Cyberbezpieczny Samorząd

Opis Przedmiotu Zamówienia

Aspekty techniczne

POWIAT BARTOSZYCKI

Bartoszyce, 03.04.2025

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

Wstęp

Niniejszy dokument stanowi Opis Przedmiotu Zamówienia (OPZ) w zakresie dostawy i wdrożenia oprogramowania i sprzętu służącego realizacji projektu. Wszystkie parametry techniczne określone w

niniejszym OPZ określają **minimalne** wymagania stawiane oferowanym urządzeniom i oprogramowaniu. Wykonawca nie ma prawa żądać dodatkowego wynagrodzenia, jeśli dostarczone elementy systemów posiadały będą większą funkcjonalność niż wymagana niniejszym OPZ.

1. Wymagania ogólne

Dostarczane rozwiązania muszą być zbudowane i wdrożone zgodnie z obowiązującymi przepisami prawa, zgodnie ze strukturą organizacyjną i regulaminami Zamawiającego, rozporządzeniami oraz dobrymi praktykami.

Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień jego instalacji (tzn. powinno być dostosowane do zmieniających się powszechnie obowiązujących przepisów prawa lub regulacji wewnętrznych Zamawiającego).

Dostarczany w ramach postępowania System nie może być przeznaczony do wycofania z produkcji, sprzedaży lub wsparcia technicznego.

2. Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania dokumentacji projektowej realizacji każdego Zadania. Dokumentacja projektowa będzie przechowywana przez cały okres realizacji projektu.

2.1 Wytyczne do analizy przedwdrożeniowej

Wykonawca jest zobowiązany na żądanie zamawiającego do przygotowania i dostarczenia w wyznaczonym przez Zamawiającego terminie analizy przedwdrożeniowej.

Analiza przedwdrożeniowa ma na celu opisać sposób wdrożenia wymaganych przez OPZ funkcjonalności tak aby spełniały one swoje funkcje. Wykonawca winien wskazać konieczność zaplanowania przerwy ale także określić szacowany termin i szacowany czas trwania przerwy. Jeśli realizacja określonych funkcjonalności wymaga dodatkowych rozwiązań, należy wskazać proponowane metody ich osiągnięcia.

2.2 Dokumentacja powykonawcza

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika, Instrukcję użytkownika i administracji udostępnioną przez Producenta systemu zawierającą opis działania danego elementu systemu w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania – w wersji elektronicznej.

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył Politykę backupu zgodnie z dobrymi praktykami i wymaganiami dostarczonych systemów.

CZĘŚĆ 1 – OBSZAR TECHNICZNY

1. Rozwiązanie sprzętowe do wirtualizacji zapewniającej izolację sieci oraz replikację wraz z przywracaniem systemów dla Starostwa

Minimalne parametry techniczne i funkcjonalne:

Parametr	Charakterystyka
Wymagania ogólne	• Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack.
Wymagane parametry fizyczne	Wymagane parametry fizyczne a) możliwość montażu w szafie 19” b) jeden wewnętrzny zasilacze 230V AC typu hot-swap. Z możliwością dołożenia dodatkowe zasilacza o tych samych parametrach. (nie dopuszcza się rozwiązań zewnętrznych zasilaczy) c) port USB umożliwiający podłączenie zewnętrznej pamięci flash
Wymagana konfiguracja portów	Przełącznik musi posiadać minimum: Minimum 8 portów 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Wszystkie powyższe porty muszą być dostępne od frontu urządzenia. Z urządzeniem powinny być dostarczone: 4 wkładki SFP+ 10G supports multimode fiber (oficjalnie wspierane przez producenta) 2 kable DAC SFP+ 10G minimum 7m każdy (oficjalnie wspierane przez producenta)
Przełącznik	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) Zarządzanie stosem poprzez jeden adres IP b) Do min. 8 jednostek w stosie c) Magistrala statkująca o wydajności 80Gb/s d) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie e) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree f) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
Matryca przełączająca	Matryca przełączająca o wydajności min. 240 Gbps, wydajność przełączania przynajmniej 178 Mpps.

Parametr	Charakterystyka
	• Obsługa min 16 000 adresów MAC
	• Wbudowana pamięć RAM min. 1 GB
	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 2 GB
	• Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
	• Obsługa ramek jumbo o wielkości min. 9 216 bajtów
	• Obsługa protokołu GVRP lub równoważny
	Wsparcie dla protokołów: • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 16 instancji protokołu MSTP lub zastosowanie osobnej instancji STP dla każdego VLANu. • Ethernet Ring Protection version 2
Mechanizmy związane z zapewnieniem bezpieczeństwa sieci	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL b) Możliwość uwierzytelnia użytkowników przez wbudowany w przełącznik CaptivePortal – nie dopuszcza się rozwiązań z uwierzytelnieniem na zewnętrznym Captive Portal. c) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny),
	Implementacja co najmniej 4 kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
	Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3.
Wymagane opcje zarządzania	a) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN, b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC), c) urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów

Parametr	Charakterystyka
	systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych, d) dedykowany port konsoli zgodny ze standardem RS-232, e) Obsługa skryptów BASH oraz Python Możliwość zarządzania przełącznikiem przez Rest API – konieczność obsługi wszystkich funkcji przełącznika.
	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.
	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z ofertą oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.

2. Rozwiązania sprzętowe BDR dla Starostwa

Minimalne parametry techniczne i funkcjonalne:

Parametr	Charakterystyka
Obudowa	Macierz musi mieć możliwość zainstalowania w standardowej szafie rack 19". Rozmiar jednostki sterującej macierzą nie może przekraczać 2U . Dodawanie kolejnych półek lub dysków musi odbywać się bezprzerwowo. Całkowity rozmiar dostarczonej macierzy wraz z półkami rozszerzeń nie może przekraczać 2U.
Kontrolery	Wymagane dwa moduły sterujące macierzą pracujące w trybie active-active. W przypadku wystąpienia awarii sprawny moduł musi automatycznie przejąć obsługę wszystkich zasobów prezentowanych przez macierz.
Dostępne porty	Oferowana macierz musi posiadać w chwili dostawy minimum po 4 porty 10/25 Gb iSCSI SFP28 na kontroler (w sumie 8 portów na macierz). Wraz z macierzą powinny zostać dostarczone co najmniej 4 wkładki SFP+ 10Gb z przewodami LC-LC OM4 MMF o długości 3m oraz co najmniej 2 przewody DAC SFP+ o długości 3m. Oferowana macierz musi mieć możliwość wymiany portów (poprzez wymianę karty rozszerzeń) na - karty posiadające 4 porty SAS 12Gb każda - karty posiadające 4 porty 32Gb FC każda - karty posiadające 2 porty 10Gb iSCSI RJ45

Parametr	Charakterystyka
Cache	Każdy z modułów sterujących musi być wyposażony w min 8 GB pamięci cache zabezpieczonej mechanizmem mirroringu. Pamięć podręczna musi być zabezpieczona przed utratą danych w przypadku zaniku zasilania. Rozwiązania wykorzystujące do tego celu tylko i wyłącznie tzw. podtrzymanie cache za pomocą baterii nie są akceptowalne. Bateria może być użyta tylko i wyłącznie na czas zrzutu danych z cache na pamięć nieulotną. Ponadto macierz musi umożliwiać utworzenie dedykowanej przestrzeni SSD stanowiącej pamięć cache pośredniczącą w operacjach odczytów danych z macierzy. Wymaga się możliwości utworzenia takiej przestrzeni o wielkości 4TB.
Dyski	Macierz musi obsługiwać dyski SSD, SSD FIPS, SAS, NL-SAS, NL-SAS FIPS, SAS FIPS. Macierz w momencie dostarczenia musi być wyposażona w minimum 12 dysków SAS SSD o pojemności minimum 3.84TB każdy . W chwili dostawy wymagane jest dostarczenie macierzy pozwalającej na montaż co najmniej 24 dysków 2.5”. Macierz musi umożliwiać rozbudowę pozwalającą na montaż sumarycznie minimum 96 dysków 2,5 cala,
Funkcjonalność	Macierz musi obsługiwać typy protekcji RAID 0,1,3,5,6,10 oraz powinna posiadać funkcjonalność zarządzania informacjami o parzystości oraz dyskami spare w całej puli dysków utworzonej ze wszystkich dysków które mogą zastać zainstalowane w macierzy. W przypadki awarii dysku, do jego obudowy musi być używany każdy dysk z takiej puli Macierz musi umożliwiać zwiększanie i zmniejszanie online pojemności poszczególnych wolumenów logicznych oraz dynamiczne alokowanie przestrzeni dyskowej (tzw. „*thin provisioning*”). Macierz musi posiadać funkcjonalność sprawdzania integralności zapisywanych danych poprzez odczyt sumy kontrolnej z karty HBA podłączonego serwera. . Macierz musi mieć możliwość wykonywania minimum 512 kopii migawkowych typu copy-on-write (jeśli funkcjonalność wymaga licencji, nie jest wymagana w momencie dostawy). Macierz musi posiadać funkcjonalność klonowania danych. Wymagana możliwość definiowania maksymalnej ilości kopii migawkowych. W przypadku osiągnięcia zdefiniowanej ilości kopii system musi automatyczne kasować kopie najstarsze. Ponadto macierz powinna posiadać funkcjonalność tworzenia konsystentnych kopii migawkowych ze wskazanych przestrzeni dyskowych. Macierz musi mieć możliwość replikacji danych po FC w trybie asynchronicznym. Macierz musi pozwalać na wykonanie do 32 jednoczesnych replikacji bez używania systemów zewnętrznych wykonujących replikację. Nie wymaga się funkcjonalności replikacji w momencie dostawy. Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 512 partycji.

Parametr	Charakterystyka
	Wymagana możliwość definiowania globalnych dysków hot-spare. Wymagana możliwość logicznej zamiany dysków z wykorzystaniem dysków nieprzypisanych. Macierz musi posiadać automatyczny monitoring z możliwością informowania o awariach poprzez protokół smtp oraz snmp oraz możliwość wysyłania powiadomień awarii do wskazanych odbiorców. Wysyłane powiadomienia musza zawierać nazwę macierzy, informacje o typie zdarzenia, datę i czas wystąpienia zdarzenia oraz krótki opis zdarzenia. Macierz musi mieć możliwość definowania poziomu zajętości miejsca, po osiągnięciu którego nastąpi wysłanie powiadomienia pod wskazane adresy email. System zarządzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego automatycznie w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień oraz braku wykrycia jakichkolwiek zadań wykonywanych na macierzy. Macierz musi mieć funkcjonalność automatycznej detekcji podłączonych hostów (nazwa hosta oraz typ systemu operacyjnego). Musi być możliwość edycji hostów dodanych w sposób automatyczny. Wymagana jest funkcjonalność automatycznego tworzenia przestrzeni dyskowych zoptymalizowanych pod katem używanych na nich aplikacji jak SQL Server, Exchange oraz Vmware vmfs. Wymagana jest możliwość automatycznego logicznego grupowania dysków macierzy (dodawanie dysków do istniejącej grupy oraz tworzenie nowej grupy z dodanych dysków). Macierz musi mieć możliwość definiowania priorytetu operacji wprowadzanych zmian konfiguracji w odniesieniu do obciążenia generowanego przez podłączone hosty. Wymagana jest możliwość sprawdzenia aktualnych zadań macierzy. Macierz musi umożliwiać szyfrowanie zapisywanych na niej danych. Nie wymaga się tej funkcjonalności w chwili dostawy. Macierz musi posiadać możliwość fizycznej identyfikacji (dioda LED) aktywowanej z interfejsu zarządzania oraz funkcjonalność fizycznego identyfikowania dysków (dioda LED) należących do jednej przestrzeni logicznej. Macierz musi mieć możliwość przypisania wolumenu danych tylko do wybranego hosta należącego do zdefiniowanego klastra.
Wydajność	Wymaga się możliwości rozbudowania macierzy do poziomu wydajności przynajmniej 99 000 operacji wejścia wyjścia dla losowego odczytu oraz przynajmniej 34 000 operacji wejścia wyjścia dla losowego zapisu. Wymagana pojemność dla wolumenów z dynamiczna alokacja przestrzeni to przynajmniej 256 TB
Zarządzanie macierzą	Dostępne dwa porty 1Gbe Base-T w trybie primary/redundant. Zarzadzanie macierzą powinno być możliwe za pomocą graficznego interfejsu użytkownika dostępnego poprzez protokół https, oraz za pomocą linii komend cli osiągalnej poprzez protokół ssh.

Parametr	Charakterystyka
	Interfejs zarządzania powinien wylogować sesje po maksymalnie 15 minutach bezczynności. Maksymalna ilość prób podania hasła administratora nie może być większa niż 5 do momentu zablokowania dostępu. Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control. Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy: - storage admin – pełen dostęp wyłączeniem ustawień bezpieczeństwa - security admin – dostęp do ustawień bezpieczeństwa - support admin – pełen dostęp serwisowy - monitor – możliwość odczytu konfiguracji Producent powinien udostępniać konsolę umożliwiająca dodawanie do domeny zarządzania wielu macierzy jednocześnie. Wymaga się możliwości importu konfiguracji z jednej macierzy na inne.
Inne	Wymagana jest bezprzerwowa wymiana następujących elementów macierzy: kontrolery, moduły I/O, dyski, zasilacze oraz moduły SFP+. Obsługa systemów operacyjnych hosta: Microsoft Windows Server; Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES); VMware vSphere
Gwarancja	• 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7 poprzez ogólnopolską linię telefoniczną producenta. Uszkodzone dyski twarde pozostają własnością zamawiającego. • Zamawiający wymaga, aby macierz była fabrycznie nowa oraz całość przedmiotu zamówienia wraz z wszystkimi podzespołami w celu zachowania wszelkich wymogów gwarancyjnych pochodziła z oficjalnego kanału dystrybucji Producenta na terenie UE i nie była częścią żadnego innego projektu.

