Załącznik nr.11A do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

wraz ze wskazaniem wymagań technicznych , użytkowych i jakościowych

odnoszących się do głównych elementów składających się na przedmiot zamówienia

NAZWA ZAMÓWIENIA:

Dostawa sprzętu informatycznego oraz oprogramowania w ramach realizacji projektu „Cyberbezpieczny samorząd w Gminie Pawonków”

Część 1 Zamówienia : Dostawa sprzętu informatycznego oraz oprogramowania

ZAMAWIAJĄCY :

Gmina Pawonków
ul. Lubliniecka 16
42-772 Pawonków

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego Cyberbezpieczny Samorząd , Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu Fundusze Europejskie Na Rozwój Cyfrowy 2021-2027 (FERC).

1. Serwer produkcyjny dla GZEAS – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera produkcyjnego dla GZEAS.

Wymagania:

1. Obudowa Tower z możliwością instalacji minimum 4 dysków 3.5".
2. Płyta główna z możliwością zainstalowania jednego procesora.
3. Chipset dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
4. Zainstalowany jeden procesor min. 12-rdzeniowy o taktowaniu min. 2.0GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 24 500 pkt. Wynik testów dla oferowanego modelu procesora muszą być dołączone do oferty.
5. Pamięć RAM min. 32GB pamięci RAM DD54 ECC RDIM 4800MHz.
6. Wbudowane porty:
    a. min. 4 porty USB w tym min. 2 porty USB 3.0
    b. min. 1 port VGA
    c. min. 1 port RJ-45 do zarządzania
7. Min. 5 aktywnych slotów PCI-E 5.0 z czego min. 2 sloty x16
8. Zintegrowana karta sieciowa z min. 2 portami Ethernet 10/100/1000 Mb/s BaseT
9. Zintegrowana karta graficzna.
10. Zainstalowany sprzętowy kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 10, 5, 50, 6, 60. Kontroler wyposażony w 4GB Cache. Kontroler powinien posiadać wsparcie dla dysków SAS, SATA oraz NVMe.
11. Zainstalowane min. 2 dyski SSD o pojemności min. 1,92 TB każdy.
12. Wbudowany wentylator zapewniający efektywne chłodzenia
13. Minimum dwa redundantne zasilacze o mocy min. 600W. W komplecie należy dostarczyć kabel zasilający o długości min. 1,8m.
14. Zainstalowany moduł TPM 2.0.
15. Zarządzanie IPMI 2.0.
16. Razem z serwerem należy dostarczyć Windows Server 2022 Standard.

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 Microsoft Active Directory;
i. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022;
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 Microsoft Active Directory;
o. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft 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.

17. Dodatkowo należy dostarczyć 10 licencji dostępowych na użytkownika.
18. Serwer musi posiadać deklarację CE.
19. Zgodność z normą ISO 9001, ISO 14001 lub równoważnymi.
20. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
21. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta lub autoryzowanego dystrybutora oferowanego serwera i

oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.

22. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 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 w trybie onsite z gwarantowanym czasem reakcji najpóźniej Next Business Day od momentu zgłoszenia usterki.
    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,
        iv. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.
23. Zakres prac wdrożeniowych:
    a. Instalacja serwera wraz z oprogramowaniem.
    b. Konfiguracja serwera i oprogramowania zgodnie z wymaganiami zamawiającego.
    c. Integracja z istniejącymi systemami IT zamawiającego.
    d. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności.
    e. Weryfikacja poprawności działania serwera oraz oprogramowania.

2. Serwer produkcyjny dla GOPS – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera produkcyjnego dla GOPS.

Wymagania:

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków 3,5”. Serwer musi posiadać możliwość rozbudowy o 2 dodatkowe wnęki dyskowe na dyski 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. Zainstalowany procesor piątej generacji min. 16-rdzeniowy o taktowaniu min. 2GHz (base frequency) umożliwiający osiągnięcie w teście SPECrate2017_fp_base wyniku dla dwóch procesorów w oferowanym serwerze min. 420 pkt. Wynik należy dołączyć do oferty.
6. Pamięć RAM min. 64GB DDR5 RDIMM 5600MT/s.
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 7 dodatkowych slotów PCI-E.
13. Zainstalowane i w pełni funkcjonalne interfejsy sieciowe:
    a. minimum 1 x RJ-45 Ethernet management port,
    b. minimum 4 porty 1Gb/s Ethernet w standardzie BaseT
    c. 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 4GB 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 M.2 Read-Intensive o pojemności min. 480 GB każdy. Dyski nie mogą zajmować kieszeni na dyski 3.5”.
    b. Zainstalowane 6 dysków serwerowych HDD SAS 10K o pojemności min. 2.4 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. 3m.

19. Bezpieczeństwo:
    a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
    b. Moduł TPM 2.0.
20. Możliwość wyposażenia serwera 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 2022 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 Microsoft Active Directory;
    i. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022;
    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 Microsoft Active Directory;
    o. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft 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. Dodatkowo należy dostarczyć 10 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.
28. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
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.
30. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 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 godziny od momentu zgłoszenia usterki.
    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. Na wezwanie Zamawiającego wymagane oświadczenie producenta oferowanego serwera, że wymagany poziom serwisu z wymaganym SLA został zaoferowany na potrzeby oferty w niniejszym postępowaniu.
    g. Na wezwanie Zamawiającego wymaganie 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.

31. Zakres prac wdrożeniowych:
    a. Instalacja serwera wraz z oprogramowaniem.
    b. Konfiguracja serwera i oprogramowania zgodnie z wymaganiami zamawiającego.
    c. Integracja z istniejącymi systemami IT zamawiającego.
    d. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności.
    e. Weryfikacja poprawności działania serwera oraz oprogramowania.

3. Serwer produkcyjny dla UG – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera produkcyjnego dla UG.

Wymagania:

1. Obudowa Rack o wysokości maksymalnie 1U z możliwością instalacji min. 8 dysków 2,5”. Serwer musi posiadać możliwość rozbudowy o 2 dodatkowe wnęki dyskowe na dyski 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. Zainstalowany procesor piątej generacji min. 16-rdzeniowy o taktowaniu min. 2GHz (base frequency) umożliwiający osiągnięcie w teście SPECrate2017_fp_base wyniku dla dwóch procesorów w oferowanym serwerze min. 420 pkt. Wynik należy dołączyć do oferty.
6. Pamięć RAM min. 64GB DDR5 RDIMM 5600MT/s.
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 2 aktywne sloty PCI-E 5.0 x16.
12. Możliwość rozbudowy o 7 dodatkowych slotów PCI-E.
13. Zainstalowane i w pełni funkcjonalne interfejsy sieciowe:
    a. minimum 1 x RJ-45 Ethernet management port,
    b. minimum 4 porty 1Gb/s Ethernet w standardzie BaseT
    c. 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 4GB 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 M.2 Read-Intensive o pojemności min. 480 GB każdy. Dyski nie mogą zajmować kieszeni na dyski 3.5”.
    b. Zainstalowane 3 dyski serwerowe HDD SAS 10K o pojemności min. 2.4 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. 3m.
19. Bezpieczeństwo:
    a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
    b. Moduł TPM 2.0.
20. Możliwość wyposażenia serwera 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 2022 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 Microsoft Active Directory;
i. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022;
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 Microsoft Active Directory;
o. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft 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. Dodatkowo należy dostarczyć 35 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.
28. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
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.
30. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 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 godziny od momentu zgłoszenia usterki.
    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. 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.
31. Zakres prac wdrożeniowych:
    a. Instalacja serwera wraz z oprogramowaniem.
    b. Konfiguracja serwera i oprogramowania zgodnie z wymaganiami zamawiającego.
    c. Integracja z istniejącymi systemami IT zamawiającego.
    d. Migracja danych z użytkowanych przez zamawiającego systemów na nowo zainstalowane środowisko
    e. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności..
    f. Weryfikacja poprawności działania serwera oraz oprogramowania.

4. Serwer do backupu dla UG – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. serwera do wirtualizacji, backupu i monitoringu infrastruktury IT.

