RW.VI.271.17.2024 Załącznik Nr 6 do SWZ

Szczegółowy opis przedmiotu zamówienia

zamówienia publicznego pn. „Cyberbezpieczny Samorząd dla Gminy Sędziejowice" realizowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy (FERC), Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, Europejski Fundusz Rozwoju Regionalnego (EFRR), Numer naboru FERC.02.02-CS.01-001/23.

1. Serwer – 2 sztuki.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	• Minimum 256GB DDR5 RDIMM 4800MT/s,
Funkcjonalność pamięci RAM	• Demand Scrubbing, • Patrol Scrubbing, • Permanent Fault Detection (PFD)
Gniazda PCI	• Min. dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • Dodatkowa karta Dual Port (2x SFP+, 10Gb/s , SFP+, PCIe)
Dyski twarde	• Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Wbudowane porty	• 4x USB, w tym min. 1 porty USB 3.0 • 2x port VGA (jeden na panelu przednim) • Możliwość rozbudowy o Serial Port
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	• Redundantne, Hot-Plug
Zasilacze	• Redundantne, Hot-Plug min. 1100W klasy Titanium
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

	• BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: • Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej • Przesyłanie danych telemetrycznych w czasie rzeczywistym • Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze • Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji

	• Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is" do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status

	„Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Możliwość rozszerzenia gwarancji Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: • Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. • Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. • Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. • Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.

	• Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

2. Patchcord światłowodowy wielomodowy- 1 sztuki.

Minimalne wymagania:	
Rodzaj patchcorda	wielomodowy
Typ transmisji światłowodowej	duplex
Typ włókna	OM3 50/125um
Rodzaj wtyków	LC- LC
Wytrzymałość włókna	>98.1 N
Tłumienność losowa, maksymalna	<0.4 dB
Tłumienność losowa, średnie	<0.3 dB
Element wzmacniający	włókna aramidowe / włókna szklane
Długość	100 m
Średnica	3 mm
Temperatura pracy	-40 do +85 °C

3. Patchcord światłowodowy wielomodowy - 1 sztuk.

Minimalne wymagania:	
Rodzaj patchcorda	wielomodowy
Typ transmisji światłowodowej	duplex
Typ włókna	OM3 50/125um
Rodzaj wtyków	LC/UPC - LC/UPC
Wytrzymałość włókna	145 N
Tłumienność wtrąceniowa	≤0.3 dB
Tłumienność odbiciowa	≥25 dB
Element wzmacniający	włókna aramidowe
Długość	50 m
Średnica	3 mm
Powłoka	LSOH
Temperatura pracy	-40 do +85 °C

Zastosowanie	wewnątrzbudynkowe

4. Patchcord światłowodowy wielomodowy – 16 sztuk.

Minimalne wymagania:	
Rodzaj patchcorda	wielomodowy
Typ transmisji światłowodowej	duplex
Typ włókna	OM3 50/125um
Rodzaj wtyków	LC/UPC - LC/UPC
Wytrzymałość włókna	145 N
Tłumienność wtrąceniowa	≤0.3 dB
Tłumienność odbiciowa	≥25 dB
Element wzmacniający	włókna aramidowe
Długość	3 m
Średnica	3 mm
Powłoka	LSOH
Temperatura pracy	-40 do +85 °C
Zastosowanie	wewnątrzbudynkowe
Cechy:	- Powtarzalność pomiarów, - Praca w szerokim zakresie temperatur, - Niska tłumienność, - Zgodne z normami EN-50173-1, EIA/TIA 568, EN 50377

5. Zarządzane urządzenia sieciowe z obsługą VLAN – 4 sztuk.

Minimalne wymagania:	
Port	SFP1000BASE-T 10/100/1000 RJ-45
Zasięg portu	100m
Okablowanie portu	UTP/STP kat. 5
Typ modułu	SFP
Okres gwarancji	36 miesięcy
Moduł kompatybilny z przełącznikami	Mikrotik, Ubiquiti, TP-LINK, D-LINK, Netgear, Zyxel, Planet, Cisco.

Zarządzane urządzenia sieciowe z obsługą VLAN - 16 sztuki.

Minimalne wymagania:	
Rodzaj modułu	SFP+
Typ transmisji	duplex
Prędkość transmisji	10 Gbps
Rodzaj złącza modułu optycznego	LC/UPC
Zasięg portu	0,3 km
Standard ethernet	10GBase-SR
Długość fali TX	850 nm
Długość fali RX	850 nm

Okablowanie	wielomodowe
Moc	-7 do -1 dBm
Czułość	-11 dBm
Temperatura pracy	0 do 70 °C
Napięcie zasilania	3,3 V
Moduł kompatybilny z przełącznikami	Mikrotik, Ubiquiti, TP-LINK, D-LINK, Netgear, Zyxel, Planet.

Zarządzane urządzenia sieciowe z obsługą VLAN - 1 sztuki.

Minimalne wymagania:	
Procesor taktowanie	800 MHz
Pamięć RAM	512 MB
Pamięć wbudowana	16 MB
Rodzaj pamięci wbudowanej	Flash
Sloty SFP	20
Sloty SFP+	4
Porty Combo SFP / Ethernet	4
Port serial	RJ45
Napięcie wejściowe	100 - 240 V AC
Maksymalny pobór mocy	43 W
Dopuszczalna temperatura pracy	Od -20 do 60 st. C

8. Zarządzane urządzenia sieciowe z obsługą VLAN - 2 sztuki.

Minimalne wymagania:	
Procesor taktowanie	650 MHz
Pamięć RAM	64 MB
Pamięć wbudowana	16 MB
Interfejsy	2x sloty 40Gb/s QSFP+ 4x sloty 10Gb/s SFP+ 48x portów gigabitowych 10/100/1000Mb/s 1x port Fast Ethernet 10/100Mb/s 1x serial port RJ45
Napięcie wejściowe	100 - 240 V AC
Maksymalny pobór mocy	60 W
Dopuszczalna temperatura pracy	Od -20 do 60 st. C
Zasilanie	2x wbudowane zasilacze redundantne

9. Zarządzane urządzenia sieciowe z obsługą VLAN - 1 sztuki.

Minimalne wymagania:

Procesor taktowanie	2000 MHz
Architektura CPU	ARM 64bit
Ilość rdzeni procesora	16
Pamięć RAM	16 GB DDR4
Pamięć wbudowana	128 MB NAND
Porty gigabit Ethernet	13x 1 Gb/s
Sloty SFP+	4x 10 Gb/s
lot PCIe M.2	1x
Napięcie wejściowe	100 - 240 V AC
Maksymalny pobór mocy	72 W
Dopuszczalna temperatura pracy	Od -20 do 60 st. C

10. Zarządzane urządzenia sieciowe z obsługą VLAN - 2 sztuki.

Minimalne wymagania:	
Procesor taktowanie	800 MHz
Pamięć RAM	512 MB
Pamięć wbudowana	Flash 16 MB
Porty Ethernet	24 gigabitowe porty 10/100/1000 Mb/s
Sloty SFP	2x SFP+
Port serial	RJ45
Zakres napięcia wejściowego	9 - 30 V DC
Maksymalny pobór mocy	24 W
Dopuszczalna temperatura pracy	Od -40 do 60 st. C

11. Zarządzane urządzenia sieciowe z obsługą VLAN - 1 sztuki.

Minimalne wymagania:	
Procesor taktowanie	800 MHz
Architektura procesora	ARM 32bit
Pamięć RAM	256 MB DDR3
Pamięć wbudowana	Flash 32 MB
Porty Ethernet	17x 1G
Sloty SFP+ (10 Gb/s)	4
Port serial	RJ45
Zakres napięcia AC	100 - 240 V
Maksymalny pobór mocy	1150 W
Dopuszczalna temperatura pracy	Od -10 do 50 st. C
Wyjście PoE	802.3 af/at/bt
Smart PoE	Kontroler
Wyjście PoE	Ether 1 - Ether 8 (af/at) Ether 9 - Ether 16 (bt)

12. Zarządzane urządzenia sieciowe z obsługą VLAN - 20 sztuki.

Minimalne wymagania:	
Rodzaj modułu	SFP
Okablowanie	jednomodowe
Tryb transmisji	WDM
Prędkość transmisji	1,25 Gbps
Rodzaj złącza modułu optycznego	SC/UPC
Zasięg portu	3 km
Standard ethernet	1000Base-BX
Długość fali TX	1310 nm
Długość fali RX	1550 nm
Moc (tx power)	-12 do -24 dBm
Czułość (rx sensitivity)	-22 dBm
Napięcie zasilania	3,3 V
Temperatura pracy	0 do 70 °C

13. Zarządzane urządzenia sieciowe z obsługą VLAN - 20 sztuki.

Minimalne wymagania:	
Rodzaj modułu	SFP
Okablowanie	jednomodowe
Tryb transmisji	WDM
Prędkość transmisji	1,25 Gbps
Rodzaj złącza modułu optycznego	SC/UPC
Zasięg portu	3 km
Standard ethernet	1000Base-BX
Długość fali TX	1550 nm
Długość fali RX	1310 nm
Moc (tx power)	-12 do -24 dBm
Czułość (rx sensitivity)	-22 dBm
Napięcie zasilania	3,3 V
Temperatura pracy	0 do 70 °C

14. serwer NAS – 1 sztuka.

