Załącznik nr 8 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Serwer – 1 szt.

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

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 oraz przednim panelem zamykanym 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. Zainstalowana dwa procesory min. 16-rdzeniowe o taktowaniu min. 2.7GHz (base frequency) umożliwiający osiągnięcie w teście PassMark – CPU Mark wyniku dla dwóch procesorów min. 72500 pkt. Wynik należy dołączyć do oferty.

6. Pamięć RAM min. 256 GB RAM DDR5 RDIMM 5600MT/s, w modułach po 64 GB RAM.

7. Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci RAM.

8. Zabezpieczenie pamięci:

a. Memory mirroring

b. ECC

c. patrol scrubbing

d. SDDC

e. memory thermal throttling

f. ADDDC-SR

g. PPR

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).

h. Memory SMBus hang recovery.

9. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200

10. Wbudowane porty:

a. 5 x USB z czego nie mniej niż 1 x USB 2.0, 1 x USB 3.0 TYP-C na przednim panelu obudowy, 2 x USB 3.0 na tylnym panelu obudowy oraz 1 x USB 2.0 na płycie głównej. Złącze USB TYP-C na przednim panelu musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS.

b. 1 x VGA na tylnym panelu obudowy.

c. Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń.

11. Minimum 4 aktywne sloty PCI-E 5.0 x8 obsługujące karty FHHL.

12. Możliwość rozbudowy o 4 dodatkowe aktywne sloty PCI-E 5.0 x8 obsługujące karty HHHL.

13. Zainstalowane i w pełni funkcjonalne interfejsy sieciowe:

a. minimum 1 x RJ-45 Ethernet management port,

b. minimum 2 porty 10Gb/s Ethernet w standardzie SFP+ wraz z odpowiednimi wkładkami optycznymi SFP+ Multimode

c. minimum 2 porty 10Gb/s Ethernet w standardzie Base-T

d. powyższe porty nie może 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 Hot-Plug o pojemności min. 480 GB każdy. Dyski powinny być uruchomione w trybie RAID 1 przy użyciu dedykowanego kontrolera i 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

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).

dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera.

19. Bezpieczeństwo:

a. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.

b. Moduł TPM 2.0.

20. Serwer wyposażony w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający:

a. wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS

b. wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy

c. przywracanie konta administratora

d. wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera

e. wyświetlanie w czasie rzeczywistym temperatury procesorów

f. konfigurowanie ustawień sieciowych modułu zarządzania.

21. Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca:

a. monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.),

b. monitorowanie w czasie rzeczywistym poboru prądu przez serwer,

c. zbieranie logów błędów hardware,

d. przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury,

e. montowanie wirtualnych napędów,

f. zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego,

g. wysyłanie zawiadomień droga mailową i poprzez SNMP

h. wsparcia dla IPMI, SSH, Redfish

i. wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows,

j. nadawanie ról użytkownikom,

k. możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, zasilaczy, LCD,

l. możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem.

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).

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 cztery maszyny wirtualne uwzględniając oferowaną ilość rdzeni w serwerze. Dodatkowo należy dostarczyć 80 licencji CAL User.

24. Zgodność z normą ISO 9001 oraz ISO 14001 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. Certyfikat lub inny dokument potwierdzający zgodność z dostarczanym systemem operacyjnym należy dołączyć do oferty.

27. Oferowany serwer musi posiadać certyfikat lub inny dokument potwierdzający zgodność z dostarczanym oprogramowaniem do wirtualizacji, który należy dołączyć do oferty.

28. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

29. 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.

30. Gwarancja:

a. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta na terenie RP.

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).

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. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego serwera, że wymagany poziom serwisu z wymaganym SLA został zaoferowany na potrzeby oferty w niniejszym postępowaniu.

g. Wykonawca musi dołączyć do oferty 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. Analiza przedwdrożeniowa:

i. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.

ii. Opracowanie planu wdrożenia.

b. Wdrożenie i konfiguracja:

i. Instalacja serwera wraz z oprogramowaniem.

ii. Konfiguracja serwera i oprogramowania zgodnie z wymaganiami zamawiającego.

iii. Integracja z istniejącymi systemami IT zamawiającego.

c. Testy akceptacyjne:

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).

i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.

ii. Weryfikacja poprawności działania serwera oraz oprogramowania.