Wymagania:

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 12 dysków 3,5”. Serwer musi posiadać możliwość rozbudowy o 4 dodatkowe wnęki dyskowe na dyski SAS/SATA/NVMe 2.5”.
2. Serwer wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych wraz z ramieniem na kable 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. Zainstalowany procesor piątej generacji min. 16-rdzeniowy o taktowaniu min. 2GHz (base frequency) umożliwiający osiągnięcie w teście SPECrate2017_fp_base wyniku dla dwóch procesorów w oferowanym serwerze min. 420 pkt. Wynik należy dołączyć do oferty.
6. Pamięć RAM min. 64GB DDR5 RDIMM 5600MT/s.
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 7 dodatkowych slotów PCI-E.
13. Zainstalowane i w pełni funkcjonalne interfejsy sieciowe:
    a. minimum 1 x RJ-45 Ethernet management port,
    b. minimum 4 porty 1Gb/s Ethernet w standardzie BaseT
    c. 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 M.2 Read-Intensive o pojemności min. 480 GB każdy. Dyski nie mogą zajmować kieszeni na dyski 3.5”.
    b. Zainstalowane 8 dysków serwerowych HDD SAS 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. 3m.
19. Bezpieczeństwo:
    a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
    b. Moduł TPM 2.0.
20. Możliwość wyposażenia serwera 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 2022 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 Microsoft Active Directory;
    i. Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022;
    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 Microsoft Active Directory;
o. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft 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. Zgodność z normą ISO 9001 lub równoważnymi.
25. Serwer musi posiadać deklarację CE.
26. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemu Microsoft Windows Server 2022.
27. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
28. 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.
29. Gwarancja:
    a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 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 godziny od momentu zgłoszenia usterki.
    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. 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.

30. Zakres prac wdrożeniowych:
    a. Instalacja serwera wraz z oprogramowaniem.
    b. Konfiguracja serwera i oprogramowania zgodnie z wymaganiami zamawiającego.
    c. Integracja z istniejącymi systemami IT zamawiającego.
    d. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności.
    e. Weryfikacja poprawności działania serwera oraz oprogramowania.

5. Oprogramowanie do backupu maszyn wirtualnych – 1 kpl.

Przedmiotem zamówienia jest dostawa oprogramowania do tworzenia kopii zapasowych oraz przywracania danych dla maszyn wirtualnych. W ramach zamówienia przewiduje się zakup licencji wieczystych na oprogramowanie umożliwiające kompleksowe zarządzanie procesem backupu oraz przywracania danych dla 10 maszyn wirtualnych ze wsparciem technicznym na minimum 24 miesięcy. Oprogramowanie ma zapewniać niezawodność, skalowalność oraz pełną integrację z istniejącą infrastrukturą wirtualną zamawiającego. Jeśli przy danym punkcie wymogu występuje informacja „jako opcja” oznacza to iż zaproponowany system posiada daną funkcjonalność, a jej uruchomienie może wymagać zakupu dodatkowych licencji – Zamawiający nie oczekuje oferty na nią a jedynie chce mieć możliwość w przyszłości rozbudowy o tę funkcjonalność.

Wymagania:

1. Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych.
2. Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia.

3. Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z częstotliwością replikacji bazy katalogowej nie dłuższym niż 15 minut (RPO nie większe niż 15 min dla uruchomienia zapasowego serwera zarządzającego). Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej trzech lokalizacji, gdzie pierwsza jest lokalizacja produkcyjną, druga i trzecia są typu standby dla serwera zarządzającego.
4. Jako opcja musi istnieć możliwość zainstalowania serwera zarządzającego na systemie operacyjnym Linux z zachowaniem możliwości replikacji bazy katalogowej i tworzeniem serwerów typu standby.
5. Możliwość jako opcja testowania (walidacja) odtwarzania serwera zarządzającego w chmurze producenta w celu weryfikacji możliwości DR w przypadku jego awarii
6. Proces przełączenia serwera zarządzającego musi umożliwiać:
    a. Przełączenie automatyczne inicjalizowane przez administratora
    b. Przełączenie automatyczne (bezobsługowe) w przypadku wykrycia awarii (w przypadku awarii serwera zarządzającego system automatycznie wykrywa awarie i przełącza działanie systemu na serwer zapasowy – standby, bez jakiejkolwiek interwencji administratora)
7. Przełączenie serwera zarządzającego musi odbywać się w pełni automatycznie poprzez administratora, który decyduje kiedy ma ono nastąpić, przełączanie serwera zarządzającego musi być możliwe pomiędzy różnymi typami infrastruktury:
    a. serwer fizyczny -> serwer fizyczny
    b. serwer fizyczny -> serwer wirtualny (onpremis)
    c. serwer fizyczny -> serwer wirtualny (AWS, Azure, Google)
    d. serwer wirtualny (onpremis) -> serwer fizyczny
    e. serwer wirtualny (onpremis) -> serwer wirtualny (onpremis)
    f. serwer wirtualny (onpremis) -> serwer wirtualny (AWS, Azure, Google)
8. Mechanizm przełączania serwera zarządzającego musi pozwalać (minimum) na wybór trybu:
    a. Test failover (testowanie mechanizmu przełączania)
    b. Failover (produkcyjne przełączenie działania na serwer standby)
    c. Maintenance failover (przełączenie w celu np. aktualizacji oprogramowania)
9. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji.
10. Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich
11. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.
12. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania i musi pozwalać na wyczyszczenie przestrzeni dyskowych (zamazanie) tak aby narzędziami niskiego poziomu nie było możliwości odzyskania tych danych.
13. Administrator systemu musi mieć możliwość wybrania (minimum) plików z danej kopii backupowej i ich skasowania, tak aby nie było możliwości ich późniejszego odtworzenia z tej kopii.

14. Dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych – funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie
    System musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie nie zdeduplikowanej (nawodnione) po to by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu
15. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej
16. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ
17. Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtenczas automatycznie zestawia połączenie tunelowe wykorzystujące tylko jeden port TCP/IP
18. System musi umożliwiać nie tylko szyfrowanie danych (kopii backupowych) ale także całej komunikacji pomiędzy komponentami systemu (minimum pomiędzy agentem backupowym a serwerem składującym i zarządzającym kopiami).
19. System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interface musi odbywać się co najmniej poprzez nazwę domeny, subnet, zakres IP
    System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN
20. System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 500 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowej przestrzeni do składowania danych poprzez dodanie dysków, półki dyskowej a nie przez wymianę urządzenia).
21. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh
22. Logiczna Globalna deduplikacja – system musi oferować deduplikację globalną co oznacza iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej
23. Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu. Niedopuszczalne jest łączenie systemu z dodatkowym oprogramowaniem czy sprzętem (appliance) dla uzyskania funkcjonalności deduplikacji danych.
24. Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB.
25. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji.
26. System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być

wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu.

27. Proces przesyłania danych (replikacji) na inny serwer systemu celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej, a więc dowolny producent serwera, dowolny producent macierzy/półki dyskowej.
28. System musi składować dane po deduplikacji (kopie backupowe) na storage obiektowym zgodnym z S3 czy to w środowisku onpremis czy cloud, musi wspierać technologię WORM na tych typach storage, transfer danych musi odbywać się z wykorzystaniem deduplikacji i muszą być wysyłane tylko unikalne bloki danych. Nie dopuszczalne jest aby tworzenie kolejnej kopii danych na storage obiektowym wymagało nawodnienia danych – transfer musi odbywać się tylko unikalnych bloków danych.
29. System musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób aby awaria pojedynczego serwera nie powodowała utraty możliwości backupu z deduplikacją i odtwarzania wcześniejszych kopii danych.
30. System musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces odtwarzania (nawadniania) zdeduplikowanych danych nie korzysta z bazy deduplikacyjnej.
31. Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) może być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu.
32. System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum Active Directory, a więc tak zwany „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną
33. Możliwość uruchomienia logowania wieloskładnikowego (SAML) dla dostępu do konsoli administracyjnej
34. System musi być odporny na tzw. „atak na wzorzec czasu”: to znaczy iż przy radykalnej zmianie czasu na serwerze zarządzającym System musi automatycznie zatrzymać co najmniej proces kasowania (ekspiracji) kopii backupowych generując odpowiednie alerty do czasu potwierdzenia tej zmiany przez administratora.
35. System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD.
36. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach
37. System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych)
38. System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail

39. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu.
40. Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem
41. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO
42. System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym zgodnymi z KMIP – minimum dla:
    a. AWS CloudHSM
    b. Fortanix Data Security Manager
    c. HashiCorp Vault
    d. IBM Security Key Lifecycle Manager (SKLM)
    e. Safenet
    f. StorMagic SvKMS
    g. Thales CipherTrust Manager
    h. Vormetric
    i. Amazon Web Services (AWS) key management service
    j. Microsoft Azure Key Vault
43. System musi umożliwiać składowanie kopii bazy katalogowej w chmurze producenta oprogramowania, funkcjonalność ta musi być w cenie produktu i pozwalać na automatyczne składowanie kopii bazy
44. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:
    a. Dedykowany dashboard będący częścią konsoli administracyjnej systemu do identyfikacji i zarządzania zagrożeniami, pozwalający administratorowi na działania proaktywne lub reaktywne w momencie wykrycia zagrożenia
    b. Monitorowanie nietypowych zachowań systemu backupowego obejmującego obszary:
        i. Czyszczenia bazy deduplikacyjnej (DDB)
        ii. Zadarzeń w Systemie (events)
        iii. Ilości nieudanych zadań
        iv. Ilości zadań czekających
        v. Ilości zadań zakończonych sukcesem
        vi. Konsoli monitorującej zadania
        vii. Czasu trwania zadań
    c. Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane
    d. Monitorowanie (jako opcja) nietypowych aktywności na serwerach plikowych
    e. Monitorowanie nietypowych aktywności na serwerach za pomocą metody: Honeypot (plików pułapek/wabików) – system cyklicznie i automatycznie sprawdza czy pliki pułapki nie były modyfikowane
    f. Monitorowanie (jako opcja) możliwego zagrożenia dotyczącego zaszyfrowania plików na serwerach
    g. Monitorowanie (jako opcja) różnych typów plików i weryfikowanie czy typ pliku jest zgodny i czytelny z nagłówkiem tego pliku (detekcja uszkodzeń plików czy ich zaszyfrowania)

h. Monitorowanie klientów Systemu i alertowanie o tych którzy tracą komunikację z Systemem
i. Air Gap (izolowanie i segmentowanie składowanych kopii backupowych) – musi polegać na wbudowanym automatycznym mechanizmie wyłączania komunikacji pomiędzy pozostałymi komponentami systemu backupowego. Tak więc komunikacja z wybranym segmentem środowiska backupowego odbywa się tylko w określonym przedziale czasowym dla potrzeb replikacji kopii backupowych, natomiast przez pozostały czas żadne procesy systemu backupowego nie mają możliwości komunikacji z tym środowiskiem.
j. Możliwość definiowania serwerów komunikacyjnych (tzw. bram/gateway) przez które wykonywana jest komunikacja pomiędzy modułami systemu backupowego, w szczególności pomiędzy serwerem zarządzającym a serwerem medii czy serwerem z dowolnym agentem backupowym
k. Możliwość definiowania kierunku inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego
l. Mechanizm WORM - możliwość zablokowania zmiany retencji (czas przechowywania kopii backupowych) na krótszą dla kopii backupowych składowanych na dowolnych typach nośników w tym na dyskach i taśmach
m. Wsparcie dla mechanizmu WORM dla macierzy obiektowych
n. MFA (Multi Factor Authentication) - uwierzytelnianie wieloskładnikowe
o. MPA (Multi Person Autorysation) – dwuosobowa autoryzacja działań (w przypadku wykonywania przez administratora systemu działania, które spowoduje skasowanie danych inna/dodatkowa osoba musi potwierdzić lub odrzucić takie działanie)

45. Identyfikacja złośliwego oprogramowania i zapobieganie ponownej infekcji dla backupów plikowych (Threat Scan) jako opcja, która skanuje pliki kopii zapasowych wykorzystując różne techniki: File Entropy, SIM Hash, Signature o funkcjonalnościach minimum:
    a. Częstotliwość aktualizacji silnika skanującego nie mniejsza niż co 24 godziny wykonywana automatycznie
    b. Manualny lub automatyczny wybór kopii backupowych zasobów plikowych do skanowania
    c. Wykrywanie zagrożeń typu malware
    d. Analiza zbackupowanych plików pod kątem zaszyfrowania
    e. Automatyczne blokowanie zainfekowanych plików z kopii backupowych przed odtwarzaniem
    f. Możliwość detekcji i odtwarzania danych historycznych nie zainfekowanych
    g. Raportowanie i zarządzanie komponentem poprzez konsolę administracyjna systemu backupowego
    h. Skanowanie danych z pierwszej (podstawowej) lub drugiej kopii backupowej
46. Identyfikacja złośliwego oprogramowania i zapobieganie ponownej infekcji dla backupów stacji roboczych (Threat Scan) jako opcja, która skanuje pliki kopii zapasowych wykorzystując różne techniki: File Entropy, SIM Hash, Signature o funkcjonalnościach minimum:
    a. Częstotliwość aktualizacji silnika skanującego nie mniejsza niż co 24 godziny wykonywana automatycznie

   b. Manualny lub automatyczny wybór kopii backupowych zasobów plikowych do skanowania
   c. Wykrywanie zagrożeń typu malware
   d. Analiza zbackupowanych plików pod kątem zaszyfrowania
   e. Automatyczne blokowanie zainfekowanych plików z kopii backupowych przed odtwarzaniem
   f. Możliwość detekcji i odtwarzania danych historycznych nie zainfekowanych
   g. Raportowanie i zarządzanie komponentem poprzez konsolę administracyjna systemu backupowego
   h. Skanowanie danych z pierwszej (podstawowej) lub drugiej kopii backupowej
47. Identyfikacja złośliwego oprogramowania i zapobieganie ponownej infekcji dla kopii backupowych maszyn wirtualnych (Threat Scan) jako opcja, która skanuje zawartość dysków zbackupowynych maszyn wirtualnych różne techniki: File Entropy, SIM Hash, Signature o funkcjonalnościach minimum:
   a. Częstotliwość aktualizacji silnika skanującego nie mniejsza niż co 24 godziny wykonywana automatycznie
   b. Manualny lub automatyczny wybór maszyny wirtualnej z kopii backupowej
   c. Skanowanie musi odbywać na odtworzonej maszynie wirtualnej
   d. Raportowanie i zarządzanie komponentem poprzez konsolę administracyjna systemu backupowego
   e. Skanowanie danych z pierwszej (podstawowej) lub drugiej kopii backupowej
48. Wszelkie działania w systemie, także działania użytkowników końcowych muszą być logowane i przechowywane
49. Integracja z systemami SOAR minimum: Microsoft Sentinel, Cortex Xsoar (dedykowany plug-in dla tych systemów)
50. System musi posiadać zaawansowane mechanizmy exportu i analizy logów poprzez Syslog serwer
51. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:
   a. Raport zmian/wzrostu środowiska systemu
   b. Raport wykorzystania licencji
   c. Raport wykonanych zadań backupowych
   d. Raporty obciążenia serwerów backupowych – minimum monitorowanie użycia CPU i pamięci RAM
52. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail
53. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV
54. Notyfikacje alertów muszą być wysyłane minimum poprzez mail.
55. System musi zapewniać funkcjonalność wznawiania zadań backupowych.
56. System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych.
57. System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe.

Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy

58. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu
59. System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków
60. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.
61. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.
62. System ma realizować procesy backupu oraz odzyskiwania danych, procesy te muszą być uruchamiane ręcznie i poprzez wbudowany kalendarz, możliwość definiowania zadań poprzez wbudowany w system kalendarz musi być możliwa nie tylko dla zadań backupowych ale także dla zadań odtwarzania danych a więc restore
63. System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane zbackupowane i zarchiwizowane już znajdujące się w systemie.
64. System musi realizować funkcjonalność weryfikacji wykonanych kopii.
65. System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:
    a. Windows
    b. Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu
66. System powinien umożliwiać składowanie kopii backupowych na storage obiektowym w chmurze, minimum: Azure, Amazon, Google Cloud, jeśli do włączenia tej funkcjonalności potrzebne są jakieś dodatkowe komponenty to muszą być zaoferowane
67. System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows
68. Możliwość backupu i odtwarzania (jako opcja) dedykowanym agentem dokumentów i maili dla Office 365 z:
    a. SharePoint Online
    b. Exchange Online
    c. OneDrive
    d. Teams
    e. Ruch pocztowy SMTP
69. Możliwość (jako opcja) pełnokontekstowego indeksowania i wyszukiwania treści (eDiscovery i Compliance Search) z danych backupowanych z:
    a. Skrzynek pocztowych (Exchange onpremis)
    b. Skrzynek journalingowych (Exchange onpremis)
    c. Ruchu pocztowego SMTP
    d. Exchange Online
    e. Serwerów plikowych
    f. Laptopów i desktopów
    g. OneDrive for Business
    h. SharePoint Online