3. Środowisko sprzętowe do wirtualizacji zapewniającej izolację sieci oraz replikację wraz przywracaniem systemów dla Starostwa

Minimalne parametry techniczne i funkcjonalne:

Parametr	Charakterystyka
Obudowa	• Typu RACK, wysokość nie więcej niż 1U; • Szyny umożliwiające wysunięcie serwera z szafy stelażowej • Możliwość zainstalowania 8 dysków twardych hot plug 2,5”; • Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych; • Zainstalowane 2 szt. dysków PCIe4 480GB skonfigurowane w RAID podpięte do sprzętowego kontrolera; • Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.

Parametr	Charakterystyka

Płyta główna	• Dwuprocesorowa;
	• Wyprodukowana i zaprojektowana przez producenta serwera;
	• Możliwość instalacji procesorów 60-rdzeniowych;
	• Zainstalowany moduł TPM 2.0;
	• 4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5;
	• 32 gniazda pamięci RAM;
	• Obsługa 8 TB pamięci operacyjnej RAM DDR5;
	• Wsparcie dla technologii:
	  ◦ Memory Scrubbing;
	  ◦ SDDC;
	  ◦ ECC;
	  ◦ Memory Mirroring;
	  ◦ ADDDC;

Procesory	• Zainstalowane dwa procesory 8-rdzeniowe, taktowanie bazowe 3.2 GHz, architektura x86_64; • osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 283 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie http://spec.org/cpu2017/results/cpu2017.html dla dowolnego serwera z oferty producenta.
Pamięć RAM	• 256 GB pamięci RAM; • DDR5 Registered 4800MT/s; • Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność;

Kontrolery LAN	• Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:
	  ◦ 1x 1Gbit Base-T;
	  ◦ 2x 10Gbit SFP+ obsadzone wkładkami 10Gbit MMF LC;
	  ◦ Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;
	• Interfejsy LAN zainstalowane w slotach PCI-e:
	  ◦ Dwuportowa karta 10Gbit SFP+ obsadzona wkładkami 10Gbit MMF LC;

Porty	• Zintegrowana karta graficzna ze złączem VGA z tyłu serwera • 2 porty USB 3.0 dostępne z tyłu serwera; • 2 porty USB 3.0 na panelu przednim; • Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
Zasilanie, chłodzenie	• Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 900W; • Redundantne wentylatory hotplug.

Parametr	Charakterystyka
System Operacyjny	Microsoft Windows Server 2022 Standard lub równoważne. ● Licencja bezterminowa zgodna z liczbą fizycznych rdzeni procesorów zainstalowanych. ● 80szt. Licencji dostępowych na użytkownika do ww. wersji systemu.
Zarządzanie	● Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii; ● informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: ● karty rozszerzeń zainstalowane w dowolnym slocie PCI Express; ● procesory CPU; ● pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM; ● status karty zarządzającej serwera; ● wentylatory; ● bateria podtrzymująca ustawienia BIOS płyty głównej; ● zasilacze; ● system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym); ● Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: ● Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; ● Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; ● Dostęp poprzez przeglądarkę Web, SSH; ● Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; ● Zarządzanie alarmami (zdarzenia poprzez SNMP); ● Możliwość przejęcia konsoli tekstowej; ● Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); ● Obsługa serwerów proxy (autentykacja); ● Obsługa VLAN; ● Możliwość konfiguracji parametru Max. Transmission Unit (MTU); ● Wsparcie dla protokołu SSDP; ● Obsługa protokołów TLS 1.2, SSL v3; ● Obsługa protokołu LDAP; ● Synchronizacja czasu poprzez protokół NTP;

Parametr	Charakterystyka
	● Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej; ● Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna); ● Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.
Wspierane OS	● Microsoft Windows Server 2025, 2022, 2019; ● VMWare vSphere 8.0;; ● Suse Linux Enterprise Server 15; ● Red Hat Enterprise Linux 9, 8; ● Microsoft Hyper-V Server 2019
Gwarancja	● Minimum 36 miesięcy gwarancji producenta serwera w trybie on-site ze skuteczną naprawą w miejscu użytkowania sprzętu do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej; ● Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; ● Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie; ● Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki
Dokumentacja, inne	● Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta; ● Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; ● Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera ● W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość

Parametr	Charakterystyka
	fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; ● Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; ● Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 10 - 85 %; ● Zgodność z normami: CB, RoHS, WEEE, GS oraz CE.

4. Rozwiązania klasy EDR oraz NDR dla Starostwa

Rozwiązanie powinno składa się z dwóch urządzeń:

1. Analizator ruchu 1 szt.
2. Urządzenie do aktywnej reakcji na analizowany ruch sieciowy 1 szt.

System klasy NDR musi integrować się natywnie lub poprzez API z oferowanym systemem, minimum w zakresie wyzwalania akcji blokowania niebezpiecznego, podejrzanego lub nietypowego ruchu sieciowego w celach zminimalizowania ryzyka naruszenia bezpieczeństwa oraz przeprowadzenia aktywnej ochrony.

Ruch niebezpieczny może być blokowany na określoną jednostkę czasu (określoną w minutach, godzinach, dniach) lub permanentnie.

Blokowanie musi opierać się co najmniej o adres źródłowy, adres docelowy oraz port.

Istnieje możliwość zastosowania odpowiednich filtrów (takich jak podsieci, typ wykrycia), pozwalających dostosować parametry blokowanego ruchu.

Uwagi do wdrożenia:

a) Wdrożenie musi obejmować 3 dni robocze
b) Wdrożenie musi się odbyć na miejscu u Zamawiającego
c) Wdrożenie musi zostać przeprowadzone przez certyfikowanego Inżyniera. Certyfikat musi być wydany przez Producenta na poziomie minimum Advanced.

Minimalne parametry techniczne i charakterystyka dla Ad. 1:

Parametr	Charakterystyka
Architektura	a. Wysokość 1U do montażu w szafie rack. b. Posiadać co najmniej dwa porty USB c. Urządzenie musi posiadać dedykowany port do zarządzania d. Urządzenie musi posiadać minimum interfejsów: 2x SFP+, 8x SFP, 8x GE e. Musi obsługiwać co najmniej 1T przestrzeni dyskowej. f. Minimum 1 Gb/s przepustowości wykrywania naruszeń w dwukierunkowym ruchu HTTP z włączonymi wszystkimi funkcjami wykrywania zagrożeń

	g. Proponowane rozwiązanie musi obsługiwać minimum 750 tys . jednoczesnych sesji. h. Proponowane rozwiązanie musi obsługiwać 32000 nowych sesji /s w ruchu HTTP.
Metody analizy i obsługiwane protokoły	a. Musi obsługiwać pasywny tryb pracy (TAP), nie ingerując w sieć klienta. b. Rozwiązanie musi być w stanie zintegrować się z zaporami ogniowymi tej samej marki w celu ograniczenia zagrożeń c. Musi posiadać możliwość rozwiązywania wiadomości przez protokół MPLS, VXLAN oraz QinQ i wykrywania zagrożeń w tych wiadomościach. d. System musi posiadać możliwość deszyfrowania ruchu kierowanego na/wracającego z kluczowych serwerów. Funkcjonalność musi być realizowana na tej samej platformie co pozostałe elementy systemu
Kontrola aplikacji	a. Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka oraz wspierać komunikatory internetowe, p2p, pocztę e-mail, przesyłanie plików, gry online, strumieniowe przesyłanie multimediów itp. b. Rozwiązanie musi być w stanie zidentyfikować aplikacje mobilne typu iOS lub Android. c. Rozwiązanie musi być w stanie identyfikować aplikacje w chmurze, musi zapewniać wielowymiarowe monitorowanie i statystyki dla aplikacji w chmurze, w tym kategorię ryzyka i funkcje.
Wykrywanie zagrożeń	a. Rozwiązanie musi obsługiwać co najmniej 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, ręczne i automatyczne aktualizacje, wyodrębnianie sygnatur oraz wbudowaną encyklopedię zagrożeń. b. Rozwiązanie musi obsługiwać ochronę przed atakami SQL injection, XSS, buffer overflow zarówno dla IPv4 jak i IPv6 c. Rozwiązanie powinno obsługiwać ochronę przez atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, Musi obsługiwać wykrywanie co najmniej metod uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA d. Rozwiązanie musi obsługiwać wykrywanie anomalii protokołów HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS itp. e. Niestandardowe reguły wykrywania włamań muszą obsługiwać konfigurowanie kierunku ruchu ataku w celu poprawy dokładności analizy źródła ataku. f. Rozwiązanie powinno umożliwiać tworzenie białych list dla modułu IPS. g. Rozwiązanie musi mieć wstępnie zdefiniowane profile IPS. h. Rozwiązanie musi mieć opcję przechwytywania pakietów i. Rozwiązanie musi umieć wykrywa reverse-shell j. Rozwiązanie potrafi zdefiniować odpowiednie treshholdy chroniące przed atakami Flood, bazując na parametrach dostarczonego ruchu k. System musi mapować wykryte zagrożenia na framework MITRE ATT&CK
Skanowanie antywirusowe	a. Rozwiązanie musi obsługiwać co najmniej 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur. b. Rozwiązanie musi wspierać antywirus oparty na przepływie dla protokołów min. HTTP, SMTP, POP3, IMAP, FTP/SFTP.

	c. Rozwiązanie powinno obsługiwać wykrywanie wirusów w skompresowanych plikach, takich jak RAR, ZIP, GZIP, BZIP2, TAR oraz wspierać wielowarstwowe wykrywanie skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji po wykryciu zagrożenia w tych plikach d. Rozwiązanie musi obsługiwać wykrywanie zaszyfrowanych skompresowanych plików
Wykrywanie botnetów C&C	a. Rozwiązanie powinno wspierać skuteczne wykrywanie botów intranetowych i zapobieganie dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównywanie uzyskanych informacji z bazą adresów C&C. b. Rozwiązanie musi obsługiwać automatyczną aktualizację sygnatur botnetów C&C c. Rozwiązanie musi obsługiwać dwa typy bazy adresów C&C: bazę adresów IP i bazę danych domen. d. Rozwiązanie musi obsługiwać wykrywanie C&C protokołów w protokołach TCP, HTTP i DNS. e. Rozwiązanie musi wspierać właczenie wykrywania DGA w celu analizy odpowiedzi DNS i wykrywania, czy urządzenie jest atakowane przez nazwę domeny DGA. f. Musi wspierać wykrywanie tunelowania w protokole DNS w tym analizowanie zapytań DNS a także rejestrować logów zagrożeń wykrytych tuneli DNS
Sandbox w chmurze	a. Rozwiązanie musi obsługiwać oparte na chmurze wirtualne środowisko analizy złośliwego oprogramowania w celu znalezienia nieznanych zagrożeń b. Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do piaskownicy w chmurze w celu analizy. c. Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów, w tym HTTP/HTTPS, POP3, IMAP4, SMTP i FTP. d. Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF oraz skrypty e. Rozwiązanie powinno dostarczyć kompletny raport analizy behawioralnej dla złośliwych plików. f. Rozwiązanie musi obsługiwać globalne udostępnianie informacji o zagrożeniach, aby wykryć nowe nieznane zagrożenie.
Wykrywanie spamu	a. Rozwiązanie musi wspierać klasyfikację i wykrywanie spamu w czasie rzeczywistym b. Rozwiązanie musi obsługiwać wykrywanie spamu niezależnie od języka, formatu lub treści wiadomości. c. Rozwiązanie musi obsługiwać protokoły poczty e-mail smtp i pop3 d. Rozwiązanie musi obsługiwać białe listy wiadomości e-mail z zaufanych domen.
Dodatkowe funkcje ochrony	a. Rozwiązanie musi obsługiwać wykrywanie DoS / DDoS, SYN Flood, DNS query flood itp. b. Rozwiązanie musi obsługiwać wykrywanie ataków ARP w tym spoofing ARP c. Rozwiązanie musi obsługiwać wykrywanie anormalnych ataków protokołu. d. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu pop

Inteligentne funkcje bezpieczeństwa	a. Rozwiązanie powinno obsługiwać analizę korelacji zagrożeń, korelację między nieznanymi zagrożeniami, nietypowym zachowaniem i zachowaniem aplikacji, aby wykryć potencjalne zagrożenia lub ataki. b. Rozwiązanie powinno umożliwiać aktualizację bazy danych modelu zachowania szkodliwego oprogramowania online w czasie rzeczywistym. c. Rozwiązanie powinno obsługiwać wykrywanie ponad 2000 znanych i nieznanych rodzin złośliwego oprogramowania, w tym wirusów, robaków, trojanów itp d. Rozwiązanie musi obsługiwać zaawansowane wykrywanie złośliwego oprogramowania oparte na obserwacji zachowania e. Rozwiązanie musi wspierać wykrycia oprogramowania ransomware i złośliwego oprogramowania do wydobywania kryptowalut. f. Rozwiązanie powinno obsługiwać modelowanie zachowania w oparciu o ruch bazowy L3-L7, aby ujawnić nietypowe zachowanie sieci, takie jak skanowanie HTTP, Spider, SPAM, słabe hasła SSH / FTP dla serwerów i hostów. g. Rozwiązanie musi obsługiwać wykrywanie DDoS, w tym Flood, Sockstress, zip of death, reflect, dns query, SSL DDos i aplikacyjny DDoS h. Rozwiązanie musi obsługiwać inspekcję zaszyfrowanego ruchu tunelowego dla nieznanych aplikacji i. Rozwiązanie musi obsługiwać aktualizację bazy danych modelu nieprawidłowego zachowania online w czasie rzeczywistym j. Rozwiązanie musi zapewniać analizę kryminalistyczną , w tym analizę zagrożeń, bazę wiedzy, historię i topologię zagrożeń. k. Rozwiązanie musi obsługiwać działania administratora w celu zmiany stanu zagrożenia na false positive, naprawionego, zignorowanego, potwierdzonego zdarzenia l. Rozwiązanie musi obsługiwać czyszczenie zagrożeń serwera jednym kliknięciem i ponowną ocenę bezpieczeństwa hosta m. Rozwiązanie powinno obsługiwać białą listę zagrożeń, w tym nazwę zagrożenia, źródłowy/docelowy adres IP, liczbę odwiedzin itd. n. Rozwiązanie musi obsługiwać przechwytywanie pakietów online o. Rozwiązanie musi obsługiwać lokalną technologię honeypot, aby wychwytywać ataki zagrożeń sieciowych i potwierdzać źródło zagrożenia, typ zagrożenia i częstość występowania p. Rozwiązanie musi obsługiwać wykrywanie oszustw na podstawie behawioralnej dla ftp, HTTP, MYSQL, SSH, TELNET, dokumentów lub baz danych q. Rozwiązanie musi obsługiwać funkcję polowania na zagrożenia (threat hunting), aby zebrać kompleksowe dowody i zapewnić dogłębną analizę r. Rozwiązanie powinno obsługiwać rejestrowanie IOC w celu śledzenia zagrożeń, takich jak brute force remote dekto, tworzenia podejrzanych plików, złośliwych procesów PowerShell itp. w celu poprawy wykrywalność funkcji śledzenia zagrożeń.
Widoczność ryzyka / zagrożeń	a. Rozwiązanie musi obsługiwać wizualizację zagrożeń intranetowych dla serwerów (zasobów krytycznych), a także wykrywanie nietypowego ruchu z nimi związanego. b. Rozwiązanie musi obsługiwać widoczność zagrożeń dla ryzykownych hostów,