2. Zestaw macierz oraz deduplikator – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja zestawu składającego się z macierzy blokowo-plikowej do zadań produkcyjnych oraz deduplikatora do zadań backupowych.

Wymagania dotyczące macierzy:

1. Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowana macierz nie może przekroczyć rozmiaru 2U. Oferowana obudowa musi umożliwiać instalację min 25 dysków.

2. Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Akceptowalne architektury to ALUA oraz symmetric active-active. To oznacza, że obydwa kontrolery muszą brać aktywny udział w procesie zapisu danych na dyski jak i odczytu. Kontrolery nie mogą pracować w trybie active-passive. Kontrolery muszą komunikować się z dyskami protokołem NVMe. Macierz musi umożliwiać rozbudowę do co najmniej 4 kontrolerów.

3. Oferowane urządzenie musi być przystosowane do zasilania z sieci AC oraz wyposażone w kable zasilające PDU. Macierz musi być wyposażona w zdublowany, redundantny system zasilania, umożliwiający prawidłową, nieprzerwaną pracę urządzenia w przypadku awarii dowolnego pojedynczego źródła zasilania.

4. Macierz nie może posiadać pojedynczego punktu awarii (SPOF), który powodowałby brak dostępu do danych. Wszystkie krytyczne komponenty takie jak kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo.

5. Model macierzy w oferowanej konfiguracji w teście wydajnościowym musi osiągnąć min 1400 MB/s przy następujących parametrach:

a. Zapełnienie macierzy – powyżej 70% fizycznej pojemności,

b. Protokół: NFS,

c. Porty: 10G,

d. Read: 70%,

e. Write: 30%,

f. typ workloadu: Random,

g. wielkość plików: 32KB,

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).

h. Latency: max 1ms,

i. RAID 6 lub równoważny

6. Zamawiający może zażądać wyników testów lub wyników symulacji z oryginalnego sizera/estymatora producenta macierzy na etapie analizy ofert. Zamawiający ma prawo przeprowadzić test po dostawie macierzy aby sprawdzić czy dostarczone rozwiązanie osiąga deklarowane parametry wydajnościowe. Wydajność średnia nie mniejsza niż 1400 MB/s uzyskiwana przez co najmniej 60 min testu. Środowisko testowe – serwery wirtualne. Ewentualny test zostanie przeprowadzony ogólnodostępnym narzędziem Vdbench.

7. Fizyczna przestrzeń dyskowa zbudowana tylko i wyłącznie za pomocą dysków SSD NVMe/modułów NVMe musi wynosić min 30 TB. Przestrzeń użytkowa musi być zbudowana z RAID 6 z 1 dyskiem/modułem hot-spare lub przestrzenią hot-spare równą pojemności 1 dysku/modułu. Ze względów wydajnościowych oraz niezawodnościowych pojemność RAW pojedynczego dysku/modułu nie może być większa niż 4 TB, co przełoży się na większą liczbę dysków zapewniających krótszy czas odbudowy po awarii pojedynczego dysku. Dyski SSD NVMe/moduły NVMe muszą być wyposażone w podwójne, redundantne interfejsy PCIe. Nie dopuszcza się dysków SSD NVMe/modułów NVMe wyposażonych w chipset QLC.

8. Oferowana macierz musi umożliwiać rozbudowę do min. 125 dysków tego samego typu, czyli SSD NVMe/modułów NVMe bez konieczności klastrowania dodatkowych kontrolerów. Rozbudowa pojemności musi być możliwa poprzez instalację dysków w ramach oferowanej obudowy kontrolerów lub poprzez podłączanie półek dyskowych obsługujących NVMe. Wymagane jest zastosowanie wydajnego linku 100G RDMA (co najmniej 2) pomiędzy kontrolerami oraz półką dyskową, co zapewni możliwie najwyższą przepustowość oraz krótkie czasy odpowiedzi. Macierz nie może obsługiwać dysków HDD.

9. Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.

10. Co najmniej 192GB pamięci cache na całą macierz (dwa kontrolery). Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin.

11. Razem kontrolery muszą udostępnić minimum 8 portów 1G Eth RJ45 oraz min 8 portów 10Gb Eth z wkładkami optycznymi MM. Wymagana możliwość rozbudowy o kolejne 8 portów 10G Eth bez konieczności wymiany lub zakupu nowych kontrolerów i klastrowania z kontrolerami oferowanymi w tym postępowaniu, tylko poprzez dodanie nowych kart sieciowych.