Minimalne wymagania Zamawiającego	
Typ urządzenia	Serwer NAS
Obudowa	Tower
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark co najmniej 4580 punktów

Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 4 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	• Sprzęt powinien być wyposażony w min. 8 kieszeni na dyski twarde typu hot-swap z możliwością rozszerzenia do 18 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą dedykowanych przewodów rozszerzeń • Wbudowane 2 gniazda M.2 obsługujące dyski SATA/NVMe (pamięć podręczna)
Porty zewnętrzne	Minimum: • 4 porty USB 3.2.1 • 2 porty eSATA
Porty sieciowe	Minimum: • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 3.0	Min. 1x 8-liniowe gniazdo x4 (Gen.3)
Wentylator obudowy	Min. 2 wentylatory 120 mm x 120 mm
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Synology Hybrid RAID (SHR), Podstawowy (Basic), JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń CIFS/AFP/FTP: 1000
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane systemy klienckie	Windows® 7 i nowsze, macOS® 10.12 i nowsze
Obsługiwane przeglądarki	Chrome®, Firefox®, Edge®, Internet Explorer® 10 i nowsze, Safari® 10 i nowsze, Safari (iOS 10 i nowsze), Chrome (Android™ 6.0 i nowsze) na tabletach
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz 250 W
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania

	sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Gwarancja	Wykonawca udzieli gwarancji: • 3 lat na urządzenia główne z możliwością przedłużenia do 5 lat za pomocą dedykowanego pakietu gwarancyjnego

Dyski twarde do serwera NAS – 4 sztuki.

Minimalne wymagania:	
Pojemność	min. 2000 GB
Typ	SSD
Format obudowy	M.2
Interfejs	PCIe NVMe 3.0 x4
Odczyt losowy	480,000 IOPS
Zapis losowy	540,000 IOPS
Prędkość odczytu	3400 MB/s
Prędkość zapisu	2900 MB/s
Niezawodność MTBF	do 1 750 000 godzin
Wytrzymałość	2500.

16. Dyski twarde do serwera NAS – 18 sztuk.

Minimalne wymagania:	
Pojemność	min. 8000 GB
Typ	HDD (magnetyczny)
Format	Format 3,5 cala
Interfejs	Serial ATA III
Pamięć cache	min. 256 MB
Prędkość obrotowa	7200 obr./ min.

Macierz dyskowa – 1 sztuka.

Element konfiguracji/cecha/funkcjonalność	Wymagania minimalne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U oraz umożliwiać montaż min. 12 dysków 3.5”
Przestrzeń dyskowa	Zainstalowane: 4x dysk SSD SAS o pojemności min. 1.92TB, Hot-Plug 8x dysk SAS o pojemności min. 16TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów iSCSI 25Gb (4 porty na kontroler),
Kable/wkładki	4x kabel DAC 25GbE SFP+ 10Gb/s, QSFP+40Gb/s min. 5m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu

	znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.

	Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zasilacze użyte w macierzy powinny posiadać certyfikat sprawności zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Warunki gwarancji	5 lat gwarancji producenta Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do

	oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

UPS – 2 sztuki.

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań
1	Moc pozorna	3000VA
2	Moc rzeczywista	3000W
3	Topologia (klasyfikacja IEC 62040-3)	Podwójna konwersja on-line z korekcją wejściowego współczynnika mocy systemu (PFC)
4	Sprawność przy pracy normalnej (100% obc.)	<94%
5	Sprawność w trybie podwyższonej sprawności (100% obc.)	>98%
6	Współczynnik mocy	1
7	Czas przełączenia na baterię	0 ms
8	Możliwość pracy równoległej	tak
9	Liczba, typ gniazd wyjściowych	8 gniazd IEC C13 (10A) + 2 gniazda IEC C19 (16A), w tym 2 zarządzalne grupy wraz z pomiarem zużytej energi
10	Typ gniazda wejściowego	1 IEC C20 (16A) lub blok zacisków w wersji HotSwap MBP HW
11	Czas podtrzymania dla 100% obciążenia dla pf=1	3 min
12	Czas podtrzymania przy 50% obciążenia dla pf=1	10 min
13	Dodatkowe bateriie	Możliwość dołożenia maksymalnie 4 zewnętrznych modułow bateryjnych
14	Napięcie znamionowe	200/208/220/230/240 V
15	Tolerancja napięci prostownika	176V – 276 V (100-276V przy <33% obciążeniu)
16	Częstotliwość znamionowa	50/60 Hz autodetekcja
17	Tolerancja częstotliwości	40– 70 Hz
18	Kształt napięcia	Sinusoidalny
19	Napięcie znamionowe wyjściowe	230 V (domyślnie) / możliwość wyboru 200/208/220/240 V
20	Zakres zmian napięcia	+/-1% napięcia nominalnego
21	Częstotliwość wyjściowa	50/60 Hz +/-0,5%

22	Współczynnik szczytu	3:1
23	Dopuszczalny zakres współczynnika mocy obc. Liniowego	0,5 indukcyjny - 0,5 pojemnościowy
24	Baterie wymieniane przez użytkownika "na gorąco"	Tak
25	Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
26	Ochrona przed głębokim rozładowaniem	Tak
27	Okresowy automatyczny test baterii	Tak
28	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
29	Zdolność zwarciowa	90A
30	Możliwość uruchomienia bez napięcia w sieci	Tak
31	Baterie wewnętrzne o pojemności nie mniejszej niż	9Ah 12V, minimum 6 szt.
32	Czas ładowania baterii do poziomu 90%	< 1,5 godz. do 90% pojemności użytkowej
33	Interfejs komunikacyjny	• USB
		• RS232 DB-9 żeński (HID)
		• 1 blok mini-zacisków dla zdalnego załączania/wyłączania
		• 1 blok mini-zacisków do zdalnego wyłączania
		• 1 blok mini-zacisków przekaźnika wyjściowego
34	Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa). Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe , częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny,napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii).
		• Poziomy rząd przycisków sterowania
		• Poziomy rząd wskaźników stanu : 4 LED
		• Sygnalizator akustyczny
35	Sygnały akustyczne	• Awaria
		• Niski stan naładowania baterii
		• Przeciążenie
		• Serwis
36	Przyciski sterujące i wskaźniki diodowe LED	• Przycisk Escape (anulowanie)
		• Przyciski funkcyjne (przewijanie w górę i w dół)
		• Przycisk Enter (potwierdzający)
		• Przycisk ON/OFF załączenia i wyłączenia

		• LED trybu zasilania z siec i(kolor zielony)
		• LED trybu baterii (kolor żółty)
		• LED usterki (kolor czerwony)
		• LED w trybie obejścia (kolor pomarańczowy)
37	Kolor	Czarny RAL 9005
38	Typ obudowy	Uniwersalna Tower/Rack 2U
39	Wyposażenie standardowe	UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa, instrukcja szybkiego montażu
		1 x kabel szeregowy RS-232,
		1 x kabel komunikacyjny USB
		1 x kable wyjściowe IEC 16A
		2 x kable wyjściowe IEC 10A
		uchwyty kablowe
		1 x zestaw szyn montażowych 19’
		podstawki do montażu wieżowego
40	Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych: - Windows: 7 / 8 / 2008 / Vista / 2003 / XP - Microsoft SCVMM 2012 - Linux: Debian GNU Linux: Lenny, SUSE/Novell: SLES 11, OpenSUSE 11.2, Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12 Ubuntu: 10.04 - VMWare: vCenter / ESXi 5.1 - Citrix XEN 6.0
41	Zgodność ze standardem Energy Star	Tak
42	Maksymalna szerokość	440 mm
43	Maksymalna wysokość	86,5 mm
44	Maksymalna głębokość	605 mm
45	Maksymalny ciężar	27,4 kg
46	Poziom hałasu w odl. 1m	<47 dBA dla pracy normalnej
47	Znaki bezpieczeństwa	CE, C-Tick, IEC/EN 62040-1, IEC/EN 62040-2: Kat. C1, IEC/EN 62040-3
48	Gwarancja producenta	3 lata na elektronikę, 2 lata na baterie akumulatorów

19. Licencje systemu operacyjnego -2 sztuki.

Microsoft Windows Server 2022 Datacenter 16-core – 2 sztuki

Licencje systemu operacyjnego Microsoft Windows Server 2022 Datacenter 16-core lub oprogramowania równoważnego nie mogą posiadać ograniczeń czasowych, muszą pochodzić z oficjalnego kanału dystrybucji. Licencje nie mogą być dedykowane tylko do jednego producenta sprzętu serwerowego.

RÓWNOWAŻNOŚĆ:

1. Warunki równoważności dla licencji systemu Microsoft Windows Server 2022 Datacenter.

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 Datacenter. Zamawiający wymaga, aby produkt równoważny spełniał niżej wymienione wymagania:

Współpraca z procesorami o architekturze x86 – 64bit.

2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 16 rdzeni.
5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:

1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
4. umożliwiają zdefiniowanie list kontroli dostępu (ACL).

18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
22. Możliwość wykorzystania standardu http/2.
23. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
26. Mechanizmy logowania w oparciu o: a) login i hasło,
1. karty z certyfikatami (smartcard),
2. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
1. określonych grup użytkowników,
2. zastosowanej klasyfikacji danych,
3. centralnych polityk dostępu w sieci,
4. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
28. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
29. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
30. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
31. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
32. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
33. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
- podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
- ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
- odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
- bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,
3. zdalna dystrybucja oprogramowania na stacje robocze,
4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
5. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
- Dystrybucję certyfikatów poprzez http,
- Konsolidację CA dla wielu lasów domeny,
- Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
- Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
6. szyfrowanie plików i folderów,
7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
8. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
9. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,

10. serwis udostępniania stron WWW,
11. wsparcie dla protokołu IP w wersji 6 (IPv6),
12. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
13. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
14. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
15. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
16. mechanizmy wirtualizacji mające wsparcie dla:

- dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- obsługi ramek typu jumbo frames dla maszyn wirtualnych.
- obsługi 4-KB sektorów dysków,
- nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
- możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

17. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
18. wsparcie dla rozwiązania Kubernetes.
19. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
20. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
21. mechanizmy deduplikacji i kompresji na wolumenach.
22. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
23. mechanizm konfiguracji połączenia VPN do platformy Azure.
24. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
25. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
26. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).