	w tym nazwy hosta, systemu operacyjnego, przeglądarki, typu usługi, aby rejestrować zagrożenia hosta i nietypowy ruch. c. Rozwiązanie musi obsługiwać widoczność podstawowych informacji opartych na hoście, indeksu ryzyka, zagrożeń i nietypowego ruchu. d. Rozwiązanie powinno wspierać widoczność zagrożeń, w tym nazwę zagrożenia, typ zagrożenia, poziom ryzyka, bazę wiedzy, pakiet kryminalistyczny itp. e. Rozwiązanie powinno dostarczyć wszystkie statystyki klasyfikacji zdarzeń zagrożeń w oparciu o IOC i trend zdarzeń zagrożeń w ciągu co najmniej 2 tygodni. f. Rozwiązanie musi wspierać wskazanie ścieżki ataku.
Analiza i odpowiedzi na incydenty	a. Rozwiązanie musi obsługiwać aktualizację w czasie rzeczywistym najpoważniejszych informacji o zagrożeniach znalezionych w branży do urządzenia z chmury b. Obsługa wyświetlania najnowszych informacji o zagrożeniach w wyskakujących okienkach. c. Obsługa rejestrowania i sprawdzania, czy w sieci wystąpiło odpowiednie zagrożenie. d. Pomoc techniczna w celu dostarczenia szczegółowych informacji o zagrożeniach i sugestii dotyczących rozwiązania. e. Wsparcie konfigurowania reguł ostrzegania o zagrożeniach, w tym warunków zagrożenia i metody działania, które w przypadku wystąpienia zdarzenia stanowiącego zagrożenie, system powiadomi użytkownika lub podejmie odpowiedź w odpowiednim czasie zgodnie z metodą działania określoną w regule (np. połączenie z firewall, przypomnienie głosowe lub wysłanie pocztą e-mail.
Administracja	a. Rozwiązanie musi mieć zintegrowany sieciowy interfejs użytkownika (WebUI) i interfejs wiersza poleceń (CLI) b. Rozwiązanie powinno obsługiwać zarządzanie dostępem z HTTP/HTTPS, SSH, telnet, konsoli c. Rozwiązanie musi być w stanie chronić system przed atakami brute-force na nazwę użytkownika i hasło d. Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów. e. Rozwiązanie musi obsługiwać monitorowanie hostów i serwerów w sieci wewnętrznej, identyfikując nazwę, system operacyjny, przeglądarkę, typ i rejestr statystyk zagrożeń sieciowych f. Oferowany zestaw urządzeń musi pochodzić o jednego producenta i być w pełni kompatybilny g. Oferowany zestaw urządzeń musi posiadać aplikację mobilną pozwalającą na monitoring pracy urządzeń i analizę zdarzeń
Logowanie i raportowanie	a. Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. Raport można wyeksportować co najmniej w formacie PDF i/lub wysłać na adres e-mail lub FTP. b. Rozwiązanie powinno obsługiwać ustawianie alarmów dotyczących wykorzystania procesora, wykorzystania pamięci, wykorzystania miejsca na

	dysku, nowych połączeń itp. c. Rozwiązanie powinno obsługiwać wysyłanie alarmów przez e-mail, SMS. d. Alerty powinny być generowane na podstawie przepustowości aplikacji i nowych połączeń. e. Logi powinny być możliwe do eksportu za pośrednictwem Syslog lub poczty e-mail i zawierać minimum logi zdarzeń, sieci, zagrożenia, konfigurację i sesje f. Wstępnie zdefiniowane zadania raportowania g. Rozwiązanie powinno mieć scentralizowane monitorowanie wielu urządzeń, w tym procesora, pamięci, ruchu, sesji, aplikacji, użytkowników, zagrożeń itp. za pośrednictwem aplikacji mobilnej z danymi z ostatnich 7 dni. h. Rozwiązanie musi wspierać restAPI
Gwarancja / dostawa:	a. 60-miesięczną gwarancję producenta na dostarczone elementy systemu b. Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 24 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C) c. Wsparcie techniczne dystrybutora rozwiązań w języku polskim d. Oferta musi być złożona przez autoryzowanego partnera

Minimalne parametry techniczne i charakterystyka dla Ad. 2:

Parametr	Charakterystyka
Architektura	a. Proponowane rozwiązanie powinno mieć maksymalną wysokość 1U. b. Proponowane rozwiązanie musi posiadać co najmniej dwa porty USB. c. Proponowane rozwiązanie musi posiadać co najmniej jeden port konsoli d. Proponowane rozwiązanie musi posiadać co najmniej jeden dedykowany port do zarządzania systemem e. Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów Gigabit Ethernet. f. Proponowane rozwiązanie musi posiadać co najmniej 8 stałych portów SFP. g. Proponowane rozwiązanie musi posiadać co najmniej 2 stałe porty SFP+. h. Proponowane rozwiązanie musi posiadać co najmniej 480GB przestrzeni dyskowej. i. Proponowane rozwiązanie musi obsługiwać przepustowość IPS 3 Gb/s j. Proponowane rozwiązanie musi obsługiwać jednoczesne sesje o długości 1.2 M k. Proponowane rozwiązanie musi obsługiwać min 40000 nowych sesji/sekundę w ruchu HTTP, z włączonym silnikiem IPS. l. Opóźnienia (tzw. Latency) nie mogę przekraczać 300µs m. Funkcjonalności nie mogą być realizowane na rozwiązaniu NGFW
Metody analizy i obsługiwane protokoły	a. Proponowane rozwiązanie musi być w stanie pracować jednocześnie w trybie warstwy 3 (routing), trybie online (most) i warstwie 2 (kopia ruchu) (bez konieczności wirtualizacji sprzętu)
Kontrola aplikacji	a. Rozwiązanie powinno obsługiwać identyfikację IP hostów, ilość endpointów , czasu online, czasu offline. b. Rozwiązanie musi obsługiwać ponad 6000 aplikacji, musi obsługiwać

	filtrowanie aplikacji według nazwy, kategorii, podkategorii, technologii i ryzyka. c. Rozwiązanie powinno rozpoznawać aplikacje IPv6. d. Rozwiązanie musi obsługiwać identyfikację aplikacji dla ruchu szyfrowanego SSL e. Rozwiązanie musi wspierać identyfikację aplikacji mobilnych na Androida i iOS. f. Rozwiązanie powinno obsługiwać wyświetlanie opisu, czynników ryzyka, zależności, typowych używanych portów i adresów URL dla dodatkowych odwołań i informacji dla każdej aplikacji w interfejsie WebUI. g. Rozwiązanie musi obsługiwać blokowanie, ponowne uruchamianie sesji, monitorowanie i kształtowanie ruchu dla aplikacji. h. Rozwiązanie musi być w stanie identyfikować i kontrolować aplikacje w chmurze
Wykrywanie zagrożeń	a. Rozwiązanie musi obsługiwać ponad 16000 sygnatur IPS. Musi obsługiwać niestandardowe sygnatury, automatyczne wstawianie lub wyodrębnianie sygnatur oraz zintegrowaną encyklopedię zagrożeń. b. Rozwiązanie musi obsługiwać zapobieganie włamaniom dla ruchu szyfrowanego SSL. c. Rozwiązanie musi obsługiwać ochronę środowiska IPV6. d. Rozwiązanie musi obsługiwać ochronę przed sql injection, CC i atakom XSS. e. Rozwiązanie musi obsługiwać sprawdzanie linków zewnętrznych. f. Rozwiązanie powinno obsługiwać ochronę przed atakami C&C z limitem żądań, limitem proxy, niestandardowym progiem, metodami przyjaznymi dla robotów. Wspierane powinny być 4 metody uwierzytelniania: JS Cookie, Redirect, Access confirm, CAPCHA g. Rozwiązanie powinno obsługiwać wykrywanie anomalii protokołu. h. Rozwiązanie musi obsługiwać następujące akcje IPS: monitorowanie, blokowanie, resetowanie (adres IP atakujących lub IP ofiary, interfejs wejściowy) z czasem wygaśnięcia i. Rozwiązanie musi obsługiwać opcję logowania pakietów. j. Rozwiązanie musi obsługiwać profil zabezpieczeń IPS na podstawie ważności, obiektu docelowego, systemu operacyjnego, aplikacji lub protokołu. k. Rozwiązanie musi obsługiwać zapobieganie włamaniom dla protokołów HTTP, SMTP, IMAP. POP3, VOIP, NETBIOS itp. l. Rozwiązanie musi być wspierać weryfikację protokołów http typu Get, Head, Put, Post. m. Rozwiązanie musi obsługiwać wyłączenie IP z określonych sygnatur IPS. n. Rozwiązanie musi obsługiwać tryb działania sniffera IDS. o. Rozwiązanie musi obsługiwać predefiniowaną konfigurację profili IPS. p. Rozwiązanie musi obsługiwać tworzenie zdefiniowanych przez użytkownika sygnatur IPS. q. Proponowane rozwiązanie musi obsługiwać wykrywanie reputacji IP i blokowanie adresów IP serwera botnetów za pomocą globalnej bazy danych reputacji IP. r. Proponowane rozwiązanie powinno wspierać szczegółowy opis

	predefiniowanych profili IPS. s. Rozwiązanie musi obsługiwać rejestrację zagrożeń IPv6: obsługa przechwytywania i pobierania pakietów IPv6 t. Szczegóły zagrożeń muszą obsługiwać identyfikator URI i dekodowanie danych ataków u. Obsługa wykrywania anomalii protokołów HTTP/DNS/FTP/MSRPC/POP3/SMTP/SUNRPC i Telnet v. Obsługa inspekcji Reverse Shell w. Blokowanie plików po rozszerzeniu dla minimum 100 typów plików x. Rozwiązanie musi wykrywać i blokować wrażliwe zrefowanych informacje w przesyłanych plikach dla minimum doc/docx, xls/xlsx, ppt/pptx, txt w protokołach HTTP, FTP, SMTP, POP3, IMAP, SMB y. Ochrona i wykrywanie skanowania protokołow IP oraz UDP z. Rozwiązanie musi mieć możliwość inspekcji payloudu w ramkach MPLS aa. Rozwiązanie pozwala na automatyczne określanie wartości proponowanych dla ochrony przed atakami Flood bb. System pozwala na zdefiniowanie globalnej białej listy, pozwalając na dany ruch i nie sprawdzając go na warstwie aplikacyjnej cc. System musi mapować wykryte zagrożenia na taktyki MITRE ATT&CK
Skanowanie antywirusowe	a. Rozwiązanie musi obsługiwać ponad 13 milionów sygnatur antywirusowych z ręcznymi lub automatycznymi aktualizacjami sygnatur. b. Rozwiązanie musi obsługiwać antywirus oparty na przepływie dla protokołów HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB c. Rozwiązanie powinno obsługiwać wykrywanie wirusów dla skompresowanych plików, takich jak RAR, ZIP, GZIP, BZIP2, TAR; obsługa wielowarstwowego wykrywania skompresowanych plików dla nie mniej niż 5 warstw dekompresji i dostosowanie akcji d. Rozwiązanie musi obsługiwać akcje niestandardowe dla zaszyfrowanych plików skompresowanych. e. Rozwiązanie musi obsługiwać co najmniej 3 działania: usuwanie złośliwego kodu, resetowanie połączenia lub logowanie tylko po wykryciu wirusa lub złośliwej strony internetowej f. Rozwiązanie powinno obsługiwać ostrzeganie przed wirusami i złośliwymi stronami internetowymi, ostrzegać użytkownika, że witryna jest szkodliwą witryną lub że wykryto wirusa. g. Rozwiązanie musi obsługiwać funkcje AV w środowiskach IPV6.
Filtrowanie	a. Rozwiązanie musi obsługiwać dynamiczne filtrowanie sieci Web za pomocą chmurowej bazy danych kategoryzacji w czasie rzeczywistym: ponad 140 milionów adresów URL z co najmniej 64 kategoriami (z których nie mniej niż 8 jest związanych z bezpieczeństwem) b. Rozwiązanie musi obsługiwać ręcznie zdefiniowane filtrowanie sieci Web na podstawie adresu URL, zawartości sieci Web i nagłówka MIME c. Rozwiązanie musi obsługiwać następujące dodatkowe funkcje filtrowania. - Aplet Java, ActiveX lub filtr plików cookie. - Blokowanie postów HTTP - Rejestrowanie wyszukiwania słów kluczowych

