast (w trybie ręcznym oraz według ustalonego przez użytkownika harmonogramu),</li> <li>b. kolor (w trybie ręcznym oraz automatycznym dla określonych aplikacji),</li> <li>c. rozdzielczość wyświetlania, częstotliwość odświeżania ekranu oraz orientacja ekranu.</li> </ol> </li> <li>b) Sposobu wyświetlania wielu okien poszczególnych aplikacji jednocześnie w predefiniowanym lub niestandardowym (stworzonym przez użytkownika) układzie, z możliwością przypisania układu wyświetlania okien do konkretnych aplikacji.</li> <li>c) Aktualizacji oprogramowania układowego monitora oraz oprogramowania zarządzającego.</li> <li>d) Możliwość wyeksportowania oraz importowania ustawień.</li> </ol>
<b>Dostępność dla osób z niepełnosprawnościami</b>	Monitory muszą dysponować następującymi funkcjonalnościami, dzięki którym będą dostępne osób z niepełnosprawnością:

	<ul style="list-style-type: none"> <li>• Możliwość regulacji wysokości, kąta nachylenia</li> <li>• Możliwość zmiany kontrastu, jasności i nasycenia kolorów</li> <li>• Podstawa lub możliwość montażu VESA, co pozwala na bezpieczne dostosowanie stanowiska pracy do indywidualnych potrzeb</li> </ul>
<b>Zasada DNSH</b>	<p>Zamówienie będzie zgodne z zasadą DNSH „niewyrządzania znaczącej szkody środowisku” (DNSH – „do no significant harm”) w rozumieniu art. 17 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2020/852 z dnia 18 czerwca 2020 r. w sprawie ustanowienia ram ułatwiających zrównoważone inwestycje, zmieniającego rozporządzenie (UE) 2019/2088 (Dz. U. UE. L. z 2020 r. Nr 198, str.13 z późn. zm.), czego potwierdzeniem będzie m.in.:</p> <p>a) w odniesieniu do zasady: Przejście na gospodarkę o obiegu zamkniętym:</p> <ul style="list-style-type: none"> <li>• dostawa zostanie zrealizowana przy jak najmniejszej liczbie opakowań w celu ograniczenia ilości odpadów,</li> <li>• opakowania (tam, gdzie to możliwe) będą wykonane z materiałów podlegających powtórnemu przetworzeniu</li> <li>• w trakcie instalacji monitorów zapewnione zostaną rozwiązania ograniczające ryzyko powstania nadmiernej liczby odpadów, w tym niepodlegających recyklingowi</li> </ul> <p>b) w odniesieniu do zasady: ochrona i odbudowa bioróżnorodności i ekosystemów:</p> <ul style="list-style-type: none"> <li>• elementy składające się na monitory nie posiadają cech szkodliwych dla stanu zachowania siedlisk i gatunków, w tym siedlisk i gatunków objętych zakresem zainteresowania Unii Europejskiej.</li> </ul>

#### 4. Część 4 - Wdrożenie wirtualnych stanowisk pracy

Przedmiotem zamówienia jest dostawa **2 (dwóch)** serwerów VDI, przeznaczonych do obsługi wirtualnych stanowisk pracy w środowisku Zamawiającego, wraz z usługą instalacji i konfiguracji.

##### 4.1. Zakres wdrożenia

W ramach realizacji zamówienia Wykonawca zobowiązany jest do:

- przekazania Zamawiającemu dokumentacji potwierdzającej instalację.

W ramach realizacji zamówienia Wykonawca zobowiązuje się do wykonania następujących czynności:

- **Dostawa oraz fizyczna instalacja infrastruktury VDI** w lokalizacji wskazanej przez Zamawiającego, obejmująca montaż urządzeń, okablowanie oraz podłączenie do zasilania i sieci LAN zgodnie z obowiązującymi standardami.
- **Aktualizacja oprogramowania sprzętowego (firmware) oraz oprogramowania systemowego komponentów VDI** do najnowszych stabilnych wydań zalecanych przez producenta, zapewniających pełne wsparcie i kompatybilność.
- **Instalacja oraz uruchomienie platformy wirtualizacyjnej dla środowiska VDI**, obejmująca konfigurację klastrów, zasobów obliczeniowych, magazynu danych i sieci wirtualnych.

