Tekst alternatywny: u góry strony Logotyp Cyberbezpieczny samorząd, w stopce dokumentu umieszczono logotypy Funduszy Europejskich na rozwój cyfrowy, flagę Rzeczpospolitej Polskiej, Centrum Projektów Polska Cyfrowa i flaga Unii Europejskiej z informacją o dofinansowaniu

Załącznik nr 2 do SWZ – Szczegółowy Opis Przedmiotu Zamówienia

<u>Nazwa zadania</u>: „Gmina Niegowa cyberbezpiecznym samorządem" realizowanego w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC)

Spis treści

1. Serwer do backupu – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera przeznaczonego do wirtualizacji, backupu i SIEM.

Wymagania:

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 12 dysków 3,5". Serwer musi posiadać możliwość rozbudowy o min. 2 dodatkowe wnęki dyskowe na dyski SAS/SATA 2.5".
2. Serwer wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz wyposażeniem w przedni panel zamykany na klucz, chroniącym dyski przed nieuprawnionym wyjęciem.
3. Płyta główna z możliwością zainstalowania do dwóch procesorów.
4. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
5. Zainstalowane dwa procesory piątej generacji min. 16-rdzeniowe o taktowaniu min. 2.8GHz (base frequency) umożliwiający osiągnięcie w teście SPECrate2017_fp_base wyniku dla dwóch procesorów w oferowanym serwerze min. 500 pkt. Wynik należy dołączyć do oferty.
6. Pamięć RAM min. 256GB DDR5 RDIMM 5600MT/s, w modułach po min. 32 GB RAM.
7. Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM.
8. Zabezpieczenie pamięci:
    a. Memory mirroring
    b. ECC
    c. patrol scrubbing
    d. SDDC
    e. memory thermal throttling
    f. ADDDC-SR
    g. PPR
    h. Memory SMBus hang recovery.
9. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
10. Wbudowane porty:
    a. 4 porty USB z czego nie mniej niż 1 port USB 3.0 na przednim panelu obudowy, 2 porty USB 3.0 na tylnym panelu obudowy oraz 1 port USB 2.0 na płycie głównej.
    b. Złącze USB TYP-C na przednim panelu, które musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS.
    c. 1 port VGA na tylnym panelu obudowy.
    d. Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
11. Minimum 3 aktywne sloty PCI-E 5.0 z czego min. 1 slot x16.
12. Możliwość rozbudowy o 4 dodatkowe sloty PCI-E 4.0.
13. Zainstalowane i w pełni funkcjonalne interfejsy sieciowe:
    a. minimum 1 x RJ-45 Ethernet management port,

   b. minimum 2 porty 10Gb/s Ethernet w standardzie SFP+ z modułami optycznymi MM w komplecie.
   c. minimum 4 porty 1Gb/s Ethernet w standardzie BaseT.
   d. powyższe porty nie mogą zajmować slotów PCI-E.
14. Zainstalowany sprzętowy kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 10, 5, 50, 6, 60. Kontroler wyposażony w 8GB Cache i podtrzymanie bateryjne. Kontroler powinien posiadać wsparcie dla dysków SAS, SATA oraz NVMe, jak również powinien wspierać mechanizmy szyfrowania, bądź obsługę dysków SED.
15. Pamięć masowa:
   a. Zainstalowane 2 dyski serwerowe SSD Read-Intensive Hot-Plug o pojemności min. 480 GB każdy
   b. Zainstalowane 9 dysków serwerowych HDD SATA 7.2K o pojemności min. 8 TB każdy.
16. Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo.
17. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
18. Min. dwa identyczne zasilacze o mocy min. 1600W klasy Titanium zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera. W komplecie z zasilaczami należy dostarczyć kable zasilające o długości min. 2m.
19. Bezpieczeństwo:
   a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
   b. Moduł TPM 2.0.
20. Serwer wyposażony w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający:
   a. wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS
   b. wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy
   c. przywracanie konta administratora
   d. wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera
   e. wyświetlanie w czasie rzeczywistym temperatury procesorów
   f. konfigurowanie ustawień sieciowych modułu zarządzania.
21. Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca:
   a. monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.),
   b. monitorowanie w czasie rzeczywistym poboru prądu przez serwer,
   c. zbieranie logów błędów hardware,
   d. przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury,
   e. montowanie wirtualnych napędów,
   f. zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego,

g. wysyłanie zawiadomień droga mailową i poprzez SNMP
h. wsparcia dla IPMI, SSH, Redfish
i. wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows,
j. nadawanie ról użytkownikom,
k. możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD,
l. możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.

22. Wraz ze serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na:
    a. włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów.
    b. tworzenie szablonów instalacyjnych dla systemów operacyjnych.
    c. tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów.
    d. zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera.
    e. aktualizacja sterowników i BIOS serwerów.
    f. zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.
23. Razem z serwerem należy dostarczyć Windows Server Standard na dwie maszyny wirtualne uwzględniając oferowaną ilość rdzeni w serwerze. Opis równoważności licencji oprogramowania:
    a. Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzinowego użytkowanego aktualnie w urzędzie oraz pełną współpracę z ActiveDirectory, które jest aktualnie wykorzystywane. Licencja zostanie wykorzystana do uruchomienia oprogramowania na serwerze zakupionym w ramach niniejszego postępowania;
    b. Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski;
    c. Licencja bez ograniczeń czasowych;
    d. Instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;
    e. Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych);
    f. Wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB;
    g. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu;

h. Praca w roli klienta domeny Active Directory;
i. Zawarta możliwość uruchomienia roli kontrolera domeny Active Directory;
j. Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP);
k. Zawarta możliwość uruchomienia roli serwera DNS;
l. Możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
m. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP);
n. Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Active Directory;
o. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Active Directory;
p. Zawarta możliwość uruchomienia roli serwera stron WWW;
q. Zawarta funkcjonalność szyfrowania dysków;
r. Dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera;
s. W ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera;
t. W ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;
u. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów);
v. Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
w. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
x. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
y. Obsługa zdalnego pulpitu;
z. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
aa. Obsługa PowerShell 4.0.

24. Należy dostarczyć 45 licencji dostępowych na użytkownika.
25. Zgodność z normą ISO 9001, ISO 14001 lub równoważnymi.
26. Serwer musi posiadać deklarację CE.
27. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemu Microsoft Windows Server 2022. Certyfikat lub inny dokument potwierdzający zgodność z dostarczanym systemem operacyjnym należy dołączyć do oferty.

28. Zamawiający wymaga dokumentacji w języku polskim lub angielskim, w wersji papierowej lub elektronicznej .
29. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.
30. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta na terenie RP.
    b. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji w trybie onsite z gwarantowanym czasem reakcji najpóźniej Next Business Day od momentu zgłoszenia usterki (nie dotyczy awarii krytycznej).
    c. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
    d. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.
    e. Usługi gwarancyjne świadczone przez producenta lub autoryzowanego partnera serwisowego producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.
    f. Wraz z ofertą Wykonawca musi dostarczyć oświadczenie producenta oferowanego serwera, że wymagany poziom serwisu z wymaganym SLA został zaoferowany na potrzeby oferty w niniejszym postępowaniu.
    g. Wraz z ofertą Wykonawca musi dostarczyć oświadczenie producenta potwierdzające, że elementy, z których zbudowany jest serwer, są produktami producenta tych serwerów lub są przez niego certyfikowane oraz całe są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.
    h. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
        i. możliwość pobierania najnowszego firmware,
        ii. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
        iii. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
        iv. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.

2. Oprogramowanie do kopii zapasowych – 1 kpl.

Przedmiotem zamówienia jest oprogramowanie na licencji wieczystej do tworzenia kopii zapasowych i odzyskiwania danych dla min. 45 stacji roboczych oraz min. 3 serwerów fizycznych.