	- Wykluczanie ze skanowania połączeń szyfrowanych w niektórych kategoriach dla prywatności. d. Rozwiązanie musi obsługiwać zastępowanie profilu filtrowania adresów URL, aby administrator mógł tymczasowo przypisać różne profile do użytkownika/grupy/adresu IP e. Rozwiązaniem powinno być umożliwienie dostosowania strony ostrzeżenia do filtrowania adresów URL.
Sandbox w chmurze	a. Rozwiązanie musi obsługiwać przesyłanie złośliwych plików do chmury w celu analizy b. Rozwiązanie powinno obsługiwać przesyłanie złośliwych plików z protokołów takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB c. Rozwiązanie musi obsługiwać typy plików, w tym PE, ZIP, RAR, Office, PDF, APK, JAR , SWF i Skryptów d. Rozwiązanie musi obsługiwać kierunek transferu plików i kontrolę rozmiaru pliku. e. Rozwiązanie musi zawierać kompletny raport analizy zachowania złośliwych plików f. Rozwiązanie powinno obsługiwać blokowanie zgodnie z wynikami wykrywania, aby szybko zablokować nieznane zagrożenie. g. Rozwiązanie musi obsługiwać udostępnianie globalnych informacji o zagrożeniach i blokować nieznane zagrożeni na całym świecie
Zapobieganie C&C i botnetom	a. Rozwiązanie musi być w stanie skutecznie wykrywać boty intranetowe i zapobiegać dalszym atakom ze strony zaawansowanych zagrożeń poprzez porównanie uzyskanych informacji z bazą adresów C&C b. Rozwiązanie musi obsługiwać regularne aktualizacje adresów serwerów botnetu. c. Rozwiązanie musi obsługiwać dwa typy bazy danych adresów C&C: bazę danych adresów IP (z wyłączeniem adresów IPv6) i bazę danych domen d. Rozwiązanie musi obsługiwać wykrywanie dla protokołów TCP, HTTP i DNS. e. Rozwiązanie musi obsługiwać ręczne umieszczanie adresów IP i domen na białej liście. f. Rozwiązanie musi umożliwiać ręczny import/eksport i automatyczny import czarnych list g. Rozwiązanie musi obsługiwać funkcjonalność DNS Sinkhole i wykrywanie tunelowania DNS.
Wykrywanie spamu	a. Rozwiązanie musi obsługiwać klasyfikację spamu w czasie rzeczywistym i zapobieganie mu. b. Rozwiązanie musi obsługiwać ochronę niezależnie od języka, formatu lub zawartości wiadomości. c. Rozwiązanie musi obsługiwać protokoły poczty e-mail SMTP i POP3. d. Rozwiązanie musi obsługiwać wykrywanie zarówno ruchu przychodzącego, jak i wychodzącego. e. Rozwiązanie musi obsługiwać białe listy, aby umożliwić wysyłanie wiadomości e-mail z zaufanych domen. f. Rozwiązanie musi obsługiwać listę obejść opartą na nadawcy i niestandardowe reguły spamu.

	g. Rozwiązanie musi mieć możliwość konfiguracji czarnych i białych list dla modułu Anti-Spam
Monitoring	a. Rozwiązanie musi posiadać pełne monitorowanie zagrożeń, w tym nazwę ataku, ważność, czasem, adresem, protokołem, zalecanym rozwiązaniem itp. b. Rozwiązanie musi obsługiwać usługę Threat Intelligence Pushing Service c. Rozwiązanie musi obsługiwać statystyki i analizy ruchu w czasie rzeczywistym. d. Rozwiązanie powinno obsługiwać monitorowanie stanu procesora, pamięci, temperatury, wentylatora, modułów zasilania itp.
Polityki bezpieczeństwa	a. Proponowane rozwiązanie musi obsługiwać kontrolę dostępu do strefy (zone), użytkownika, usługi, aplikacji, IPS, AV w jednej regule polityki. b. Proponowane rozwiązanie musi obsługiwać wstępnie zdefiniowane i niestandardowe obiekty c. Proponowane rozwiązanie musi obsługiwać weryfikację nadmiarowości polityki bezpieczeństwa oraz zliczanie trafień polityki przez interfejs WebUI d. Rozwiązanie musi obsługiwać import i eksport polityk
QoS	a. Rozwiązanie musi obsługiwać maksymalną lub gwarantowaną kontrolę przepustowości dla adresów IP lub użytkowników. b. Rozwiązanie powinno obsługiwać tunelowanie w oparciu o domenę zabezpieczeń, interfejs, adres, pulę użytkowników/użytkowników, pulę serwer/serwer, pulę aplikacji/aplikacji, TOS, sieci VLAN. c. Rozwiązanie musi obsługiwać przepustowość przydzieloną w zakresie- czas, priorytet lub tę samą współdzieloną przepustowość d. Rozwiązanie musi obsługiwać typ usługi (TOS) i zróżnicowane usługi (DiffServ) e. Rozwiązanie musi obsługiwać tworzenie zaplanowanych polityk QoS. f. Rozwiązanie musi obsługiwać elastyczną, priorytetową alokację pozostałej niewykorzystanej przepustowości. g. Rozwiązanie musi obsługiwać dwa poziomy konfiguracji ruchu, które umożliwiają konfigurację ruchu w różnych wymiarach, takich jak użytkownicy i aplikacje. Rozwiązanie musi obsługiwać co najmniej cztery tunele na poziom, co zapewnia hierarchię kontroli ruchu. h. Rozwiązanie musi obsługiwać alokację przepustowości na podstawie kategorii adresu URL i. Rozwiązanie musi obsługiwać adresy IPv6 w funkcji QoS.
Administracja	a. Rozwiązanie musi być obsługiwane przez WebUI i interfejs wiersza poleceń (CLI) b. Rozwiązanie powinno obsługiwać zarządzanie dostępem przez HTTP/HTTPS, SSH, telnet, konsolę c. Rozwiązanie musi obsługiwać uwierzytelnianie dwuskładnikowe: nazwa użytkownika/hasło, plik certyfikatu HTTPS d. Rozwiązanie musi obsługiwać integrację systemu: SNMP, syslog. e. Rozwiązanie musi obsługiwać co najmniej 3 role administratora, w tym administratora, operatora i audytora f. Rozwiązanie musi być w stanie chronić system przed atakami brute force na nazwę użytkownika i hasło g. Rozwiązanie musi obsługiwać zasady zabezpieczeń haseł dla kont administratorów.

	h. Rozwiązanie musi obsługiwać serwery Radius, AD i LDAP. i. Rozwiązanie musi obsługiwać szybkie wdrażanie poprzez automatyczne instalowanie z USB, uruchamianie skryptów lokalnych i zdalnych. j. Rozwiązanie musi obsługiwać dynamiczny dashboard w czasie rzeczywistym i szczegółowe widżety monitorowania k. Urządzenie musi obsługiwać zarządzanie urządzeniami pamięci masowej: dostosowywanie i alarmowanie progu przestrzeni dyskowej, nakładanie starych danych, zatrzymywanie nagrywania ruchu. l. Urządzenie musi obsługiwać szczegółowe logi ruchu: przekazane, sesje naruszone, ruch lokalny, nieprawidłowe pakiety m. Urządzenie musi obsługiwać pełne logi zdarzeń: audyty aktywności systemu i zarządzania, routing i sieć, VPN, uwierzytelnianie użytkowników, zdarzenia związane z Wi-Fi n. Urządzenie musi obsługiwać opcję rozpoznawania nazw portów usług i adresów IP. o. Rozwiązanie musi mieć możliwość dodania adresów IP lub MAC hostów do czarnej listy, aby zablokować dostęp przez określony czas. p. Rozwiązanie powinno obsługiwać blokowanie konta po kilku niepowodzeniach logowania. q. Rozwiązanie musi obsługiwać konfigurację zadań przechwytywania pakietów z wieloma warunkami przechwytywania pakietów w tym samym czasie oraz ich export r. Rozwiązanie musi obsługiwać standardowy SYSLOG i logowanie w formacie binarnym; rozproszone binarne przechowywanie logów na wielu serwerach logów s. Rozwiązanie powinno obsługiwać logowanie w pamięci lokalnej i/lub serwerach syslog. t. Rozwiązanie musi obsługiwać rejestrowanie zmiany w politykach u. Rozwiązanie musi obsługiwać logowanie zaufane przy użyciu opcji TCP (RFC 3195) v. Rozwiązanie musi obsługiwać raportowanie zdefiniowane przez użytkownika. w. Rozwiązanie musi obsługiwać zaplanowany raport. x. Raport można wyeksportować w formacie PDF/HTML/WORD za pośrednictwem email lub FTP. y. Rozwiązanie musi umożliwić podgląd raportów w formacie HTML i PDF.
HA Wysoka dostępność	a. Rozwiązanie musi obsługiwać tryby Active/Active i Active/Passive b. Rozwiązanie musi obsługiwać następujące opcje wdrażania HA: - HA z agregacją linków - Full mesh HA - Geograficznie rozproszony HA c. Rozwiązanie musi obsługiwać funkcję bypass sprzętowych interfejsów i dedykowany interfejs HA
Gwarancja / dostawa:	a. 36-miesięczną gwarancję producenta na dostarczone elementy systemu b. Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 24 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C)

	c. Wsparcie techniczne dystrybutora rozwiązań w języku polskim d. Oferta musi być złożona przez autoryzowanego partnera

5. Zapora sieciowa ang. Firewall lub Next Generation Firewall – PCPR

Minimalne parametry techniczne i funkcjonalne:

Parametr	Charakterystyka
Wymagania Ogólne	• Dostarczony sprzęt musi być wolny od wad prawnych i fizycznych oraz nienoszący oznak użytkowania. • Dostarczony sprzęt musi być fabrycznie nowy (tzn. wyprodukowane nie wcześniej, niż na 9 miesięcy przed ich dostarczeniem), musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez producenta dla oferowanego modelu sprzętu. • Niedopuszczalne są produkty prototypowe, nie dopuszcza się urządzeń długotrwale magazynowanych oraz pochodzących z programów wyprzedażowych producenta. Urządzenia nie mogą znajdować się na liście „end-of-sale" oraz „end-of-support" producenta. • Wymagana ilość i rozmieszczenie (na zewnątrz obudowy) jakichkolwiek portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, itp., niedopuszczalne jest zastosowanie jakichkolwiek zewnętrznych przejściówek czy konwerterów. • Wszystkie urządzenia będą zasilane bezpośrednio z sieci 230V.
Elementy systemu bezpieczeństwa:	• Urządzenie musi mieć możliwość jednoczesnej pracy w trybie Layer 3 (routing), transparentnym (most) i Layer 2 (port mirroring) bez konieczności wirtualizacji sprzętu • Możliwość stworzenia minimum 64 wirtualnych interfejsów zdefiniowanych jako VLAN w oparciu o standard 802.1Q. • W zakresie Firewall, obsługa nie mniej niż 450 000 jednoczesnych połączeń i 48 000 nowych połączeń na sekundę. • System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o minimalnej pojemności 8 GB do celów logowania i raportowania. • Musi posiadać 2x USB 3.0 • Musi posiadać 1x port konsoli • Musi posiadać 1 dedykowany port do zarządzania, minimum Gigabit Ethernet • System realizujący funkcję Firewall musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zgromadzonych na urządzeniu. • System pełniący funkcję zapory musi posiadać nie mniej niż: 8 interfejsów sieciowych GE • System musi posiadać możliwość wykorzystania portu USB jako Modemu WAN 4G

Parametr	Charakterystyka
	• System musi posiadać zewnętrzy przycisk, pozwalając na reset urządzenia do ustawień fabrycznych, bez konieczności logowania się do urządzenia • Urządzenie musi zostać dostarczone w formie desktopowej
Funkcjonalności	• Kontrola dostępu — zapora sieciowa Stateful Inspection • Ochrona przed wirusami - komercyjny antywirus [AV] • Poufność danych - IPSec VPN i SSL VPN • Kontrola witryn sieci Web — filtr URL • Kontrola zawartości poczty - antyspam (dla protokołów SMTP, POP3) • Kontrola przepustowości i ruchu [QoS i kształtowanie ruchu] z alokacją Tunnel w oparciu o strefę bezpieczeństwa, interfejs, adres, użytkownika/grupę użytkowników, serwera/ grupę serwerów, aplikację/grupę aplikacji, TOS, VLAN • Kontrola aplikacji i rozpoznawanie ruchu P2P (wideo, gry itp.) oraz ograniczanie nowych połączeń i jednoczesnych sesji • Reputacja IP • Cloud Sandbox • API – możliwość wgrywania i wyciągania informacji z systemu dedykowanym interfejsem Rest API
Wydajność	• Analiza ruchu szyfrowanego protokołem SSL • Wydajność Firewall co najmniej 5 Gb/s • Wydajność skanowania strumienia danych z włączonymi funkcjami: NGFW z włączonym IPS i kontrolą aplikacji 1.7 Gb/s • Wydajność ochrony przed atakami (IPS) minimum 2.8 Gb/s • Wydajność AV nie mniej niż 1.8 Gb/s • Wydajność skanowania z włączoną kontrolą aplikacji, AV, IPS, filtrem URL nie mniejsza niż 800 Mb/s.