Zamawiający wymaga dostarczenia serwerów (ilość: 2 sztuki) na potrzeby środowiska wirtualnych stanowisk pracy spełniających poniższe funkcjonalności:

Nazwa elementu, parametru lub cechy	Opis wymagań serwera
<b>Obudowa</b>	Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Wymagana możliwość instalacji ramienia do zarządzania okablowaniem.
<b>Procesor</b>	Architektura x86, maksymalny TDP dla procesora – maksymalnie 210W. Minimalna częstotliwość pracy procesora 3.0GHz. Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być niższy niż 873 punkty base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org ( <a href="http://www.spec.org">www.spec.org</a> ) dla konfiguracji dwuprocesorowej.
<b>Liczba procesorów</b>	2
<b>Płyta główna</b>	Płyta główna dedykowana do pracy w serwerach musi posiadać możliwość zainstalowania minimum dwóch procesorów wykonujących 64-bitowe instrukcje.
<b>Pamięć operacyjna</b>	Zainstalowane minimum 1.1TB pamięci RAM o częstotliwości 6400MHz. Minimum 24 sloty na pamięć. Możliwość rozbudowy do 6TB RAM.
<b>Zabezpieczenie pamięci</b>	Min. ECC, SDDC, ADDDC, Patrol/Demand Scrubbing, On-die ECC, Post Package Repair, Bounded Fault, DRAM Address Command Parity with Replay.
<b>Procesor Graficzny</b>	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. Min. 1 port VGA na tylnym panelu oraz jeden port VGA na przednim panelu.
<b>Rozbudowa dysków</b>	<p>W chwili dostawy serwer musi posiadać zainstalowane minimum 2 sztuki dysków M.2 o pojemności przynajmniej 480 GB sterowanych dedykowanym kontrolerem sprzętowym umożliwiającym redundancję raid-1.</p> <p>Dyski oraz dedykowany kontroler nie mogą zajmować żadnego slotu pci wymienionego w punkcie <b>Dodatkowe sloty I/O</b>. Wymagane parametry zainstalowanych dysków:</p> <ul style="list-style-type: none"> <li>• DWPD (5 lat): minimum 1,</li> <li>• TBW: minimum 870,</li> <li>• MTBF: przynajmniej 2mln godzin,</li> <li>• wydajność dla losowych odczytów: min. 81 000 iops,</li> <li>• wydajność dla losowych zapisów: min. 14 000 iops</li> </ul> <p>Wymagana możliwość rozbudowy serwera na potrzeby instalacji przynajmniej 16 sztuk dysków, przy czym wszystkie zatoki dyskowe powinny umożliwiać instalację wymiennie (bez konieczności jakichkolwiek zmian) dysków SAS oraz NVMe. Powinna być możliwość obsługi wszystkich 16 sztuk dysków niezależnie od tego czy są to</p>