System powinien zapewniać automatyczną ochronę danych, elastyczność konfiguracji oraz możliwość szybkiego odzyskiwania danych w przypadku awarii. Wymagania:

1. Wsparcie dla różnych środowisk:
    a. Obsługa systemów operacyjnych: Windows 7, 8, 10, 11 oraz Windows Server 2012 R2, 2016, 2019, 2022 oraz 2025.
    b. Obsługa systemów Linux: CentOS, Red Hat Enterprise Linux (RHEL), Ubuntu, Debian, SUSE Linux Enterprise Server, Rocky Linux, Oracle Linux.
    c. Obsługa wirtualizacji: zgodność z maszynami wirtualnymi działającymi na Microsoft Hyper-V, VMware vSphere, Proxmox VE, OpenStack, Oracle Linux Virtualization Manager.
2. Metody tworzenia kopii zapasowych:
    a. Możliwość wykonywania pełnych, przyrostowych oraz różnicowych kopii zapasowych.
    b. Obsługa kopii zapasowych na poziomie plików oraz całych maszyn (bare-metal backup).
    c. Obsługa backupu dla baz danych takich jak Microsoft SQL Server, MySQL, PostgreSQL, MariaDB oraz Oracle Database.
    d. Możliwość wykonywania backupu NAS oraz zasobów współdzielonych.
3. Automatyzacja i harmonogramowanie:
    a. Możliwość tworzenia harmonogramów backupów z opcją codziennego, tygodniowego, miesięcznego wykonywania kopii zapasowych.
    b. Obsługa polityki retencji (krótkoterminowej i długoterminowej) z możliwością definiowania liczby przechowywanych kopii.
4. Szybkie odzyskiwanie danych:
    a. Możliwość pełnego przywracania systemu oraz przywracania pojedynczych plików i folderów.
    b. Funkcja natychmiastowego przywracania maszyn wirtualnych (RTO < 15 sekund).
    c. Możliwość odzyskiwania baz danych do określonego punktu w czasie (point-in-time recovery).
5. Bezpieczeństwo danych:
    a. Szyfrowanie danych w trakcie przesyłania oraz przechowywania (AES-256).
    b. Obsługa zabezpieczeń przed ransomware (np. poprzez mechanizmy wykrywania anomalii i ochronę przed nadpisaniem).
    c. Możliwość tworzenia kopii zapasowych na nośnikach taśmowych oraz w chmurze (AWS S3, Azure Blob, Ceph S3, Wasabi).
6. Wydajność i optymalizacja:
    a. Obsługa technologii deduplikacji i kompresji danych w celu oszczędności miejsca.
    b. Obsługa wielowątkowej transmisji danych.
    c. Wsparcie dla technologii Changed Block Tracking (CBT) dla szybkiego backupu przyrostowego.
7. Przechowywanie danych:
    a. Możliwość zapisu kopii zapasowych na lokalnym serwerze, sieciowym NAS, SAN oraz w chmurze.
    b. Możliwość wykonywania kopii na nośniki taśmowe (bibliotekę taśmową).
8. Wymagania sieciowe:
    a. Obsługa LAN-Free Transmission dla zmniejszenia obciążenia sieci.
    b. Możliwość konfiguracji limitu pasma wykorzystywanego przez backup.

   c. Wsparcie dla protokołów CIFS, NFS, iSCSI.
9. Interfejs użytkownika:
   a. Intuicyjny panel zarządzania dostępny przez przeglądarkę internetową.
   b. Możliwość zarządzania poprzez CLI oraz API.
   c. Powiadomienia e-mail i raporty o stanie backupu oraz ewentualnych błędach.
10. Funkcje monitorowania:
   a. Monitorowanie statusu backupów, zajętości przestrzeni dyskowej oraz obciążenia systemu.
   b. Możliwość generowania raportów i logów z wykonywanych operacji.
11. Wymagania dotyczące wsparcia technicznego:
   a. Gwarancja i wsparcie techniczne przez okres min. do 31.12.2026.
   b. Możliwość uzyskania pomocy technicznej w języku polskim.
   c. Aktualizacje oprogramowania w okresie gwarancyjnym.
12. Dodatkowe wymagania:
   a. Oprogramowanie powinno umożliwiać bezagentowy backup maszyn wirtualnych z oprogramowania wirtualizacyjnego dostarczonego w ramach tego postępowania.
   b. Możliwość migracji danych pomiędzy różnymi środowiskami wirtualizacji (V2V oraz V2C/C2V).
   c. Wsparcie dla funkcji automatycznego failover i failback w przypadku awarii systemu.
   d. Wsparcie dla testowego odtwarzania backupu w celu weryfikacji integralności danych.
13. Wykonawca zobowiązany jest do dostarczenia pełnej dokumentacji technicznej w języku polskim lub angielskim, w tym instrukcji instalacji, konfiguracji oraz obsługi oprogramowania.

3. UTM – 2 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 2 szt. zapory sieciowej z pakietem bezpieczeństwa UTM, które zapewnia zaawansowaną ochronę w infrastrukturze informatycznej zamawiającego. Zamówienie obejmuje zarówno dostawę urządzeń fizycznych firewall jak i licencje na oprogramowanie UTM na okres minimum 36 miesięcy.
Wymagania:

1. System musi realizować wymagane funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy wykorzystywanego łącza internetowego.
2. System realizujący funkcję Firewall musi umożliwiać pracę co najmniej w trybie routera z funkcją NAT, trybie transparentnym oraz trybie monitorowania ruchu poprzez port SPAN.
3. System musi umożliwiać utworzenie co najmniej 2 niezależnych fizycznych lub logicznych instancji w zakresie routingu, Firewall, IPSec VPN, ochrony antywirusowej, IPS oraz kontroli aplikacji.
4. System musi umożliwiać utworzenie co najmniej 5 niezależnych kont administratorów z możliwością przypisania odpowiednich uprawnień.
5. System musi wspierać protokoły IPv4 oraz IPv6 co najmniej w zakresie Firewall, ochrony w warstwie aplikacyjnej oraz routingu dynamicznego.
6. System musi umożliwiać pracę w klastrze wysokiej dostępności Active-Active lub Active-Passive wraz z synchronizacją sesji.

7. System musi umożliwiać monitorowanie awarii elementów sprzętowych, programowych oraz dostępności łączy sieciowych.
8. System musi umożliwiać monitoring stanu połączeń VPN.
9. System musi obsługiwać agregację łączy statyczną oraz w oparciu o protokół LACP, a także umożliwiać tworzenie interfejsów redundantnych.
10. Urządzenie musi posiadać co najmniej 10 portów Gigabit Ethernet RJ-45.
11. Urządzenie musi posiadać wbudowany port konsoli szeregowej.
12. Urządzenie musi posiadać port USB umożliwiający instalację lub aktualizację oprogramowania.
13. System musi umożliwiać utworzenie co najmniej 200 interfejsów wirtualnych VLAN zgodnych ze standardem IEEE 802.1Q.
14. Urządzenie musi być wyposażone w zasilanie AC.
15. Liczba jednoczesnych sesji Firewall musi wynosić minimum 1 400 000.
16. Liczba nowych sesji na sekundę musi wynosić minimum 100 000.
17. Przepustowość Stateful Firewall dla pakietów 512 B musi wynosić minimum 10 Gbps.
18. Przepustowość Firewall przy włączonej kontroli aplikacji musi wynosić minimum 3,5 Gbps.
19. Przepustowość IPSec VPN AES-128 musi wynosić minimum 7 Gbps.
20. Przepustowość IPS dla ruchu odpowiadającego typowemu środowisku przedsiębiorstwa musi wynosić minimum 2,2 Gbps.
21. Przepustowość przy jednocześnie aktywnych funkcjach IPS, Application Control i Antywirus musi wynosić minimum 1 Gbps.
22. Przepustowość inspekcji SSL dla ruchu HTTP musi wynosić minimum 1,4 Gbps.
23. System musi zapewniać zaporę sieciową klasy Stateful Inspection.
24. System musi zapewniać kontrolę aplikacji.
25. System musi zapewniać obsługę IPSec VPN.
26. System musi zapewniać ochronę przed złośliwym oprogramowaniem.
27. System musi posiadać funkcjonalność Intrusion Prevention System.
28. System musi zapewniać filtrowanie stron www.
29. System musi zapewniać ochronę poczty elektronicznej dla protokołu SMTP.
30. System musi umożliwiać zarządzanie pasmem, QoS oraz Traffic Shaping.
31. System musi umożliwiać uwierzytelnianie wieloskładnikowe.
32. Należy dostarczyć co najmniej 2 programowe lub sprzętowe tokeny MFA przeznaczone dla administratorów lub użytkowników VPN Client-to-Site.
33. System musi umożliwiać inspekcję ruchu szyfrowanego SSL/TLS co najmniej dla HTTP, HTTP/2, SMTP, FTP oraz POP3.
34. System musi umożliwiać filtrowanie zapytań DNS.
35. System musi posiadać mechanizmy automatyzacji umożliwiające wykonanie określonej sekwencji czynności po wystąpieniu wskazanego zdarzenia bezpieczeństwa.