Funkcjonalności VPN	• Wydajność IPSec VPN, nie mniej niż 2.7 Gb/s
	• Tworzenie połączenia lokalizacja-lokalizacja i oraz klient-lokalizacja
	• Producent oferowanego rozwiązania VPN powinien zapewnić klienta VPN współpracującego z proponowanym rozwiązaniem.
	• Monitorowanie stanu tuneli VPN i utrzymywanie ich aktywności
	• Praca w toplogiach Hub and Spoke i Mesh
	• Wspierane mechanizamy : IPSec NAT Traversal, DPD, Replay Detection, Xauth, DHCP over IPsec,
	• Wsparcie grup DH dla IKEv1: 1,2,5,19,20,21,24
	• Wsparcie grup DH dla IKEv2: 1,2,5,14,15,16,19,20,21,24
	• Wsparcie dla SSL VPN z możliwością testowania zgodności hosta (compliance) co najmniej w zakresie:
	  ○ Wersji systemu operacyjnego
	  ○ Zaaplikowanych patchy
	  ○ Ustawień internetowych
	  ○ Zainstalowanego oprogramowania antywirusowego

Parametr	Charakterystyka
	○ Włączonego Firewalla ○ Walidacji kluczy rejestru ○ Walidacji istnienia plików ○ Walidacji uruchomionych procesów ○ Walidacji uruchomionych lub zainstalowanych serwisów • Możliwość rozszerzania ilości użytkowników VPN odpowiednią licencją • Obsługa PnPVPN (Plug and Play VPN) • Możliwość jednoczesnego uwierzytelnienia co najmniej 128 użytkowników VPN
Routing	• Rozwiązanie musi zapewniać: obsługę Policy Routing, routingu statycznego i dynamicznego w oparciu o protokoły: RIPv2, OSPF, BGP, IS-IS • Obsługa Policy Based Routing • Funkcjonalność Virtual Wire
Translacja adresów NAT	• Tłumaczenie adresu NAT adresu źródłowego i adresu NAT adresu docelowego. • Obsługa NAT46, NAT64, DNS64 • Wsparcie dla STUN
Polityka bezpieczeństwa systemu	• Polityka bezpieczeństwa systemu bezpieczeństwa musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje bezpieczeństwa, rejestrowanie zdarzeń i zarządzanie pasmem sieci (w tym gwarantowaną i maksymalną przepustowość, priorytety). • Możliwość budowania min. 4000 polityk • Musi posiadać funkcjonalność asystenta polityk, dzięki której możliwe jest generowanie reguł bezpieczeństwa w oparciu o przepływ ruchu sieciowego • Musi być w stanie skonfigurować agregowane polityki • Musi być w stanie ograniczyć sesje na podstawie źródłowego adresu IP, docelowego adresu IP, harmonogramu, protokołu aplikacji (mysql, ms-sql, sqlnet, pobieranie P2P)
Wydzielenie stref bezpieczeństwa	• Możliwość tworzenia osobnych stref bezpieczeństwa Firewall, np. DMZ, LAN, VPN • Musi mieć możliwość konfiguracji oddzielnych wirtualnych routerów • Musi mieć możliwość konfigurowania oddzielnych wirtualnych przełączników
Ochrona antywirusowa	• Silnik antywirusowy musi być oparty na przepływie tzw. flow-based • Musi umożliwiać skanowanie protokołów HTTP, SMTP, POP3, IMAP, FTP / SFTP, SMB • Możliwość ręcznego dodawania lub usuwania sygnatury MD5 do bazy danych AV • Musi obsługiwać wykrywanie wirusów w plikach skompresowanych, takich jak RAR, ZIP, GZIP, BZIP2, TAR, a także wykrywać wielowarstwowe pliki skompresowane dla nie mniej niż 5 warstw dekompresji

Parametr	Charakterystyka
Równoważenie obciążenia	• Obsługa redundantnego równoważenia obciążenia ISP i ISP z wykrywaniem łącza dla określonej nazwy domeny oraz monitorowanie stanu łącza poprzez aktywną metodę wykrywania • Obsługa równoważenia obciążenia serwerów w oparciu o weighted hashing, weighted leastconnection i weighted round-robin • Kontrola stanu serwera, monitorowanie sesji i ochrona sesji
Ochrona IPS	• Ochrona IPS musi opierać się przynajmniej na analizie protokołu i sygnatury. • Baza danych wykrytych ataków musi zawierać co najmniej 8000 sygnatur. Dodatkowo musi być w stanie wykrywać anomalie protokołów i ruchu, które stanowią podstawową ochronę przed atakami DoS i Ddos. • Funkcjonalność zapobiegania atakom SQL injection, XSS injection • Możliwość budowania własnych niestandardowych reguł IPS
Obrona przed atakiem	• Ochrona przed nieprawidłowym działaniem protokołu • Anti-DoS/DDoS, zawierający ochronę przed SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment itp. • Wsparcie IPv4 jak i IPv6 dla ochrony przed DNS query flood i DNS reply flood • Biała lista docelowych adresów IP
Ochrona antyspam	• Rozwiązanie musi zapewniać ochronę przed spamem w czasie rzeczywistym • Wspieranymi protokołami są minimum SMTP, SMTPS, POP3, POP3S • Skanowanie antyspamowe musi odbywać się w ruchu w obu kierunkach • Musi istnieć możliwość dodawania wyjątków w zakresie skanowania antyspamowego, minimum białych list domen
Kontrola aplikacji	• Kontrola aplikacji musi być w stanie kontrolować ruch w oparciu o głęboką analizę pakietów, a nie tylko w oparciu o wartości portów TCP/UDP • Baza danych aplikacji zawierająca ponad 4700 aplikacji, które można filtrować według nazwy, kategorii, podkategorii, technologii i ryzyka
Filtr adresów URL	• Baza filtrów URL pogrupowana w co najmniej 64 kategorie tematyczne. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków. • Możliwość zdefiniowania własnej bazy kategorii www. • Automatyczne pobieranie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy danych dostarczającej filtr URL. • Kategoria takie jak hazard, malware, spam, botnety • Obsługa Safe Search • Blokowanie i logowanie stron URL z określonymi słowami, które można budować przez wyrażenia regularne • Dostosowanie strony ostrzeżenia
Ochrona danych	• Kontrola transferu plików na podstawie typu pliku, rozmiaru i nazwy

Parametr	Charakterystyka
	• Identyfikacja protokołu pliku, w tym HTTP,FTP、SMTP, POP3、IMAP • Obsługa deszyfracji SSL do filtrowania plików przesyłanych przez HTTPS, SMTPS, POP3S, IMAPS • Filtrowanie plików przesyłanych przez SMB
Reputacja IP	• Identyfikacja i filtrowanie ruchu z ryzykownych adresów IP, takich jak hosty botnet, spamerzy, węzły Tor, podejrzane hosty i adresy IP atakujące metodą brute force • Logowanie, odrzucanie pakietów lub blokowanie dla różnych rodzajów ryzykownego ruchu IP

Zapobieganie zagrożeniom botnet	• Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware
	• Wsparcie DNS sinkhole
	• Wsparcie wykrywania tunelowania DNS
	• Wyrywanie i blokowanie DGA
	• Wykrywanie co najmniej poniższych typów połączeń botnet:
	  ○ APT
	  ○ Miner
	  ○ CnC
	  ○ Trojan

Cloud Sandbox	• Złośliwe oprogramowanie emulowane w wirtualnym środowisku oparte na architekturze chmury w celu wykrywania nieznanych zagrożeń • Obsługa protokołów, takich jak HTTP/HTTPS, POP3, IMAP, SMTP, FTP i SMB • Obsługa typów plików : PE, ZIP, RAR, Office, PDF, APK, JAR, SWF i skryptów • Obsługa blokowania wyników wykrywania w celu szybkiego blokowania nieznanych zagrożeń
Uwierzytelnianie użytkownika	• System bezpieczeństwa musi być w stanie przeprowadzić uwierzytelnianie tożsamości użytkownika z nie mniej niż: • Statyczne hasła i definicje użytkowników przechowywane w lokalnej bazie danych systemu • Statyczne hasła i definicje użytkowników przechowywane w bazach danych zgodnych z LDAP • Hasła dynamiczne (RADIUS) oparte o zewnętrzne bazach danych • Dynamiczna autoryzacja przez RADIUS na podstawie komunikatów CoA • Musi umożliwiać budowę architektury uwierzytelniania pojedynczego logowania w środowisku Active Directory • Wsparcie usług terminalowych • Uwierzytelnianie użytkownika przez Web przed dostępem do internetu • Obsługa dwuskładnikowego uwierzytelniania, SMSy, certyfikaty i tokeny • System musi mieć możliwość rozbudowy o moduł ZTNA, w celu uwierzytelniania użytkowników bazując na regułach i zasadach zdefiniowanych przed administratora

Parametr	Charakterystyka

Zapobieganie zagrożeniom botnet	• Wykrywanie intranetowych hostów botnetu, monitorując połączenia C&C i blokowanie dalszych zaawansowanych zagrożeń takich jak botnet i oprogramowanie ransomware
	• Wsparcie DNS sinkhole
	• Wsparcie wykrywania tunelowania DNS
	• Wyrywanie i blokowanie DGA
	• Wykrywanie co najmniej poniższych typów połączeń botnet:
	  ○ APT
	  ○ Miner
	  ○ CnC
	  ○ Trojan

Raportowanie i przeglądanie logów	• Wbudowany w system bezpieczeństwa system raportowania i przeglądania logów nie może wymagać dodatkowej licencji na jego działanie
	• W zakresie zaimplementowanych funkcjonalności systemu raportowania i przeglądania logów nie mniej niż:
	  ○ Posiadanie predefiniowanych raportów dla ruchu internetowego, modułu IPS, skanera antywirusowego
	  ○ Generowanie co najmniej 10 rodzajów raportów

Wysoka dostępność	• Rozwiązanie musi obsługiwać tryby Active/Active i Active/Passive
	• Rozwiązanie musi obsługiwać następujące opcje wdrażania HA:
	  ○ HA z agregacją linków
	  ○ Full mesh HA
	  ○ Geograficznie rozproszony HA

System logowania	• Wraz z systemem musi być zapewniony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy chmurowej, do której dostęp jest cały czas z dowolnego urządzenia oraz dedykowanej aplikacji mobilnej.
Certyfikaty	• posiadać certyfikat Common Criteria EAL4+ lub posiadać certyfikat ICSA Labs dla funkcji Firewall • być pozycjonowanym w raporcie Gartnera przez ostatnie 8 lat
Zarządzanie	• Elementy systemu muszą mieć możliwość zarządzania lokalnie (HTTPS, SSH) oraz współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja między systemami bezpieczeństwa a platformami zarządzania musi odbywać się za pomocą protokołów szyfrowanych. • Zarządzanie urządzeniem i konfiguracja musi odbywać się za pośrednictwem WebUI lub po pomocą linuii komend (COM Port, SSH, Telnet) bez instalowania oddzielnego oprogramowania, takiego jak dedykowana aplikacja • System musi posiadać możliwość uruchomienia lub otworzenia okna linii komend bezpośrednio z WebUI
Gwarancja	Dostawa musi zawierać: • 24-miesięczną gwarancję producenta na dostarczone elementy systemu

Parametr	Charakterystyka
	• Licencje na wszystkie funkcje bezpieczeństwa producentów na okres minimum 24 miesięcy (IPS, AV, AS, QoS, Cloud-Sandbox, URL, IP Reputation, Botnet C&C) • Wsparcie techniczne dystrybutora rozwiązań w języku polskim • Oferta musi być złożona przez autoryzowanego partnera

6. Środowisko sprzętowe do wirtualizacji zapewniającej izolację oraz replikację wraz przywracaniem systemów – PCPR

Minimalne parametry techniczne i funkcjonalne:

Parametr	Charakterystyka
Obudowa	Obudowa o wysokości 1U dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. 10 zatok 2,5” hot-swap SAS/SATA/NVMe. Obudowa wyposażona w zestaw diod LED umieszczonych z przodu, informujący o statusie serwera.
Procesory	Zainstalowany jeden procesor oferujący nie więcej niż 16 rdzeni o taktowaniu podstawowym minimum 2.4 GHz oraz minimum 24MB L3 Cache. Moc cieplna (TDP) procesora nie może przekraczać 135W. Osiągający w testach SPECrate®2017_int_base wynik nie mniejszy niż 225 dla platformy dwuprocesorowej.
Pamięć RAM	minimum 64 GB pamięci ECC DDR4 RDIMM o taktowaniu minimum 3200MHz w jednakowych modułach zajmujące nie więcej niż 4 sloty pamięci. Możliwość rozbudowy pamięci do 4TB.
Płyta główna	Dedykowana do pracy w serwerach. Wyposażona w dwa gniazda CPU oraz minimum 16 slotów pamięci. Z zainstalowanym wymiennym modułem TPM 2.0 Umożliwiająca instalację co najmniej 2 dysków M.2 PCIe 3.0 x4 NVMe. Wyposażona w dedykowany chipset dla oferowanego procesora.
	Płyta korzystająca z technologii Silicon Root of Trusts (Cryptographically Signed Firmware,Secure Boot, Secure Firmware Updates, Automatic Firmware Recovery, Supply Chain Security, Remote Attestation, Runtime BMC Protections, System Lockdown)
Złącza PCIe	Wymagane minimum 4 złącza PCIe Gen4 pracujących z prędkością x16 (2 FHHL oraz 2 kompatybilne z OCP 3.0),
	Z czego wymagane jedno wolen złącze OCP3.0 oraz jedno złącze PCIe
Dysk twardy	4 dyski NVMe 2,5" o pojemności minimum 1600 GB każdy, dyski muszą być klasy Enterprise o żywotności min 3DWPD,
Karta sieciowa	Minimum 2 porty sieciowe 10GbE RJ-45 i 2 porty 10 GbE SFP+
Karta graficzna	Zintegrowana z układem zdalnego zarządzania karta graficzna.
Porty	1 port Ethernet RJ-45 dedykowany dla interfejsu zdalnego zarządzania
	minimum cztery porty USB w tym dwa porty z przodu serwera oraz dwa porty USB 3.0 z tył serwera
	1 port VGA (15-pin video),
	1 port szeregowy
Kontroler dyskowy	Sprzętowy kontroler SATA/SAS/NVMe 12G RAID 0,1,5,6,10,50,60 8GB cache 16-portowy, kontroler musi umożliwiać zainstalowania dodatkowego modułu ochrony danych pamięci podręcznej RAID
Zasilanie	Dwa redundantne zasilacze hot-plug, każdy o mocy minimum 860 W posiadające certyfikat efektywności energetycznej 96%+ titanium.

