**Załącznik nr 9 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

# Serwer backup – 1 szt.

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| **Obudowa** | Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia)  Serwer wyposażony w zdejmowany panel przedni z możliwością instalacji zamka chroniącego przed nieuprawionym dostępem do dysków oraz czujnika otwarcia obudowy współpracującego z BIOS/UEFI. |
| **Procesor** | Jeden procesor 16-rdzeniowy, x86 - 64 bity, 3GHz osiągający w testach <https://www.cpubenchmark.net/high_end_cpus.html> wynik nie gorszy niż 42000 punktów  Płyta główna wspierająca zastosowanie procesorów do 64 rdzeni, mocy do min. 280W i taktowaniu CPU do min. 3.7GHz. |
| **Liczba procesorów** | 1 procesor |
| **Pamięć operacyjna** | Min. 64GB RDIMM DDR4 3200 MT/s w modułach pamięci o pojemności 32 GB każdy  Płyta główna z minimum 16 slotami na pamięć i umożliwiająca instalację do minimum 4TB. |
| **Sloty rozszerzeń** | Min. 4 aktywne gniazda PCI-Express generacji 4, gniazda pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi, w tym min. 2 sloty x16 (szybkość slotu – bus width). |
| **Dysk twardy** | Zatoki dyskowe gotowe do zainstalowania min. 12 dysków LFF typu Hot Swap, SAS/SSD.  Zainstalowane 2 dyski m.2 NVMe 480GB, skonfigurowane w RAID1 oraz 8 dysków 8TB SAS 12Gb. |
| **Kontroler** | Serwer wyposażony w kontroler sprzętowy z max. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, min.16 portowy (16 dedykowanych linii SAS do podłączenia dysków SAS), obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę min. 12 napędów dyskowych SSD/SATA/SAS/NVMe  Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie. |
| **Interfejsy sieciowe** | Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.  Minimum 2 porty 10G SFP+ obsadzone wkładkami SFP+ 10G SR  Minimum 2 porty 16G FC obsadzone wkładkami SFP+ 16G SW |
| **Karta graficzna** | Zintegrowana karta graficzna |
| **Porty** | 4 x USB 3.0 (w tym 1 port wewnętrzny)  1x VGA |
| **Zasilacz** | 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W. |
| **Chłodzenie** | Zestaw wentylatorów redundantnych |
| **Diagnostyka** | Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze. |
| **Bezpieczeństwo** | Serwer wyposażony w moduł TPM 2.0 |
| **System operacyjny** | Licencja na Windows Server 2022 Standard na 16 rdzeni procesora. |
| **Karta/moduł zarządzający** | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:   * monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe * praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP * dostęp do karty zarządzającej poprzez   + dedykowany port RJ45 z tyłu serwera lub   + przez współdzielony port zintegrowanej karty sieciowej serwera   dostęp do karty możliwy   * + z poziomu przeglądarki webowej (GUI)   + z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)   + z poziomu skryptu (XML/Perl)   + poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) * wbudowane narzędzia diagnostyczne * zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego * obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie * wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników * przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) * obsługa zdalnego serwera logowania (remote syslog) * wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów * mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie * funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności * monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji * konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) * zdalna aktualizacja oprogramowania (firmware) * zarządzanie grupami serwerów, w tym:   + tworzenie i konfiguracja grup serwerów   + sterowanie zasilaniem (wł/wył)   + ograniczenie poboru mocy dla grupy (power capping)   + aktualizacja oprogramowania (firmware)   + wspólne wirtualne media dla grupy * możliwość równoczesnej obsługi przez 6 administratorów * autentykacja dwuskładnikowa (Kerberos) * wsparcie dla Microsoft Active Directory * obsługa SSL i SSH * enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli * wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API * wsparcie dla Integrated Remote Console for Windows clients * możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) |
| **Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych** | Serwer jest dostarczany bez Systemu operacyjnego  Zapewnia wsparcie dla:  Microsoft Windows Server 2016, 2019, 2022  Ubuntu 20.04 LTS, 22.04 LTS  Red Hat Enterprise Linux (RHEL) 8.0, 9.0  SUSE Linux Enterprise Server (SLES) 12 SP5 oraz 15 SP2  VMware ESXi 6.7U3, 7.x, 8.x |
| **Wsparcie techniczne** | Minimum 5-letnia gwarancja producenta w miejscu instalacji.  Czas reakcji 2h w standardowe dni robocze w godzinach od 9:00 do 17:00. Przybycie serwisu do miejsca instalacji w ciągu następnego dnia roboczego od zgłoszenia usterki. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera.  Uszkodzone dyski pozostają u Zamawiającego. |
| **Inne** | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta w Polsce.  Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. |
| **Wdrożenie** | **W związku ze specyfiką wdrożenia i posiadanego systemu do backupu Veeam, osoba wdrażająca Wykonawcy musi posiadać (załączyć do oferty) certyfikat:**   * **Certyfikat Veeam Certified Engineer 2023 – min. 1 osoba**   **Wskazana osoba powinna mieć poświadczenie dostępu do danych o klauzuli min. poufne (załączyć do oferty).**   1. Instalacja urządzeń w szafie RACK w miejscu wskazanym przez Zamawiającego 2. Okablowanie urządzeń dla komunikacji LAN, zarządzenie w sposób zalecany przez producentów sprzętu i systemu operacyjnego. 3. Migracja obecnie funkcjonującego systemu Veeam B&R na nowy serwer z zachowaniem obecnej konfiguracji i wszystkich podłączonych repozytoriów 4. Skonfigurowanie zadań backup na dyski lokalne serwera, na oferowane w punkcie 2 i 3 deduplikator i taśmy, według ustalonej retencji przez Zamawiającego 5. Skonfigurowanie snapshotów immutable na deduplikatorze (pkt 3) zgodnie z ustaloną retencją przez Zamawiającego 6. Dokumentacja poświadczeń i topologii 7. Szkolenie administratora z wdrożonych rozwiązań. |