20. Oprogramowanie antywirusowe – 45 stanowisk.

Przedłużenie licencji oprogramowania antywirusowego Bitdefender GravityZone Business Security dla 45 stanowisk o 12 miesięcy.
Minimalne wymagania Zamawiającego:
Ochrona antywirusowa i antyspyware

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

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

1. Plik
2. Folder
3. Rozszerzenie
4. Proces
5. Hash pliku
6. Hash certyfikatu
7. Nazwa zagrożenia
8. Wiersz poleceń
9. IP/maska

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

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

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

-Ochrony przeglądarki internetowej
-Sieć i poświadczenia
-Błędna konfiguracja systemu operacyjnego
System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.

2. System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.
3. System który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.

4. System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.
5. System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.
6. System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie

53. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:

1. Możliwość wymuszenia funkcji DEP systemu Windows
2. Możliwość wymuszenia relokacji modułów (ASLR)

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

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

- Wczesny dostęp
- Dostęp do poświadczeń
- Wykrycie
- Crimeware

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

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

Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania.

56. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak:

1. Ukierunkowane ataki
2. Podejrzane pliki i ruch w sieci
3. Exploity
4. Ransomware
5. Grayware

57. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego

58. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na:

1. Tolerancyjny
2. Normalny
3. Agresywny

59. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku

1. Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora
2. Możliwość przesłania archiwum zabezpieczonego hasłem
3. Możliwość przesłania adresu URL
4. W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.

60. Wbudowany sandbox musi działać w trybie monitorowania i blokowania
61. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny
62. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.
63. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
64. Minimalny rozmiar pliku jaki może zostać przesłany do sandboxa to 1KB
65. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa to 50MB.
66. Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows do SIEM Splunk (wymaga TLS 1.2 lub wyższy).
67. Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników zagrożeń, wskaźniki te obejmują:

Maszyny Wirtualne

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

Stacje robocze i serwery Windows

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

20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.

Ochrona Exchange

1. Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
2. Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w przeciągu ostatnich kilku godzin / dni.
3. Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz nie możliwych do przeskanowania.
4. Możliwość wykluczenia potencjalnie niechcianych aplikacji (PUA) z filtrowania antymalware.
5. Możliwość skanowania w poszukiwania malware wewnątrz archiwów.
6. Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
7. Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
8. Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
9. Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10. Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowania maila do konkretnej skrzynki pocztowej.
11. Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
12. Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.

Konsola zdalnej administracji

1. Dwa typy konsoli administracyjnej:
   - Konsola Cloud – serwer administracyjny po stronie producenta
   - Konsola On-premise – lokalny serwer administracyjny
2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows.
3. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.
4. Możliwość integracji Domeny Active Directory w obu typach konsoli.
5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
6. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
7. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi
8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.
9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.

10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
11. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.
12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv.
14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.
15. Możliwość generowania raportu co godzinę.
16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.
17. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
18. Możliwość dodania etykiety do stacji roboczej.
19. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
20. Możliwość przechowywania kwarantanny maksymalnie 180 dni
21. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.
22. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
23. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.
24. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym.2
25. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.
26. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.
27. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie

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

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

- Zarządzane punkty końcowe
- Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne
- Pięć najczęściej blokowanych zagrożeń
- Podział zagrożeń na urządzenia takie jak stacje robocze i serwery
- Status incydentów bezpieczeństwa które wystąpiły

- Stan modułów punktów końcowych
- Ocena ryzyka firmy
- Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa.
- Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware

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

1. Pakiety
2. Sieć
3. Kwarantanna
4. Licencjonowanie
5. Integracje
6. Polityki
7. Raporty
8. Konta
9. Firmy

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

1. Lotnictwo
2. Rolnictwo
3. Automotive
4. Usługi komercyjne
5. Doradztwo
6. Energia
7. Usługi finansowe
8. Rząd
9. Opieka zdrowotna
10. Technologie

11. Transport
12. Non-profit
13. Górnictwo
14. Media
50. Funkcja kontroli aplikacji która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów.
51. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym.
52. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat.
53. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
54. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
55. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS.
56. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym.
57. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
58. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
59. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1.
60. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
61. Możliwość skanowania SSL dla połączeń RDP.
62. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.
63. Program testowy – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Program wczesnego dostępu powinien umożliwiać testowanie najnowszych funkcji oprogramowania których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.
64. Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych.
65. Oprogramowanie musi umożliwiać przypisywanie znaczników ręcznie lub automatycznie.
66. Oprogramowanie musi umożliwiać filtrowanie punktów końcowych na podstawie wybranych znaczników, musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
67. Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.

21. Oprogramowanie do wykonywania kopii zapasowych – 10 licencji uniwersalnych.

Licencja musi być na bezterminowa, bez żadnych dodatkowych opłat a wsparcie na minimum 12 miesięcy.

Lp.	Minimalne wymagania Zamawiającego
1. Wymagania ogólne	
1.	Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
2.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne

	na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
3.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
2. Całkowite koszty posiadania	
1.	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
2.	Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
3.	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
4.	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
5.	Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
6.	Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
7.	Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
8.	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
9.	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
10.	Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
11.	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
12.	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
13.	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
14.	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
15.	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
16.	Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
3. Wymagania RPO	
1.	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
2.	Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
3.	Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego

	datastoru
4.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
5.	Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
6.	Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
7.	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
8.	Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
9.	Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
10.	Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
11.	Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
12.	Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
13.	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
14.	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
15.	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
4. Wymagania RTO	
1.	Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
2.	Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
3.	Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
4.	Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
5.	Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
6.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
7.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

8.	Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
9.	Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
10.	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
11.	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
12.	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
13.	Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
14.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
15.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
16.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
17.	Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
18.	Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
19.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
20.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
21.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
22.	Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
5. Ograniczenie ryzyka	
1.	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
2.	Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
3.	Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
4.	Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
5.	Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska

	produkcyjnego.
6.	Środowiska fizyczne
1.	Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
2.	Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
3.	Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
4.	Rozwiązanie musi wspierać system operacyjny macOS
5.	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
6.	Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
7.	Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
8.	Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
9.	Rozwiązanie musi wspierać backup podłączonych dysków USB
10.	Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
11.	Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
12.	Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
13.	Rozwiązanie musi wspierać kontrolę pasma sieciowego
14.	Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
15.	Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
16.	Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
17.	Rozwiązanie musi wspierać technologię BitLocker
18.	Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
19.	Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
20.	Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
21.	Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.
22.	Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
23.	Rozwiązanie musi wspierać szyfrowanie
24.	Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
25.	Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania

	danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
26.	Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
27.	Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
7. Monitoring	
1.	System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
2.	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
3.	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
4.	System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
5.	System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
6.	System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
7.	System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
8.	System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
9.	System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
10.	System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
11.	System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
12.	System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
13.	System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
14.	System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
15.	System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
16.	System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
17.	System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4
8. Raportowanie	
1.	System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
2.	System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows

	Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
3.	System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
4.	System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
5.	System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
6.	System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
7.	System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
8.	System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
9.	System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
10.	System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
11.	System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
12.	System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
13.	System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
14.	System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
15.	System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
16.	System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
17.	System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

22. Oprogramowanie antywirusowe - dla 45 stanowisk

Oprogramowanie musi spełniać następujące wymagania:

- Proaktywnie zatrzymuje malware, hacking, kampanie phishingowe oraz inne zagrożenia przed dostaniem się do użytkownika końcowego.
- Zdobywa raporty o potencjalnych atakach z bazy danych.
- Bazuje na podstawie aplikacji, które odpowiadają za bezpieczeństwo. Aplikacje te można włączyć i wyłączyć, aby wspierać systemy ochronne na potrzeby użytkowników.
- Dostarcza ochronę poprzez kontrolę adresów IP, protokołów oraz portów.
- Robi analizę adresów IP i blokuje na jej podstawie dostęp do stron internetowych.
- Sprawdza wirusy po ich sygnaturach.
- Eliminuje reklamy na stronach internetowych.
- Blokuje spam.

- Kontroluje dostęp do aplikacji.
- Blokuje nieodpowiednie treści przed pojawieniem się dla użytkownika.
- Automatycznie przekierowuje ruch, gdy jedno połączenie internetowe ulegnie awarii.
- Zarządzanie dostępem do Wi-Fi dla użytkowników i gości.
- Tworzy połączenia oparte na VPN.
- Posiada zarządzanie politykami bezpieczeństwa.
- Pozwala definiować i zarządzać uprawnieniami na podstawie takich parametrów jak: użytkownicy, grupy, czas, dzień lub protokół.

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.
Potencjał techniczny przedstawia się poprzez posiadanie narzędzi takich jak automatyczny skaner podatności posiadający funkcje pozwalające na:

- wykonanie skanowań z wykorzystaniem wbudowanych szablonów;
- skanowanie sieciowe (wykrywanie otwartych portów i rozpoznanie uruchomionych na nich usług, wskazywanie listy podatności na wykryte usługi);
- weryfikacje domyślnych haseł według zadanego słownika;
- skanowanie systemów operacyjnych z uwierzytelnieniem (sprawdzenie wersji systemu, zainstalowanych na nim aplikacji, brakujących aktualizacji, wskazywanie listy podatności na wykryte systemy i aplikacje) oraz weryfikację uprawnień zadanego użytkownika;
- ustawienia harmonogramu skanowań;
- możliwość porównania wyników poszczególnych skanowań;
- możliwość konfigurowania zawartości raportu ze skanowania oraz dobieranie różnych formatów wyjściowych raportów (w tym HTML, CVS i XML);
- możliwość wyświetlania wyników na bieżąco oraz możliwość grupowania podobnej klasy podatności i możliwość sortowania po IP i podatnościach.