70. System (jako opcja) musi pozwalać na wyszukiwanie danych wrażliwych (np. numery PESEL) i pozwalać osobie uprawnionej nie tylko na raportowanie takich zdarzeń ale także umożliwiać kasowanie plików nie tylko z systemów produkcyjnych ale i z kopii backupowej
71. Możliwość zwiększenia bezpieczeństwa systemu poprzez integrację z CyberArk pozwalająca na przechowywanie kont i haseł także dla aplikacji w środowisku CyberArk a nie w środowisku backupowych. Integracja musi pozwalać na rotacyjną zmianę haseł i ich synchronizację w środowisku
72. Musi istnieć możliwość wskazania klucza szyfrującego (Bring Your Own Key – BYOK), który będzie wykorzystywany do szyfrowania kopii backupowych
73. Automatyzacja – zarządzanie systemem poprzez API, Terraform, Ansible i PowerShell
74. Workflow – dedykowany komponent do tworzenia i uruchamiania procesów obejmujących działania w obszarze backupu, odtwarzania oraz pozwalający na wykonywanie poleceń czy skryptów z systemów zewnętrznych
75. Podstawowe komponenty systemu jak: serwer zarządzający, serwery składujące i deduplikujące dane muszą wspierać system operacyjny Linux, a więc musi istnieć możliwość bezpośredniego zainstalowania na systemie Linux tych komponentów bez jakiejkolwiek warstwy wirtualizacyjnej
76. System (jako opcja) musi posiadać zaawansowaną funkcjonalność analizy zasobów plikowych minimum o funkcjonalnościach:
    a. Detekcja powtarzających się zasobów
    b. Raportowanie praw dostępu do plików
    c. Raportowanie i analiza dostępu do zasobów i ich modyfikacji
    d. Możliwość kasowania plików z zasobów produkcyjnych
77. System (jako opcja) musi pozwalać na wyszukiwanie danych wrażliwych (np. numery PESEL) i pozwalać osobie uprawnionej nie tylko na raportowanie takich zdarzeń ale także umożliwiać kasowanie plików nie tylko z systemów produkcyjnych ale i z kopii backupowej
78. System musi wspierać backup całych maszyn wirtualnych/kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:
    a. Alibaba Cloud
    b. Amazon
    c. Citrix Xen
    d. Google Cloud Platform
    e. Huawei FusionCompute
    f. Microsoft Azure
    g. Microsoft Azure Stack Hub
    h. Microsoft Azure Stack HCI
    i. Microsoft Hyper-V
    j. Kubernetes
    k. Nutanix Acropolis Hypervisor (AHV)
    l. OpenStack
    m. Oracle Cloud Classic
    n. Oracle Cloud Infrastructure
    o. Oracle VM
    p. Red Hat OpenShift
    q. Red Hat Virtualization

   r. vCloud Director
   s. VMware
      To znaczy musi posiadać dedykowany komponent do backupu minimum całej maszyny wirtualnej/kontenera/aplikacji/wolumenu bez konieczności instalowania agenta wewnątrz np. maszyny z możliwością granualnego odtwarzania pojedynczych plików.
79. Dla maszyn wirtualnych musi być możliwość zainstalowania agenta plikowego i bazodanowego dla zabezpieczenia zasobów z wewnątrz maszyny wirtualnej – funkcjonalność ta musi być zawarta dla wszystkich wymaganach wirtualizatorów i być w cenie rozwiązania.
80. Przy odtwarzaniu danych środowisk kontenerowych musi istnieć możliwość selekcji zasobów podlegającym odtworzeniu
81. Dla backupu i odtwarzania środowisk wirtualnych opartych o Vmware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS
82. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.
83. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla Vmware i Hyper-V.
84. System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:
    a. Vmware do: Hyper-V, Azure, Amazon, Google Cloud Platform, Openstack, Oracle Cloud Infrastructure
    b. Hyper-V do: Azure, Amazon, Vmware
    c. Amazon do: Azure, Vmware
    d. Azure do: Amazon, Hyper-V, Vmware
       Co oznacza, iż w przypadku odtwarzania zbackupowanej maszyny wirtualnej istnieje możliwość wybrania innego wirtualizatora jako miejsce odtwarzania i uruchomienia odtworzonej maszyny wirtualnej.
85. System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V
86. System musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku:
    a. Hyper-V
    b. Vmware
87. Możliwość (jako opcja) synchronizacji maszyn wirtualnych Vmware do środowiska Amazon, Azure, Hyper-V, Vmware celem budowy rozwiązania DR (Disaster Recovery) z funkcjonalnościami:
    a. Failover (planowane i niezaplanowane/awaryjne)
    b. Failback
88. System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym

89. System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to Catalyst i urządzenie StoreOnce. Integracja z StoreOnce musi być dostępna nie tylko dla Windows ale także dla Linux i wspierać tzw. client direct (transfer danych bezpośrednio na urządzenia deduplikacyjne a tylko metadane wysyłane do systemu backupowego)
90. System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to DDBoost i urządzenie StoreOnData Domain. Integracja z Data Domain musi być dostępna nie tylko dla Windows ale także dla Linux i wspierać tzw. client direct (transfer danych bezpośrednio na urządzenia deduplikacyjne a tylko metadane wysyłane do systemu backupowego)
91. Niedopuszczalne jest aby licencjonowanie było zależne od ilości składowanych danych (kopii backupowych) na dowolnych nośnikach (np. dysk, taśma VTL…) czy to z deduplikacją czy bez.
92. Niedopuszczalne jest aby licencjonowanie było zależne od ilości komponentów środowiska backupowego, które będą wykorzystywane w procesie backupu czy odtwarzania danych.
93. Niedopuszczalne jest aby licencjonowanie zależne było od ilości serwerów fizycznych czy ich mocy (ilości procesorów) niezależnie czy dane są z nich backupowane bezpośrednio czy tworzą platformę wirtualizacyjną, która jest backupowana.
94. Zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu
95. Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na:
    a. nielimitowana ilość bibliotek taśmowych i napędów fizycznych
    b. nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google)
96. W przypadku wielu lokalizacja licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami
97. Zaoferowane licencje nie mogą mieć żadnych ograniczeń czasowych (muszą być wieczyste) dla wszystkich wymaganych funkcjonalności backupowych
98. Zaoferowane oprogramowanie musi być licencjonowane per ilość maszyn wirtualnych podlegających backupowi niezależnie czy będą wykorzystywani agenci plikowi czy bazodanowi zainstalowani wewnątrz maszyny.
99. Do dostarczonych licencji jest wymagane 24 miesięczne wparcie producenta lub autoryzowanego partnera serwisowego (pierwsza i druga linia wsparcia świadczona w języku polskim) zapewniające wsparcie techniczne w trybie 8x5 oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień.
100. Zaoferowane licencje na system muszą zapewnić backup danych z środowiska maszyn wirtualnych o ilości min. 10 sztuk.
101. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
102. Zamawiający wymaga licencji wieczystych z gwarancją i serwisem na okres minimum 24 miesięcy, z możliwością przedłużenia. Serwis powinien obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.

103. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
104. Wdrożenie:
    a. Instalacja i konfiguracja oprogramowania do backupu wskazanych maszyn wirtualnych.
    b. Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
    c. Testy funkcjonalne systemu.
    d. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.

6. Serwer plikowy (NAS) dla UG – 1 kpl.

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

Wymagania:

1. Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 12 zatokami o wielkości 3,5 cala oraz dodatkowo min. 6 zatokami o wielkości 2,5 cala.
2. Serwer wraz z kompletem szyn umożliwiających montaż w szafie rack. Maksymalna głębokość urządzenia nie powinna przekraczać 520 mm z uwagi na możliwość instalacji w kompaktowych szafach serwerowych z ograniczoną przestrzenią.
3. Zainstalowany procesor klasy x86 min. 6-rdzeniowy o taktowaniu min. 2.9GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla jednego procesora min. 16 500 pkt. Wynik testów dla oferowanego modelu procesora muszą być dołączone do oferty.
4. Pamięć RAM min. 64 GB RAM DDR4 z możliwością rozbudowy do co najmniej 128 GB bez wymiany zainstalowanych modułów.
5. Wbudowane min. 4 porty USB 3.2
6. Powyższe porty USB nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.
7. Min. 3 aktywne sloty PCI-E 3.0 umożliwiające instalację dodatkowych kart rozszerzeń, takich jak karty sieciowe 25GbE, procesory graficzne, gniazdo M2, port HDMI lub inne, które mogą zwiększyć funkcjonalność i wydajność systemu.
8. Zainstalowane i w pełni funkcjonalne minimum 2 porty Ethernet 2.5GbE RJ45 oraz 2 porty Ethernet 10GbE RJ45 z obsługą Link Aggregation w celu zwiększenia wydajności transferu i odporności na awarie. Porty nie mogą zajmować slotów PCI-E
9. Kontroler RAID umożliwiający skonfigurowanie poziomów RAID 0, 1, 5, 6, 10, 50, 60.
10. Pamięć masowa:
    a. Zainstalowane 2 dyski SSD SATA o pojemności min. 1 TB każdy, które umożliwiają korzystanie z technologii buforowania SSD w celu zapewnienia optymalnej wydajności serwera.
    b. Zainstalowane min. 8 dysków HDD SATA o pojemności min. 8 TB każdy.
11. Minimum 4 wentylatory.
12. Min. 2 identyczne zasilacze o mocy min. 550W zainstalowane wewnątrz serwera, pracujące redundantni w celu zapewnienia ciągłości pracy w przypadku awarii jednego z nich.
13. Urządzenie powinno oferować zaawansowane funkcje zabezpieczeń, takie jak szyfrowanie AES-NI, dwustopniowe uwierzytelnianie, zapora sieciowa, oraz ochrona przed atakami typu brute-force.
14. Diody LED umieszczone z przodu obudowy serwera informujące o statusie: dysków, portów LAN, portów USB i zasilaniu.