# Biblioteka taśmowa – 1 szt.

1. Obudowa biblioteki przystosowana do montażu w standardowej szafie rack 19’’. Maksymalna wysokość 2U.
2. Biblioteka taśmowa musi być wyposażona w co najmniej 1 napęd taśmowy typu LTO9 o natywnej przepustowości min. 300MB/s oraz interfejsie FC min. 8 Gbit/s.
3. Każdy napęd taśmowy musi odczytywać i zapisywać taśmy typu LTO8 oraz LTO7 z kompresją.
4. Wszystkie sloty znajdujące się w bibliotece muszą być aktywne –jeżeli do aktywacji wymagana jest licencja musi być dostarczona. Biblioteka musi udostępniać dla serwerów nie mniej niż 24 sloty na taśmy typu LTO.
5. Biblioteka musi mieć funkcjonalność partycjonowania na co najmniej dwie niezależne biblioteki logiczne. Każda z logicznych bibliotek musi mieć przypisany magazynek z taśmami.
6. Biblioteka musi umożliwiać wymianę taśm bez przerywania pracy urządzenia. Operator musi mieć możliwość zdefiniowania co najmniej 1 slotu biblioteki jako portu wejścia/wyjścia.
7. Biblioteka musi być wyposażona w czytnik kodów kreskowych umożliwiający automatyczne rozpoznawanie i inwentaryzację taśm załadowanych do biblioteki.
8. Biblioteka musi być wyposażona w robota obsługującego automatyczne załadowanie i rozładowanie taśm pomiędzy slotami i napędami taśmowymi.
9. Biblioteka musi być wyposażona w komplet magazynków na co najmniej 24 taśm, tak by możliwa była szybka obsada biblioteki taśmami LTO.
10. Możliwość monitorowania stanu biblioteki i napędów co najmniej dwiema niezależnymi metodami: przez panel sterowania umieszczony na frontowej obudowie biblioteki oraz GUI. Bezpieczeństwo dostępu musi być chronione co najmniej poprzez nazwę użytkownika i pin/hasło.
11. Możliwość zdalnego zarządzania biblioteką poprzez interfejs WWW. Biblioteka musi być wyposażona w port 1 Gb Ethernet. Biblioteka musi wspierać protokoły: IPv4, IPv6, SNMP, http, SSL, SMTP, NTP, DNS, DHCP.
12. Do biblioteki należy dostarczyć:
    1. niezbędne kable zasilające,
    2. niezbędny zestaw do montażu w szafie rack 19”,
    3. taśmęLTO9 –20 szt.,
    4. taśmę czyszczącą –1 szt.,
    5. przewód FC OM3 łączący bibliotekę z kartą HBA (switchem FC) o długości co najmniej 3m. –1 szt.
13. Biblioteka musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu (najnowsza wersja firmware na dzień dostawy).
14. Biblioteka musi być fabrycznie nowa.
15. Wymagana jest gwarancja świadczona w trybie 9x5 NBD na wszystkie elementy biblioteki na okres 60 miesięcy. Zamawiający wymaga, aby gwarancja świadczona była przez producenta biblioteki.