Aplikacje do testów stron i aplikacji internetowych posiadającej funkcje pozwalające na:

- przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową, nawet gdy używany jest HTTPS;
- przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta;
- dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia;
- wykonywanie różnych automatycznych modyfikacji odpowiedzi w calu ułatwienia testowania;
- tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy;
- precyzyjna konfiguracja reguł przechwytywania wiadomości;
- możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS;
- pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL;
- żądania i odpowiedzi dostępne w edytorze http;
- narzędzie do ręcznej edycji i ponownego wstawiania żądań;
- narzędzie do analizy statystycznej tokenów sesji;
- możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz powrót do zapisanego miejsca;
- biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami;

- możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach;
- skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań;
- możliwość analizy docelowej aplikacji internetowych.
- narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.
- Oprogramowanie posiada wsparcie na 1 rok.

1. Wdrożenie systemów teleinformatycznych

Krok 1: Planowanie i Przygotowanie

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

Krok 2: Instalacja roli oprogramowania do wirtualizacji

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

Krok 3: Konfiguracja klastra

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

Krok 4: Konfiguracja wysokiej dostępności klastra

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

Krok 5: Tworzenie i Zarządzanie Maszynami Wirtualnymi

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

Krok 6: Testowanie i Monitorowanie

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

2. Wdrożenie oprogramowania do wykonywania kopii zapasowych.

1: Planowanie i Przygotowanie

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

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

2: Instalacja i Konfiguracja

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

3: Konfiguracja Backupu

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

4: Konfiguracja Replikacji (opcjonalnie)

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

5: Testowanie i Wdrażanie

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

6: Monitorowanie i Administracja

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

3. Opracowanie i wdrożenie dokumentacji SZBI.

Cel Usługi:
Zasadniczym zamierzeniem proponowanej usługi jest kreacja kompleksowej, szczegółowo opracowanej dokumentacji dla Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), która będzie w pełni zharmonizowana z międzynarodowymi normami i aktualnymi najlepszymi praktykami, przy jednoczesnym dostosowaniu do unikatowych aspektów i wymogów strukturalnych Zamawiającego. Celem jest, aby wspomniana dokumentacja służyła jako kluczowy fundament dla efektywnego implementowania, utrzymania oraz ciągłego udoskonalania SZBI, gwarantując tym samym wytrzymałość ochrony informacji wobec szerokiego spektrum potencjalnych zagrożeń oraz podnosząc poziom zaufania wśród interesariuszy.
Zakres Usługi:
1. Analiza Stanu Istniejącego i Określenie Wymagań:
- Realizacja audytu wstępnego mającego na celu szczegółową analizę obecnych procesów, procedur operacyjnych oraz mechanizmów kontroli związanych z bezpieczeństwem informacji, w celu zidentyfikowania istniejących luk i obszarów wymagających usprawnienia.
- Dokładna identyfikacja i agregacja wymagań prawnych, regulacyjnych oraz biznesowych dotyczących bezpieczeństwa informacji, aby zapewnić pełną zgodność przyszłego SZBI z obowiązującymi ramami normatywnymi.
2. Opracowanie Dokumentacji SZBI:
- Konstrukcja polityki bezpieczeństwa informacji, która będzie definiować kierunkowe cele, zakres działania, zasady oraz zakres odpowiedzialności w ramach struktury SZBI, stanowiąc podstawę dla wszystkich dalszych działań.
- Rozwój i formalizacja procedur, instrukcji operacyjnych, wytycznych oraz innych dokumentów kluczowych dla wdrożenia i efektywnego funkcjonowania SZBI, uwzględniając przy tym specyfikę organizacyjną Zamawiającego.
3. Weryfikacja i Walidacja Dokumentacji:

- Krytyczny przegląd i ocena zgodności opracowanej dokumentacji z międzynarodowymi standardami, wyznacznikami branżowymi oraz oczekiwaniami Zamawiającego, mający na celu zapewnienie jej maksymalnej adekwatności i użyteczności.
- Organizacja warsztatów, konsultacji oraz sesji feedbackowych z kluczowymi stakeholderami organizacji, w celu osiągnięcia konsensusu co do finalnej formy i treści dokumentów.

4. Wsparcie przy Wdrożeniu Dokumentacji:
- Oferowanie doradztwa w zakresie implementacji najlepszych praktyk dotyczących wdrożenia procedur i polityk określonych w dokumentacji SZBI, z myślą o optymalizacji procesów bezpieczeństwa.
- Asystowanie w implementacji zaleceń oraz w organizacji szkoleń dla personelu, aby zapewnić im kompleksowe zrozumienie nowych procedur i polityk.

5. Przygotowanie do Certyfikacji:
- Dostosowanie dokumentacji do wymogów procesu certyfikacji według wybranych standardów, na przykład ISO/IEC 27001, co zapewni organizacji gotowość do podjęcia procedur weryfikacyjnych.

Cel Końcowy Usługi:
Finalizacja usługi zapewni Zamawiającemu kompleksową, spójną oraz w pełni funkcjonalną dokumentację SZBI, która stanie się solidnym fundamentem dla efektywnego zarządzania bezpieczeństwem informacji. Dzięki temu, organizacja uzyska dogłębne zrozumienie metod zarządzania ryzykiem, ochrony informacji oraz adaptacji do zmieniających się zagrożeń, co w konsekwencji umożliwi ciągłe doskonalenie systemu bezpieczeństwa informacji. Opracowana dokumentacja SZBI stanie się kluczowym elementem w strukturze zarządzania organizacją, zapewniając nie tylko zgodność z międzynarodowymi normami i najlepszymi praktykami, ale również dopasowanie do specyficznych wymogów i oczekiwań Zamawiającego.
Dokumentacja ta będzie również służyć jako instrukcja operacyjna dla wszystkich pracowników i zainteresowanych stron, ułatwiając zrozumienie ich ról i odpowiedzialności w kontekście bezpieczeństwa informacji. W rezultacie, wszyscy uczestnicy procesu będą mieli jasne wytyczne dotyczące sposobu postępowania, co znacznie zwiększy ogólną świadomość bezpieczeństwa w organizacji oraz efektywność wdrażanych środków ochronnych.
Takie podejście zapewni organizacji nie tylko obronę przed potencjalnymi zagrożeniami, ale także pozytywnie wpłynie na reputację wśród klientów, partnerów biznesowych oraz innych interesariuszy, budując zaufanie poprzez demonstrację zaangażowania w ochronę poufnych informacji i danych osobowych. Finalnie, kompletna i zaktualizowana dokumentacja SZBI będzie stanowić nieoceniony zasób w procesie ciągłego monitorowania, przeglądania i ulepszania procesów bezpieczeństwa, umożliwiając organizacji dynamiczne reagowanie na nowe wyzwania i zapewniając stabilność operacyjną w zmieniającym się środowisku cyfrowym.

1. Szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami:

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

2. wykonanie kopii strony internetowej Zamawiającego i umieszczenie jej pod spreparowanym adresem;
3. wygenerowanie niezbędnych certyfikatów SSL;
4. przygotowanie spreparowanego aktywnego dokumentu PDF, wyposażonego w autorski, niezłośliwy skrypt, którego celem jest zebranie informacji o użytkownikach, którzy dokonali otwarcia pliku PDF i uruchomienia niezłośliwego skryptu (w prawdziwej kampanii byłoby to złośliwe oprogramowanie);
5. utworzenie nowej podstrony, na której umieszczony zostanie spreparowany plik PDF;
6. przygotowanie konta mailowego, którego celem jest podszycie się pod jedną z osób wtajemniczonych w prowadzone testy phishingowe;
7. przygotowanie treści wiadomości e-mail i wyposażenie jej w mechanizmy pozwalające na przeprowadzenie tzw. detekcji umiejscowienia (uzyskanie adresu IP potencjalnej „ofiary").
3. Przeprowadzenie kampanii socjotechnicznej (wysłanie przygotowanej uprzednio wiadomości e-mail do pracowników wskazanych w bazie mailingowej).
4. Wykonanie raportu z testu socjotechnicznego w języku polskim.
5. Przeprowadzenie szkolenia dla pracowników z zakresu cyberbezpieczeństwa, ukierunkowanego na omówienie wyników kampanii socjotechnicznej oraz co najmniej:

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

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

3. zasady bezpieczeństwa i praktyki:
- zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
- zasady bezpieczeństwa e-mail;
- bezpieczeństwo w sieciach bezprzewodowych;
- bezpieczne przeglądanie internetu;
- backup i odzyskiwanie danych.

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

Czas trwania szkolenia przewidziano na co najmniej dwie grupy po 4 godziny robocze z uwzględnieniem przerw 15 minut w każdym szkoleniu. Po szkoleniu Wykonawca udostępni co najmniej 30 minut na pytania i odpowiedzi uczestników.