15. 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.
h. Wykonawca powinien zapewnić wsparcie techniczne oraz dostęp do aktualizacji oprogramowania przez okres minimum 3 lat od daty dostawy. Wsparcie powinno obejmować pomoc w instalacji, konfiguracji, oraz rozwiązywaniu problemów związanych z działaniem oprogramowania.

16. Wraz ze serwerem dostarczone powinno być oprogramowanie na stacje robocze i serwery fizyczne 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.
17. Zgodność z normą ISO 9001 lub równoważnymi.
18. Serwer musi posiadać deklaracja CE.
19. Zainstalowany specjalistyczny system operacyjny przeznaczony dla serwerów do przechowywania danych, oferujący zaawansowane funkcje takie jak: zarządzanie plikami, wirtualizacja, obsługa kontenerów, backup, synchronizacja z chmurą, oraz wsparcie dla wielu użytkowników z zaawansowanymi ustawieniami uprawnień.
20. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
21. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego serwera i oprogramowania, potwierdzające, że serwer jest fabrycznie nowy i pochodzi z oficjalnego kanału dystrybucyjnego producenta.
22. Serwer musi być kompatybilny z popularnymi systemami backupu oraz oprogramowaniem do wirtualizacji, takimi jak Vmware i Hyper-V.
23. Gwarancja:
   a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 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,
24. Zakres prac wdrożeniowych:
   a. Instalacja serwera oraz oprogramowania oprogramowanie do tworzenia i zarządzania kopiami zapasowymi na serwerze.
   b. Konfiguracja dysków SSD w RAID 1 oraz dysków HDD w RAID 5.
   c. Konfiguracja zabezpieczeń.
   d. Konfiguracja serwera oraz oprogramowania zgodnie z wymaganiami zamawiającego.
   e. Integracja z istniejącymi systemami IT zamawiającego.

f. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności..
g. Weryfikacja poprawności działania serwera wraz z oprogramowaniem.

7. Switch dostępowy 48p. – 1 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. przełącznika dostępowego klasy Enterprise.

Wymagania:

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
    a. możliwość montażu w stelażu/szafie 19”
    b. wysokość maksymalna 1U
    c. głębokość bez zainstalowanego zasilacza nie większa niż 25 cm
    d. minimum jeden zasilacz 230V AC
    e. zakres temperatur pracy ciągłej co najmniej od -5°C do +45 °C
    f. zakres wilgotności pracy co najmniej 5% - 95%
    g. waga bez zainstalowanego zasilacza nie większa niż 3,5 kg
3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:
    a. 48 portów 100/1000BASE-T
    b. 4 porty 1GE SFP
4. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
5. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
    a. Zarządzanie stosem poprzez jeden adres IP
    b. Do min. 9 jednostek w stosie
    c. Porty do stackowania mogą być współdzielone z portami typu uplink.
    d. Magistrala stackująca o wydajności minimum 16Gb/s
    e. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
    f. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
    g. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
    h. W stosie musi być możliwość budowania stosu pomiędzy wszystkimi przełącznikami w ramach tego postępowania
6. Układ przełączający o wydajności min. 104 Gbps, wydajność przełączania przynajmniej 78 Mpps
7. Obsługa min. 16 000 adresów MAC
8. Wbudowana pamięć RAM min. 512MB.
9. Procesor min. 800MHz
10. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 256MB
11. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
12. Możliwość skonfigurowania min. 32 interfejsów vlan działających równocześnie
13. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad

14. Obsługa minimum 120 grup LAG
15. Obsługa ramek jumbo
16. Obsługa sFlow
17. Wsparcie dla G.8032 ERPS
18. Obsługa protokołu VRRP
19. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP)
20. Wsparcie dla mechanizmu PVST
21. Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.
22. Obsługa min. 1 000 tras dla routingu IPv4
23. Obsługa min. 230 tras dla routingu IPv6
24. Obsługa min. 230 IPv6 neighbor discovery (ND)
25. Obsługa protokołów związanych z obsługą ruchu typu multicast:
    a. IGMP Snooping
    b. PIM Snooping
    c. MLD Snooping
    d. minimum 1000 tras multicast dla IPv4
26. Minimalny rozmiar tablicy ARP 1000 wpisów
27. Obsługa protokołów LLDP i LLDP-MED.
28. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client
29. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
    a. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
    b. wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR
30. Wymagane opcje zarządzania:
    a. możliwość lokalnej obserwacji ruchu na określonym porcie
    b. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)
    c. wsparcie dla skyptów python uruchamianych na urządzeniu
    d. wsparcie dla RMON
31. Wraz z urządzeniami muszą zostać dostarczone:
    a. pełna dokumentacja w języku polskim lub angielskim
    b. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana
32. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 12 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
33. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta..
34. Zamawiający wymaga, aby urządzenia posiadały 36 miesięczny serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu

zamówienia. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
35. Usługa serwisu musi być świadczona w języku polskim.
36. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.
37. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.
38. System centralnego zarządzania może być dostarczony w formie:
    a. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej
    b. Lub dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.
39. Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.
40. W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.
41. System centralnego zarządzania musi umożliwiać:
    a. tworzenie VLANów
    b. ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu
    c. tworzenie połączeń zagregowanych
    d. monitorowanie statusu pracy przełącznika i portów
    e. możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania
    f. możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego
    g. interfejs do zarządzania w języku polskim lub angielskim
42. Zakres prac
    a. Instalacja przełącznika oraz podłączenie do sieci.
    b. Konfiguracja przełącznika zgodnie z wymaganiami zamawiającego.
    c. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności.
    d. Weryfikacja poprawności działania przełącznika.

8. UPS dla GZEAS – 1 szt.

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

Wymagania:

1. MOC min. 1500VA/1500W
2. Obudowa Tower.
3. Topologia Line-interactive
4. Kształt napięcia w trybie bateryjnym: Czyste napięcie sinusoidalne
5. Czas przełączania do 4ms
6. Czas ładowania akumulatorów do 3 godzin
7. Możliwość podłączenia dodatkowych modułów bateryjnych
8. Czas podtrzymania UPSa dla obciążenia 900 W minimum 14 minut.
9. Możliwość rozbudowy systemu do uzyskania podtrzymania min. 12 godzin dla w/w obciążenia
10. Ilość gniazd wyjściowych C13: co najmniej 10

11. UPS musi posiadać wydzieloną grupę gniazd dla obciążeń kluczowych/krytycznych oraz dla pozostałych obciążeń .
12. Porty komunikacyjne: USB/RS232/EPO/Dry contact
13. Komunikacja po protokole SNMP oraz http
14. Oprogramowanie w języku polskim do zarządzania UPSem z możliwością monitorowania zużycia energii oraz współpracy ze środowiskiem VMware ESXi 8.0 U2
15. Rozproszenie ciepła online do 75 BTU/h
16. Gwarancja min. 24 miesiące
17. Urządzenie i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na zlecenie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego UPSa, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
18. Zakres prac wdrożeniowych:
    a. Instalacja UPS oraz podłączenie do wskazanych serwerów oraz urządzeń.
    b. Konfiguracja UPS zgodnie z wymaganiami zamawiającego.
    c. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności.
    d. Weryfikacja poprawności działania UPS.

9. UPS dla GOPS – 1 szt.

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

Wymagania:

1. MOC min. 3000VA/3000W
2. Obudowa Rack o wysokości max. 2U
3. Topologia Line-interactive
4. Kształt napięcia w trybie bateryjnym: Czyste napięcie sinusoidalne
5. Czas przełączania do 4ms
6. Czas ładowania akumulatorów do 3 godzin
7. Możliwość podłączenia dodatkowych modułów bateryjnych
8. Czas podtrzymania systemu dla obciążenia 2000 W minimum 12 minut przy wykorzystaniu przestrzeni w szafie rack max. 4U dla UPSa i modułów bateryjnych łącznie.
9. Możliwość rozbudowy systemu do uzyskania podtrzymania minimum 160 minut dla w/w obciążenia
10. Ilość gniazd wyjściowych C13: co najmniej 6
11. Ilość gniazd wyjściowych C19: co najmniej 2
12. UPS musi posiadać wydzieloną grupę gniazd dla obciążeń kluczowych/krytycznych oraz dla pozostałych obciążeń.
13. Porty komunikacyjne: USB/RS232/EPO/Dry contact
14. Komunikacja po protokole SNMP oraz http
15. Oprogramowanie w języku polskim do zarządzania UPSem z możliwością monitorowania zużycia energii oraz współpracy ze środowiskiem VMware ESXi 8.0 U2
16. Rozproszenie ciepła online (BTU/h) – do 125 BTU/h
17. Gwarancja min. 24 miesiące.
18. Urządzenie i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego UPSa, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
19. Zakres prac wdrożeniowych:
    a. Instalacja UPS oraz podłączenie do wskazanych serwerów oraz urządzeń.
    b. Konfiguracja UPS zgodnie z wymaganiami zamawiającego.

c. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności.
d. Weryfikacja poprawności działania UPS.