12. Wymagane wsparcie dla FC, iSCSI.

13. Wymagane wsparcie dla NFS, CIFS. Nie dopuszcza się spełnienia wymogu poprzez zastosowanie główki/gateway NAS.

14. Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków bez utraty danych.

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).

15. Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) oraz file system'ów o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Wymagane dostarczenie w/w funkcjonalności na zainstalowaną przestrzeń dyskową. Macierz musi wspierać nie mniej niż 2000 LUNów.

16. Wymagana możliwość logicznego podziału macierzy na wiele wirtualnych/logicznych systemów z dedykowanymi portami logicznymi, użytkownikami oraz uprawnieniami. Użytkownik danego wirtualnego/logicznego systemu nie może mieć dostępu do file system'u z innego wirtualnego/logicznego systemu.

17. Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagany także dostęp do CLI. Zarządzanie poprzez min 2 porty 1Gb Eth typu management oraz port serial.

18. Wymagane jest stałe monitorowanie stanu macierzy w tym monitorowanie wydajności obiektów takich jak:

a. cała macierz

b. kontrolery

c. porty front-end

d. porty logiczne

e. dyski

f. LUNy

g. file systemy

h. hosty

i. CPU

19. Wymagane jest stałe monitorowanie stanu macierzy pod kątem parametrów takich jak:

a. operacje wejścia/wyjścia IOPS

b. przepustowość (KB/s lub MB/s)

c. czas odpowiedzi (latency)

d. średnie użycie CPU w % dla kontrolerów

20. Wymagana możliwość monitorowania stanu żywotności dysków SSD NVMe/modułów NVMe. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

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).

21. Wymagana możliwość konfigurowania zasobów macierzy. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

22. Wymagana możliwość tworzenia polityk logowania. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

23. Wymagane wsparcie multi-factor authentication do logowania się do macierzy. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

24. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych. Snapshoty muszą być wykonywanie w technologii ROW (Redirect On Write). Macierz musi umożliwiać utworzenie min 5000 snapshotów. Wymagana możliwość prezentacji folderu ze snapshotami w ramach udziału CIFS pod kątem przywracania pojedynczych plików. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model macierzy.

25. Tworzenie na żądanie kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z wolumenu źródłowego na docelowy oraz resynchronizację danych z wolumenu docelowego na źródłowy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

26. Macierz musi wspierać funkcjonalności deduplikacji i kompresji danych w trybie in-line (w locie). Musi istnieć możliwość wyłączenia deduplikacji dla wybranych wolumenów (LUN). Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania.

27. Możliwość zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym z wykorzystaniem portów IP. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Dostarczenie licencji na tą funkcjonalność nie jest wymagane na tym etapie postępowania.

28. Macierz musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00). Dostarczenie licencji na tą funkcjonalność nie jest wymagane na tym etapie postępowania.

29. Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybie asynchronicznym lub synchronicznym przy wykorzystaniu portów FC lub IP. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

30. Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

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).

31. Wymagana możliwość skonfigurowania polityki filtrowania zapisywanych plików na wystawionych udziałach CIFS/NFS poprzez wykluczenie ich konkretnych rozszerzeń. Wymagana także możliwość wskazania rozszerzeń które mogą być zapisywane. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

32. Wymagana możliwość nadawania uprawnień do określonych operacji dla wybranych użytkowników na udziałach CIFS/NFS. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

33. Wymagana możliwość ograniczenia dostępu do udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

34. Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem na poziomie całego file system'u (WORM). Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

35. Wymagana możliwość podłączenia serwera z oprogramowaniem antywirusowym celem skanowania plików wykorzystywanych przez użytkowników na zasobach wystawionych przez macierz protokołem CIFS. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

36. Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). Macierz musi dostarczać funkcjonalność klastra klasy "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych po protokole FC lub IP pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" pozwala na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automated failover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

37. Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o maksymalne progi wydajności IOPS i MB/s. Musi istnieć możliwość określenia polityk QoS na poziomie wolumenów. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

38. Wsparcie, dla co najmniej Microsoft Server Windows 2016/2019/2022, VMware 7.x/8.x, Linux RedHat 7.x/8.x, CentOS 7.x/8.x

39. Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.

40. Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania.

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).

41. Macierz musi umożliwiać zdalne zarządzanie.

42. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.

43. Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanej macierzy, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.

44. Wymagana gwarancja na 36 miesięcy w trybie 9x5 NBD.

45. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.

46. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

Wymagania dotyczące deduplikatora:

1. Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowany deduplikator nie może przekroczyć rozmiaru 2U. Oferowana obudowa musi umożliwiać instalację min 12 dysków.

2. Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler.

3. Oferowany model deduplikatora musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu co najmniej 5 TB/h (dane podawane przez producenta). Dodatkowo wymagana zagregowana wydajność backupu przy zastosowaniu deduplikacji na źródle co najmniej 8 TB/h (dane podawane przez producenta).

4. Przestrzeń fizyczna stworzona w oparciu o dyski NL SAS musi wynosić min. 32 TB. Dyski muszą być skonfigurowane w RAID 6 z min. 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności min. 1 dysku. Dodatkowo wymagane jest zastosowanie co najmniej 4 dysków SSD SAS o łącznej pojemności RAW min 1,92 TB jako cache pod zapis backupu.

5. Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej tolerującej jednoczesną awarię 2 dysków bez utraty danych. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem DoD 5220.22-M poprzez mechanizm nadpisywania danych.

6. Wymagana możliwość rozbudowy przestrzeni użytkowej poprzez instalację dysków i półek dyskowych oraz dodanie licencji (jeśli będzie wymagana) do min 250 TB.

7. Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania.

8. Urządzenie musi posiadać minimum:

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).

a. 8 portów RJ45 Ethernet 1 Gb/s oraz 4 porty SFP+ Ethernet 10 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS, NFS.

b. Wszystkie porty SFP+ wyposażone we wkładki optyczne MM.

9. Wymagana możliwość agregowania portów (bond port).

10. Wymagane wsparcie dla FC, iSCSI, NFS, CIFS.

11. Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak:

a. cały deduplikator

b. kontrolery

c. CPU

d. porty front-end

e. porty logiczne

f. dyski

g. file systemy

12. Wymagane jest stałe monitorowanie stanu deduplikatora pod kątem parametrów takich jak:

a. operacje wejścia/wyjścia IOPS

b. przepustowość (KB/s lub MB/s)

c. czas odpowiedzi (latency)

d. średnie użycie (w % dla CPU)

13. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

14. Wymagany dostęp do informacji o wykorzystanej fizycznej przestrzeni oraz aktualnym współczynniku redukcji danych. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

15. Wymagane wsparcie dla Multi-factor authentication. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

16. Wymagana możliwość definiowania polityk logowania. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.

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).

17. Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

18. Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

19. Musi być oficjalne wsparcie producenta dla oferowanego deduplikatora maksymalnego stopnia redukcji danych co najmniej 65:1. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

20. Wymagana możliwość skonfigurowania tzw. quoty ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

21. Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

22. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system'ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.

23. Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM) na poziomie całego file system'u. Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania.

24. Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję. Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.

25. Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00). Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.

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).

26. Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam Backup&Replication.

27. Deduplikator musi posiadać możliwość upgrade'u firmware-u kontrolerów bez przerywania dostępu do danych.

28. Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączania.

29. Urządzenie musi umożliwiać zdalne zarządzanie.

30. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.

31. Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego deduplikatora, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.

32. Wymagana gwarancja na 36 miesięcy w trybie 9x5 NBD.

33. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.

34. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

Wymagania dotyczące zakresu prac wdrożeniowych dla macierzy i deduplikatora:

1. Analiza przedwdrożeniowa:

a. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.

b. Opracowanie planu wdrożenia.

2. Wdrożenie i konfiguracja:

a. Instalacja macierzy oraz deduplikatora wraz z wymaganymi licencjami i oprogramowaniem.

b. Konfiguracja macierzy oraz deduplikatora zgodnie z wymaganiami zamawiającego.

c. Integracja z istniejącymi systemami IT zamawiającego.

3. Testy akceptacyjne:

a. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.

b. Weryfikacja poprawności działania macierzy i deduplikatora.

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).

3. Klaster Firewall z UTM – 1 kpl.

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja rozwiązania firewall z rozszerzonym pakietem bezpieczeństwa UTM pracującego w klastrze co najmniej Active-Passive, które zapewnia zaawansowaną kompleksową ochronę w infrastrukturze informatycznej zamawiającego. Zamówienie obejmuje zarówno dostawę urządzeń fizycznych firewall pracujących w klastrze co najmniej Active-Passive jak i licencje na oprogramowanie UTM na minimum 24 miesiące oraz usługi wdrożeniowe, dlatego wymagane jest uwzględnienie wszystkich elementów w ofercie.