2. Audyty bezpieczeństwa.

Potencjał osobowy przedstawia się poprzez posiadanie przez osoby testujące łącznie takie certyfikaty jak: OSCP (offensice security), CEH (EC-Council), Burp Suite Certified Practitioner (PortSwinger), eWPTX (eLearnSecurity), eCPPT (eLearnSecurity). Skanowania nie mogą być realizowane tylko z wykorzystaniem narzędzi automatycznych, konieczna jest manualna weryfikacja podatności znalezionych w testach automatycznych. Przeprowadzenie testów nie może wymagać od Zamawiającego zakupu żadnych dodatkowych licencji lub wyposażenia.
W ramach przeprowadzonych testów penetracyjnych infrastruktury, Wykonawca wykona:

1. Rekonesans.
1. Zgromadzenie wszystkich dostępnych publicznie informacji nt. osób reprezentujących instytucję w celu stworzenia potencjalnej bazy loginów i haseł.
2. Zgromadzenie informacji nt. zasobów instytucji dostępnych publicznie (strona internetowa, serwer www, serwer ftp, inne usługi).
3. zgromadzenie informacji nt. potencjalnie niejawnych zasobów dostępnych dla wyszukiwarek internetowych.
4. Sprawdzenie występowania w wyciekach znalezionych loginów.
2. Enumeracja zasobów.
1. Analiza zasobów zidentyfikowanych w pkt. 1 w celu określenia precyzyjnej listy aplikacji (wraz z określeniem ich wersji) działających w ramach usług.
2. Skanowanie publicznej infrastruktury.
3. Skanowanie wewnętrznej infrastruktury z wykorzystaniem automatycznego skanera podatności.
4. Sprawdzenie udostępnionych w sieci wewnętrzej plików i folderów w szczególności pod kątem występowania danych wrażliwych.
5. Analiza dostępnych wewnątrz sieci, usług, protokołów i urządzeń.
3. Eksploitacja.
1. Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force oraz domyślnych haseł.
2. Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji) – po uzgodnieniu z Zamawiającym.
3. Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, architektury sieci, błędy w konfiguracji serwera www i architektury aplikacji internetowych oraz innych usług).
4. Eskalacja uprawnień.
1. Wykorzystanie zasobów skompromitowanych w pkt. 3 w celu ewentualnego podniesienia uprawnień.
2. Rozpoznanie zasobów wewnętrznych, przechodzenie na inne środowiska dostępne ze skompromitowanych w pkt.3 zasobów (lateral movement).
5. Raport z testu penetracyjnego.

Wykonawca dostarczy raport zawierający:

1. Podsumowanie dla kierownictwa.
2. Opis zakresu wykonanych prac.
3. Wyłączenia z testów jeżeli były.
4. Listę danych zebranych w trakcie rekonesansu (w tym listę zidentyfikowanych adresów IP w sieci wewnętrznej).
5. Listę znalezionych podatności wraz z określoną dla niej waga zgodnie z ze standardem Common Vulnerability Scoring System Version 4.0 oraz modelem STRIDE.
6. Szczegółowy opis znalezionych podatności.
7. Zalecenia naprawy nieprawidłowości bądź mitygacji zagrożeń z nich wynikających.

1. Szkolenie dla pracowników administracyjnych w zakresie cyberbezpieczeństwa.

Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników administracyjnych.
Szkolenie stacjonarne lub online z zakresu cyberbezpieczeństwa skierowane do pracowników administracyjnych, obejmujące co najmniej następujące obszary:

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

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

3. zasady bezpieczeństwa i praktyki:
- zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;
- zasady bezpieczeństwa e-mail;
- bezpieczeństwo w sieciach bezprzewodowych;
- bezpieczne przeglądanie internetu;
- backup i odzyskiwanie danych.

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

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

2. Szkolenie dla pracowników IT w zakresie cyberbezpieczeństwa.

Przedmiotem zamówienia jest przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa:
Szkolenie z cyberbezpieczeństwa dla pracowników IT.
Indywidualne warsztaty online z zakresu cyberbezpieczeństwa skierowane do administratorów sieci teleinformatycznej, obejmujące co najmniej następujące obszary:

1. Wprowadzenie do cyberbezpieczeństwa:
- Czym jest cyberbezpieczeństwo?
- Dlaczego cyberbezpieczeństwo jest ważne?
- Kluczowe zagadnienia związane z cyberbezpieczeństwem.
- Przegląd statystyk i trendów w cyberbezpieczeństwie.

2. Typy zagrożeń w cyberprzestrzeni:
- Malware (wirusy, trojany, robaki itp.)
- Ataki typu phishing i spear phishing
- Ataki DDoS
- Ataki ransomware
- Zagrożenia związane z sieciami społecznościowymi.

3. Zasady bezpieczeństwa i praktyki:

- Zarządzanie hasłami i uwierzytelnianie wieloskładnikowe
- Zasady bezpieczeństwa e-mail
- Bezpieczeństwo w sieciach bezprzewodowych
- Bezpieczne przeglądanie internetu
- Backup i odzyskiwanie danych

4. Bezpieczeństwo systemów i sieci
- Zasady bezpieczeństwa systemów operacyjnych
- Bezpieczeństwo sieci i firewall
- Wprowadzenie do VPN
- Bezpieczeństwo urządzeń IoT
- Bezpieczeństwo w chmurze

5. Reagowanie na incydenty i planowanie awaryjne
- Jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem
- Zasady reagowania na incydenty
- Planowanie awaryjne i kontynuacja działalności
- Przegląd realnych przypadków naruszeń bezpieczeństwa i lekcje z nich wyniesione

6. Aktualne trendy i przyszłość cyberbezpieczeństwa
- Sztuczna inteligencja i machine learning w cyberbezpieczeństwie
- Kryptografia i blockchain
- Bezpieczeństwo danych w erze Big Data
- Przyszłość cyberbezpieczeństwa: wyzwania i możliwości

Przewiduje się, że szkolenie potrwa łącznie minimum 8 godzin roboczych, rozłożonych na co najmniej 2 dni. Każda sesja będzie trwała 4 godziny obejmować 4 przerwy po 15 minut, a po zakończeniu zajęć każdego dnia przewidziano 30 minut na sesję pytań i odpowiedzi z uczestnikami.

3. Zaawansowane Szkolenie z Cyberbezpieczeństwa dla Kadry Zarządzającej.

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

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

W ramach przeprowadzonego szkolenia wykonawca

1. Podstawowe informacje o obecnej sytuacji rynkowej powiązanej z tematyką cyberbezpieczeństwa:
- Podstawy i definicje: zapewnienie uczestnikom solidnych podstaw w dziedzinie cyberbezpieczeństwa poprzez omówienie kluczowych pojęć i zasad. Ponadto, zostanie przedstawiona rola menedżera w formowaniu bezpiecznego środowiska cyfrowego, co pozwoli zrozumieć jak ważne jest aktywne zaangażowanie kierownictwa w procesy zapewnienia bezpieczeństwa informacji. W ten sposób uczestnicy będą mieć pełniejsze zrozumienie zarówno teoretycznych, jak i praktycznych aspektów cyberbezpieczeństwa oraz będą lepiej przygotowani do podejmowania decyzji w tym obszarze.
- Statystyki i trendy: skoncentrowanie się na przekazaniu uczestnikom szczegółowej analizy globalnych i lokalnych danych dotyczących cyberataków. Poprzez omówienie ewolucji tych ataków oraz ich metodologii, uczestnicy zyskają

wgląd w aktualne trendy i sposoby działania cyberprzestępców. Ponadto, zostaną przedstawione skutki, jakie cyberatak może mieć dla biznesu, co pozwoli uczestnikom lepiej zrozumieć znaczenie inwestycji w bezpieczeństwo informacji oraz skuteczne zarządzanie ryzykiem cybernetycznym dla organizacji. Dzięki temu będą mogli podejmować bardziej świadome decyzje w zakresie ochrony swoich danych i infrastruktury cyfrowej.

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

- Omówienie znaczenia powyższych norm i ich w zapewnianiu wysokiego poziomu bezpieczeństwa informacji oraz praktycznego zastosowania w organizacjach.
- Inne standardy: Przedstawienie i dyskusja na temat innych standardów:
  - ramy dotyczące zarządzania ryzykiem cyberbezpieczeństwa - NIST Cybersecurity Framework;
  - ramy dotyczące wdrażania, rozwoju i doskonalenia polityki IT – COBIT;
  - zbiór praktyk dotyczący zarządzania usługami IT – ITIL;
  - akceptowalna polityka szyfrowania SANS;
  - techniki kryptograficzne - ENISA ;
  - ramy ochrony informacji i zasobów federalnych agencji rządowych USA - 800-53 rev3.
- Rola powyższych zagranicznych standardów w kształtowaniu efektywnych polityk bezpieczeństwa w organizacjach.
3. Omówienie zaawansowanych strategii ochrony organizacji:
- Zarządzanie ryzykiem: Metody identyfikacji, oceny, mitygacji i monitorowania ryzyka cybernetycznego. Wykorzystanie narzędzi i technologii do analizy ryzyka.
- Wprowadzenie do zarządzania incydentami, zdefiniowanie incydentów i wektorów ataku: atak przeprowadzony z nośnika wymiennego lub urządzenia peryferyjnego, atak wykorzystujący metody brute-force w celu złamania, degradacji lub zniszczenia systemów, sieci lub usług, ataki wykonane z poziomu witryny internetowej lub aplikacji internetowej, atak przeprowadzony za pośrednictwem wiadomości e-mail lub załącznika, naruszenia zasad

dopuszczalnego użytkowania organizacji przez autoryzowanego użytkownika, z wyłączeniem powyższych kategorii, utrata lub kradzież urządzenia komputerowego lub nośnika używanego przez organizację, na przykład laptopa lub urządzenia typu smartfon.
- Szczegółowy opis i kroki zarządzania incydentami:

- wykrywanie: inicjacja procesu inicjującego, mającego na celu detekcję niestandardowych aktywności lub zdarzeń infrastrukturalnych, które mogą sygnalizować potencjalne zagrożenia w obszarze cybernetycznym;
- rejestrowanie: operacja dokumentacyjna, polegająca na chronologicznym zapisie zaobserwowanych dysfunkcji w dedykowanych bazach danych, by zapewnić dokumentację dowodową dla późniejszych faz postępowania;
- analizowanie: metodyczne badanie zgromadzonych artefaktów zdarzeń w celu zrozumienia ich genezy, dynamiki oraz wpływu na ekosystem informacyjny;
- klasyfikowanie: systematyzacja incydentów według ustalonego kodu klasyfikacyjnego, uwzględniająca ich naturę, zasięg oraz potencjalne konsekwencje dla organizacji.
- priorytetyzowanie: alokacja zasobów reakcyjnych na bazie oceny krytyczności, która koresponduje z możliwymi konsekwencjami incydentu dla misji instytucji;
- podejmowanie działań naprawczych: inicjowanie interwencji korygujących mających na celu restytucję funkcji systemowych i prewencję przed podobnymi naruszeniami w przyszłości;
- ograniczanie skutków incydentu: implementacja taktyk zaradczych, które mają za zadanie minimalizację negatywnych rezultatów incydentu oraz odbudowę stanu równowagi operacyjnej.