# Urządzenie do backupu z deduplikacją – 1 szt.

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| **Obudowa** | Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. |
| **Kontrolery** | Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler. |
| **Wydajność backupu** | Oferowany model deduplikatora musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu co najmniej 5 TB/h (dane podawane przez producenta). Dodatkowo wymagana zagregowana wydajność backupu przy zastosowaniu deduplikacji na źródle co najmniej 8 TB/h (dane podawane przez producenta). |
| **Wymagana przestrzeń** | Przestrzeń użytkowa po zbudowaniu RAID 6 z min. 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności min. 1 dysku musi wynosić min 32TB. Rozmiar RAW pojedynczego dysku nie może być większy niż 8 TB. Dodatkowo wymagane jest zastosowanie co najmniej 4 dysków SSD SAS o pojemności RAW min 1.92 TB jako cache pod zapis backupu. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń *spare* i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji. |
| **Zabezpieczenia RAID** | Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej tolerującej jednoczesną awarię 2 dysków bez utraty danych. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem DoD 5220.22-Mpoprzez mechanizm nadpisywania danych. |
| **Pamięć Cache** | Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania. |
| **Dostępne interfejsy** | Urządzenie musi posiadać minimum:  4 porty Ethernet 10 Gb/s z możliwością obsługi każdym portem Ethernet protokołów iSCSI, CIFS, NFS, wszystkie porty wyposażone we wkładki optyczne. |
| **Obsługiwane protokoły** | Wymagane wsparcie dla FC, iSCSI, NFS, CIFS. |
| **Zarządzanie** | Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak:  - cały deduplikator  - kontrolery  - CPU  - porty front-end  - porty logiczne  - dyski  - file systemy  Pod kątem parametrów takich jak:  - operacje wejścia/wyjścia IOPS  - przepustowość (KB/s lub MB/s)  - czas odpowiedzi (latency)  - średnie użycie (w % dla CPU)  Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych.  Wymagana możliwość monitorowania poboru prądu deduplikatora z rozbiciem na miesiące oraz dni. Pobór prądu podawany w kWh.  Wymagany dostęp do prognozy zużycia przestrzeni.  Wymagana możliwość tworzenia wielu użytkowników deduplikatora w oparciu o wbudowane role. Rozwiązanie musi umożliwiać tworzenie własnych ról.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| **Redukcja danych** | Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.  Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci.  Musi być oficjalne wsparcie producenta dla oferowanego deduplikatora maksymalnego stopnia redukcji danych co najmniej 60:1 |
| **Kontrola zasobów plikowych** | Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni.  Wymagana możliwość skonfigurowania polityki filtrowania zapisywanych plików poprzez wykluczenie ich konkretnych rozszerzeń.  Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp.  Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania. |
| **Ochrona zasobów plikowych** | Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system’ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.  Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM). Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania. |
| **Replikacja danych** | Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję.  Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00).  Wymagana możliwość zastosowania funkcjonalności typu AirGap czyli fizyczne wyłączanie portów dedykowanych do replikacji w czasie kiedy replikacja nie jest wykonywana. Dopuszcza się realizację tej funkcjonalności poprzez zastosowanie dodatkowego oprogramowania.  Dostarczenie powyższych funkcjonalności nie jest wymagane na tym etapie postępowania. |
| **Wspierane systemy backup** | Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam Backup&Replication. |
| **Obsługa serwisowa** | Deduplikator musi posiadać możliwość upgradeu firmware-u kontrolerów bez przerywania dostępu do danych.  Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania.  Urządzenie musi umożliwiać zdalne zarządzanie.  Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.  Wymagana gwarancja na 5 lat w trybie 24/7 NBD w miejscu instalacji. |