Wymagania:
Funkcje modułu Firewall:
1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
2. Uruchomienie w formie klastra wysokiej dostępności (HA) co najmniej Active-Passive.
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5. Musi obsługiwać Multicast routing.
6. Musi obsługiwać Policy Based routing.
7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.

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).

26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
27. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego agenta na stacjach roboczych użytkowników.
28. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
29. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
30. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
31. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
32. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
33. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
34. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
35. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
36. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
37. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
38. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
39. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.

Specyfikacja UTM:
1. Firewall musi zapewnić obsługę na poziomie minimalnym: 5.8 Gbps dla pracy w trybie firewall, 1.18 Gbps dla pracy w trybie full scan (włączone mechanizmy bezpieczeństwa takie jak: AV, IPS)
2. Ilość obsługiwanych sieci VLAN: 100
3. Firewall musi obsługiwać 3 500 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 34 000 połączeń na sekundę.
4. Minimalna ilość portów 10/100/1000 BaseT: 8
5. Możliwość rozszerzenia portów o dodatkowe: 4x 1 Gb Copper lub 4x SFP lub 2x SFP+ lub 4x 10Gb multi-speed.
6. Wsparcie połączeń VPN site-to-site lub client-to-site dla minimum 75 użytkowników.
7. Minimalna ilość uwierzytelnionych użytkowników: 500.

Dostarczony system bezpieczeństwa (UTM) musi zapewniać:
1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Ochronę przed niechcianą pocztą.
4. Kontrolę wykorzystywanych aplikacji.
5. Możliwość filtrowania URL.

W ramach ochrony przed atakami system musi zapewniać:

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. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 8000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.
6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

W ramach kontroli antywirusowej system musi zapewniać:
1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie
2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
4. Możliwość skanowania plików o rozmiarze co najmniej 20MB.
5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

W ramach kontroli antyspamowej system musi zapewniać:
1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

W ramach filtrowania zawartości URL system musi zapewniać:
1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym, dlaczego dostęp do strony www został zablokowany.
5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.

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).

8. Możliwość określenia różnego rodzaju akcji dla połączeń do wybranych adresów URL na podstawie reputacji.
9. Możliwość filtrowania treści w oparciu o typy MIME.
10. Możliwość blokowania plików cookies dla określonych domen.
11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
12. Analizę treści dla protokołu https.
13. Wyłączenie inspekcji https dla wybranych kategorii stron www.

W ramach kontroli aplikacyjnej system musi zapewniać:
1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.

Wymagane funkcje VPN systemu:
1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.

Zarządzanie:
1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.

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).

4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:
1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline
5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
7. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
8. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
9. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
10. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
11. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
12. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
13. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
14. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
15. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
16. System ma mieć możliwość generowania raportów w formacie PDF oraz opcję eksportowania szczegółowych informacji do pliku CSV.
17. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
18. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
19. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
20. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
21. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
22. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

Gwarancja:

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. Urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i muszą być objęte serwisem producenta na terenie RP.
2. Urządzenia objęte minimum 24 miesięcznym okresem gwarancji.
3. Wykonawca musi dołączyć do oferty oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
4. Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego rozwiązania, potwierdzające pochodzenie urządzeń z licencjami z oficjalnego kanału dystrybucyjnego producenta.
5. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
6. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:
a. możliwość pobierania najnowszego firmware,
b. dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń,
c. dostęp do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego producenta,
d. otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.

Zakres prac wdrożeniowych:
1. Analiza przedwdrożeniowa:
a. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.
b. Opracowanie planu wdrożenia.
2. Wdrożenie i konfiguracja:
a. Instalacja urządzeń firewall wraz z oprogramowaniem UTM.
b. Konfiguracja urządzeń w klastrze co najmniej Active-Passive i oprogramowania UTM zgodnie z wymaganiami zamawiającego.
c. Integracja z istniejącymi systemami IT zamawiającego.
3. Testy akceptacyjne:
a. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.
b. Weryfikacja poprawności działania urządzeń firewall pracujących w klastrze Active-Passive oraz oprogramowania UTM.