36. System musi umożliwiać budowę polityk bezpieczeństwa uwzględniających co najmniej adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje, profile zabezpieczeń oraz rejestrowanie zdarzeń.
37. System musi obsługiwać NAT źródłowy, NAT docelowy oraz PAT.
38. System musi obsługiwać translację jeden-do-jednego oraz jeden-do-wielu.
39. System musi obsługiwać ALG dla protokołu SIP.
40. System musi umożliwiać tworzenie wydzielonych stref bezpieczeństwa, w tym LAN, WAN i DMZ.
41. System musi umożliwiać korzystanie w politykach z zewnętrznych repozytoriów adresów IP oraz URL.
42. System musi umożliwiać filtrowanie ruchu w zależności od kraju przypisanego do źródłowego lub docelowego adresu IP.
43. System musi umożliwiać określenie przedziału czasu aktywności reguły Firewall.
44. System musi obsługiwać IKEv1 oraz IKEv2.
45. System musi obsługiwać szyfrowanie AES minimum 128 i 256 bitów, w tym tryb GCM.
46. System musi obsługiwać Diffie-Hellman minimum grupy 19 i 20.
47. System musi obsługiwać topologie Hub-and-Spoke oraz Mesh.
48. System musi obsługiwać połączenia Site-to-Site oraz Client-to-Site.
49. System musi zapewniać monitoring stanu tuneli VPN.
50. System musi obsługiwać routing statyczny oraz dynamiczny przez tunele VPN.
51. System musi obsługiwać uwierzytelnianie przy użyciu Pre-Shared Key oraz certyfikatów.
52. System musi obsługiwać mechanizmy IPSec NAT Traversal, DPD, XAuth oraz Split Tunneling.
53. System musi umożliwiać automatyczne przełączenie na tunel zapasowy w przypadku niedostępności tunelu podstawowego.
54. Producent rozwiązania musi posiadać oprogramowanie klienckie VPN kompatybilne z oferowanym urządzeniem.
55. System musi obsługiwać routing statyczny.
56. System musi obsługiwać Policy Based Routing.
57. System musi obsługiwać RIPv2 oraz RIPng.
58. System musi obsługiwać OSPF oraz OSPFv3.
59. System musi obsługiwać BGP.
60. System musi obsługiwać PIM.
61. System musi umożliwiać filtrowanie tras.
62. System musi obsługiwać ECMP.
63. System musi obsługiwać BFD.
64. System musi umożliwiać monitorowanie dostępności wskazanych adresów IP oraz automatyczną zmianę tablicy routingu w przypadku niedostępności trasy.
65. System musi posiadać funkcjonalność SD-WAN.
66. System musi umożliwiać wykorzystanie w ramach SD-WAN interfejsów fizycznych i wirtualnych, w tym VLAN oraz IPSec.

67. System musi umożliwiać wykorzystanie dynamicznych protokołów routingu przy realizacji równoważenia obciążenia pomiędzy łączami WAN.
68. System musi umożliwiać określenie maksymalnego i gwarantowanego pasma.
69. System musi umożliwiać oznaczanie ruchu DSCP.
70. System musi umożliwiać nadawanie priorytetów ruchowi.
71. System musi umożliwiać definiowanie limitów pasma dla konkretnych aplikacji.
72. System musi umożliwiać definiowanie limitów dla konkretnych użytkowników niezależnie od ich adresu IP.
73. System musi umożliwiać definiowanie pasma dla określonych kategorii URL.
74. System musi umożliwiać skanowanie ruchu w obu kierunkach.
75. System musi rozpoznawać protokoły niezależnie od standardowo wykorzystywanego portu TCP/UDP.
76. System musi skanować co najmniej protokoły HTTP, HTTPS, FTP, POP3, IMAP, SMTP oraz CIFS.
77. System musi umożliwiać analizę archiwów zagnieżdżonych.
78. System musi umożliwiać blokowanie i logowanie archiwów niemożliwych do przeskanowania.
79. System musi posiadać sygnatury ochrony urządzeń mobilnych co najmniej dla systemu Android.
80. Baza sygnatur musi być aktualizowana automatycznie.
81. System musi współpracować z usługą lub platformą typu Sandbox.
82. System musi umożliwiać wykorzystanie mechanizmów sztucznej inteligencji do identyfikacji zagrożeń.
83. System musi umożliwiać przypisanie ochrony antymalware do wybranych zakresów ruchu.
84. System IPS musi wykorzystywać analizę sygnaturową oraz analizę anomalii protokołów sieciowych.
85. System IPS musi chronić aplikacje działające na niestandardowych portach.
86. Baza IPS musi zawierać minimum 5000 sygnatur ataków.
87. Baza IPS musi być aktualizowana automatycznie.
88. Administrator musi mieć możliwość definiowania własnych wyjątków oraz sygnatur.
89. System musi zapewniać podstawową ochronę przed atakami DoS oraz DDoS.
90. System musi umożliwiać wykrywanie i blokowanie komunikacji z sieciami botnet oraz serwerami Command & Control.
91. System musi umożliwiać aktywowanie ochrony IPS dla wybranych zakresów komunikacji.
92. Identyfikacja aplikacji musi opierać się na analizie ruchu i nie może bazować wyłącznie na numerach portów TCP/UDP.
93. Baza aplikacji musi zawierać minimum 2000 sygnatur.
94. Baza aplikacji musi być aktualizowana automatycznie.
95. System musi umożliwiać kontrolę operacji wykonywanych w aplikacjach chmurowych.
96. System musi rozpoznawać kategorie aplikacji istotne z punktu widzenia bezpieczeństwa, w szczególności Proxy oraz P2P.
97. Administrator musi mieć możliwość definiowania własnych wyjątków i sygnatur aplikacji.