# Przełącznik core – 2 szt.

|  |  |
| --- | --- |
| **Element konfiguracji** | **Wymagania minimalne** |
| **Typ** | Przełącznik sieciowy zarządzalny rack SFP+.  W ofercie wymagane jest podanie modelu, symbolu oraz producenta. |
| **Porty** | 1. Minimum 24 porty 1G/10G SFP+ 2. Minimum 4 porty SFP56 z możliwością pracy 1G/10G/25G/50Gbit 3. Port konsoli – RS232 on USB typ C 4. Minimum 1 port USB typu A 5. Minimum 1 Bluetooth dongle 6. Port zarządzanie OOBM   Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, oraz Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX/LH  Co najmniej 4 porty (typu uplink) SFP56 muszą umożliwiać ich obsadzanie wkładkami SFP28 Gigabit Ethernet, SFP+ 10Gbit oraz SFP 1Gbit a także kablami DAC 50Gbit.  Możliwość łączenia w stos do 10 przełączników z wykorzystaniem uplinków, łączną przepustowość stosu do 200 GB/s na przełącznik. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. |
| **Parametry fizyczne** | Wysokość maksymalnie 1U, montowany w szafie typu rack 19’’, redundantny zasilacz |
| **Pamięć** | Co najmniej 8GB pamięci DDR4  Co najmniej 32GB pamięci flash |
| **Wielkość tablicy adresów MAC** | Co najmniej 32 000 |
| **Ilość obsługiwanych sieci VLAN** | Co najmniej 4094 |
| **Wydajność** | * Przepustowość przełączania: min. 880 Gbit/s * Przełączanie dla pakietów: min. 654 Mpps. * Bufor pakietów: minimum 7.5 MB * IPv4 multicast routers: 8192 * IPv4 unicast routers: 61000 * IPv6 Unicast Routes 60000 * IPv6 Multicast Routes 8000 |
| **Obsługa ramek Jumbo** | O wielkości co najmniej 9198 bajtów |
| **Funkcjonalność urządzenia** | * + obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad),   + Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie   + obsługa protokołu NTP,   + wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree,   + Obsługa sFlow lub Netflow   + Obsługa skryptów w języku Python   + Obsługa REST API   + musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB,   + musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli,   + musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN   + 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). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.   + Obsługa 4000 jednoczesnych sieci VLAN 802.1Q   + Obsługa standardu 802.1v   + Obsługa protokołu MVRP   + Obsługa Ethernet Ring Protection Switching (ERPS)   + Wsparcie dla VXLAN   + Obsługa Microsoft Network Load Balancer (NLB)   + Obsługa SNTPv4 lub NTP   + Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)   + Obsługa protokołów rutingu: ruting statyczny, RIPv2, RIPng, OSPF, OSPFv3, BGP, MP-BGP,   + Obsłyga ruchu multicast: IGMPv1/v2/v3, PIM-SM, PIM-DM, MSDP   + Obsługa VRRP   + Obsługa ECMP   + Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)   + Wbudowany serwer DHCP   + Obsługa funkcji User Datagram Protocol (UDP) helper |
| **Bezpieczeństwo** | * + autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN  i z możliwością dynamicznego przypisania listy ACL,   + możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,   + możliwość uzyskania dostępu do urządzenia przez SNMP, SSH, HTTP/HTTPS z wykorzystaniem IPv4 i IPv6,   + obsługa mechanizmów Port Security, Dynamic ARP Inspection   + możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne). |
| **Wsparcie dla mechanizmów zapewnienia jakość usług w sieci** | * + klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie co najmniej następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,   + implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Deficit Weighted Round Robin lub podobnego dla obsługi tych kolejek,   + możliwość obsługi jednej z powyżej wymienionych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),   + możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi. |
| **Zasilanie** | Zasilacz 230V AC wymieniany hot-swap.  Możliwość zastosowania redundantnego zasilacza wewnętrznego także hot-swap,  Switch należy dostarczyć razem z dodatkowym zasilaczem redundantnym.  Przełącznik dodatkowo powinien posiadać wentylację wymienną redundantną w postaci modułów hot-swap. |
| **Akcesoria** | Razem z przełącznikami należy dostarczy:  Kabel DAC 50Gbit o długości 0,65m do zestawienia stack – sztuk 1 |
| **Gwarancja** | Dożywotnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory), obowiązując tak długo jak produkt jest oferowany przez producenta + 5 lat od momentu zakończenia produkcji.  Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |
| **Dokumenty** | Wykonawca winien przedłożyć dokumenty:   1. Deklaracja zgodności CE oferowanego urządzenia – certyfikat potwierdzony za zgodność z oryginałem, 2. Oświadczenie producenta lub oświadczenie autoryzowanego przedstawiciela producenta potwierdzające zgodność wszystkich parametrów oferowanego urządzenia wskazanych w Opisie przedmiotu zamówienia. |
| **Wdrożenie** | **W związku ze specyfiką wdrożenia, osoba wdrażająca Wykonawcy musi posiadać (załączyć do oferty) certyfikat:**   * **Certyfikat na poziomie Professional z zaoferowanych przełączników sieciowych – min. 2 osoby**   **Wskazana osoba powinna mieć poświadczenie dostępu do danych o klauzuli min. poufne (załączyć do oferty).**   1. Instalacja w ustalonym z zamawiającym miejscu 2. Połączenie z istniejącymi elementami infrastruktury 3. Stworzenie stosu przełączników 4. Konfiguracja uzgodnionej funkcjonalności L2 (VLANy, agregacje, UDLD/DLDP, STP) 5. Konfiguracja uzgodnionej funkcjonalności L3 (adresy, bramy, DNSy, NTP, syslog) 6. Konfiguracja uzgodnionych funkcjonalności bezpieczeństwa (arp protect, dhcp snooping) jeżeli istnieje możliwość 7. Segmentacja sieci z podziałem na VLANy. |

# System do izolowania zaawansowanych zagrożeń w czasie rzeczywistym – 1 szt.

**System ochrony przed zaawansowanymi zagrożeniami**

System proaktywnej ochrony przed zaawansowanymi zagrożeniami - którego zadaniem będzie wykrywanie i blokowanie ataków w infrastrukturę sieci, a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. System może składać się z jednego lub kilku elementów zapewniając opisany poniżej zestaw funkcji.