Zarządzanie	Serwer musi być wyposażony w moduł zdalnego zarządzania (konsoli) pozwalający na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera, możliwość sprawdzenia aktualnego poziomu pobieranej energii, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu systemu operacyjnego). Funkcjonalność przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów bez konieczności dokładania dodatkowych kart sprzętowych. Możliwość przekierowania konsoli KVM i wirtualnych napędów w trybie HTML5. Możliwość wykonania zdalnego upgrade IPMI/BMC i BIOS płyty głównej. Wysyłanie wiadomości e-mail o ewentualnej awarii. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną i z dedykowanym portem RJ45 niezależnym od wymaganych w serwerze kart sieciowych. Jeśli któraś z funkcjonalności wymaga dodatkowej licencji musi ona być dostarczona jako bezterminowa.
Wymagania dodatkowe i certyfikaty	Deklaracja CE. Certyfikaty ISO 9001, ISO 14001, ISO 50001, ISO 22301 oraz ISO 20000-1 dla producenta sprzętu
	Dostęp do strony internetowej producenta oferowanego sprzętu, a także prawo do pobierania / instalacji aktualizacji, sterowników, poprawek, uaktualnień oprogramowania układowego (firmware), bez dodatkowych opłat dla Zamawiającego;
	Dostęp do ogólnopolskiej infolinii w języku polskim dostępnej 24h 7 dni w tygodniu przez 365 dni w roku.
	Zamawiający zastrzega sobie prawo do dokonywania rozbudowy sprzętu wynikających z nowych potrzeb (obudowa bez plomb). Możliwość sprawdzenia konfiguracji oraz warunków gwarancji oferowanego sprzętu na stronie producenta po podaniu numeru seryjnego.
	Zamawiający musi mieć możliwość dokonywania zgłoszeń poprzez:
	a) wyznaczone autoryzowane, polskojęzyczne punkty serwisowe producenta oraz serwis telefoniczny producenta, pracujący co najmniej w godzinach 9:00-16:00 we wszystkie dni robocze, bezpłatnie lub w cenie połączenia lokalnego w całej Polsce
	b) stronę WWW producenta w języku polskim zapewniającą przyjmowanie zgłoszeń serwisowych,
	c) zgłoszenie jak i obsługa zgłoszenia realizowana będzie w języku polskim
Inne	3 lat gwarancji oraz serwisu realizowanego przez producenta serwera w następnym dniu roboczym w miejscu instalacji.
	W przypadku awarii dysków uszkodzone dyski zostają u klienta

7. Środowisko programistyczne do wirtualizacji zapewniającej izolację oraz replikację wraz z przywracaniem systemów – PCPR

Minimalne parametry techniczne i funkcjonalne:

Parametr	Charakterystyka
Ogólne	• Oprogramowanie wprowadzające zaawansowane wielowarstwowe zabezpieczenia, możliwości hybrydowe z platformą Azure oraz elastyczną platformę aplikacji. Zapewniające funkcje rdzenia zabezpieczonego, które pomagają chronić sprzęt, oprogramowanie układowe i funkcje systemu operacyjnego przed zaawansowanymi zagrożeniami bezpieczeństwa. Serwer z bezpiecznym rdzeniem minimalizuje ryzyko związane z lukami w oprogramowaniu układowym i zaawansowanym złośliwym oprogramowaniem.
Inne funkcje	• Admin Center – możliwość raportowania. • Wprowadzanie poprawek bez konieczności ponownego uruchamiania maszyny. • Moduł zaufanej platformy - zapewnia przechowywanie danych bezpieczeństwa. Działa z Bezpiecznym rozruchem, aby zapewnić, że całe oprogramowanie rozruchowe nie zostało zmienione przez rootkita. • Bezpieczeństwo oparte na wirtualizacji – technika VBS, która pomaga chronić serwer przed atakami. • Ochrona pamięci - chroni serwer przed złośliwymi aplikacjami uszkadzającymi pamięć legalnych programów. • Ulepszona usługa migracji pamięci masowej - ułatwiają administratorom migrację magazynu z większej liczby lokalizacji źródłowych.
Oprogramowanie	• Wymagany system operacyjny Microsoft Windows Server 2022 Standard PL x64 16Core oraz 35 licencji User CAL lub równoważny

8. Zapora sieciowa ang. Firewall lub Next Generation Firewall – Starostwo

Minimalne parametry techniczne i funkcjonalne:

Parametr	Charakterystyka
Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	• W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. • Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. • Monitoring stanu realizowanych połączeń VPN. • System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	• System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 16 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 4 gniazdami SFP+ 10 Gbps.

Parametr	Charakterystyka
	• System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. • System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. • System jest wyposażony w zasilanie AC.
Parametry wydajnościowe	• W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 140 tys. nowych połączeń na sekundę. • Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B. • Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.7 Gbps. • Wydajność szyfrowania IPSec VPN nie mniej niż 35 Gbps. • Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps. • Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps. • Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.=

Parametr	Charakterystyka
Funkcje Systemu Bezpieczeństwa	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. • Ochrona przed malware. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. • Zarządzanie pasmem (QoS, Traffic shaping). • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). • Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. • Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. • Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	• Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. • System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: ○ Translację jeden do jeden oraz jeden do wielu.

Parametr	Charakterystyka
	○ Dedykowany ALG (Application Level Gateway) dla protokołu SIP. • W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. • Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. • Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. • Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. • Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. ○ Amazon Web Services (AWS). ○ Microsoft Azure. ○ Cisco ACI. ○ Google Cloud Platform (GCP). ○ OpenStack. ○ VMware NSX. ○ Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.

Parametr	Charakterystyka
	• Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: • Routingu statycznego. • Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. • Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. • ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. • BFD (Bidirectional Forwarding Detection).

Parametr	Charakterystyka
	• Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	• System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. • SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	• System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. • System daje możliwość określania pasma dla poszczególnych aplikacji. • System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. • System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	• Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). • Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. • System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. • System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. • System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). • Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami

Parametr	Charakterystyka
	lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. • System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. • Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. • Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu
Ochrona przed atakami	• Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • System chroni przed atakami na aplikacje pracujące na niestandardowych portach. • Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. • System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. • Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). • Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. • Wykrywanie i blokowanie komunikacji C&C do sieci botnet. • Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	• Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. • Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. • Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

Parametr	Charakterystyka
	• Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. • Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. • Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). • System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	• Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. • W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. • Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. • Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. • Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). • Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. • Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. • Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. • System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.`

Uwierzytelnianie użytkowników w ramach sesji	• System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
	  ○ Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
	  ○ Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

Parametr	Charakterystyka
	○ Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. • System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. • System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. • Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	• Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. • Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. • Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. • System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. • System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. • Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. • Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. • Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). • Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	• Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci

Parametr	Charakterystyka
	odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. • W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. • Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. • Możliwość włączenia logowania per reguła w polityce firewall. • System zapewnia możliwość logowania do serwera SYSLOG. • Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
Gwarancja oraz wsparcie	• System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. • Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden inżynier musi posiadać najwyższy stopień certyfikacji dla danego rozwiązania) oraz ISO 9001 , ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty.

9. Rozwiązanie do podtrzymania zasilania energetycznego typu UPS – PCPR

Minimalne parametry techniczne i funkcjonalne:

Parametr	Charakterystyka
Topologia	• online, VFI-SS-111
Bypass zewnętrzny	• Wymagany (odpowiedni do oferowanego zasilacza, w obudowie naściennej), instalacja zostanie przeprowadzona przez serwis producenta
Moc wyjściowa	• 20kVA/20kW; PF=1
Moc bierna pojemnościowa (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika)	• 0 var
Napięcie wejściowe	• 173 ÷ 485 V AC ± 2 %
Napięcie wyjściowe (wartość skuteczna)	• 3x400 V AC
Częstotliwość napięcia wejściowego (oraz tolerancja)	• 45 ÷ 55 Hz ± 1 Hz
Częstotliwość napięcia wyjściowego praca sieciowa / rezerwowa	• Synchroniczne / 50Hz ± 0,1 Hz
Współczynnik szczytu CF	• 4:1
Parametry styków przekaźników wyjść programowalnych	• 1A / 250 V AC / w standardzie NO i NC dla każdego wyjścia
Zniekształcenia prądu wejściowego THDi (bez zewnętrznych układów filtrujących, realizowane za pomocą układu prostownika)	• < 3%
Zniekształcenia napięcia wyjściowego THDu	• < 2% dla Pmax (liniowe) < 5% (nieliniowe wg PN EN 62040-3
Współczynnik tg ϕ (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika)	• < 0,4
Czas podtrzymania dla obciążenia 20kW	• Minimum 25 minut (w oparciu o minimum 128szt akumulatorów 12V8,8Ah zamontowanych wewnątrz UPS oraz/lub w zewnętrznym module bateryjnym)
Przeciążalność	• 130% - 10min / 160% - 1min / 300% 100ms
EPO	• Wymagane – standard NC
Sygnalizacja	• akustyczno-diodowa, wyświetlacz LCD, menu w języku polskim i angielskim (do wyboru przez użytkownika)
Język oprogramowania i menu	• polski i angielski do wyboru z poziomu interfejsu użytkownika

Wymagane certyfikaty	• ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument)
Komunikacja z urządzeniem	• RS232, USB, MODBUS RTU, bezpotencjałowe wyjścia programowalne (min. 4), wejścia sterujące (min 4),
Wymiary UPS (wys x szer x gł)	• Nie więcej niż 896 x 436 x 860 mm
Podłączenie zasilania	• Umiejscowione z tyłu UPS'a, w dolnej części obudowy
Oprogramowanie do monitorowania pracy zasilacza UPS	• Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów
Dodatkowe wymagania	• UPS musi pochodzić z autoryzowanego kanału sprzedaży, wyprodukowane na terenie Unii Europejskiej, nowe, nieużywane, wyprodukowane nie później niż na 2 miesiące przed dostawą
Serwis producenta	• wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty
Inne wymagania gwarancyjne	• w przypadku niemożności naprawy urządzenia w trakcie trwania gwarancji na miejscu u klienta podstawiony zostanie bezpłatnie UPS o minimum tych samych, a na pewno nie gorszych parametrach na czas naprawy (podmiana i dostawa na koszt dostawcy lub autoryzowanego serwisu producenta UPS) – oświadczenie producenta
Gwarancja	• Minimum 24 miesiące elektronika, 12 miesięcy akumulatory, serwis onsite
Dokumentacja	• Instrukcja w języku polskim
Szkolenie	• Przeszkolenie pracownika z zakresu obsługi urządzenia w dniu instalacji. Przedstawienie wykazu obowiązków pracownika w zakresie konserwacji oraz monitoringu urządzenia oraz postępowania na wypadek awarii.

10. Rozwiązanie do wirtualizacji zapewniającej izolację sieci oraz replikację wraz z przywracaniem systemów – PCPR

Minimalne parametry techniczne i funkcjonalne przełącznika:

Parametr	Charakterystyka
Liczba portów	• Minimum 48 PoE 10/100/1000 Mbps PoE+
Liczba portów SFP+	• Minimum 4

Obsługa PoE	• TAK
Standardy, protokoły oraz funkcje	• IEEE® 802.3 10BASE-T • IEEE 802.3u 100BASE-TX • IEEE 802.3ab 1000BASE-T • IEEE 802.3z 1000BASE-X • IEEE 802.3x full-duplex flow control • IEEE 802.3az (EEE) • IEEE 8021.Q VLAN (256 groups, Static) • IEEE 802.1p Class of Service (CoS) • 8 kolejek sprzętowych • Port-based QoS • IEEE 802.3ad Static or Dynamic Link Aggregation (LACP) • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1w Rapid Spanning Tree Protocol • IEEE 802.1s Multiple Spanning Tree Protocol • SNMP v1, v2c, v3 • RFC 1213 MIB II • RFC 1643 Ethernet Interface MIB • RFC 1493 Bridge MIB • RFC 2131 DHCP client • IEEE 802.1x (RADIUS) • RADIUS accounting • IEEE 802.1x Dynamic VLAN Assignment • HTTPS/SSL: Secure HTTP GUI • Layer 3 (DSCP) Quality of Service (QoS) • TACACS+ • Port-based security by locked MAC addresses • TCP/UDP-based priority mapping • IGMP snooping v1, v2, v3 • MLD snooping • ACLs (MAC, IPv4, IPv6 and TCP/UDP based) • Ograniczenie przepustowości na wejściu oraz wyjściu • SNTP • DNS • Ochrona przed DoS • MVR • IPv6 management, multicast and QoS • Static Routing • DHCP snooping • Protocol and MAC-based VLAN

	• RMON group 1, 2, 3, 9 • Private Enterprise MIB • Port mirroring – many-to-one • IEEE 802.3ab LLDP • LLDP-MED • Protected ports • Możliwość wykonania prostego testu okablowania
Przepustowość przełącznika	• Magistrala min. 176 Gbps • MPPS min.: 130.94 • Budżet PoE: min. 380W • Bufor pakietów: 1,5 MB • Pamięćć RAM min. 512 MB • Ilość MAC: 16 K • Ilość VLANs: min 256; • Ilość LAGs: 16 • Ilość statycznych tras: 32 • Ilość wpisów ARP: 512 • Ilość ACLs (IPv4/IPv6): min 100 • Ilość grup multicast: 512 • Czas bezawaryjnej pracy: min. 1296949 godzin
Funkcje oszczędności energii	• Zgodność z EEE (Energy Efficient Ethernet) • Obniżenie poboru energii w trybie bezczynności, lub krótkiego kabla
Gwarancja	• Minimum 2 lata

Access Point – 5 szt. kompatybilnych z dostarczonym przełącznikiem

Minimalne parametry techniczne i funkcjonalne:

Parametr	Charakterystyka
Standard	• IEEE 802.11 ac/n/g/b/a
WDS/Mesh	• Tak
Szybki Roaming	• Pre-autoryzacja, PMK caching i 802.11 r/k/v
Szyfrowanie	• WEP/WPA/WPA2-PSK
VLAN	• TAK
Prędkość	• 2.4 GHz: 300 Mbps • 5 GHz: 1300 Mbps

Gwarancja	• Minimum 3 lata

11. Oprogramowanie antywirusowe ang. AntiVirus, AV – PCPR

Zamawiający posiada 36 licencji na oprogramowanie antywirusowe:

Oferując rozwiązanie równoważne dla oprogramowania wymienionego przez Zamawiającego, Wykonawca zobowiązany jest wykazać, że rozwiązania równoważne zachowują cechy techniczne, funkcjonalne i jakościowe w stosunku do oprogramowania wskazanego przez Zamawiającego.