- Priorytetyzacja incydentów na 3 kategorie: krytyczny, wysoki, średni na podstawie poniższych opisów:

- Priorytet krytyczny - Incydent wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT. Procesy wewnętrzne są sparaliżowane lub zakłócone w znaczącym stopniu. Istnieje wysokie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
- Priorytet wysoki - Incydent wymaga szybkiego działania oraz zgłoszenia do właściwego CSIRT w ciągu 24 godzin. Procesy wewnętrzne są częściowo zakłócone lub sparaliżowane. Istnieje niskie ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji.
- Priorytet średni - Incydent prawdopodobnie nie wymaga niezwłocznego działania oraz zgłoszenia do właściwego CSIRT ze względu na brak symptomów działania z zewnątrz. Procesy wewnętrzne nie są sparaliżowane lub zakłócone w żadnym stopniu. Ryzyko wycieku danych (np. danych osobowych) oraz utraty poufności, integralności i/lub dostępności informacji nie występuje.

- Budowanie zespołów ds. bezpieczeństwa: Definicja ról, odpowiedzialności, umiejętności oraz ścieżek rozwoju dla członków zespołu bezpieczeństwa.
- Lista omówionych kompetencji w szkoleniu:

- Szef działu bezpieczeństwa (kierownik, dyrektor);
- Pełnomocnik ds. Bezpieczeństwa Informacji;
- Specjalista ds. Zarządzania Ryzykiem;
- Specjalista ds. Zgodności;
- Specjalista ds. Bezpieczeństwa Fizycznego;
- Architekt Systemów Bezpieczeństwa;
- Koordynator Programu Bezpieczeństwa;
- Analityk Bezpieczeństwa (II linia wsparcia);
- Inżynier ds. Bezpieczeństwa (II linia wsparcia);
- Administrator Systemów Bezpieczeństwa (II linia wsparcia);
- Specjalista ds. Odpowiedzi na Incydenty (III linia wsparcia);
- Specjalista ds. Testów Penetracyjnych (III linia wsparcia);
- Specjalista ds. Testów Socjotechnicznych (III linia wsparcia).

4. Regulacje prawne i compliance:
- Zharmonizowanie działalności Podmiotu z imperatywami Ustawy o Krajowym Systemie Cyberbezpieczeństwa, z naciskiem na implementację procedur i protokołów zapewniających wytrzymałość infrastruktury informatycznej na potencjalne zagrożenia cyfrowe.

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

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

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

- Techniki hardeningu: Wzmocnienie infrastruktury IT oraz zarządzanie patchami bezpieczeństwa.
- Testy penetracyjne i socjotechniczne: Organizacja i przeprowadzanie testów w celu oceny gotowości organizacji Szkolenie powinno odbyć się w czasie nie krótszym niż 4 godziny robocze w ciągu jednego dnia z uwzględnieniem conajmniej 4 przerw po 15 minut. Powinno jest 30 minut na pytania i odpowiedzi uczestników.

MagikINFO

O
gólne wymagania:
1. Oprogramowanie musi posiadać bezterminową licencję.
2. Oprogramowanie musi posiadać interface użytkownika w języku polskim.
3. Wsparcie techniczne mailowe oraz telefoniczne musi byś dostępne w języku polskim.
4. Dane muszą być przechowywane w bazie MS SQL (wersja płatna lub darmowa).
5. System musi posiadać mechanizm automatycznego usuwania danych z audytu oraz monitoringu starszych niż wybraną ilość dni, co zapewni automatyczne pilnowanie wielkości bazy.
6. Moduły systemu muszą być wzajemnie zintegrowane. Korzystanie z tych samych słowników, katalogu użytkowników, informacji o majątku itp.
7. System musi zapewnić możliwość logowania do systemu z różnymi poziomami uprawnień. System musi umożliwić podział bazy danych na homogeniczne całości (możliwość odizolowania np. poszczególnych jednostek organizacyjnych pod względem zarządzania w systemie oraz pracy z wynikami na podstawie uprawnień użytkowników systemu).
8. System musi posiadać opcję automatycznego przypisywania użytkowników do komputerów na podstawie zalogowanego użytkownika na stacji.
9. Musi istnieć opcja podziału komputerów do grup według struktury organizacyjnej, lokalizacji i użytkownika.
10. Musi istnieć opcja przypisania administratora do pewnej grupy komputerów i na tej podstawie system musi zabezpieczyć, by przypisany administrator po zalogowaniu widział wyłącznie dane z przypisanych do niego komputerów.
11. Systemu musi umożliwiać określenie dostępu do poszczególnych części systemu na podstawie uprawnień użytkownika. W zależności od ustawionego poziomu dostępu system musi ukryć odpowiednie elementy interfejsu, np. administrator majątku po zalogowaniu widzi tylko elementy dotyczące majątku.
12. System musi umożliwić integrację z Active Directory - wsparcie wielu domen - dla komputerów oraz osób można ustawić dowolną ilość domen lub kontenerów, które będą synchronizowane.
13. Musi być dostępna opcja cyklicznej synchronizacji użytkowników i komputerów z Active Directory. Po synchronizacji możliwość automatycznego uruchomienia dowolnych poleceń SQL.
14. System musi posiadać natywny sposób instalacji agentów (bez użycia paczek msi lub exe; bezpośrednio z konsoli/strony zarządzania system) i zarazem umożliwiać instalację z paczek msi.
15. System oprócz domyślnego sposobu przesyłania wyników musi umożliwić agentom wysyłanie wyników na serwer FTP.
16. Możliwość pracy systemu w: sieciach rozproszonych, sieciach spiętych VPN-em, w Internecie (za NAT-em).
17. Interface systemu musi umożliwiać eksport wszystkich tabeli oraz raportów do formatów: .csv, .xls lub .xlsx, .html, .pdf, .rtf, .jpeg, .png.
18. System musi posiadać interface webowy dla całego systemu – umożliwiający przeglądanie wyników z audytu oraz monitoringu za pośrednictwem przeglądarki www według definiowanych uprawnień. Dostępna musi być opcja przeglądania wyników z własnego komputera lub z danej jednostki organizacyjnej czy lokalizacji.
19. System musi umożliwiać zapisanie ustawień tabelek, musi istnieć opcja, by zapisać: widoczność, szerokość i kolejność poszczególnych kolumn.
20. Musi istnieć opcja dostosowania głównego menu konsoli zarządzającej. Dodatkowo system powinien posiadać pasek zawierający skróty do najczęściej używanych ekranów systemu..
21. System musi umożliwiać dostosowanie interface (www lub aplikacja natywna) za pomocą tematów (schematy kolorów elementów interface).
22. System musi umożliwiać tworzenie kopii zapasowej bazy danych oraz jej odtwarzanie bezpośrednio z konsoli zarządzającej.
23. W związku z rozporządzeniem RODO system musi umożliwiać monitorowanie modyfikacji w katalogu osób oraz anonimizację danych użytkowników.
najczęściej używanych ekranów systemu.

Synchronizacja z Active Directory:
1. System musi umożliwiać pobieranie danych z wielu domen - dla komputerów oraz osób można ustawić dowolną ilość domen lub kontenerów, które będą synchronizowane.
2. System musi umożliwiać automatyczne zmiany stanu komputerów

usuniętych z AD. Na przykład: jeżeli komputer (jako obiekt) zostanie wyłączony w AD lub zostanie skasowany z domeny - automatycznie zostanie zmieniony stan na „Usunięty” (lub podobny). Ta funkcjonalność musi być opcjonalna.
3. System musi mieć opcję cyklicznego pobierania i zapisywania nowych osób oraz komputerów z AD.

Audyt
1. System musi umożliwiać przeprowadzenia audytu na komputerach z systemami Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server, Windows 2008 R2 Server, Windows 2012 Serve, Windows Serwer 2016, Windows Serwer 2019, Windows Serwer 2022.
2. System musi umożliwiać audyt stacji z system Linux – wsparcie dystrybucji takich jak Debian, Ubuntu, RHEL, Centos oraz wszystkich ich pochodnych. Skan musi wykrywać oprogramowanie zainstalowane z paczek, sprzęt, daemony (usługi) oraz pliki danych. Agent musi umożliwiać uruchamianie audytu wg ustawionego harmonogramu.
3. Musi istnieć opcja, by w ramach audytu wyświetlić ankietę użytkownikowi komputera, zdefiniowaną przez administratora. Wyświetlanie/niewyświetlanie musi być konfigurowalne.
4. System musi posiadać opcję audytowania komputerów za pośrednictwem zewnętrznego nośnika (pendrive) lub wersji przenośnej agenta. Chodzi o audyt komputerów niepodłączonych do sieci lub w sieciach odseparowanych.
5. Agent musi zebrać szczegółowe dane na temat komputera i jego podzespołów (procesorów, pamięci, płyty głównej, dysków twardych, nośników danych itp.) wraz z numerami seryjnymi (lub możliwość ręcznego dopisania numerów seryjnych).
6. System musi automatycznie wykrywać typ komputera podczas audytu – i potem wyraźnie rozgraniczać stacjonarne, przenośne, serwery oraz wirtualne komputery.
7. Podczas audytu musi być wykrywana wersja systemu operacyjnego wraz z kluczem licencyjnym i numerem seryjnym.
8. System musi dokładnie wykrywać oprogramowanie zainstalowane na komputerze. Nie zależnie od tego, czy program został zainstalowany przez użytkownika (do profilu użytkownika), czy przez administratora. Niezależnie od tego, czy program został skopiowany (np. kopia „Program Files” ze starego komputera), czy zainstalowany z paczki msi lub pliku exe. W tych wszystkich wypadkach program musi się pojawić na liście wykrytego oprogramowania.
9. MS Office musi być wykryty wraz z kluczem licencyjnym, jeżeli jest używany dla tej wersji Office/Microsoft 365.
10. System musi umożliwiać dostosowanie wyświetlanej szczegółowości wersji dla każdego programu (np. możliwość grupowania 4.x lub 4.1.x itd.).
11. System musi umożliwić zbieranie informacji (nazwa, ścieżka, wielkość pliku) na temat wszystkich plików na dysku. Musi umożliwiać administratorowi zdefiniowanie rozszerzeń plików, które będą brane pod uwagę podczas skanowania.
12. System musi wyświetlać ścieżki do plików deinstalatorów wszystkich programów instalowanych z plików exe.
13. System musi posiadać ekran, na którym można sprawdzić dokładne nazwy aplikacji oraz producenta tak, jak są zapisane w „Dodaj i usuń programy” w systemie Windows.
14. System musi posiadać agenta na urządzenia z systemem Android. Musi on umożliwiać zebranie danych na temat zainstalowanych programów oraz informacje o sprzęcie. Audytowanie urządzeń z Androidem nie może wymagać dodatkowych licencji w systemie.
15.Musi istnieć możliwość przeglądania wyników z audytu za pośrednictwem przeglądarki www. Dostępne muszą być raporty zbiorcze oraz szczegółowe wyniki z poszczególnych komputerów.