System powinien umożliwiać lokalne logowanie oraz raportowanie oraz współpracować z systemem centralnego logowania i raportowania. Powinna istnieć możliwość implementacji systemu w trybie nasłuchu oraz współpracy z systemami zabezpieczeń NGFW (Next Generation Firewall) lub SWG (Security Web Gateway), SEG (Secure Email Gateway) oraz w oparciu o interfejsy programistyczne API (np. icap). Musi istnieć możliwość pełnej integracji z urządzeniami będącymi w posiadaniu przez Zamawiającego: FortiGate 60F, FortiMail-VM01, FortiAnalyzer VM**.**

Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie bazowały na rozwiązaniach komercyjnych, dla których producenci poszczególnych elementów dostarczają wsparcia i aktualizacji oprogramowania.

**System operacyjny**

Dla zapewnienia wysokiej sprawności i skuteczności działania systemu musi pracować w oparciu o dedykowany, wzmocniony system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.

**Parametry fizyczne systemu**

System musi zapewniać:

1. 4 interfejsy Ethernet 10/100/1000,
2. Powierzchnie dyskową - minimum 960 GB.

W celu zwiększenia niezawodności system powinien mieć możliwość pracy w konfiguracji HA (High Availability) z podziałem obciążenia.

Elementy systemu o maksymalnej wysokości 1U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

**Funkcjonalności podstawowe i uzupełniające**

Ochrona przez zaawansowanymi atakami:

1. Funkcjonalność Sandbox dla instancji Windows: sprawdzanie procesów i rejestru, połączenia z Botnet C&C oraz złośliwymi URL, dostęp do pakietów przeprocesowanych przez VM, logów działania badanego oprogramowania oraz zrzutów ekranu w badanej VM.
2. Procesowanie plików o rozmiarze co najmniej 8 MB.
3. Sanboxing dla plików zarchiwizowanych (.tar, .gz, .tar.gz, .tgz, .zip, .bz2, .bz, .tar.Z, .cab, .rar, .arj), wykonywalnych (.exe, .dll), PDF, Windows Office Document, Javascript, AdobeFlash oraz JavaArchive (JAR).
4. Plików multimedialnych: .avi, .mpeg, .mp3, .mp4.
5. Skanowane protokoły sieciowe: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM oraz ich wersje zaszyfrowane SSL. Jeżeli do spełnienia tego wymagania konieczne jest dostarczenie dodatkowych urządzeń sieciowych (przekierowujących zawartość pakietów dla wskazanych protokołów sieciowych, rozszywających ruch SSL), urządzenia te powinny zostać uwzględnione w ofercie. Ich wydajność powinna umożliwiać procesowania ruchu o przepływności 500 Mbps.
6. Skanowanie stron www z linkami URL.
7. Czarne i białe listy dla sum kontrolnych plików.
8. Szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci, snapshotu VM.
9. Dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów pcap.

**Parametry wydajnościowe**

Możliwość uruchomienia min. 6 instancji wirtualnych systemów MS Windows zawierających Windows 7, Windows 8 i Windows 10 oraz 1 pakiet biurowy MS Office w celu wykonania analizy Sandbox w wymiarze co najmniej 120 plików na godzinę.

Zarządzanie

System udostępnia:

1. Lokalny graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS.
2. Dostęp do CLI przez SSH.

**Serwisy, szkolenia i usługi**

Wymaga się aby dostawa obejmowała również:

* Gwarancję i serwis producenta na okres 24 miesięcy.
* Subskrypcje funkcji bezpieczeństwa Antivirus, IPS, Web Filtering na okres: 24 miesięcy.