10. Oprogramowanie do zbierania i analizy logów – 1 kpl.
Przedmiotem zamówienia jest dostawa oprogramowania do zbierania logów, skanowania podatności oraz analizy danych i incydentów z całej infrastruktury IT. Zamówienie obejmuje dostawę licencji wieczystej ze wsparciem technicznym na minimum 24 miesiące. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie.

Wymagania:
1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
2. System musi pracować w oparciu o architekturę Linux.
3. System musi mieć możliwość centralnego zbierania i zarządzania logami
4. System działać w trybie zbliżonym do rzeczywistego
5. System musi umożliwiać funkcjonowanie bez dostępu do sieci Internet
6. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu.
7. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
8. System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20 GB danych dziennie
9. System musi zapewniać retencję danych w okresie minimum 365 dni.
10. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
11. Licencja na oferowany system nie może ograniczać ilości źródeł danych, z których pobierane są dane i zdarzenia.
12. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
13. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
14. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
15. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
16. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu .
17. Komunikacja pomiędzy komponentami systemu odpowiadającymi za agregacji, retencję i wizualizację danych musi odbywać się w sposób szyfrowany z wykorzystaniem protokołu TLS w wersji minimum 1.3.
18. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
19. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
20. Interfejs musi posiadać polską wersję językową.

21. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
22. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
23. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius
24. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
25. System musi wspierać mechanizm logowania typu Single Sign On.
26. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
27. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
28. System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
29. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
30. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
31. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
32. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
33. System musi pozwalać na tworzenie parserów z poziomu GUI
34. System musi umożliwiać predykcję danych w oparciu o dowolne dane historyczne zgromadzone w systemie.
35. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
36. System musi być wyposażony w zaawansowane metody analizy danych oparte na algorytmach sztucznej inteligencji.
37. Algorytmy sztucznej inteligencji muszą umożliwiać przewidywanie zachowań systemu poprzez zrozumienie liczby generowanych zdarzeń oraz wartości liczbowych w tych zdarzeniach, takich jak wysłane bajty (sent_bytes), rozmiar pliku (file_size) i czas trwania sesji (session_duration).
38. Algorytmy sztucznej inteligencji muszą wspierać pracę operatora w wykrywaniu anomalii w danych: pojedynczego parametru liczbowego, wielu parametrów liczbowych, tekstu oraz danych mieszanych. Oczekuje się, że wykrywanie anomalii będzie połączone z obliczaniem punktów, co umożliwi operatorowi skoncentrowanie swojej pracy na zdarzeniach o najwyższych wynikach.
39. Algorytmy sztucznej inteligencji muszą umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.

40. Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
41. Algorytmy sztucznej inteligencji musi umożliwiać nienadzorowane, dynamiczne grupowanie zdarzeń na podstawie ich wspólnych cech. Dodatkową wartością będzie możliwość graficznej wizualizacji zdarzeń tworzących większe lub mniejsze grupy, aby izolowane zdarzenia można było łatwo zidentyfikować.
42. Wykrywanie anomalii musi umożliwiać tworzenie reguł detekcji, aby możliwa była szybka reakcja w sytuacjach, które się pojawiają.
43. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
44. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
45. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
46. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
47. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:
    a. Syslog,
    b. WEF,
    c. Flat file,
    d. Event log,
    e. WMI,
    f. SNMP trap,
    g. XML,
    h. JSON,
    i. JDBC/ODBC
    j. CSV,
    k. Email,

    Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.
48. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
49. System musi umożliwiać gromadzenie danych z baz danych relacyjnych, NoSQL, czasu rzeczywistego, m.in. MSSQL, Oracle, PostgreSQL, SQL Server, MongoDB, Apache Cassandra, InfluxDB i Apache Kafka
50. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
51. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
52. Operacja z rekordami bazy danych musza być wykonywane jedynie za pomocą składni JSON z wykorzystaniem udokumentowanego API.
53. Wykorzystanie bazy danych musi odbywać się za pomocą REST API z pominięciem wykorzystania klienta typu SQL client.
54. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.

55. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
56. System musi posiadać predefiniowany zestaw parserów zdarzeń.
57. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
58. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
59. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
60. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
61. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
62. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
63. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
64. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
65. System musi posiadać wbudowany komponent budowania elektronicznej dokumentacji z możliwością ręcznego i automatycznego dodawania treści oraz uzupełniania jej o wartości pochodzące ze zgromadzonych w Systemie danych.
66. Komponent budowania elektronicznej dokumentacji musi mieć możliwość m.in. tworzenia lub dodawania diagramów architektury zasobów informatycznych, tabel oraz list.
67. System musi umożliwiać łączenie wyników dwóch niezależnych zapytań w postaci jednej odpowiedzi, bez użycia składni SQL.
68. System musi posiadać interfejs umożliwiający zmianę wybranej wartości w zgromadzonych danych.
69. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
70. System musi umożliwiać budowanie zapytań z wykorzystaniem składni SQL.
71. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
72. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
73. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
    a. Wykrycia dowolnej treści w logach,
    b. Wykrycia wystąpienia wartości pola na wybranej liście,
    c. Wykrycia niewystępowania wartości pola na wybranej liście,
    d. Wykrycia zmiany jednego z kilku pól,

e. Wykrycia zdarzeń występujących z zadaną częstotliwością,
f. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
g. Wykrycia zaniku Wiadomości,
h. Wykrycia nowej wartości pola w zadanym okresie czasu,
i. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności

74. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów
75. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
76. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
77. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
78. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
79. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
80. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
81. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
82. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
83. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
84. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
85. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
86. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
87. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
88. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
89. System musi posiadać wbudowany, dostepny z poziomu GUI moduł tworzenia i edycji elektronicznej dokumentacji bazującej oraz wzbogacającej dane gromadzone ze środowiska informatycznego.
90. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.

91. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
92. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
93. System musi dostarczony z licencją wieczystą oraz wsparciem producenta na okres minimum 24 miesięcy.
94. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
95. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
96. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
97. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
98. System musi być dostarczony z repozytorium danych IoC utrzymywanym i rozwijanym przez producenta.
99. System musi umożliwiać integrację z Mitre ATT@CK.
100. System musi posiadać bazę minimum 700 predefiniowanych reguł korelacyjnych
101. System musi dostarczać funkcjonalność badania integralności plików i rejestrach na monitorowanych hostach, w tym: monitorowanie zmian na zawartości plików i katalogów, zmiany uprawnień dostępu do pliku, zmiany w atrybutach plików oraz zmian na sumach kontrolnych MD5 i SHA1.
102. System musi posiadać funkcjonalność monitorowania konfiguracji systemów oraz aplikacji w celu zapewnienia zgodności z politykami i standardami bezpieczeństwa oraz praktykami dotyczącymi hardeningu, takimi jak CIS Benchmark.
103. System musi posiadać gotowe wizualizacje i polityki zgodności z GDPR, PCI-DSS, NIST.
104. System musi posiadać możliwość skanowania środowiska pod kątem detekcji rootkit'u i wykrywania ukrytych procesów, plików, portów
105. System musi posiadać funkcjonalności skanowania podatności dla aplikacji oraz systemów operacyjnych Linux i Windows
106. System musi posiadać funkcjonalność ciągłego śledzenia polityk OpenSCAP
107. System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
108. Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
109. Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online.
110. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.
111. Dokumentacja techniczna i baza wiedzy dotycząca oferowanego systemu musi być opublikowana na ogólnodostepnej stronie internetowej producenta.
112. Producent systemu musi umożliwiać rozbudowę oferowanego rozwiązania o moduł funkcjonalny SOAR lub zapewnić gotową integrację z systemem SOAR tego samego producenta.
113. W komplecie należy dostarczyć oprogramowanie do monitorowania infrastruktury IT. Oprogramowanie ma zapewnić kompleksową kontrolę nad zasobami sieciowymi, serwerami, aplikacjami oraz usługami IT oraz pełne wsparcie dla operacji IT, wczesne