	dyski SAS czy NVMe lub zarówno SAS jak i NVMe, poprzez ten sam sprzętowy kontroler raid.
<b>Kontroler dyskowy</b>	<p>Wymagana jest możliwość zainstalowania w serwerze sprzętowego kontrolera dyskowego wyposażonego w przynajmniej 4GB cache oraz obsługującego min. poziomy RAID 0/1/10/5/50/6/60. W przypadku awarii zawartość cache powinna być kopiowana do pamięci nieulotnej.</p> <p>Rozwiązania zapewniające tzw. podtrzymanie cache tylko przy użyciu baterii nie będą akceptowane.</p> <p>Kontroler powinien obsługiwać zarówno dyski SAS jak i dyski NVMe. Wymaga się obsługi globalnych dysków hot-spare. Kontroler powinien umożliwiać rozszerzanie pojemności skonfigurowanych logicznych przestrzeni dyskowych w trybie on-line.</p>
<b>Zasilacz</b>	Minimum dwa redundantne zasilacze o mocy minimum 2600W.
<b>Interfejsy sieciowe</b>	<p>Zainstalowane przynajmniej dwie dwuportowe karty 10Gb/25Gb wyposażone w dedykowane wkładki 10/25Gbs. Dla zachowania spójności procesu administracji, wymaga się, aby karty były tego samego producenta.</p> <p>Wymagana funkcjonalność portów 10/25Gbs: min. sprzętowa obsługa protokołów VXLAN, NVGRE, GENEVE, funkcjonalność RoCEv2, obsługa ruchu sieciowego z podziałem na poszczególne maszyny wirtualne poprzez bezpośrednie przypisanie maszyn wirtualnych do karty - obsługa do 512 przypisań. Karty sieciowe powinny zapewniać bezpieczeństwo aktualizacji oprogramowania układowego z użyciem kluczy RSA. Wymagana jest obsługa funkcjonalności Root-of-trust.</p> <p>Jeden port RJ-45 o przepustowości min. 1GbE dedykowany dla karty zarządzającej.</p> <p>Wymagana możliwość zainstalowania drugiego redundantnego portu 1Gbs dedykowanego dla karty zarządzającej.</p> <p>Zainstalowane przynajmniej dwa porty Fiber Channel 32Gbs.</p>
<b>Karty GPU</b>	<p>W chwili dostawy serwer powinien być wyposażony w przynajmniej dwie karty GPU posiadające przynajmniej 48GB pamięci każda o przepustowości przynajmniej 864GB/s. Wymagana wydajność karty GPU: przynajmniej 91.6 TFLOPS w teście FP32 performance oraz przynajmniej 1466 TOPS w teście INT8 integer. Maksymalne zużycie mocy nie powinno przekraczać 350W. Karta powinna posiadać przynajmniej 4 porty DisplayPort 1.4a.</p> <p>Dostarczony serwer powinien umożliwiać instalację dodatkowej (trzeciej) karty GPU bez konieczności jakiegokolwiek zmiany wewnętrznej konfiguracji sprzętowej.</p>
<b>Dodatkowe sloty I/O</b>	Serwer w chwili dostawy musi posiadać minimum 6 slotów PCIe x16 Gen5. Wymagana jest możliwość rozbudowy serwera o dwa kolejne sloty PCIe Gen 5.
<b>Dodatkowe porty</b>	<ul style="list-style-type: none"> <li>• <u>z przodu obudowy</u>: min. 1x USB 3.2, 1x USB 2.0 (z możliwością zarządzania serwerem), zewnętrzny dedykowany port diagnostyczny, jeden port VGA</li> <li>• <u>z tyłu obudowy</u>: min. 3x USB 3.2, 1x VGA, 1x RJ-45 do zarządzania serwerem. Możliwość instalacji portu DB9.</li> <li>• <u>wewnątrz obudowy</u>: min. 1x USB 3.2</li> </ul>

	Tylnie porty USB, port RJ-45 służący do zarządzania, tylny port VGA, wewnętrzny port USB, wewnętrzny port na kartę Micro SD będą umieszczone na osobnej dedykowanej płycie I/O, którą łączy się bezpośrednio z płytą główną serwera.
<b>Chłodzenie</b>	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
<b>Zarządzanie</b>	<p>Na potrzeby administracji lokalnej, wraz z serwerem musi być dostarczony przenośny panel LCD podłączany do portu na przednim panelu serwera, umożliwiający wyświetlenie poniższych informacji:</p> <ul style="list-style-type: none"> <li>a) Aktywne ostrzeżenia</li> <li>b) Status serwera</li> <li>c) Typ oraz model serwera, numer seryjny</li> <li>d) Wersje oprogramowania UEFI oraz modułu zarządzania</li> <li>e) Informacje nt. modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS</li> <li>f) Dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii</li> <li>g) Aktywne sesje połączeniowe do interfejsu zarządzania</li> <li>h) Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, posiadający poniższe funkcjonalności:             <ul style="list-style-type: none"> <li>• Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna)</li> <li>• Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres IP karty zarządzającej, użycie CPU, użycie pamięci oraz komponentów I/O, lokalizacji</li> <li>• Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów</li> <li>• Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń</li> <li>• Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3</li> <li>• Update systemowego firmware</li> <li>• Monitoring i możliwość ograniczenia poboru prądu</li> <li>• Zdalne włączanie/wyłączanie/restart</li> <li>• Zapis video zdalnych sesji</li> <li>• Podmontowanie lokalnych mediów z wykorzystaniem Java client, które jest wykorzystywane u Zamawiającego</li> <li>• Przekierowanie konsoli szeregowej przez IPMI</li> <li>• Zrzut ekranu w momencie zawieszenia systemu</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• Możliwość przejęcia zdalnego ekranu</li> <li>• Możliwość zdalnej instalacji systemu operacyjnego</li> <li>• Alerty Syslog</li> <li>• Przekierowanie konsoli szeregowej przez SSH</li> <li>• Wyświetlanie danych aktualnych i historycznych dla użycia energii oraz temperatury serwera</li> <li>• Możliwość mapowania obrazów ISO z lokalnego dysku operatora</li> <li>• Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS</li> <li>• Możliwość jednoczesnej pracy dla min. 6 użytkowników przez wirtualną konsolę</li> <li>• wspierane protokoły/interfejsy: min. IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API</li> <li>• Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiegokolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.</li> <li>• Kontroler zarządzania musi posiadać min. 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.</li> <li>• Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.</li> <li>• Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.</li> <li>• Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.</li> </ul> <p>Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające:</p> <ol style="list-style-type: none"> <li>a) Zarządzanie infrastrukturą serwerową storage bez udziału dedykowanego agenta</li> <li>b) Przedstawianie graficznej reprezentacji zarządzanych urządzeń</li> <li>c) Możliwość skalowania do minimum 1000 urządzeń</li> <li>d) Obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla norm NIST 800-131A oraz FIPS 140-2</li> <li>e) Wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych</li> <li>f) Udostępnianie szybkiego podglądu stanu środowiska</li> </ol>
--	---