98. System musi umożliwiać blokowanie aplikacji uruchamianych na niestandardowych portach.
99. System filtrowania WWW musi korzystać z bazy minimum 40 milionów adresów URL sklasyfikowanych według kategorii.
100. System musi rozpoznawać co najmniej kategorie malware, phishing, spam, Dynamic DNS oraz Proxy.
101. System musi umożliwiać tworzenie własnych białych i czarnych list URL.
102. System musi umożliwiać nadpisywanie kategorii stron.
103. System musi umożliwiać stosowanie wyrażeń regularnych Regex.
104. System musi umożliwiać wyświetlenie ostrzeżenia wymagającego potwierdzenia użytkownika przed wejściem na określoną stronę.
105. System musi obsługiwać funkcję Safe Search.
106. System musi umożliwiać wyłączenie wskazanych kategorii lub adresów URL z inspekcji SSL.
107. System musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem lokalnej bazy użytkowników.
108. System musi obsługiwać integrację z LDAP.
109. System musi obsługiwać integrację z RADIUS.
110. System musi obsługiwać RSA SecurID lub rozwiązanie równoważne.
111. System musi umożliwiać integrację z Active Directory.
112. System musi obsługiwać SAML.
113. System musi umożliwiać realizację mechanizmów Single Sign-On.
114. System musi umożliwiać zastosowanie uwierzytelniania wieloskładnikowego.
115. Zarządzanie lokalne musi być możliwe co najmniej przy wykorzystaniu HTTPS oraz SSH.
116. System musi umożliwiać współpracę z centralną platformą zarządzania i monitorowania.
117. Komunikacja z centralną platformą musi być szyfrowana.
118. Dostęp administracyjny musi umożliwiać zastosowanie MFA.
119. System musi obsługiwać SNMP v2c, SNMP v3 oraz NetFlow lub sFlow.
120. System musi udostępniać udokumentowane API.
121. System musi posiadać co najmniej narzędzia ping, traceroute, podgląd pakietów, monitoring sesji oraz monitoring procesowania sesji.
122. System musi umożliwiać przygotowanie zmian konfiguracyjnych przed ich zatwierdzeniem i zastosowaniem.
123. System musi umożliwiać definiowanie różnych zakresów uprawnień administratorów.
124. System musi umożliwiać ograniczenie dostępu administracyjnego do wskazanych źródłowych adresów IP.
125. System musi zapewniać logowanie zdarzeń wszystkich funkcji bezpieczeństwa.
126. System musi rejestrować co najmniej ruch zaakceptowany, ruch zablokowany, działania administratorów, zużycie zasobów oraz stan pracy urządzenia.
127. System musi umożliwiać jednoczesne wysyłanie logów do wielu serwerów.
128. System musi umożliwiać aktywowanie logowania dla pojedynczej reguły Firewall.

129. System musi umożliwiać eksport logów poprzez SYSLOG.
130. Przesyłanie SYSLOG do zewnętrznych systemów musi być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
131. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.
132. System musi być objęty serwisem producenta przez okres minimum 36 miesięcy, obejmującym dostęp do aktualizacji oprogramowania, aktualnych baz zabezpieczeń, wsparcie techniczne producenta oraz naprawę lub wymianę urządzenia w przypadku awarii.

4. Przełącznik dostępowy – 3 szt.

Przedmiotem zamówienia jest dostawa zarządzalnego przełącznika sieciowego przeznaczonego do pracy w warstwie dostępowej sieci LAN, wyposażonego w porty Gigabit Ethernet oraz porty uplink 10 Gigabit Ethernet.

Wymagania:

1. Przełącznik musi być przeznaczony do montażu w standardowej szafie rack 19".
2. Wysokość urządzenia nie może przekraczać 1U.
3. Urządzenie musi być zasilane napięciem 230 V AC.
4. MTBF urządzenia musi wynosić powyżej 10 lat.
5. Urządzenie musi posiadać co najmniej 48 portów Gigabit Ethernet RJ-45.
6. Urządzenie musi posiadać co najmniej 4 porty 10 Gigabit Ethernet SFP+.
7. Urządzenie musi posiadać port konsoli szeregowej RJ-45.
8. Urządzenie musi umożliwiać zarządzanie poprzez CLI, SSH oraz graficzny interfejs www.
9. Urządzenie musi umożliwiać współpracę z centralnym systemem zarządzania przełącznikami.
10. Centralny system zarządzania musi umożliwiać automatyczne wykrywanie i centralną konfigurację przełączników.
11. Centralny system zarządzania musi umożliwiać automatyczne wykonywanie wybranych czynności konfiguracyjnych w zależności od wykrytej topologii sieci.
12. System musi umożliwiać automatyczną konfigurację mechanizmów Spanning Tree.
13. System musi umożliwiać automatyczną konfigurację tagowania VLAN zgodnie z IEEE 802.1Q.
14. System musi umożliwiać automatyczne przejęcie zarządzania nad wykrytym przełącznikiem.
15. Centralny system zarządzania musi umożliwiać aktualizację oprogramowania układowego zarządzanych przełączników.
16. System musi umożliwiać identyfikację typu urządzenia podłączonego do wybranego portu przełącznika.
17. System musi umożliwiać automatyczną instalację wskazanej wersji firmware po podłączeniu przełącznika.
18. Oprogramowanie układowe przełączników musi mieć możliwość przechowywania na centralnym kontrolerze.

19. Przepustowość przełączania urządzenia musi wynosić minimum 176 Gbps.
20. Wydajność przekazywania pakietów musi wynosić minimum 260 Mpps.
21. Tablica adresów MAC musi umożliwiać zapis co najmniej 32 000 adresów.
22. Opóźnienie urządzenia musi wynosić poniżej 1 µs.
23. Bufor pakietów musi mieć pojemność minimum 2 MB.
24. Urządzenie musi posiadać minimum 512 MB pamięci DRAM.
25. Urządzenie musi posiadać minimum 64 MB pamięci Flash.
26. Urządzenie musi umożliwiać automatyczną negocjację prędkości oraz trybu duplex.
27. Urządzenie musi obsługiwać IEEE 802.1D Spanning Tree Protocol.
28. Urządzenie musi obsługiwać IEEE 802.1W Rapid Spanning Tree Protocol.
29. Urządzenie musi obsługiwać IEEE 802.1S Multiple Spanning Tree Protocol.
30. Urządzenie musi obsługiwać agregację portów zgodną z IEEE 802.3ad.
31. Urządzenie musi obsługiwać co najmniej 4000 sieci VLAN zgodnych z IEEE 802.1Q.
32. Urządzenie musi umożliwiać realizację routingu statycznego.
33. Urządzenie musi obsługiwać Port Mirroring.
34. Urządzenie musi obsługiwać kontrolę dostępu do portów zgodną z IEEE 802.1X.
35. Urządzenie musi umożliwiać uwierzytelnianie za pośrednictwem RADIUS.
36. Urządzenie musi umożliwiać zarządzanie i monitoring przy wykorzystaniu Telnet, SSH, HTTP, HTTPS, SNMP v1, v2 i v3, SNTP oraz LLDP.
37. Urządzenie musi umożliwiać zarządzanie poprzez interfejs graficzny oraz tekstowy.
38. Urządzenie musi umożliwiać aktualizację oprogramowania poprzez TFTP, FTP oraz interfejs graficzny.
39. Urządzenie musi umożliwiać integrację z systemem bezpieczeństwa sieciowego klasy NGFW.
40. Integracja z systemem NGFW musi umożliwiać uruchamianie Captive Portalu w celu identyfikacji użytkowników.
41. Integracja z systemem NGFW musi umożliwiać obsługę białych i czarnych list adresów MAC.
42. Integracja z systemem NGFW musi umożliwiać kontrolę dostępu do sieci.
43. Integracja z systemem NGFW musi umożliwiać routing statyczny oraz routing dynamiczny co najmniej w oparciu o OSPF.
44. Wraz z przełącznikami należy dostarczyć moduły 10GE SFP+ SR w liczbie 4 szt.
45. Wszystkie dostarczone moduły muszą być oficjalnie wspierane przez producenta oferowanego przełącznika.
46. Urządzenia muszą być objęte gwarancją producenta zapewniającą wymianę wadliwego sprzętu.
47. Wymagana jest gwarancja producenta obowiązująca przez cały okres użytkowania urządzenia, nie krócej niż do 5 lat od ogłoszenia zakończenia jego produkcji.
48. Urządzenia muszą być objęte serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy.
49. Serwis gwarancyjny musi być realizowany na terytorium Rzeczypospolitej Polskiej.