wykrywanie problemów, automatyzację zadań oraz zapewnienie wysokiej dostępności i wydajności infrastruktury. System musi być dostarczony z licencją bezterminową dla 50 hostów/adresów IP o poniższej funkcjonalności:

a. Monitorowanie serwerów i urządzeń sieciowych:
    i. Możliwość monitorowania różnorodnych systemów operacyjnych (Windows, Linux, Unix).
    ii. Obsługa monitorowania urządzeń sieciowych (routery, switchy, firewalle).
    iii. Monitorowanie zasobów fizycznych (CPU, pamięć, dyski twarde).
b. Monitorowanie aplikacji i usług:
    i. Monitorowanie dostępności i wydajności aplikacji webowych oraz baz danych.
    ii. Wsparcie dla monitorowania aplikacji chmurowych (AWS, Azure, Google Cloud).
    iii. Możliwość monitorowania usług takich jak HTTP, HTTPS, FTP, SMTP, DNS itp.
c. Monitorowanie użytkowników i aplikacji www:
    i. Realizacja automatycznych testów pracy użytkownika w aplikacji www
    ii. Monitorowanie wydajności aplikacji z perspektywy użytkownika końcowego.
    iii. Kontrola międzyczasów podstron/kroków scenariusza pracy użytkownika aplikacji www.
d. Alertowanie i powiadomienia:
    i. Definiowanie progów alarmowych i automatyczne powiadamianie (e-mail, SMS, powiadomienia PUSH).
    ii. Możliwość konfiguracji alertów w zależności od krytyczności incydentu.
    iii. Integracja z systemami zarządzania incydentami (ITSM).
    iv. Eskalacja powiadomień
e. Raportowanie i analiza danych
    i. Generowanie raportów dotyczących dostępności, wydajności oraz wykorzystania zasobów.
    ii. Wizualizacja danych w postaci wykresów i dashboardów.
    iii. Możliwość eksportu raportów do formatów takich jak PDF, CSV.
    iv. Tworzenie i modyfikacja raportów za pośrednictwem interfejsu WWW bez konieczności instalacji dodatkowego oprogramowania (poza przeglądarką i ew. technologiami Java, Flash itp.).
    v. Narzędzie raportujące musi umożliwiać automatyczną generację dowolnych raportów według zdefiniowanego harmonogramu, możliwość generowania raportów dostępności (wg hostów lub usług), raportów SLA (wg hostów lub usług), raportowanie incydentów, awarii itp., raportowanie wydajności sieci, zapis raportów do plików PDF, okresowe wysyłanie raportów e-mailem do wskazanych użytkowników, powiadomienia e-mail o incydencie, zapis zdefiniowanych parametrów raportów celem późniejszego wywołania.
f. Automatyzacja i orkiestracja
    i. Automatyczna konfiguracja nowych urządzeń
    ii. Automatyczne wykonywanie skryptów w odpowiedzi na zdarzenia.

iii. Integracja z narzędziami do zarządzania konfiguracją (Ansible, Puppet, Chef).
iv. Możliwość definiowania i uruchamiania zadań uwzględniając harmonogram dni i godzin.

g. Bezpieczeństwo i audyt
   i. Zapewnienie szyfrowanej komunikacji między komponentami systemu.
   ii. Monitorowanie i audytowanie zdarzeń związanych z bezpieczeństwem.
   iii. Wbudowany mechanizm tworzenia kopii zapasowych ustawień systemu (monitorowane hosty i usługi).
   iv. Wbudowany mechanizm zarządzania użytkownikami systemu.
   v. Możliwość tworzenia grup użytkowników.
   vi. Historia danych statystycznych.
   vii. Mechanizm przydzielania uprawnień użytkowników (dostęp do danych nt. hostów lub usług, możliwość konfiguracji obiektów, powiadomienia).
   viii. Audyt pracy uzytkownika w systemie
h. Integracje i API
   i. Otwarte API umożliwiające integrację z innymi systemami.
   ii. Wsparcie dla integracji z popularnymi narzędziami do zarządzania IT (np. ServiceNow, Jira).
   iii. Natywna integracja z systemami do centralnego gromadzenia logów i analizy zdarzeń opartymi o architekturę Elasticsearch, Opensearch
   iv. Natywna integracja z systemami klasy SOAR
   v. Możliwość korzystania z webhooków do przesyłania danych w czasie rzeczywistym.
   vi. Możliwość konfiguracji oprogramowania poprzez stronę www oraz programistyczne, udokumentowane API.
i. Interfejs użytkownika
   i. Interfejs graficzny do wizualizacji struktury sieci.
   ii. Interfejs graficzny do wizualizacji poszczególnych wybranych parametrów urządzeń.
   iii. Przyjazny i intuicyjny interfejs webowy dostępny z poziomu przeglądarki.
   iv. Możliwość personalizacji podstawowego ekranu aplikacji w powiązaniu z użytkownikiem systemu oraz dowolnej konfiguracji składników wyświetlanych na podstawowym ekranie aplikacji poprzez wybór odpowiednich widget'ów.
   v. Możliwość tworzenia wielu dashboardów
   vi. Możliwość tworzenia dashboardów prywatnych jak i współdzielnych pomiędzy innymi użytkownikami aplikacji
   vii. Możliwość tworzenia dashboardów typu iFrame - będącymi oknem aplikacji zewnętrznych
   viii. Możliwość tworzenia własnych dodatków do dashboardów w formie obietków programistycznych typu Widget. Aplikacja musi wspierać dodawanie własnych rozszerzeń do dashboardów.
   ix. Wsparcie dla systemów mobilnych (Android, iOS) w zakresie powiadomień push.
   x. Możliwość tworzenia i zapisywania filtrów dla monitorowanych urządzeń i ich parametrów

xi. Możliwość wykorzystania filtrów podczas tworzenia dashboardów

j. Monitorowanie specyficznych parametrów i elementów infrastruktury:
   i. Monitorowanie podstawowych parametrów sprzętowych bez użycia dodatkowych agentów oraz pozostałych parametrów działania systemu operacyjnego i usług za pomocą dedykowanych agentów (w zależności od konfiguracji monitorowanego hosta).
   ii. Możliwość monitorowania aplikacji i procesów o dynamicznym zachowaniu.
   iii. Możliwość monitorowania min. krytycznych elementów infrastruktury, aplikacji, usług sieciowych, protokołów sieciowych, wskaźników systemowych, infrastruktury sieciowej, portów.
   iv. Możliwość śledzenia parametrów takich jak:
      A. Telnet na wybrany port - nasłuch na porcie,
      B. Ping dostępność urządzenia,
      C. Odczyt, przetwarzanie i generowanie alertów z pułapek SNMP,
      D. Poprawne działanie serwera DHCP,
      E. Poprawne działanie serwera czasu NTP,
      F. Zajętość danych na poszczególnych partycjach,
      G. Zajętość RAM,
      H. Obciążenie systemu,
      I. Obciążenie dysków,
      J. Ilość zalogowanych użytkowników,
      K. Ilość procesów,
      L. Obecność procesów w systemie,
      M. Synchronizacja dysków programowego RAID,
      N. Synchronizacja dysków sprzętowego RAID,
      O. Kontrola parametrów polecenia VMSTAT,
      P. Obecność SSH.
   v. Możliwość śledzenia parametrów monitoringu systemu poczty:
      A. Poprawne działanie serwera SMTP,
      B. Poprawne działanie serwera POP3,
      C. Poprawne działanie serwera IMAP,
      D. Ilość listów w kolejkach serwera Postfix.
   vi. Możliwość śledzenia parametrów monitoringu DNS:
      A. Poprawne działanie DNS,
      B. Rozwiązywanie zadanych domen na adresy IP,
      C. Parametry serwerów WWW,
      D. Poprawne działanie serwera WWW,
      E. Kontrola występowania oczekiwanych treści na stronie,
      F. Czas odpowiedzi serwera WWW.
   vii. Możliwość śledzenia parametrów monitoringu bazy danych:
      A. Poprawna praca bazy,
      B. Kontrola stanu synchronizacji baz,
      C. Zajętość przestrzeni danych.
   viii. Możliwość śledzenia parametrów DRBD i HEARTBEAT:
      A. Poprawne działanie klastra,
      Poprawne działanie replikacji danych.