Raportowanie
1. System musi posiadać raport wyświetlający wkrótce wygasające licencje i gwarancje.
2. Muszą być dostępne raporty wyświetlające zbiorczo znalezione oprogramowanie z możliwością wyświetlania danych statystycznych dla poszczególnych jednostek organizacyjnych lub lokalizacji (np. odpowiedź na pytanie: Ile mamy Office w dziale informatyki?).
3. Muszą istnieć raporty wyświetlające, do których programów została przypisana licencja), a które jej nie posiadają.
4. System musi wyświetlać ilość wolnego miejsca na dyskach komputerów. Powinna być dostępna informacja o ilości wolnego miejsca w procentach i GB.
5. Muszą istnieć raporty wyświetlające nazwę, rozmiar oraz dokładną lokalizację (ścieżka dostępu) plików danych.
6. System musi umożliwiać automatyczne porównywanie zmian pomiędzy stanem aktualnym a poszczególnymi audytami dla oprogramowania i sprzętu.

7. System musi umożliwiać szybkie fulltextowe wyszukiwanie we wszystkich tabelach oraz obliczeń statystycznych w kolumnach.
8. System musi posiadać raporty graficzne. Minimum to 5 różnych rodzajów danego raportu. Raporty graficzne muszą dotyczyć danych sprzętowych (np. wykaz rodzajów procesorów w formie graficznej) oraz statystyk oprogramowania (np. top X najczęściej występujących programów).
9. W oprogramowaniu musi istnieć opcja tworzenia dokumentów dotyczących przekazania majątku, np.: protokół przekazania komputera, karta majątku itp.
10. Baza SQL musi być utworzona logicznie, nazwy tabelek muszą sugerować ich zawartość a relacje pomiędzy nimi muszą być oczywiste lub udokumentowane przez producenta. System musi mieć możliwość tworzenia i uruchamiania własnych raportów – zapytań SQL bezpośrednio z programu.
11.System musi posiadać wbudowany designer raportów, możliwość pracy z szablonami raportów.
12. System powinien posiadać dashboard – zestaw raportów przeglądowych. Najważniejsze informacje dotyczące oprogramowania, licencji, sprzętu, majątku, na jednym ekranie.
13. System musi posiadać raport dotyczący majątku w organizacji. Ma on umożliwiać statystyczny widok posiadanego majątku. Zestawienia w postaci wykresów, tabelek lub innych elementów muszą umożliwienie odpowiedzi na pytania typu „Ile mamy drukarek w organizacji?”.

Licencjonowanie i baza wzorców
1. System musi umożliwiać zarządzanie posiadanymi licencjami – bieżące śledzenie licencji i porównywanie zakupionych licencji z użytkowanymi.
2. Musi istnieć możliwość wprowadzania licencji Upgrade, czasowych, ewidencja licencji CAL, MOLP, OEM.
3. System musi mieć opcję przypisania różnych programów lub wielu wersji programu do jednej licencji. Licencje są automatycznie przeliczane wg ustawionego priorytetu (np. pod jedną pozycję wpisujemy 10szt. licencji systemu operacyjnego a licencja może obowiązywać dla Windows 10 oraz Windows 11).
4. Zarządzanie licencjami musi umożliwiać automatyczne przypisywanie oraz odbieranie. Dla multilicencji lub licencji retailowych można wykorzystać oprócz automatycznego przypisywania również automatyczne odbieranie. Jeżeli program zostanie usunięty z komputera, licencja wróci do puli wolnych licencji. Jeżeli program zostanie zaktualizowany to, jeżeli licencja na to pozwala, zostanie przeniesiona na aktualną wersję programu.
5. Identyfikacja zainstalowanego oprogramowania na podstawie własnej bazy wzorców aplikacji, programów – system sam natychmiast automatycznie rozpoznaje każdą nową wersję znanego oprogramowania bez ręcznego uzupełniania wpisu w bazie.
6. System musi oferować bezterminowe uprawnienia do aktualizacji bazy wzorców aplikacji, programów (bez konieczności wykupienia wsparcia, subskrypcji, abonamentu itp.).
7. System musi posiadać rozpoznawanie oprogramowania na podstawie wzoru generowanego za pomocą zdefiniowanych reguł (automatyczne wykrycie i rozpoznanie nowej wersji wcześniej zidentyfikowanego programu).
8. Musi istnieć opcja edycji bazy wzorców – tworzenie reguł, wyjątków.

Zarządzanie majątkiem
1. System musi automatycznie wykrywać typ komputera (stacjonarny, przenośny, wirtualny, …).
2. System musi umożliwiać ewidencjonowanie dowolnego sprzętu elektronicznego (skaner, drukarka, pendrive, switch, komórka itd.), ale również np. szafa, biurko, samochód, ...
3. System musi umożliwiać zachowanie danych dotyczących wycofanego komputera w bazie danych nie zajmując licencji systemu audytującego.
4. System musi posiadać funkcję importu sprzętu do programu z pliku csv.
5. W module majątku musi istnieć opcja dodania własnych pól dla obiektu majątku.
6. System musi umożliwiać rejestrowanie napraw sprzętu.
7. System powinien umożliwiać przeglądy majątku – wykonywanie cyklicznych działań, takich jak regularne przeglądy, testy czy serwis. System ma ostrzegać o zbliżających się przeglądach za pośrednictwem komunikatów lub wysyłając maila pod wskazane adresy.
8. Operacje na majątku muszą umożliwiać wykonywanie ich na wielu pozycjach na raz. Zbiorcze działania muszą umożliwiać szybkie przenoszenie do magazynu, zmiany stanu, przeniesienia pomiędzy jednostkami, lokalizacjami lub osobami.
9. Dostępna musi być opcja załączenia elektronicznych dokumentów do wybranych pozycji w majątku lub licencji (faktury, dokumenty, itd.), preferowanie jest zapisywanie załączników w formie plików przed zapisywaniem ich w bazie danych.

10. Raporty w postaci list majątku, kart, specyfikacji, protokołów przeniesienia, usunięcia... powinny być łatwo dostępne i uruchamiać się bezpośrednio z głównego ekranu wyświetlającego majątek. Raporty dodawane lub modyfikowane przez administratora muszą być dostępne z tego samego menu.
11. System musi umożliwiać ewidencjonowanie działań takich jak np. wprowadzenie do użytkowania, naprawy, przesunięcia i wycofanie.
12.System musi posiadać opcje potwierdzenia przekazania majątku użytkownikowi za pomocą strony www.
13. System musi posiadać aplikację na urządzenia z systemem Android do sczytywania kodów kreskowych (zamiast terminali). Aplikacja po zeskanowaniu kodu kreskowego musi wyświetlać dane dotyczące zeskanowanego obiektu (nazwa, użytkownik, lokalizacja, nr ewidencyjny, ...). Aplikacja musi umożliwiać także wprowadzanie nowych pozycji majątku podczas inwentaryzacji, określenie dokładnego położenia majątku (piętro, pokój, użytkownik itp.), daty inwentaryzacji.
14.Aplikacja mobilna do sczytywania kodów kreskowych powinna umożliwiać bezpośrednią synchronizację z bazą danych. Aplikacja musi umożliwiać również tryb "offline", czyli do synchronizacji powinno dochodzić tylko wtedy, kiedy osoba inwentaryzująca zdecyduje o tym. Aplikacja musi umożliwiać przeprowadzenie całego procesu inwentaryzacji bez dostępu do sieci/bazy danych.
15.System musi posiadać opcję Inwentaryzacji za pomocą interface webowego. Każdy użytkownik musi zostać powiadomiony o konieczności wypowiedzenia się na temat posiadanego sprzętu. Po kliknięciu na link, ma mu się otworzyć strona, na której musi potwierdzić lub skorygować informacje o posiadanym sprzęcie.
16. Automatyczne tworzenia historii komputera – system musi umożliwiać stwierdzenie, kiedy np. doszło do zmiany użytkownika komputera bez aktywnego wprowadzenia informacji o przeniesieniu (automatyczne wykrywanie/rejestrowanie zmiany użytkownika).
17. Moduł do ewidencji majątku musi umożliwiać ewidencjonowanie akcesoriów do danego sprzętu. Akcesoria mają być pozycją, którą można bardzo szybko przypisać do danego obiektu i nie posiadają szczegółów (takich jak nr ewidencyjny, seryjny, …). Przykładem niech będzie np. etui i ładowarka przypisana do laptopa.
18. Powinna istnieć opcja oznaczania symbolem (np. gwiazdką) ulubionych pozycji w module majątku.
19. Musi istnieć opcja powielania majątku. Powielanie spowoduje skopiowanie cech wybranej pozycji takich jak typ, nazwa, lokalizacja, itd.