Minimalne parametry techniczne i funkcjonalne:

Parametr	Opis
Administracja zdalna w chmurze	• Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. • Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW. • Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. • Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. • Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu http Proxy. • Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. • Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. • Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. • Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. • Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. • Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. • Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
Ochrona stacji roboczych	• Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). • Rozwiązanie musi wspierać architekturę ARM64. • Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

- Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
- Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
- Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
- Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
- Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
- Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
- Rozwiązanie musi integrować się z Intel Threat Detection Technology.
- Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
- Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
- Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
- Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
- Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
  - ✓tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
  - ✓tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
  - ✓tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
  - ✓tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,

	✓tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach. • Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. • Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. • Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. • Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). • Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. • Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. • Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: ✓tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, ✓tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, ✓tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, ✓tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. ✓Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. • Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. • Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. • Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. • Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. • Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. • W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
Ochrona serwera	• Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej:

✓RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu
✓Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.

- Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
- Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
- Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
- Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

- Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
- Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
- Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
- Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
- Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
- Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
- Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

- Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
- Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i

	instalacji dodatkowego rozwiązania w postaci usługi serwera Web. • Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. • Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
Szyfrowanie	• System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit. • System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault). • Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia. • Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
Ochrona urządzeń mobilnych opartych o system operacyjny Android	• Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. • Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. • Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). • Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. • Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: ✓ usunięcie zawartości urządzenia, ✓ przywrócenie urządzenie do ustawień fabrycznych, ✓ zablokowania urządzenia, ✓ uruchomienie sygnału dźwiękowego, ✓ lokalizację GPS. • Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. • Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: ✓ nazwę aplikacji, ✓ nazwę pakietu, ✓ kategorię sklepu Google Play, ✓ uprawnienia aplikacji, ✓ pochodzenie aplikacji z nieznanego źródła.
Sandbox w chmurze	• Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day. • Rozwiązanie musi wykorzystywać do działania chmurę producenta. • Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi. • Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki

	muszą zostać usunięte z serwerów producenta. • Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek. • Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania. • Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów. • Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy. • Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione. • Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych. • Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo. • Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem: ✓ Czysty, ✓ Podejrzany, ✓ Bardzo podejrzany, ✓ Szkodliwy. • W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum. • W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki. • Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.
Licencjonowanie	• Licencja musi obejmować ochronę dla co najmniej 36 stacji roboczych. • Okres obowiązywania licencji nie może być krótszy niż 24 miesiące. • Licencja musi zapewniać dostęp do pełnej funkcjonalności zgodnie z określonym zakresem wymagań.

12. Rozwiązania programistyczne BDR ang. Backup and Disaster Recovery – PCPR

Minimalne parametry techniczne i funkcjonalne:

Parametr	Charakterystyka
Wymagania ogólne	1. Produkt dostępny w polskiej wersji językowej. 2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej

	3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków 4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów 5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych 6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT 7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft 8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe 9. System zarządzania nie może być oparty o relacyjne bazy danych. 10. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej). 11. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów). 12. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych. 13. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych. 14. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle. 15. Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez powiązania i poleganiu na komponentach wyłącznie jednego dostawy (tzw. "no propietary vendor lock"). 16. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami. 17. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej. 18. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie. 19. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia. 20. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu. 21. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych 22. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.

	23. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego. 24. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii). 25. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane. 26. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione. 27. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika, 28. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta. 29. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym. 30. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych). 31. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych. 32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów. 33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych 34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie. 35. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta. 36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego. 37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.

38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
39. System musi pozwalać na automatyczne aktualizacje oprogramowania.
40. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
41. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.
42. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
43. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
44. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
45. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
46. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
47. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
48. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
49. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
50. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
51. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
52. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: Custom, Basic, G-F-S, Forever incremental,
53. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
54. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.
55. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny

	56. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS). 57. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu. 58. Możliwość generowania raportów dobowych w oparciu o harmonogram 59. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Polski) 60. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna) 61. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP. 62. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)
Wsparcie	Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: • Alpine 3.10+, • Debian: 9+, • Ubuntu: 16.04+, • Fedora: 29+, • centOS: 7+, • RHEL: 6+, • openSUSE: 15+, • SUSE Enterprise Linux(SLES): 12 SP2+, • macOS: 10.13+, • Windows: 7, 8.1, 10(1607+), • Windows Server: 2008 R2+, Środowisk wirtualnych: • Hyper-V 2016+, • VMware: 6.7+. Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: • Debian: 9+ • Ubuntu: 16.04+ • Fedora: 29+ • centOS: 7+ • RHEL: 6+

	• openSUSE: 15+ • SUSE Enterprise Linux (SLES): 12 SP2+ • Windows Client: 7, 8.1, 10 (1607+) • Windows Server: 2012 R2+,
Środowiska fizyczne i bazy danych	1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami. 2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń. 3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej. 4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption. 5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji. 6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych. 7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux. 8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem. 9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. 10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych. 11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V. 12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK). 13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych. 14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).
Środowiska wirtualne	1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.

	2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych. 3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych. 4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner. 5. System kopii zapasowej 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 oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych. 6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna). 7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere. 8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.
Aplikacje SaaS	1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza. 2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji) 3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365. 4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi 5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe. 6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git. 7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium. 8. System musi umożliwiać zabezpieczenie środowisk Jira 9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego. 10. System musi umożliwiać zabezpieczenie środowisk Jira

Licencjonowanie i wsparcie techniczne	1. Wszystkie linie supportu muszą być obsługiwane w języku polskim. 2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta. 3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu. 4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów) 5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego. 6. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk. 7. Licencje powinny być dostępne w opcji wieczystej . 8. Dostęp do wsparcia technicznego producenta powinno obowiązywać przez okres min. 24 miesięcy 9. Sposób licencjonowania opiera się na: - ilości serwerów/endpointów- dla fizycznych urządzeń, - ilości socketów w hostach- dla środowisk wirtualnych, - ilość repozytoriów- dla GIT. 10. Licencje powinny umożliwiać zabezpieczenie w wersji wieczystej: - 10 stacji roboczych, - 1 serwera fizycznego
Anty-ransomware oraz bezpieczeństwo	1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane- "niezmienny system plików"). 2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System 3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty. 4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowały by działanie Systemu. System nie może posiadać pojedynczego punktu awarii. 5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.

13. Rozwiązanie IAM/IDM ang. Identity Access Manager, Identity Manager – PCPR

Minimalne parametry techniczne i funkcjonalne:

Charakterystyka
Funkcjonalności ogólne
System odpowiedzialny za zarządzanie licencjami, monitorowanie ich terminu ważności, zarządzanie uprawnieniami z dowolnych systemów w ramach pracy jednostki organizacyjnej, procesem akceptacji przydzielanych uprawnień, integracji w zakresie możliwości nadawania uprawnień w systemach zintegrowanych, użytkownikami i uprawnieniami w aplikacji do zarządzania licencjami i uprawnieniami, zarządzaniem parametrami, zadaniami wsadowymi, monitoringiem wykonanych czynności oraz sterowanie wysyłką powiadomień za pośrednictwem brokera powiadomień, który zapewnia mechanizm wysyłki powiadomień dowolnym kanałem komunikacji (SMS, eMail, poprzez dedykowane interfejsy). 1. System umożliwia definiowanie dowolnej ilości użytkowników. 2. System w całości spolonizowany, a więc posiada polskie znaki i instrukcję obsługi po polsku dla użytkownika oraz administratora. 3. System posiada graficzny interfejs użytkownika gwarantujący wygodne wprowadzanie danych, przejrzystość prezentowania danych na ekranie oraz wygodny sposób wyszukiwania danych po ergonomicznie dobranych kryteriach. 4. System gwarantuje integralność danych, bieżącą kontrolę poprawności wprowadzanych danych, spójność danych. 5. System pracuje w środowisku sieciowym i posiada wielodostępność pozwalającą na równoczesne korzystanie z bazy danych przez wielu użytkowników. 6. System posiada mechanizmy umożliwiające weryfikację integralności danych tj. identyfikację użytkownika i ustalenie daty wprowadzenia i modyfikacji danych. W systemie jest dostępny dziennik zdarzeń systemowych zapewniający pełną rozliczalność przez przechowywanie szczegółów dotyczących wykonywania każdej czynności wykonanej przez wszystkich użytkowników. 7. System posiada mechanizmy ochrony danych przed niepowołanym dostępem, nadawania uprawnień dla użytkowników do korzystania z modułów jak również do korzystania z wybranych funkcji. System jest oparty o mechanizm ról i uprawnień.
Lista funkcjonalności Systemu do zarządzania uprawnieniami i licencjami
1. System umożliwia bezpieczne zalogowanie poprzez przeglądarkę. 2. System, oprócz logowania standardowego (eMail i hasło) umożliwia logowanie domenowe. 3. Użytkownik ma możliwość zmiany hasła oraz ponownego jego nadania w przypadku zagubienia hasła. 4. System udostępnia użytkownikowi o charakterze administratora funkcjonalności zarządzania konfiguracją systemu, w tym przegląd i modyfikację bieżących ustawień systemu, które wpływają na jego zachowanie. 5. System pozwala administratorowi na zarządzanie konfiguracją zadań wsadowych, czyli zadań, które uruchamiane są w cyklicznie zdefiniowanych momentach (dniach, godzinach, minutach, itp.). 6. System posiada funkcje umożliwiające zapis, odczyt i usunięcie plików w systemie. 7. System umożliwia przegląd rejestru licencji dodanych w aplikacji, z możliwością filtrowania po następujących kryteriach: a. Nazwa licencji; b. Rodzaj licencji;

c. Data obowiązywania od;
d. Data obowiązywania do;
e. Status;
f. Przypisany użytkownik.

8. System pozwala na sortowanie rosnąco i malejąco wyświetlanych danych rejestru licencji po wartościach: rodzaj, nazwa, data obowiązywania od, do, status.
9. System udostępnia możliwość wydruku raportu licencji.
10. System posiada funkcje umożliwiające podgląd danych szczegółowych licencji przez uprawnionego użytkownika aplikacji, w tym przegląd danych podstawowych, dołączonych dokumentów oraz przypisanych użytkowników.
11. System udostępnia funkcjonalność monitorowania i powiadamiania (eMail) o kończącym się terminie ważności danej licencji.
12. System udostępnia możliwość przypisania (odebrania) dowolnej licencji wskazanemu pracownikowi wraz z możliwością wysłania maila o tym fakcie z danymi dostępowymi w przypadku przypisania licencji.
13. System umożliwia definiowanie dowolnych uprawnień. Dla tworzonych uprawnień istnieje możliwość określenia atrybutów m.in.: nazwa, notatka, szablon opisu uprawnienia (domyślna treść wysyłana przy nadawaniu).
14. System dla zdefiniowanego uprawnienia udostępnia możliwość ustawienia wysyłki powiadomienia (eMail) przy nadawaniu / odbieraniu uprawnienia.
15. System umożliwia tworzenie dowolnych grup uprawnień, co pozwala na definiowanie zbiorów uprawnień niezbędnych do przypisania np. na danym stanowisku, bez konieczności przypisywania pojedynczych uprawnień.
16. System umożliwia przypisanie administratorów do uprawnień, którzy będą odpowiedzialni za fizyczne nadanie / odebranie oraz potwierdzenie uprawnienia.
17. System udostępnia funkcjonalność określania ścieżki akceptacyjnej dla danego uprawnienia. Definiując dane uprawnienia istnieje możliwość określenia konkretnej listy stanowisk / pracowników, którzy będą potwierdzać nadanie/odebranie uprawnienia. Opcjonalnie można ustawić dla uprawnienia akceptację automatyczną.
18. System posiada funkcjonalność powiadamiania eMail o zatwierdzeniu / odrzuceniu akceptacji na poszczególnych poziomach ścieżki akceptacyjnej.
19. System posiada rejestr zgłoszonych uprawnień do akceptacji, z możliwością przeglądu danych historycznych.
20. System udostępnia funkcjonalność tworzenia dowolnych ścieżek akceptacyjnych, prowadzenia rejestru zdefiniowanych ścieżek wraz z ich zarządzaniem.
21. System posiada funkcjonalność rejestru nadanych uprawnień z możliwością wyszukiwania min. według pracowników, uprawnieniach oraz data obowiązywania, nadania. W rejestrze można zgłosić potrzebę nadania / odebrania danego uprawnienia pracownikowi. Zgłoszenie dostępne będzie w kontekście pojedynczego uprawnienia, wybranych uprawnień, jak również uprzednio zdefiniowanej grupy uprawnień.

Ograniczenia niefunkcjonalne spełniane przez System do zarządzania uprawnieniami i licencjami

1. System jest zaprojektowany w modelu trójwarstwowym:
   - ✓ warstwa danych,
   - ✓ warstwa aplikacji,
   - ✓ warstwa prezentacji - przeglądarka internetowa - za pośrednictwem której następuje właściwa obsługa systemu przez użytkownika końcowego.