ix. Możliwość śledzenia parametrów macierzy dyskowych:
    A. Analiza statusów ogólnych urządzenia,
    B. Analiza dysków urządzenia.
    C. Dodatkowe Elementy Infrastruktury Informatycznej do Monitorowania
x. Monitorowanie zasobów wirtualnych (maszyny wirtualne, hypervisory).
xi. Monitorowanie infrastruktury kontenerowej (Docker, Kubernetes).
xii. Monitorowanie systemów backupowych i urządzeń magazynujących.
xiii. Monitorowanie systemów IoT i urządzeń edge computing.
xiv. Monitorowanie systemów SCADA i przemysłowych systemów sterowania.
xv. Monitorowanie infrastruktury zasilania (UPS, generatory).
xvi. Monitorowanie systemów HVAC (Heating, Ventilation, and Air Conditioning).

k. Architektura Systemu
    i. System musi działać w modelu klient-serwer.
    ii. System pracuje pod kontrolą środowiska systemu operacyjnego Open Source.
    iii. Możliwość wdrożenia systemu zarówno on-premises, jak i w chmurze.
    iv. Wsparcie dla skalowalności poziomej i pionowej.
    v. System musi wspierać architekturę wysokiej dostępności dla każdej warstwy systemu.
l. System musi umożliwić rozbudowę, pozwalającą na monitorowanie nieograniczonej wydajnością liczby urządzeń w sieci. Architektura musi umożliwiać rozkładanie obciążenia pomiędzy elementy systemu.
   Wymagania dotyczące składowania danych
    i. Możliwość replikacji i backupu danych.
    ii. Gromadzone dane muszą musza być składowane w nierelacyjnej bazy danych.
m. Wymagania dotyczące zgodności
    i. Wsparcie dla systemów mobilnych (Android, iOS) w zakresie powiadomień.
n. Dostępność szczegółowej dokumentacji technicznej w języku polskim dla administratorów systemu.

114. Wdrożenie:
    a. Instalacja i konfiguracja oprogramowania do zbierania logów, skanowania podatności oraz analizy danych i incydentów z całej infrastruktury IT.
    b. Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
    c. Testy funkcjonalne systemu.
    d. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.
    e. Przeprowadzenie szkolenia w siedzibie klienta z obsługi wdrożonego oprogramowania trwającego minimum 2 godziny.
115. Zamawiający wymaga licencji wieczystych z gwarancją i serwisem na okres minimum 24 miesięcy, z możliwością przedłużenia. Serwis powinien obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.
116. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta

oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

11. Firewall z UTM – 1 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. zapory sieciowej z pakietem bezpieczeństwa UTM które zapewnia zaawansowaną ochronę w infrastrukturze informatycznej zamawiającego. Zamówienie obejmuje zarówno dostawę urządzenia fizycznego firewall jak i licencji na oprogramowanie UTM na minimum 24 miesiące oraz usługi wdrożeniowe, dlatego wymagane jest uwzględnienie wszystkich elementów w ofercie.

Wymagania:

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
13. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
14. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
16. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.

17. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
18. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
19. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
20. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
21. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
22. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
23. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
24. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
25. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
26. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
27. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
28. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
29. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
30. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
31. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
32. Ochrona antyspam ma działać w oparciu o:
    a. białe/czarne listy,
    b. DNS RBL,
    c. Skaner heurystyczny.
33. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
34. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
35. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
36. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
    a. PPTP VPN,
    b. IPSec VPN,
    c. SSL VPN.
37. SSL VPN ma działać co najmniej w trybach tunelu i portalu.

38. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
39. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
40. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
41. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
42. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
43. Urządzenie ma posiadać wbudowany filtr URL.
44. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
45. Administrator ma mieć możliwość dodawania własnych kategorii URL.
46. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
    a. blokowanie dostępu do adresu URL,
    b. zezwolenie na dostęp do adresu URL,
    c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
47. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
48. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
49. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
50. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
51. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
52. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
53. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
    a. lokalną bazę użytkowników (wewnętrzny LDAP),
    b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
    c. usługę katalogową Microsoft Active Directory.
54. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
55. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
    a. SSL,
    b. Radius,
    c. Kerberos.
56. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
57. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
58. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
59. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
60. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).

61. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
62. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
63. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
    a. równoważenie względem adresu źródłowego,
    b. równoważenie względem połączenia.
64. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
65. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
66. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
67. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
68. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
69. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
70. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
71. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
72. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
73. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
74. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
75. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
76. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
77. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
78. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
79. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
80. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
81. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
82. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
83. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.

84. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
85. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
86. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
87. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
88. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
89. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    a. manualnego eksportu do pliku w dowolnym momencie czasu,
    b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
90. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
91. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
92. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
93. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
94. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
95. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
96. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
97. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
98. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
99. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
100. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
101. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
102. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
103. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
104. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
105. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
106. Urządzenie ma posiadać usługę DNS Proxy.
107. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
108. Urządzenie musi mieć zaimplementowane Open API

109. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
110. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
111. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
112. Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
113. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
114. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
115. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
116. Liczba portów Ethernet 2,5Gbps – min. 8.
117. Liczba portów światłowodowych 1Gbps – min. 1.
118. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
119. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
120. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
121. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
122. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
123. Maksymalna liczba tuneli VPN IPSec – minimum 100.
124. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
125. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
126. Obsługa interfejsów 802.11q (VLAN) – minimum 128
127. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
128. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
129. Urządzenie nie ma limitu na liczbę użytkowników.
130. Liczba reguł filtrowania – minimum 8 192.
131. Liczba tras statycznego routingu – minimum 512.
132. Liczba tras dynamicznego routingu – minimum 10 000.
133. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
134. Urządzenie musi być wyposażone w moduł TPM.
135. Gwarancja
    a. Urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 12 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także muszą być objęte serwisem producenta na terenie RP.
    b. Urządzenia objęte minimum 24 miesięcznym okresem gwarancji.
    c. Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta.
    d. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.

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,

iv. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.

136. Zakres prac wdrożeniowych:

a. Instalacja urządzeń firewall wraz z oprogramowaniem UTM.

b. Konfiguracja urządzeń i oprogramowania UTM zgodnie z wymaganiami zamawiającego.

c. Integracja z istniejącymi systemami IT zamawiającego.

d. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności.

e. Weryfikacja poprawności działania urządzeń firewall oraz oprogramowania UTM.

12. Oprogramowanie antywirusowe – 1 kpl.

Przedmiotem zamówienia jest zakup licencji na oprogramowanie antywirusowe na 50 stanowisk komputerowych wraz z możliwością centralnego zarządzania oraz wsparciem technicznym na 24 miesiące.

Wymagania:

1. Ochrona antywirusowa i antymalware

a. Wykrywanie i usuwanie wirusów, trojanów, robaków, spyware, rootkitów oraz innego złośliwego oprogramowania.

b. Ochrona w czasie rzeczywistym poprzez analizę heurystyczną i skanowanie behawioralne.

c. Skanowanie na żądanie oraz zaplanowane skanowanie systemu.

d. Automatyczna aktualizacja bazy sygnatur wirusów oraz silników skanujących.

2. Ochrona sieci i urządzeń końcowych

a. Monitorowanie ruchu sieciowego oraz ochrona przed atakami z sieci (IDS/IPS).

b. Kontrola dostępu do urządzeń peryferyjnych (np. USB, dyski zewnętrzne).

c. Blokowanie podejrzanych adresów URL i złośliwych stron internetowych.

d. Ochrona przed atakami ransomware i phishingiem.

3. Centralne zarządzanie

a. Możliwość centralnego zarządzania wszystkimi chronionymi urządzeniami za pomocą konsoli administracyjnej.

b. Generowanie raportów i statystyk dotyczących wykrytych zagrożeń i działania systemu ochrony.

c. Możliwość zdalnej instalacji i konfiguracji polityki bezpieczeństwa.

4. Kompatybilność i wymagania systemowe

a. Wsparcie dla systemów operacyjnych Windows, Linux oraz macOS.

b. Możliwość integracji z Active Directory w celu uproszczenia zarządzania użytkownikami.

c. Niskie zużycie zasobów systemowych, aby nie wpływać na wydajność urządzeń końcowych.

5. Wsparcie techniczne i aktualizacje

a. Licencja powinna obejmować dostęp do aktualizacji oprogramowania oraz bazy sygnatur wirusów przez cały okres jej obowiązywania.

b. Możliwość kontaktu z producentem lub dystrybutorem w celu uzyskania wsparcia technicznego w języku polskim.

6. Licencja powinna być dostarczona w formie elektronicznej wraz z instrukcjami aktywacji.
7. Oprogramowanie musi być legalne i pochodzić z oficjalnej dystrybucji producenta.
8. Możliwość rozszerzenia licencji w przyszłości o dodatkowe stanowiska.
9. Licencja na oprogramowanie powinna być ważna przez okres 24 miesiące od daty aktywacji, z możliwością jej przedłużenia.
10. Oprogramowanie musi obejmować 50 stanowisk komputerowych.