Zdalne zarządzanie
1. System musi posiadać opcję zdalnego zarządzania stacjami:
a. przejęcie kontroli (przejęcie obecnej sesji użytkownika), przesyłanie wiadomości, sprawdzenie jakości połączenia, możliwość kopiowania plików, przejmowanie monitora, myszy, klawiatury; zdalne wyłączanie komputera, zdalny restart.
b. skan otwartych i zamkniętych portów.
c. skan stanu usług w momencie audytu.
d. zdalne zarządzanie usługami (status, sposób uruchomienia).
e. Remote Desktop Protocol – zdalny pulpit dostępny bezpośrednio z programu.
2. Powinien być dostępny zdalny pulpit również poza siecią lokalną - połączenie ma realizowane być za pomocą elementu pośredniczącego, który może być umieszczony w strefie zdemilitaryzowanej (DMZ) lub gdziekolwiek w Internecie, bez konieczności używania pośrednika trzecich stron.
3. System powinien umożliwiać pobranie przynajmniej podstawowych danych za pomocą protokołu SNMP - możliwość wyszukiwania drukarek, urządzeń sieciowych, NAS-ów i dodawania ich do modułu majątku.

Zdalna zbiorcze zarządzanie (skryptowanie, instalacje, ...)
1. System musi umożliwiać wykonywanie następujących czynności zbiorczo, bez interakcji użytkownika docelowego sprzętu: instalacja oprogramowania, odinstalowanie programu, kopiowanie plików na docelową stację, kasowanie plików i katalogów, uruchamianie skryptów lub plików wykonywalnych, wyłączenie i restart komputera, wylogowanie użytkownika (również poza siecią lokalną).
2. Musi istnieć opcja zdefiniowania kilku serwerów, z których będą przebiegały instalacje.
3. System musi umożliwiać warunkowe wykonywanie poszczególnych kroków zadań: bez poprawnego wykonania działania, następne działania nie zostaną uruchomione.
4. Musi istnieć opcja zaplanowania wykonania działań, niezależnie od tego, czy wybranego komputery za włączone lub wyłączone.

Alertowanie zdarzeń

1. System musi umożliwiać powiadamianie za pomocą maila oraz wyskakujących okien.
2. Musi istnieć opcja definiowania dni poprzedzających notyfikację związaną z zdarzeniem (np. miesiąc przed, tydzień przed, dzień przed i każdy dzień po terminie).
3. System musi oferować przynajmniej powiadomienia o wygasających licencjach i gwarancjach. Plusem jest możliwość definiowania własnych powiadomień.
4. System musi umożliwiać wysyłanie powiadomień związanych ze zbliżającym się terminem przeglądu, lub listą urządzeń, na których nie zostały wykonane czynności serwisowe w terminie.
5. Musi istnieć opcja wysyłania alertów/maila w przypadku usunięcia użytkownika z Active Directory z informacją o tym, że powinien oddać przypisany mu majątek IT.

Podstawowe wymagania modułu:
1. Monitoring i blokowanie aplikacji.
2. Monitoring i blokowanie stron www.
3. Monitoring i blokowanie dysków USB.
4. Monitoring wydruków.
5. Monitoring obciążenia komputerów.

Monitoring
1. System musi umożliwiać monitoring czasu pracy w aplikacji, ilość naciśnięć klawiszy klawiatury, ilość kliknięć myszką, podział czasu działania aplikacji na czas pracy (od momentu włączenia do momentu wyłączenia aplikacji) oraz czas aktywności (rzeczywisty czas aktywności użytkowników, okno (on top) na ekranie), statystyki wg czasu, grup, aplikacji.
2. Monitoring musi umożliwiać ustawienie czasu nieaktywności (timeout naliczania aktywności) - po określonym czasie nieaktywności, licznik czasu spędzonego pracą w aplikacji, zostanie zatrzymany.
3. Muszą być do dyspozycji informacje o odwiedzanych przez użytkowników stronach www: czas, statystyki wg domeny, czasu, użytkownika, konkretnych stron, czas pracy, czas aktywności użytkownika, dokładny adres strony www – aktywny odnośnik, tytuł strony.
4. Monitoring musi zbierać wartości obciążenia procesora i wykorzystania pamięci.
5. Monitoring musi umożliwiać (opcjonalne) śledzenie ruchu na kartach sieciowych komputera. Monitorowana ma być ilość pobranych (download) oraz wysłanych (upload) danych.
6. Agent musi umożliwiać monitoring wydruków (jakie dokumenty, ile, z jakiej drukarki, kiedy, jaki użytkownik drukował, wysokość i szerokość kartki, liczba kopii, kolor, wydruk obustronny).
7. System musi umożliwiać monitorowanie zmian na dyskach USB (zmiana nazwy pliku, wielkości, kasowanie pliku, itp.).
8. System musi umożliwiać monitorowanie zmian w wybranych katalogach (zmiana nazwy pliku, wielkości, kasowanie pliku, modyfikacja itp.).
9. Agent musi wspierać ustawienie przedziału czasowego monitoringu (np. od 7:00 do 15:00), wyłączenie monitorowania w weekendy.
10. Agent musi się automatycznie aktualizować do najnowszej wersji – można określić częstotliwość sprawdzania nowej wersji agentów lub konfiguracji. Równocześnie można określić częstotliwość wysyłania wyników monitoringu ze stacji.
11.Agent musi umożliwiać wysyłanie wyników monitoringu z dowolnego miejsca w internecie do centrali.
12. Agent musi umożliwiać wyłączenie poszczególnych dziedzin monitoringu: www, aplikacje, obciążenie procesora, obciążenie pamięci RAM, monitoring wydruków, czas zalogowania / wylogowania użytkownika.
13. System musi umożliwiać tworzenie dowolnej ilości profili monitoringu – można określić, w jakim zakresie będą poszczególne grupy komputerów monitorowane lub ograniczane.
14.Agent musi umożliwiać włączenie wyświetlania komunikatu przy starcie agenta. Tekst tego komunikatu musi być konfigurowalny w ustawieniach.

Agent musi umożliwiać blokowanie:
1. Blokowanie aplikacji – możliwość zdefiniowania aplikacji zabronionych i uniemożliwienie ich uruchomienia (także w przypadku kiedy użytkownik zmieni nazwę pliku uruchomieniowego). Musi istnieć opcja konfiguracji notyfikacji mailowej o tym zdarzeniu. Agent musi umożliwiać wyświetlenie informacji użytkownikowi o zablokowaniu aplikacji.

2. Blokowanie stron www, blokowanie wszystkich protokołów dla danej domeny, takich jak: http, https, ftp, imap, pop3, smtp, itp.
3. Blokowanie dysków USB wg numeru seryjnego dysku.
4. Autoryzacja dysków USB - definiowanie „białej listy" dysków USB i blokowanie nieautoryzowanych.
5. Blokowanie napędów CD/DVD.

Raportowanie
1. System musi oferować raporty z monitoringu (czasowe, wg użytkownika, wg kategorii, zbiorcze, szczegółowe …).
2. Tabele z wynikami monitoringu muszą umożliwiać sortowanie i filtrowanie wg jednostki organizacyjnej, lokalizacji, nazwy komputera, użytkownika....
3. System musi generować graficzne przedstawienie wyników – 3D wykresy (minimum 5 rodzajów) z legendą lub bez legendy.
4. System musi umożliwiać szybko zorientować się w negatywnych zjawiskach w organizacji za pośrednictwem raportów graficznych wyświetlających użytkowników (TOP 5 itp.), którzy korzystają z niepożądanych programów, gier, komunikatorów, multimediów, niepożądanych www, gier i rozrywki, portali społecznościowych, sklepów internetowych, użytkowników najwięcej drukujących dokumenty, wykonujących działania na USB, komputerów najbardziej obciążających CPU i RAM. Wszystko dla wybranego przedziału czasowego oraz (opcjonalnie) wybranego działu.
5. Mile widziana jest forma Dashboardu wyświetlającego dane monitoringu aktywności. Szybkie zestawienia dotyczące różnych aspektów zachowania użytkowników.
6. System musi oferować kategoryzację programów wg wykorzystania (np.: praca, zabawa, zabronione…) oraz wg typu programu (np.: gry, przeglądarki, antywirusy, …).
7. System musi umożliwiać kategoryzację stron www wg wykorzystania (zakazane, rozrywka, wiadomości i inne) oraz ich tematów (np. dla kobiet, sport, polityka, hazard, …).
8. System musi wyświetlać chronologicznie działania użytkownika w ciągu dnia od momentu zalogowania się aż po wylogowanie. Raport musi zawierać dane umożliwiające określenie, co użytkownik robił w danej chwili.
9. Musi istnieć opcja przeglądania wyników monitoringu przez www.
Administrator musi mieć opcję ustawienia dostępu do raportów dla poszczególnych osób. Na przykład, manager działu produkcji ma dostęp do wyników swoich pracowników oraz działu przygotowania.
3. Blokowanie dysków USB wg numeru seryjnego dysku.
4. Autoryzacja dysków USB - definiowanie „białej listy" dysków USB i blokowanie nieautoryzowanych.
5. Blokowanie napędów CD/DVD.