	<ul style="list-style-type: none"> <li>g) Udostępnianie podsumowania stanu dla każdego urządzenia</li> <li>h) Tworzenie alertów przy zmianie stanu urządzenia</li> <li>i) Monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii,</li> <li>j) Konsola zarządzania oparta o HTML 5</li> <li>k) Dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, obecnie używanych u Zamawiającego, aplikacja musi umożliwiać włączenie, wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu,</li> <li>l) Automatyczne wykrywanie dołączanych systemów</li> <li>m) Możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta lub dostawcy oferowanego rozwiązania</li> <li>n) Definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzeń</li> <li>o) Definiowanie roli użytkowników oprogramowania</li> <li>p) Obsługa REST API oraz Windows PowerShell wykorzystywane obecnie u Zamawiającego</li> <li>q) Obsługa protokołów SNMP, SYSLOG</li> <li>r) Autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z Microsoft Active Directory oraz obsługa single sign on oraz SAML, używane obecnie u Zamawiającego</li> <li>s) Obsługa tzw. Forward Secrecy w komunikacji z zarządzanymi urządzeniami</li> <li>t) Przedstawianie historycznych aktywności użytkowników</li> <li>u) Blokowanie możliwości podłączenia innego systemu zarządzania do urządzeń zarządzanych</li> <li>v) Tworzenie dziennika zdarzeń ukończonych sukcesem lub błędem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku min. csv</li> <li>w) Obsługa NTP</li> <li>x) Przesyłanie alertów do konsoli firm trzecich</li> <li>y) Tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsolę albo kopiowanie konfiguracji z już zaimplementowanych urządzeń)</li> <li>z) Instalowanie systemów operacyjnych oraz wirtualizatorów VMware i Hyper-V, obecnie używanych u Zamawiającego. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie</li> </ul>
--	---



	aa) Możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta lub dostawcy dla określonych zdarzeń wraz z przesyłem plików diagnostycznych.
<b>Funkcje zabezpieczeń</b>	<p>Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł RoT wspierający TPM2.0</p> <p>Zainstalowany przedni panel zabezpieczający zamykany na klucz. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. Możliwość włączania i wyłączenia portów USB na obudowie z poziomu UEFI. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem. Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej.</p> <p>Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.</p>
<b>Urządzenia hot swap</b>	Możliwość odłączania elementów bez wyłączenia urządzenia - Dyski twarde, zasilacze, wentylatory.
<b>Diagnostyka</b>	<p>Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID</p> <p>Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.</p>
<b>Obsługiwane systemy operacyjne</b>	Min. Microsoft Windows Server 2019, 2022; Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1, SUSE Linux Enterprise Server 15 SP4 oraz 15 Xen SP4; VMware vSphere (ESXi) 7.0 U3, ESXi 8.0; Ubuntu 20.04 LTS, 22.04 LTS
<b>Waga</b>	Maximum: 38.8kg
<b>Gwarancja</b>	<p>Nie mniej niż 36 miesięcy gwarancji producenta z czasem reakcji onsite nie późniejszym niż w następnym dniu roboczym od momentu zgłoszenia usterki. Wymagana obsługa zgłoszeń w trybie 24/7. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalnie jak i wydajnościowo wymagane powyżej urządzenie. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera.</p> <p>Wymagana jest możliwość rozszerzenia wsparcia serwisowego do poziomu z gwarantowanym czasem naprawy w czasie maksymalnie 24 godzin od momentu zgłoszenia usterki.</p>