**Wdrożenie**

**W związku ze specyfiką wdrożenia (integracja z posiadanymi systemami Zamawiającego Fortinet i Vmware), osoba wdrażająca Wykonawcy musi posiadać (załączyć do oferty) certyfikaty:**

* **FNSE8 (Network Security Expert 8) – min. 1 osoba**
* **FNSE7 (Network Security Architect 7) – min. 2 osoby**
* **Vmware Certified Professional Data Center Virtualization 2023 - min. 1 osoba**

**Wszystkie wskazane osoby powinny mieć poświadczenie dostępu do danych o klauzuli min. poufne (załączyć do oferty).**

Zakres wdrożenia:

* inicjalizacja urządzenia,
* aktualizacja firmware,
* instalacja maszyn wirtualnych (Zamawiający posiada Vmware),
* konfiguracja polityk skanowania,
* integracja z NGFW oraz Email Security Gateway
* przegląd logów systemowych, wskazanie potencjalnych zagrożeń.

# System zabezpieczający sieć przed nieautoryzowanym dostępem dla niezweryfikowanych urządzeń – 1 szt.

System do kontroli dostępu musi charakteryzować się następującymi cechami:

* Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
* System musi odsługiwać minimum **100** urządzeń klienckich (w tym gości). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia
* Praca jako maszyna wirtualna
* Musi posiadać wbudowany serwer Radius oraz TACACS +
* Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:
  + Cisco Systems
  + Fortinet
  + Microsoft
  + Alcatel-lucent Enterprise
  + Aruba Networks
  + Huawei
  + Extreme Networks
  + PaloAlto
  + Producenta urządzeń sieciowych opisanych w tym postępowaniu
* System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera.
* System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.
* Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
* Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych
  + Microsoft Active Directory
  + Radius
  + Kerberos
  + LDAP
  + ODBC
  + Współpraca z serwerami tokenów
* Musi obsługiwać metody profilowania
  + DHCP
  + TCP
  + MAC OUI
  + SNMP
  + Cisco device sensor
* Wspierać protokoły
  + Radius, Radius CoA, TACACS +, web authentication, SAML v2.0
  + EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
  + PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)
  + TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)
  + EAP-TLS
  + PAP, CHAP, MSCHAPv1 i v2, EAP-MD5
  + NAC, Microsoft NAP
  + Windows machine authentication
  + MAC Auth
  + Audit (role oparte na porcie oraz skanowanie podatności)
  + OCSP (Online Certificate Status Protocol)
  + SNMP generic MIB, SNMP private MIB
  + CEF (Common Event Format), LEEF (Log Event Extended Format)
  + TLS 1.2
* Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami
* Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:
  + Co najmniej ESX 4.0, ESXi 4.1 do 6.0
  + Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise
* **Posiadać moduł odpowiedzialny za Dostęp Gościnny**. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (100). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.

System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności:

* Samodzielna rejestracja klientów gościnnych w oparciu o:
  + Adres e-mail
  + Numer telefonu (wiadomość SMS)
  + Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
* Logowanie w oparciu o portale społecznościowe
* Funkcja integracji z systemami trzecimi poprzez API
* Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową
* Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
* Funkcja personalizacji strony gościnnej
* **Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD**. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.
* Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT
* System musi wspierać obsługę następujących systemów operacyjnych
  + MS Windows
  + Mac OS X
  + iOS
  + Android
  + Ubuntu
* Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
* Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej
* Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
* Funkcja tworzenia unikalnych cerftyfikatów dla urządzeń.
* Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń
* Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID
* **Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich**. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

System kontroli końcówek klienckich musi mieć następujące funkcjonalności:

* System musi wspierać następujące systemy operacyjne:
  + Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)
  + Apple Mac OS X 10.7 i nowsze
  + Red HAT Enterprise Linux 4 i nowsze
  + CentOS 4 (Community Enterprise Operating System) i nowsze
  + Fedora Core 5 i nowsze
  + SUSE linux 10.x i nowsze
* Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall
* Wyświetlanie informacji on-line o statusie monitorowanych końcówek
* System powinien obsługiwać agenta w formie
  + Stałej (Presistent Agent)
  + Tymczasowej (Dissolvabe Agent)
  + Agenta NAP
* Minimum 3 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
* Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.
* Oferta musi zawierać kompletne zestawianie numerów katalogowych produktów i wszystkich jego dodatkowych składników umożliwiających ich jednoznaczną identyfikację u producenta sprzętu
* Zaoferowane rozwiązanie musi być uznane przez firmę analityczną Gartner Research. To znaczy, że musi być wymienione w bieżącym na moment składania oferty raporcie Market Guide for Network Access Control lub musi być wymienione w Gartner Peer Insights w kategorii Network Access Control.
* Wdrożenie: **W związku ze specyfiką wdrożenia, osoba wdrażająca Wykonawcy musi posiadać (załączyć do oferty) certyfikat:**
* **Certyfikat na poziomie Professional z zaoferowanego systemu – min. 2 osoby**

**Wskazana osoba powinna mieć poświadczenie dostępu do danych o klauzuli min. poufne (załączyć do oferty).**

* + Instalacja instancji NAC na posiadanej i wspieranej przez NAC platformie.
  + integracja ze środowiskiem zamawiającego AD, LDAP, SMTP, SNMP.
  + Konfiguracja serwisów 802.1X, MAC authentication, TACACS.
  + konfiguracja portów na przełączniku referencyjnym.