2. System umożliwia pracę na bazie typu Open Source, bądź na komercyjnym systemie bazodanowym.
3. W warstwie serwera aplikacji i bazy danych istnieje możliwość uruchomienia systemu w środowiskach opartych na systemach operacyjnych z rodziny Windows lub równoważnych oraz w środowiskach opartych na systemie Linux lub równoważnych.
4. System w warstwie klienckiej działa w różnych środowiskach z minimum 5 najbardziej popularnymi przeglądarkami w Polsce w ich najnowszych wersjach (zgodnie ze statystyką prowadzoną na stronie http://gs.statcounter.com/ za okres 6 miesięcy poprzedzających miesiąc ogłoszenia postępowania określoną dla komputerów stacjonarnych „desktop").
5. System realizuje wszystkie czynności przez przeglądarkę internetową.
6. System pracuje w wersji sieciowej z wykorzystaniem protokołu TCP/IP oraz jest w pełni kompatybilna z sieciami TCP/IP.
7. Architektura systemu umożliwia pracę jedno i wielostanowiskową, zapewnia jednokrotne wprowadzanie danych tak, aby były one dostępne dla wszystkich użytkowników.
8. W przypadku gdy system do pracy wykorzystuje silnik bazy danych, baza jest kompatybilna z systemem operacyjnym i istnieje możliwość jej instalacji i pracy na zasadach określonych dla systemu.
9. System w zakresie wydruków wykorzystuje funkcjonalność systemu operacyjnego i umożliwia wydruk na dowolnej drukarce zainstalowanej i obsługiwanej w systemie operacyjnym, na którym zostanie zainstalowane oprogramowanie (drukarki lokalne, drukarki sieciowe).
10. Interfejs użytkownika (w tym administratora) jest w całości polskojęzyczny.
11. System zapewnia weryfikację wprowadzanych danych w formularzach i kreatorach.
12. System zapewnia bezpieczeństwo danych zarówno na poziomie danych wrażliwych jak i komunikacji sieciowej przy zastosowaniu bezpiecznych protokołów sieciowych.
13. System umożliwia okresowe wykonywanie, w sposób automatyczny, pełnej kopii aplikacji i danych systemu.
14. System posiada funkcjonalność zarządzania dostępem do aplikacji:
    - ✓ administrator systemu ma możliwość tworzenia, modyfikacji oraz dezaktywacji kont użytkowników,
    - ✓ administrator systemu może nadawać uprawnienia użytkownikom,
    - ✓ pozwala na zmianę danych uwierzytelniających użytkownika (hasło).
15. System posiada możliwość określenia maksymalnej liczby nieudanych prób logowania, po przekroczeniu której użytkownik zostaje zablokowany.
16. System komunikuje z systemami zewnętrznymi w sposób zapewniający poufność danych.
17. System jest odporny na znane techniki ataku i włamań, typowe dla technologii, w której został wykonana.
18. System prowadzi dziennik zdarzeń (w postaci logów systemowych) i umożliwia dostęp do obiektów danych, dokumentów, operacji na słownikach umożliwiający odtwarzanie historii aktywności poszczególnych użytkowników systemu oraz umożliwia podgląd podstawowych statystyk użycia systemu.

CZĘŚĆ 2 – OBSZAR KOMPETENCYJNY

1. Szkolenia dla urzędników Powiatu Bartoszyckiego i PCPR w Bartoszycach

Charakterystyka

Przedmiotem zamówienia jest organizacja i przeprowadzenie szkoleń dla urzędników Powiatu Bartoszyckiego i PCPR w Bartoszycach w zakresie cyberbezpieczeństwa dotyczącego praktycznego stosowania mechanizmów bezpieczeństwa korespondencji i zabezpieczania danych, w ramach projektu pn. „Cyberbezpieczny samorząd Powiatu Bartoszyckiego" realizowanego w ramach „Cyberbezpieczny Samorząd" Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, zgodnie z poniższą specyfikacją:

1. Szkolenia podstawowe z zakresu cyberbezpieczeństwa dla JST służące zwiększeniu świadomości pracowników administracji publicznej w kwestiach związanych z bezpieczeństwem cyfrowym.

Zakres szkolenia teoretycznego i jego tematyka:

- czym jest cyberbezpieczeństwo i dlaczego jest istotne
- wyjaśnienie podstawowych pojęć związanych z cyberbezpieczeństwem, np.: https, IP, TCP, domena, ASE-256, komunikator i inne
- phishing i ransomware - zasady funkcjonowania i rozpoznawanie tych zagrożeń
- wyłudzanie danych osobowych za pomocą technik socjotechnicznych - czym jest socjotechnika i jak się przed nią bronić
- zasady korzystania z poczty elektronicznej
- bezpieczeństwo pracy zdalnej - praca na sprzęcie własnym lub służbowym
- bezpieczeństwo zakupów oraz płatności w Internecie
- sposoby zabezpieczania własnych danych
- rozpoznawanie fałszywych informacji
- bezpieczeństwo podczas korzystania z przeglądarek internetowych: Mozilla Firefox, Google Chrome, Microsoft Edge, Apple Safari - jak bezpiecznie komunikować się w Internecie
- audyt bezpieczeństwa teleinformatycznego
- odpowiedzialność prawna i zadania kierownictwa w dziedzinie cyberbezpieczeństwa

2. Szkolenia podstawowe z zakresu cyberbezpieczeństwa dla PCPR służące zwiększeniu świadomości pracowników administracji publicznej w kwestiach związanych z bezpieczeństwem cyfrowym:

- czym jest cyberbezpieczeństwo i dlaczego jest istotne
- wyjaśnienie podstawowych pojęć związanych z cyberbezpieczeństwem, np.: https, IP, TCP, domena, ASE-256, komunikator i inne
- phishing i ransomware - zasady funkcjonowania i rozpoznawanie tych zagrożeń
- wyłudzanie danych osobowych za pomocą technik socjotechnicznych - czym jest socjotechnika i jak się przed nią bronić
- zasady korzystania z poczty elektronicznej
- bezpieczeństwo podczas korzystania z przeglądarek internetowych: Mozilla Firefox, Google Chrome, Microsoft Edge, Apple Safari - jak bezpiecznie komunikować się w Internecie
- prywatność w sieci, czyli: trakery, ciastka i tryb incognito
- bezpieczeństwo pracy zdalnej - praca na sprzęcie własnym lub służbowym
- bezpieczeństwo zakupów oraz płatności w Internecie
- sposoby zabezpieczania własnych danych

- rozpoznawanie fałszywych informacji
- audyt bezpieczeństwa teleinformatycznego

3. Szkolenia z zakresu cyberbezpieczeństwa dla kadry IT związane z zakresami odpowiedzialności za infrastrukturę IT, którzy pełnią kluczową rolę w ochronie przed zagrożeniami cybernetycznymi.
Zakres szkolenia teoretycznego i jego tematyka:

- podstawy prawne krajowego systemu cyberbezpieczeństwa,
- obowiązki wynikające z przepisów rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2024 poz. 773) i ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077), zapewnienie zgodności działań IT z tymi przepisami,
- ocena ryzyka, w tym metody identyfikacji i analizy ryzyka związanego z IT, środki zaradcze w celu minimalizacji ryzyka,
- audyt wewnętrzny (cyberbezpieczeństwa) i raportowanie zgodności z przepisami,
- analiza najnowszych zagrożeń cybernetycznych, takich jak ransomware, malware, phishing, ataki DDoS oraz zaawansowane uporczywe zagrożenia (Advanced Persistent Threat – APT), oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa i inne metody socjotechniczne,
- rozpoznawanie i analiza wzorców ataków i technik stosowanych przez cyberprzestępców oraz sposoby ochrony,
- identyfikacja i klasyfikacja incydentów bezpieczeństwa,
- procedury przyjmowania zgłoszeń incydentów, reagowanie na incydenty,
- sposoby szybkiego reagowania na incydenty oraz koordynacja działań naprawczych,
- konfiguracja i monitoring systemów, w tym konfiguracja systemów operacyjnych i aplikacji w sposób zapewniający ich bezpieczeństwo oraz monitorowanie sieci i systemów w celu wykrywania nieautoryzowanych działań,
- bezpieczeństwo sieci, w tym konfiguracja zapór sieciowych, systemów wykrywania i przeciwdziałania włamaniom (Intrusion Detection/Prevention System – IDS/IPS) oraz implementacja wirtualnych sieci prywatnych (VPN) i bezpiecznych protokołów komunikacyjnych,
- kontrola dostępu, w tym implementacja polityk zarządzania tożsamością i dostępem (Identity Access Management – IAM) oraz konfiguracja systemów uwierzytelniania wieloskładnikowego (MFA), wady i zalety klucze sprzętowych.
- zarządzanie uprawnieniami, w tym audyt i zarządzanie uprawnieniami użytkowników w systemach i aplikacjach, regularna weryfikacja uprawnień i ograniczanie dostępu do niezbędnego minimum, procedury związane z nadawaniem i odbieraniem uprawnień,
- testy penetracyjne, w tym przeprowadzanie testów penetracyjnych, interpretacja wyników testów i wdrażanie poprawek,

- bezpieczeństwo i ochrona danych, w tym mechanizmy ochrony danych, takie jak szyfrowanie i tworzenie kopii zapasowych, zrozumienie zasad ochrony danych osobowych zgodnie z RODO,
- bezpieczeństwo w chmurze, w tym bezpieczne korzystanie z usług chmurowych i zarządzanie danymi w chmurze, zasady bezpieczeństwa specyficzne dla platform chmurowych (np. AWS, Azure, Google Cloud),
- profilaktyka cyberbezpieczeństwa w urzędzie, standardy i najlepsze praktyki w tym w zakresie bezpieczeństwa urządzeń i bezpieczeństwa fizycznego,
- sposoby podnoszenia świadomości pracowników Urzędu w zakresie cyberbezpieczeństwa i testowania odporności Urzędu na różnego rodzaju ataki,
- umiejętność skutecznej komunikacji z zespołem, z innymi komórkami urzędu i jednostek podległych oraz z interesariuszami zewnętrznymi w sprawach cyberbezpieczeństwa.

Uczestnik szkolenia powinni otrzymać imienny certyfikat uczestnictwa w szkoleniu zawierający informacje o omawianych na nim zagadnieniach.
Szkolenia będą przeprowadzone w siedzibie Zamawiającego, możliwa jest też formuła zdalna szkoleń w zależności od możliwości technicznych i lokalowych Zamawiającego.

Oprócz szkolenia teoretycznego, Wykonawca powinien zrealizować ćwiczenia praktyczne obejmujące tematykę (np. w formie quizu lub ćwiczeń):

1. rozpoznawanie złośliwego oprogramowania i phishingu
2. jak bezpiecznie komunikować się w Internecie
3. omówienie i prezentacja oprogramowania służącego do obrony przed złośliwym oprogramowaniem:
   a) menedżer haseł (komercyjne vs open source)
   b) szyfrowanie danych na komputerze (komercyjne vs open source)
   c) szyfrowanie danych w chmurze (komercyjne vs open source)
4. użytkowanie menadżera haseł, szyfrowanie danych
5. sposoby zabezpieczania własnych danych
6. rozpoznawanie fałszywych informacji.

Wymagania ogólne dotyczące organizacji szkolenia:

1. Szkolenie odbędzie się w siedzibie Zamawiającego, w trybie stacjonarnym lub zdalnym
2. W szkoleniu będzie brało udział około ..... osób, w podziale na 3 grupy: I grupa pracownicy JST - ..... osób, II grupa – pracownicy PCPR około ..... osoby, III grupa - kadra IT ..... osoby. Zamawiający dopuszcza rotacje w liczbie uczestników podczas każdego szkolenia.
3. Wymagane jest, aby każda z ww. grup odbyła szkolenie w innym terminie.
4. Szkolenia będą odbywać się w dni robocze, w godz. 8.00 - 15.00.
5. Szkolenia będą prowadzone w języku polskim.
6. Wykonawca zapewni materiały szkoleniowe.

W przypadku szkoleń trwających do 3 godzin, przewiduje się jedną przerwę trwającą 15 minut. W przypadku szkoleń trwających powyżej 3 godzin, organizowane będą dwie przerwy trwające 15 minut każda.

CZĘŚĆ 3 – OBSZAR ORGANIZACYJNY

Charakterystyka
1. Opracowaniu i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Powiatowym Centrum Pomocy Rodzinie w Bartoszycach zgodnie z odwiązującym prawem oraz obowiązującymi Normami w tym zakresie. **Zakres prac:**
1) Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwanej „SZBI"), w skład której wchodzą następujące dokumenty: a) Polityka Bezpieczeństwa Informacji; b) Polityka ochrony danych osobowych; c) Instrukcja zarządzania systemem informatycznym; d) Polityka zarządzania ciągłością działania; e) Procedura zarządzania incydentami cyberbezpieczeństwa f) Analiza ryzyka w zakresie Bezpieczeństwa Informacji; 2) W ramach dokumentacji SZBI ujęte zostaną następujące procedury: a) procedury korzystania z urządzeń mobilnych b) procedury pracy zdalnej c) postępowanie z nośnikami d) procedury kontroli dostępu e) zabezpieczenie pomieszczeń i obiektów f) procedury czystego biurka g) procedury czystego ekranu h) procedury kopii zapasowych i) procedury ochrony logów j) bezpieczeństwo komunikacji k) zarządzanie bezpieczeństwem sieci l) przesyłanie informacji m) plany ciągłości działania n) procedury zarządzania incydentami o) prywatność i ochrona danych osobowych p) szacowanie ryzyka w obszarze bezpieczeństwa informacji. Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zleceniodawcy w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami oraz wszelkich innych informacji uzyskanych w trakcie realizacji Umowy mogących mieć wpływ na treść dokumentacji. Doradztwo dotyczące czynności wdrażających dokumentację nastąpi po przekazaniu Zleceniodawcy przez Zleceniobiorcę całości dokumentacji SZBI.
2. Audyt zgodność z kryteriami zawartymi w Rozporządzeniu KRI/uoKSC Powiatowego Centrum Pomocy Rodzinie w Bartoszycach
1) spotkanie otwierające Audyt; 2) weryfikacja zgodności przyjętych procedur z przepisami Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań

dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t. j. Dz. U. 2024 r., poz. 773);

3) weryfikacja zgodności przyjętych procedur z zakresu cyberbezpieczeństwa wynikających z obowiązków określonych w przepisach Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. z 2023 r., poz. 913,);
4) weryfikacja zgodności przyjętych procedur z przepisami z zakresu ochrony danych wynikających z obowiązków określonych w przepisach Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych Dz. U. UE. L. 2016, poz. 119.1 i 2. – dalej „RODO") oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r., poz. 1781);
5) zamknięcie Audytu;
6) przygotowanie i przekazanie raportu z Audytu;
7) omówienie wyników Audytu końcowego oraz wydanie rekomendacji Zamawiającemu.