50. W przypadku gdy producent nie posiada własnego centrum serwisowego na terenie Polski, Wykonawca musi przedstawić dokument producenta wskazujący podmiot uprawniony do świadczenia serwisu gwarancyjnego na terenie Polski.
51. Wraz z ofertą Wykonawca musi przedstawić oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski potwierdzające posiadanie autoryzacji w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

5. UPS centralny – 1 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. UPS centralnego.
Wymagania:

1. MOC min. 15000VA/13500W
2. Obudowa Tower
3. Trójfazowa konstrukcja
4. Czyste wyjściowe napięcie sinusoidalne
5. Topologia UPS (podwójnej konwersji) online
6. Równoległe rozszerzenie UPS
7. Ochrona przed przeciążeniem
8. Kolorowy wyświetlacz LCD z panelem dotykowym
9. Topologia podwójnej konwersji online
10. Kształt napięcia w trybie bateryjnym: Czyste napięcie sinusoidalne
11. Trójfazowa konstrukcja wejścia/wyjścia
12. Efektywność trybu ECO online do 98%
13. Wejściowy prąd znamionowy: min. 21 A
14. THDI <3% (Full Linear Load)
15. Współczynnik mocy wejściowej: 0.99
16. Tolerancja napięcia wyjściowego: 1%
17. Tolerancja napięcia w trybie ECO: ± 10%
18. Współczynnik szczytu: 3 : 1
19. Zniekształcenia harmoniczne (obciążenie liniowe): THD＜1%
20. Zniekształcenia harmoniczne (obciążenie nieliniowe): THD＜5.5%
21. Czas przełączania 0 ms
22. Konstrukcja z dwoma wejściami umożliwiając podłączenie jednego wejścia ze źródła zasilania prądem przemiennym i drugiego wejścia z innego źródła zasilania.
23. Serwisowy przełącznik obejściowy do płynnego przełączania zasilania na źródło sieciowe w trybie obejścia.
24. Kompatybilność z generatorem z wbudowaną funkcją automatycznej regulacji napięcia (AVR) do stabilizacji niestabilnych poziomów napięcia prądu z generatora.
25. Zgodne typy baterii: VRLA, AGM, Gel
26. Czas podtrzymania systemu min. 20 minut dla mocy 11 kW

27. Możliwość wydłużenia czasu podtrzymania przez dołożenie zestawów bateryjnych dostarczonych w zamkniętych szafach.
28. Możliwość ładowania szaf bateryjnych z mocą do 20% mocy UPS.
29. Możliwość pracy równoległej.
30. Możliwość łączenia równoległego do min. 4 jednostek UPS
31. Gniazdo wyjściowe: Kostka zaciskowa do łączenia przewodów
32. Złącze wejściowe: Kostka zaciskowa do łączenia przewodów
33. Porty komunikacyjne: RS232, RS485, SNMP, EPO, Dry contact
34. Zdalna komunikacja po protokole SNMP oraz http
35. Oprogramowanie w języku polskim do zarządzania UPSem z możliwością monitorowania zużycia energii oraz współpracy ze środowiskiem VMware ESXi 8.0 U2
36. Certyfikaty CE, IEC62040-1, IEC62040-2.
37. Gwarancja min. 36 miesięcy.
38. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
39. Urządzenie i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wraz z ofertą wykonawca składa oświadczenie producenta oferowanego UPSa, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

6. Oprogramowanie klasy SIEM – 1 kpl.

Przedmiotem zamówienia jest oprogramowanie SIEM do zbierania logów, oraz analizy danych i incydentów z całej infrastruktury IT. System musi posiadać kompleksowe narzędzia do monitorowania, wykrywania, analizy i reagowania na zagrożenia obejmujące następujące obszary:

1. System musi gromadzić dane z różnorodnych źródeł, takich jak:
    a. Logi systemowe (systemów operacyjnych, serwerów, aplikacji, urządzeń sieciowych).
    b. Informacje o zdarzeniach (np. próby logowania, zmiany uprawnień, działania użytkowników).
    c. Dane dotyczące konfiguracji infrastruktury IT (np. plików konfiguracyjnych, polityk bezpieczeństwa).
    d. System musi automatycznie analizować te dane w czasie rzeczywistym, identyfikując potencjalne zagrożenia oraz anomalie na podstawie wcześniej zdefiniowanych reguł, sygnatur oraz zaawansowanych algorytmów analitycznych.
2. Kluczową funkcją systemu musi być ciągłe monitorowanie stanu bezpieczeństwa w czasie rzeczywistym. System musi umożliwiać:
    a. Wczesne wykrywanie zagrożeń: Wykorzystanie analizy behawioralnej oraz sztucznej inteligencji do identyfikacji nietypowych zachowań użytkowników, urządzeń i aplikacji.
    b. Pełna widoczność nad wszystkimi elementami infrastruktury IT, w tym także nad środowiskami wirtualnymi i chmurowymi.
    c. Analiza historyczna zdarzeń: System musi umożliwiać retrospektywne badanie logów i zdarzeń, co jest niezbędne do dochodzeń powłamaniowych i audytów bezpieczeństwa.

3. System musi posiadać zaawansowane wykrywanie zagrożeń w różnych środowiskach, takich jak:
    a. Środowiska chmurowe (AWS, Azure, Google Cloud).
    b. Kontenery (Docker, Kubernetes).
    c. Urządzenia końcowe.
4. System musi rozszerzać możliwości SIEM, pozwalając na:
    a. Skoordynowane wykrywanie zagrożeń w całym środowisku IT.
    b. Szybkie reagowanie na incydenty dzięki integracji z innymi narzędziami do zarządzania i automatyzacji (np. firewalle, narzędzia do zarządzania zasobami IT).
    c. Automatyzację działań naprawczych, co redukuje czas reakcji na zagrożenia oraz minimalizuje ryzyko.
5. System musi wspierać zarządzanie incydentami bezpieczeństwa poprzez:
    a. Automatyczne powiadomienia o wykrytych zagrożeniach, pozwalające administratorom na szybkie podjęcie działań.
    b. Raportowanie incydentów z pełnym zestawem informacji potrzebnych do analizy i dalszych działań naprawczych.
    c. Korelowanie zdarzeń z różnych źródeł w celu lepszego zrozumienia zagrożeń i zidentyfikowania ich źródła.
6. System musi pomagać organizacji w utrzymywaniu zgodności z regulacjami prawnymi i standardami bezpieczeństwa poprzez:
    a. Monitorowanie działań użytkowników i zapis zmian w systemach, co pozwala na śledzenie operacji oraz wykrywanie nieautoryzowanych działań.
    b. Automatyczne generowanie raportów audytowych i zgodności, które można przedstawić audytorom oraz organom nadzoru.
    c. Tworzenie alertów zgodności, które informują o potencjalnych naruszeniach polityk bezpieczeństwa.
7. Wykonawca skonfiguruje urządzenia i systemy w sieci Zamawiającego do wysyłania dzienników zdarzeń (logów) do centralnego systemu składowania dzienników zdarzeń. Prace obejmą co najmniej:
    a. 1 urządzenie klasy UTM,
    b. 3 przełączniki zarządzalne ,
    c. Serwery
    d. 45 stacji roboczych
    e. 1 aplikację centralnego zarządzania oprogramowaniem antywirusowym.

7. Oprogramowanie klasy EDR/XDR – 1 kpl.

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja oprogramowania antywirusowego oraz EDR/XDR. Oprogramowanie będzie musiało spełniać wymogi operacyjne i technologiczne Zamawiającego, zapewniając pełną integrację z istniejącą infrastrukturą oraz optymalizację działań związanych z cyberbezpieczeństwem. Zamówienie obejmuje dostawę licencji na 45 stacji roboczych oraz 3 serwery na okres do 36 miesięcy.

Wymagania:

1. Administracja zdalna:
    a. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
    b. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
    c. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
    d. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
    e. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
    f. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
    g. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
    h. 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.
    i. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
    j. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
    k. 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.
    l. 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.
2. Ochrona stacji roboczych:
    a. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
    b. Rozwiązanie musi wspierać architekturę ARM64.
    c. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
    d. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
    e. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
    f. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
    g. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
    h. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.

i. 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.
j. 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).
k. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
l. 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.
m. 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.
n. 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.
o. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    i. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    ii. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    iii. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    iv. 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,
    v. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
p. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z:
    i. zainstalowanych aplikacji
    ii. usług systemowych
    iii. informacji o systemie operacyjnym i sprzęcie
    iv. aktywnych procesów i połączeń sieciowych
    v. harmonogramu systemu operacyjnego
    vi. pliku hosts
    vii. sterowników.

q. 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.
r. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
s. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
t. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
u. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook.
v. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    i. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    ii. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    iii. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    iv. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
w. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
x. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
y. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
z. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
aa. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.