# System do zarządzania i bezpieczeństwa IT – 1 szt.

System musi posiadać:

* budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program ma umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.
* Moduły umożliwiające kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program ma wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) dzięki czemu nie może być objęty limitem ilości danych, baza danych ma być rozwiązaniem darmowym, niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających ma wymagać 64-bitowego systemu operacyjnego Windows.
* Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., mają być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Mają być one również grupowane w osobnym, dedykowanym oknie. Ma to pozwalać na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.
* Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, ma być objęty kontrolą na poziomie wybranych Administratorów – w programie ma być możliwe nadawanie kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów mają być logowane co oznacza to, że program ma posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mają być automatycznie eksportowane do zewnętrznego kolektora Syslog.
* Program ma umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Ma to pozawalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatyczne wymuszanie dostosowanie bieżących haseł do obowiązujących zasad.
* Program ma zawierać mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA ma być możliwość skonfigurowania okresu, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera.

**MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO)** ma obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

• skanowanie sieci, wykrywanie urządzeń i serwisów TCP/IP

• interaktywne mapy sieci, mapy użytkownika, oddziałów, mapy inteligentne

• serwisy TCP/IP: poprawność i czas odpowiedzi, statystyka ilości odebranych/ utraconych pakietów

(PING, SMB, HTTP, POP3, SNMP, IMAP, SQL itp.)

• liczniki WMI: obciążenie procesora, zajętość pamięci, zajętość dysków,

transfer sieciowy itp.

• działanie Windows: zmiana stanu usług (uruchomienie, zatrzymanie, restart), wpisy dziennika zdarzeń

• liczniki SNMP v1/2/3 (np. transfer sieciowy, temperatura, wilgotność, napięcie zasilania, poziom tonera i inne)

**WZAKRESIE INWENTARYZACJI** program ma automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz ma spełniać następujące funkcje:

* IT Asset Management – zarządzanie wszelkimi zasobami, za które odpowiada dział IT
* szczegółowe informacje i ewidencja czynności wykonywanych na zasobach w trakcie całego cyklu życia, możliwość defniowania statusów i pól oraz generowanie protokołu przekazania sprzętu
* widok zasobów, aplikacji, dokumentów, licencji dla poszczególnych użytkowników lub osobny widok według zasobów przypisanych do urządzeń
* jednoczesne przypisywanie dokumentu do wielu zasobów
* Software Asset Management – rozbudowany system zarządzania aplikacjami i licencjami, identyfkacja realnego zużycia licencji
* rozliczanie dowolnego typu licencji, w tym modelowanie licencji chmurowych
* rozliczanie licencji według użytkownika, urządzenia, numeru seryjnego lub na podstawie wersji zainstalowanej aplikacji
* audyt inwentaryzacji sprzętu i oprogramowania
* wgląd w licencje przypisane do użytkownika pracującego na wielu urządzeniach
* zdalny dostęp do managera plików z możliwością usuwania plików użytkownika

**W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW** program ma umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez:

• pełne zarządzanie użytkownikami, bazujące na grupach i politykach bezpieczeństwa

• blokowanie uruchamianych aplikacji

• monitorowanie wiadomości e-mail (nagłówki) – antyphishing

• szczegółowy czas pracy (godzina rozpoczęcia i zakończenia aktywności oraz przerwy)

• użytkowane aplikacje (aktywnie i nieaktywnie)

• odwiedzane strony WWW (tytuły i adresy stron, liczba i czas wizyt)

• audyty wydruków (drukarka, użytkownik, komputer), koszty wydruków

• statyczny zdalny podgląd pulpitu użytkownika (bez dostępu)

• zrzuty ekranowe (historia pracy użytkownika ekran po ekranie)

• blokowanie stron WWW

• rejestr naruszeń blokad agregujący informacje o próbie dostępu do blokowanych stron WWW, uruchamianiu zakazanych aplikacji oraz pobieraniu plików z niedozwolonymi rozszerzeniami

**PROGRAM UMOŻLIWIA REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM**. W ramach kontroli stacji użytkownika ma być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator mają widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu ma mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu ma umożliwić równoczesne podłączenie do tego samego komputera kilku administratorom.

**PROGRAM ma mieć możliwość:**

• tworzenia i procesowania zgłoszeń serwisowych poprzez intuicyjny interfejs webowy lub za pośrednictwem maila

• planowania zastępstw w przydzielaniu zgłoszeń

• wskazania osób, które muszą zaakceptować zgłoszenie

• tworzenia automatycznych ścieżek akceptacji na podstawie kategorii przypisanej do zgłoszenia

• automatycznej wysyłki powiadomień do osób akceptujących zgłoszenie

• stworzenia listy bezpiecznych aplikacji do samodzielnej instalacji przez użytkownika

• obsługi umów o gwarantowanym poziomie świadczenia usług (SLA)

• automatycznego przypisywania zgłoszeń do obsługującego na podstawie określonych warunków

• zarządzania kategoriami i priorytetami zgłoszeń oraz powiadomieniami z HelpDesku

• rozbudowana wyszukiwarka oraz aktualizacja zgłoszeń w czasie rzeczywistym

• defniowania reguł widoczności zgłoszeń oraz automatyzacji bazujących na warunkach

• ograniczenia tworzenia zgłoszeń i dostępności artykułów w bazie wiedzy przez wybrane grupy użytkowników tylko w określonych kategoriach

• rozbudowany system raportów

• przetwarzania zgłoszeń w trybie anonimowym

• komentarze i załączniki w zgłoszeniach; dodawanie pól niestandardowych

**MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM** poprzez blokowanie urządzeń.

System ma:

• dawać informacje o urządzeniach podłączonych do danego komputera

• dawać listę wszystkich urządzeń podłączonych do komputerów w sieci

• realizować audyt (historia) podłączeń i operacji na urządzeniach przenośnych oraz udziałach sieciowych i dyskach lokalnych

•mieć możliwość monitorowanie operacji na plikach w katalogach na dysku systemowym

• mieć możliwość monitorowania operacji na plikach z zasobów sieciowych udostępnianych przez urządzenia nieobsługiwane przez Agenta np. macierze Synology, Qnap itp.

• mieć możliwość zarządzania prawami dostępu (zapis, uruchomienie, odczyt) dla urządzeń, komputerów i użytkowników

• mieć centralną konfigurację: ustawienie reguł dla całej sieci oraz grup i użytkowników Active Directory

• mieć możliwość integracji bazy użytkowników i grup z Active Directory

• ma dawać alarmy: podłączono/odłączono urządzenie mobilne, operacja na plikach na urządzeniu mobilnym

oraz na dyskach lokalnych

* Wsparcie techniczne na okres minimum 2 lat
* Wdrożenie systemu

# Rozszerzenie SOC do istniejącego oprogramowania FortiAnalyzer – 1 szt.

Centrum zarządzania SOC ma pomóc zabezpieczyć całą sieć, zapewniając wgląd w logi i dane o zagrożeniach i danych o zagrożeniach. Subskrypcja m.in. 2-letnia.

Wdrożenie:

1. Instalacja licencji na systemie FortiAnalyzer.

2. Przegląd obecnie wykorzystywanych raportów, weryfikacja ich ustawień,

3. Konfiguracja nowych raportów zgodnie z dobrymi praktykami i wiedzą wdrożeniową Wykonawcy, w tym wykorzystujące dane z modułów IoC i SOC,

4. Przygotowanie na nowym urządzeniu automatyzacji incydentów w module SOC.

# Usługa szkoleniowa z zakresu cyberbezpieczeństwa – 1 szt.

Kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w internecie, dedykowana do 100 użytkownikom Zamawiającego i świadczona przez okres 3 miesięcy.

Usługa musi zawierać:

1. Platformę szkoleniową zawierającą minimum 45 szkoleń, dostępnych w języku polskim, w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.

a) Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:

* Podstawy bezpiecznego internetu
* Bezpieczeństwo poczty
* Załączniki w poczcie elektronicznej
* Phishing
* Spyware/malware
* Bezpieczeństwo danych osobowych RODO/GDRP
* Bezpieczne hasła
* Menedżery haseł
* Bezpieczeństwo urządzeń mobilnych
* Uwierzytelnianie wieloskładnikowe (MFA)
* Bezpieczna praca zdalna
* Bezpieczna praca w biurze
* Sieci społeczne
* Socjotechnika stosowana
* Zakupy w internecie

b) Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.

c) Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 8 godzin.

2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:

a) z linkiem prowadzącym do stronnym internetowej,

b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,

c) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,

d) z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.

W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.

1. dedykowaną platformę dostarczającą raporty obejmujące minimum:

a) status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,

b) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.

1. W ramach świadczonej usługi, usługodawca musi:

- przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,

- zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,

- zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,

- dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,

- wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników.

1. Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej.

Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.

Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

1. Do oferty należy załączyć oświadczenie usługodawcy o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001.