3. Ochrona serwerów:
    a. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
    b. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
    c. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
    d. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
    e. 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.
    f. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.

g. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
h. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

4. Wymagania dla ochrony serwerów Windows:
   a. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
   b. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
   c. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
   d. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
   e. 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.
   f. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
   g. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
   h. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
   i. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
5. Wymagania dla ochrony serwerów Linux:
   a. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
   b. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
   c. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
   d. 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.
6. Ochrona urządzeń mobilnych opartych o system Android:
   a. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
   b. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
   c. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
   d. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.

e. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
   i. usunięcie zawartości urządzenia,
   ii. przywrócenie urządzenie do ustawień fabrycznych,
   iii. zablokowania urządzenia,
   iv. uruchomienie sygnału dźwiękowego,
   v. lokalizację GPS.
f. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
g. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   i. nazwę aplikacji,
   ii. nazwę pakietu,
   iii. kategorię sklepu Google Play,
   iv. uprawnienia aplikacji,
   v. pochodzenie aplikacji z nieznanego źródła.

7. Szyfrowanie:
   a. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
   b. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
   c. 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.
   d. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. Moduł XDR:
   a. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
   b. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
   c. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
   d. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
   e. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
   f. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
   g. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
   h. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
   i. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

j. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
k. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
l. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
m. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
n. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
o. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
p. Konsola administracyjna musi mieć możliwość tagowania obiektów.
q. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

9. Zamawiający wymaga licencji dla 45 stacji roboczych oraz 3 serwery na okres do 36 miesięcy. Licencja powinna obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.
10. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wraz z ofertą Wykonawca składa oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

8. Urządzenie NAS – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. urządzenia do przechowywania danych.

Wymagania:

1. Obudowa do szafy RACK, szyny do montażu w szafie RACK.
2. Procesor wielordzeniowy osiągający w teście wydajności PassMark Performance Test co najmniej wynik 8 000 punktów, testy powinny być aktualne w okresie nie dłuższym niż 60 dni przed

składaniem ofert. Zamawiający żąda załączenia do oferty wyniku potwierdzającego spełnienie przez oferowany procesor żądanej przez Zamawiającego wydajności.

3. Pamięć RAM: min. 16 GB z możliwością rozbudowy do co najmniej 64 GB.
4. Funkcje: wsparcie dla wirtualizacji, scentralizowana pamięć masowa na dane, backup, udostępnianie i przywracanie systemu po awarii.
5. Możliwość zainstalowania łącznie 8 dysków 3,5 calowych.
6. Sloty PCI-E: min. 2 aktywne sloty PCI-E 3.0 umożliwiające instalację dodatkowych kart rozszerzeń, takich jak karty sieciowe, karty SSD NVMe lub inne, które mogą zwiększyć funkcjonalność i wydajność systemu.
7. Interfejsy sieciowe:
    a. zainstalowane i w pełni funkcjonalne minimum 2 porty sieciowe Ethernet 2.5GbE RJ45 z obsługą Link Aggregation w celu zwiększenia wydajności transferu i odporności na awarie (porty nie mogą zajmować slotów PCI-E);
8. zainstalowane i w pełni funkcjonalne minimum 2 porty optyczne 10GbE SFP+ z modułami optycznymi SFP+ Multimode.
9. Pamięć masowa:
    1) Zainstalowane 2 dyski SSD M2 PCIe NVMe o pojemności min. 960 GB każdy, które umożliwiają korzystanie z technologii buforowania SSD w celu zapewnienia optymalnej wydajności serwera.
    2) Zainstalowane min. 6 dysków HDD SATA o pojemności min. 8 TB każdy.
10. Kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 5, 6, 10, 50, 60.
11. Porty USB: min. 2x USB 3.0.
12. Urządzenie powinno oferować zaawansowane funkcje zabezpieczeń, takie jak szyfrowanie danych AES-256, dwustopniowe uwierzytelnianie, zapora sieciowa, oraz ochrona przed atakami typu brute-force.
13. Wraz ze serwerem dostarczone powinno być oprogramowanie do tworzenia i zarządzania kopiami zapasowymi komputerów, serwerów i maszyn wirtualnych w środowiskach wirtualizacyjnych. Oprogramowanie powinno zapewniać pełne bezpieczeństwo danych, niezawodność, oraz wsparcie dla popularnych platform wirtualizacji. Wymagania:
    a. Kompatybilność z platformami wirtualizacyjnymi: Oprogramowanie musi być kompatybilne z wiodącymi platformami wirtualizacji, w tym VMware vSphere (wersje 6.5 i wyższe) oraz Microsoft Hyper-V (wersje z Windows Server 2016 i wyższe).
    b. Funkcjonalność tworzenia kopii zapasowych:
        i. Oprogramowanie powinno umożliwiać tworzenie pełnych, różnicowych oraz przyrostowych kopii zapasowych maszyn wirtualnych, z możliwością planowania zadań backupu według harmonogramu ustalonego przez administratora.
        ii. Musi wspierać technologię deduplikacji, co pozwala na oszczędność przestrzeni dyskowej przez eliminację zduplikowanych danych w kopiach zapasowych.
        iii. Musi wspierać technologię kompresji, co znacznie skraca czas tworzenia kopii zapasowych, magazynowania i przywracania danych.

iv. Musi wspierać jednoczesne tworzenie kopii zapasowych wielu maszyn wirtualnych.
v. Musi oferować funkcję tworzenia kopii zapasowych z komputerów oraz serwerów z systemem Windows.
vi. Powinno oferować funkcję backupu bezagentowego, umożliwiającą tworzenie kopii zapasowych bez potrzeby instalacji dodatkowego oprogramowania na maszynach wirtualnych.

c. Zarządzanie kopiami zapasowymi:
i. Oprogramowanie powinno posiadać centralny interfejs zarządzania, umożliwiający monitorowanie, konfigurowanie i zarządzanie wszystkimi zadaniami backupu z jednego miejsca.
ii. Musi oferować zaawansowane raportowanie oraz generowanie logów, które ułatwią śledzenie statusu zadań oraz identyfikację potencjalnych problemów.
iii. Powinno umożliwiać automatyczne usuwanie starych kopii zapasowych na podstawie określonych polityk, co pomoże w efektywnym zarządzaniu przestrzenią dyskową.

d. Funkcje przywracania danych:
i. Oprogramowanie musi umożliwiać szybkie i elastyczne przywracanie danych, w tym pełnych maszyn wirtualnych, poszczególnych plików lub katalogów, oraz punktów w czasie (instant recovery).
ii. Powinno wspierać funkcję przywracania na poziomie plików (file-level recovery), umożliwiającą selektywne odzyskiwanie plików bez potrzeby przywracania całej maszyny wirtualnej.

e. Zabezpieczenia i ochrona danych:
i. Oprogramowanie musi oferować zaawansowane opcje szyfrowania danych zarówno podczas tworzenia kopii zapasowych, jak i w trakcie ich przesyłania (np. szyfrowanie AES-256).
ii. Powinno wspierać funkcję tworzenia zaszyfrowanych kopii zapasowych, które mogą być przechowywane w bezpiecznych lokalizacjach (np. na serwerach zdalnych lub w chmurze).

f. Wsparcie dla środowisk chmurowych:
i. Oprogramowanie powinno być kompatybilne z popularnymi usługami chmurowymi, umożliwiając przechowywanie kopii zapasowych w takich środowiskach jak Amazon S3, Microsoft Azure, Google Cloud, itp.
ii. Powinno oferować funkcję zautomatyzowanego tworzenia kopii zapasowych do chmury, z możliwością szybkiego odzyskiwania danych w przypadku awarii lokalnej infrastruktury.

g. Licencje powinny być wieczyste (perpetual) bez konieczności ponoszenia jakichkolwiek w przyszłości.

14. Wraz z urządzeniem dostarczone powinno być oprogramowanie na 45 komputerów do automatycznego tworzenia kopii zapasowych danych z komputerów osobistych oraz serwerów produkcyjnych na serwer do przechowywania danych. Oprogramowanie powinno umożliwiać

efektywne i bezpieczne zarządzanie kopiami zapasowymi, zapewniając ochronę danych oraz łatwe przywracanie plików w razie awarii. Wymagania:

a. Kompatybilność systemowa: Oprogramowanie musi być kompatybilne z najnowszymi wersjami systemów operacyjnych Windows 10 i 11 oraz Windows Server 2016, 2019 i 2022. Powinno wspierać zarówno 32-bitowe, jak i 64-bitowe wersje systemów operacyjnych.
b. Oprogramowanie musi umożliwiać automatyczne tworzenie kopii zapasowych danych użytkownika, w tym plików i folderów, zgodnie z harmonogramem ustalonym przez administratora lub użytkownika.
c. Oprogramowanie powinno obsługiwać backup pełny, różnicowy oraz przyrostowy, co pozwala na efektywne zarządzanie przestrzenią dyskową oraz czasem potrzebnym na tworzenie kopii zapasowych.
d. Aplikacja powinna umożliwiać tworzenie kopii zapasowych zarówno lokalnie, jak i na zdalnym serwerze sieciowym, poprzez połączenie z siecią LAN/WAN.
e. Aplikacja powinna obsługiwać format plikowy jak i blokowy umożliwiający tworzenie kopii zapasowych całego systemu, dysku, folderu lub pliku.
f. Oprogramowanie musi posiadać graficzny interfejs użytkownika umożliwiający łatwe zarządzanie kopiami zapasowymi, monitorowanie statusu backupu oraz szybkie przywracanie danych.
g. Oprogramowanie powinno oferować możliwość konfiguracji i zarządzania zadaniami backupu z poziomu centralnego zarządzania, w tym ustalania priorytetów oraz planowania zadań.
h. Aplikacja powinna umożliwiać automatyczne usuwanie starych kopii zapasowych na podstawie określonych przez użytkownika polityk, co pozwala na optymalne zarządzanie dostępną przestrzenią dyskową.
i. Oprogramowanie musi zapewniać zaawansowane opcje szyfrowania danych (np. AES-256) w trakcie tworzenia kopii zapasowych oraz przesyłania danych, aby zapewnić bezpieczeństwo przechowywanych informacji.
j. Powinno wspierać tworzenie kopii zapasowych chronionych hasłem, co zwiększa bezpieczeństwo danych przechowywanych na serwerze.
k. Oprogramowanie musi oferować funkcję powiadamiania administratora oraz użytkowników o statusie zadań backupu poprzez e-mail lub inne formy komunikacji.
l. Oprogramowanie powinno generować szczegółowe logi, które umożliwiają analizę i śledzenie historii zadań backupu oraz ewentualnych problemów.
m. Licencje powinny być wieczyste (perpetual) bez konieczności ponoszenia jakichkolwiek w przyszłości.

15. Jakość produktu i sposobu jego wykonania:
    a. Deklaracja zgodności CE lub inny równoważny dokument dla zaoferowanego NAS– Zamawiający dopuszcza złożenie dokumentów w języku angielskim
    b. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci deklaracji RoHS dla produktu lub oświadczenia producenta NAS lub innego dokumentu potwierdzającego

spełnienie kryteriów środowiskowych w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych – Zamawiający dopuszcza złożenie dokumentów w języku angielskim;

16. Gwarancja:
    a. 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 na terenie RP.
    b. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji.
    c. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
    d. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001 lub równoważny.
    e. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
        i. możliwość pobierania najnowszego firmware,
        ii. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
        iii. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,

9. Szkolenie stacjonarne z cyberbezpieczeństwa – 1 kpl.

Przedmiotem zamówienia jest przeprowadzenie szkolenia stacjonarnego w Urzędzie Gminy Niegowa dla 45 osób w dwóch grupach szkoleniowych dla pracowników JST dotyczącego bezpieczeństwa informacji, budującego świadomość cyberzagrożeń, wskazującego skutki naruszeń zasad bezpieczeństwa informacji oraz kwestie prawne związane z ochroną danych osobowych i sposobów ochrony. Celem szkolenia jest podniesienie świadomości uczestników w zakresie bezpieczeństwa informacji, umożliwiając im lepsze zrozumienie zagrożeń, skutków naruszeń i efektywne stosowanie środków bezpieczeństwa w codziennej pracy. Zamawiający zapewni salę szkoleniową wyposażoną w ekran i rzutnik, z minimalną liczbą 25 miejsc.

Wymagania:

1. Szkolenia muszą odbywać się w godzinach pracy Urzędu.
2. Wykonawca w ramach wykonania usługi przedstawi szczegółowy program szkolenia zawierający informacje dotyczące tematyki i czasu szkolenia, i dostarczy go w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia, do akceptacji Zamawiającego.
3. Opracowane materiały będą musiały być dostarczone w formie papierowej i elektronicznej z możliwością powiększania treści. W ramach wynagrodzenia Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia. Zamawiający dopuszcza dostarczenie kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF.

4. Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu rozpoczęcia szkolenia.
5. Szkolenie musi obejmować co najmniej następującą tematykę:
    a. podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania),
    b. znaczenie cyberbezpieczeństwa dla jednostki samorządu terytorialnego,
    c. cyberbezpieczeństwo w codziennej pracy,
    d. standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w miejscu pracy, cyberhigiena,
    e. bezpieczeństwo urządzeń i bezpieczeństwo fizyczne, bezpieczne hasła, zarządzanie hasłami, uwierzytelnienie dwu- i wieloskładnikowe, klucze sprzętowe,
    f. przegląd i rozpoznawanie najpopularniejszych zagrożeń w cyberprzestrzeni (w tym rodzaje ataków, ransomware i malware, phishing, 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), sposoby unikania zagrożeń, zasady bezpiecznego korzystania z Internetu,
    g. ochrona informacji i prywatność w Internecie,
    h. jak bezpiecznie korzystać z narzędzi teleinformatycznych – przykłady stosowania zabezpieczeń,
    i. reagowanie na incydenty bezpieczeństwa (w tym zasady postępowania w razie podejrzenia naruszenia bezpieczeństwa/ataku),
    j. procedury zgłaszania incydentów,
    k. ochrona danych osobowych i wrażliwych informacji,
    l. analiza przypadków – praktyczne scenariusze,
    m. omówienie zjawiska pracy zdalnej w oparciu o aktualnie obowiązujące przepisy prawa w zakresie bezpieczeństwa informacji,
    n. analiza 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 i ustawy o krajowym systemie cyberbezpieczeństwa.
6. Forma prezentacji połączonej z warsztatami, co najmniej 40% zawartości szkolenia mają to być treści praktyczne, aktualne, angażujące i aktywizujące uczestników szkolenia, pozwalające na podniesienie umiejętności związanych z:
    a. rozpoznawaniem zagrożeń i reagowanie na nie,
    b. wykorzystywaniem narzędzi informatycznych zapewniających bezpieczeństwo przetwarzanych informacji oraz zabezpieczeń dla poczty elektronicznej i stron WWW,
    c. radzeniem sobie w sytuacjach kryzysowych (scenariusze codziennych zagrożeń).
7. W trakcie szkolenia trener powinien odpowiadać na pytania uczestników. Dopuszczalne jest zorganizowanie sesji pytań i odpowiedzi na zakończenie szkolenia.
8. W wyniku szkolenia pracownicy mają być w stanie odróżnić typowe błędy techniczne od potencjalnego ataku, wiedzieć jak uniknąć potencjalnego zagrożenia, a w przypadku

wystąpienia naruszenia – umieć podjąć podstawowe działania ograniczające skutki wystąpienia incydentu oraz zgłosić incydent do odpowiednich komórek.

9. Czas trwania szkolenia (dla jednej grupy) – min. 4 godziny lekcyjne (po 45 min.).
10. Z przeprowadzonych szkoleń Wykonawca musi przedstawić listy obecności z podpisami uczestników szkolenia.
11. Szkolenie musi być zakończone testem weryfikującym skuteczność szkolenia oraz anonimową ankietą wśród uczestników, oceniającą co najmniej przydatność szkolenia, zakres przekazanych informacji, adekwatność przekazanych informacji do potrzeb uczestników, formę prezentacji i komunikatywność prowadzącego szkolenie. Wykonawca przedstawi Zamawiającemu podsumowanie wyników ankiety.

10. Opracowanie dokumentacji SZBI – 1 kpl.

Zakres prac dotyczących dokumentacji SZBI:

1. Aktualizacja lub opracowanie (w przypadku braku dokumentu) dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwanej „SZBI”), w skład której wchodzą następujące dokumenty:
    a. Polityka Bezpieczeństwa Informacji;
    b. Instrukcja zarządzania systemem informatycznym;
    c. Polityka zarządzania ciągłością działania;
    d. Procedura zarządzania incydentami cyberbezpieczeństwa;
    e. Analiza ryzyka w zakresie Bezpieczeństwa Informacji;
2. Wdrożenie SZBI we współpracy z kierownikiem jednostki lub osobami wyznaczonymi do wdrożenia SZBI.
3. W ramach dokumentacji SZBI ujęte zostaną następujące procedury:
    a. procedury kontroli dostępu
    b. zabezpieczenie pomieszczeń i obiektów
    c. procedury czystego biurka i ekranu
    d. procedury kopii zapasowych
    e. procedury ochrony logów
    f. bezpieczeństwo komunikacji
    g. zarządzanie bezpieczeństwem sieci
    h. przesyłanie informacji
    i. plany ciągłości działania
    j. procedury zarządzania incydentami
    k. prywatność i ochrona danych osobowych
    l. szacowanie ryzyka w obszarze bezpieczeństwa informacji
    m. szkolenia personelu
4. Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zamawiającego i wdrażanej jednostki w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami na etapie deklaracji stosowania oraz wszelkich innych informacji uzyskanych przez Wykonawcę w trakcie realizacji

Umowy mogących mieć wpływ na treść dokumentacji. Usługi dotyczące czynności wdrażających dokumentację zostanie uznana za wykonaną po przekazaniu Zleceniodawcy przez Zleceniobiorcę całości dokumentacji SZBI i podpisaniu protokołu odbioru przez Zamawiającego.

11. Audyt końcowy – 1 kpl.

Wymagania dotyczące przeprowadzenie audytu końcowego:

1. Wykonawca zapewni audytora do przeprowadzenia audytu końcowego na zgodność ISO 27001, który dokona oceny funkcjonowania SZBI i przedstawi jego wyniki w raporcie z audytu.
2. Audytor musi posiadać co najmniej poniższe certyfikaty:
    a. certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku w zakresie certyfikacji osób;
    b. certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób.
3. W ramach realizacji Przedmiotu Zamówienia Zamawiający oczekuje realizacji Audytu końcowego SZBI – termin zakończenia najpóźniej na 14 dni przed końcem realizacji umowy.
4. Audyt końcowy SZBI musi obejmować zakres:
    a. Polityka i Procedury Bezpieczeństwa
        i. Przeprowadzanie analizy dokumentacji dotyczącej bezpieczeństwa IT
        ii. Sprawdzenie polityki bezpieczeństwa informacji
    b. Przegląd dokumentacji procedur bezpieczeństwa informacji i ich skuteczności w praktyce
    c. Zarządzanie Ryzykiem i Bezpieczeństwem
        i. Ocena procesów identyfikacji, oceny i zarządzania ryzykiem
        ii. Analiza skuteczności działań zapobiegawczych i kontroli ryzyka
    d. Zarządzanie Zabezpieczeniem Aktywów
        i. Ocena klasyfikacji aktywów informacyjnych oraz skuteczności ich ochrony
        ii. Przegląd procedur związanych z identyfikacją i zabezpieczaniem aktywów
    e. Bezpieczne Zarządzanie Dostępem
        i. Sprawdzenie mechanizmów kontroli dostępu do systemów i danych
        ii. Ocena skuteczności systemów uwierzytelniania i autoryzacji
    f. Kryptografia
        i. Analiza zastosowania kryptografii do ochrony poufności i integralności danych
        ii. Ocena zgodności z wymaganiami dotyczącymi stosowania kryptografii
    g. Bezpieczeństwo Fizyczne i Środowiskowe
        i. Ocena zabezpieczeń infrastruktury fizycznej i działań zapobiegawczych przeciwko awariom i katastrofom

ii. Przegląd procedur związanych z zapewnieniem bezpieczeństwa środowiskowego

h. Bezpieczeństwo Personelu
   i. Przegląd procesów selekcji, szkolenia i monitorowania personelu pod kątem bezpieczeństwa informacji
   ii. Ocena świadomości pracowników na temat polityki bezpieczeństwa informacji

i. Bezpieczne Operacje
   i. Ocena procedur dotyczących bezpiecznej eksploatacji systemów i usług
   ii. Sprawdzenie zgodności z wymaganiami dotyczącymi bezpiecznych operacji

j. Zarządzanie Komunikacją
   i. Przegląd zabezpieczeń zapewniających bezpieczny przepływ informacji wewnątrz i na zewnątrz organizacji
   ii. Ocena procedur komunikacji w kontekście bezpieczeństwa informacji

k. Zarządzanie Incydentami Bezpieczeństwa Informacji
   i. Sprawdzenie procedur reagowania na incydenty bezpieczeństwa informacji
   ii. Analiza skuteczności działań podejmowanych w przypadku incydentów

l. Monitorowanie, Przeglądy i Audyty
   i. Ocena systemu monitorowania skuteczności zarządzania bezpieczeństwem informacji
   ii. Przegląd przeprowadzonych audytów i ich wyników

m. Ciągłe Doskonalenie
   i. Analiza procesów ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji
   ii. Ocena działań podejmowanych w celu identyfikacji i eliminacji słabych punktów

n. Opracowanie raportu zawierającego opis zidentyfikowanych niezgodności oraz obserwacji wraz z rekomendacjami

o. Opracowanie rekomendowanych zmian

Zamawiającemu zapewnia się:

- Możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i /lub przez Internet.

- Czas diagnostyki do 2 godzin od zgłoszenia

  Podjęcie zgłoszenia, rozpoczęcie zdalnej diagnostyki przez certyfikowanego inżyniera i przekazanie informacji zwrotnej do Zamawiającego o przyczynie usterki. Zamawiający zapewnia współpracę pracownika urzędu na miejscu.

- Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.

- W przypadku **Awarii Krytycznej**, terminy kształtują się następująco :

Parametr SLA	Definicja	Maksymalny czas
Czas Reakcji (Diagostyka)	Podjęcie zgłoszenia, rozpoczęcie zdalnej diagnostyki przez certyfikowanego inżyniera i przekazanie informacji zwrotnej do Zamawiającego o przyczynie usterki.	**do 2 godzin** od zgłoszenia
Czas Obejścia (Tymczasowy)	Wdrożenie rozwiązania tymczasowego przywracającego kluczowe funkcje Urzędu, jeżeli ostateczna naprawa wymaga wymiany komponentów sprzętowych.	**do 2 dni roboczych** od zgłoszenia
Czas Naprawy Ostatecznej	Pełne usunięcie awarii, wymiana uszkodzonych podzespołów na fabrycznie nowe lub regenerowane przez producenta i przywrócenie stanu pierwotnego.	**do 5 dni roboczych od diagnozy)**

Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.