4. Oprogramowanie do backupu stacji roboczych – 1 kpl.

Przedmiotem zamówienia jest dostawa oprogramowania do tworzenia kopii zapasowych oraz przywracania danych dla stacji roboczych użytkowników końcowych. W ramach zamówienia jest zakup 33 licencji wieczystych na oprogramowanie umożliwiające kompleksowe zarządzanie procesem backupu oraz przywracania danych w środowisku Zamawiającego ze wsparciem technicznym na minimum 24 miesiące. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie

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).

odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania podstawowe

1. Oprogramowanie ma umożliwiać realizację pełnego procesu ochrony danych na stacjach roboczych, w tym tworzenie kopii zapasowych, zarządzanie kopiami, przywracanie danych, a także monitorowanie i raportowanie stanu zabezpieczeń.
2. Oprogramowanie musi zapewniać niezawodność, bezpieczeństwo oraz skalowalność, umożliwiając ochronę danych na poziomie pojedynczych plików, katalogów, a także całych systemów operacyjnych.
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. Proces przełączenia serwera zarządzającego musi umożliwiać:
• Przełączenie automatyczne inicjalizowane przez administratora
• 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)
5. Mechanizm przełączania serwera zarządzającego musi pozwalać (minimum) na wybór trybu:
• Test failover (testowanie mechanizmu przełączania)
• Failover (produkcyjne przełączenie działania na serwer standby)
• Maintenance failover (przełączenie w celu np. aktualizacji oprogramowania)
5. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji w języku polskim lub angielskim.
6. 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.
7. 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.
8. 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
9. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej
10. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ
11. 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

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).

12. 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).
13. 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
14. 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.
15. 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.
16. System musi pozwalać na zarządzanie z poprzez „cmd" z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH.
17. System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix
18. 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
19. Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na:
• nielimitowana ilość bibliotek taśmowych i napędów fizycznych
• nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google)
20. W przypadku wielu lokalizacji licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami.
21. Zaoferowane licencje nie mogą mieć żadnych ograniczeń czasowych (muszą być wieczyste) dla wszystkich wymaganych funkcjonalności backupowych
22. 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 trybie9x5 oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień.
23. Zaoferowane licencje na system muszą zapewnić backup danych ze środowiska o wielkości 33 szt. stacji roboczych.
24. Zaoferowane oprogramowania musi tego samego producenta co oprogramowania do backupu maszyn wirtualnych, będące przedmiotem tego postępowania.

Wymagania funkcjonalne
1. Tworzenie kopii zapasowych
• Automatyzacja: Oprogramowanie powinno umożliwiać automatyczne tworzenie kopii zapasowych danych na stacjach roboczych w zaplanowanych interwałach czasowych, z możliwością dostosowania harmonogramów do potrzeb użytkownika.
• Ochrona ciągła: Powinno wspierać tworzenie kopii zapasowych w trybie ciągłym, zapewniając ochronę danych w czasie rzeczywistym i minimalizując ryzyko utraty danych. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego oraz syntetycznego.

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).

• Backupy różnicowe i przyrostowe: Oprogramowanie powinno wspierać tworzenie kopii różnicowych i przyrostowych, aby optymalizować zużycie przestrzeni dyskowej i czas tworzenia kopii zapasowych.
• Kopie zapasowe na żądanie: Użytkownicy powinni mieć możliwość ręcznego uruchamiania procesu tworzenia kopii zapasowych w dowolnym momencie. System ma realizować procesy backupu oraz odzyskiwania danych 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.
• Ochrona przed nieuprawnionym dostępem: Wszelkie dane w kopiach zapasowych powinny być szyfrowane zarówno w trakcie transferu, jak i podczas przechowywania. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.
• Różnorodność typów danych: Oprogramowanie musi obsługiwać tworzenie kopii zapasowych różnorodnych typów danych, w tym dokumentów, plików multimedialnych, konfiguracji systemów operacyjnych, a także plików aplikacji. System musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna dla backupu danych plikowych.
• Deduplikacja i kompresja: Musi wspierać deduplikację oraz kompresję danych, aby zoptymalizować wykorzystanie przestrzeni dyskowej. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i MacOS. 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.
• Logiczna Globalna deduplikacja: System musi oferować deduplikację globalną co oznacza iż niezależnie z jakich klientów dane będą deduplikowane, deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej.
• Weryfikacja: System musi realizować funkcjonalność weryfikacji wykonanych kopii
2. Przywracanie danych
• Elastyczne opcje przywracania: Oprogramowanie musi umożliwiać przywracanie danych na różne sposoby, w tym przywracanie pojedynczych plików, katalogów, a także całych systemów operacyjnych.
• Przywracanie w wybranym punkcie w czasie: Powinno oferować możliwość przywrócenia danych do konkretnego punktu w czasie, na przykład przed wystąpieniem awarii lub utraty danych.
• Szybkie przywracanie: Oprogramowanie musi zapewniać szybki proces przywracania, minimalizując czas przestoju i przywracając funkcjonalność systemu w możliwie najkrótszym czasie.
• Możliwość przywracania na inny sprzęt: Powinno wspierać przywracanie danych na inne stacje robocze lub sprzęt o odmiennych konfiguracjach sprzętowych.
3. Zarządzanie kopiami zapasowymi
• Centralne zarządzanie: Oprogramowanie musi oferować możliwość centralnego zarządzania kopiami zapasowymi wszystkich stacji roboczych, w tym zdalne zarządzanie harmonogramami backupów, monitorowanie statusu kopii oraz konfigurację ustawień ochrony danych. System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę

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).

administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane.
• Zarządzanie politykami: Powinno umożliwiać definiowanie i egzekwowanie polityk backupu, takich jak częstotliwość tworzenia kopii, retencja danych, oraz zasady przechowywania kopii w różnych lokalizacjach.
• Integracja z chmurą: Oprogramowanie musi wspierać integrację z rozwiązaniami chmurowymi, umożliwiając przechowywanie kopii zapasowych w chmurze oraz ich przywracanie z chmury.
4. Bezpieczeństwo
• Szyfrowanie: Wszystkie operacje związane z tworzeniem kopii zapasowych, przechowywaniem i przywracaniem danych muszą być zabezpieczone przy użyciu zaawansowanych mechanizmów szyfrowania. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu. 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.
• Ochrona przed ransomware: Oprogramowanie powinno oferować funkcje ochrony przed atakami typu ransomware, takie jak:
  ◦ Monitorowanie nietypowych zachować systemu backupowego obejmującego obszary:
    ▪ Czyszczenia bazy deduplikacyjnej (DDB)
    ▪ Zadarzeń w Systemie (events)
    ▪ Ilości nieudanych zadań
    ▪ Ilości zadań czekających
    ▪ Ilości zadań zakończonych sukcesem
    ▪ Konsoli monitorującej zadania
    ▪ Czasu trwania zadań
  ◦ Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane.
  ◦ Monitorowanie nietypowych aktywności na serwerach za pomocą metody: Honeypot (plików pułapek/wabików).
  ◦ Monitorowanie klientów Systemu i alertowanie o tych którzy tracą komunikację z Systemem .
  ◦ 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.
  ◦ 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.
  ◦ Możliwość definiowania kierunku inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego.
  ◦ 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.

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).

• Zarządzanie uprawnieniami: Powinno wspierać szczegółowe zarządzanie uprawnieniami dostępu do danych kopii zapasowych oraz narzędzi administracyjnych. 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).
• Autentykacja: 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.
5. Monitorowanie i raportowanie
• Monitorowanie w czasie rzeczywistym: Oprogramowanie powinno umożliwiać monitorowanie stanu kopii zapasowych w czasie rzeczywistym, z możliwością natychmiastowego wykrywania i powiadamiania o błędach oraz problemach.
• Raporty: Powinno generować raporty dotyczące stanu backupów, zgodności z politykami, użycia przestrzeni dyskowej, a także wszelkich incydentów związanych z bezpieczeństwem danych. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:
  ◦ Raport zmian/wzrostu środowiska systemu
  ◦ Raport wykorzystania licencji
  ◦ Raport wykonanych zadań backupowych
  ◦ Raporty obciążenia serwerów backupowych – minimum monitorowanie użycia CPU i pamięci RAM
• Powiadomienia: Oprogramowanie musi obsługiwać konfigurację alertów, które będą informować administratorów o krytycznych zdarzeniach, takich jak błędy podczas tworzenia kopii zapasowych, zakończenie procesów, oraz inne istotne informacje. Notyfikacje alertów muszą być wysyłane minimum poprzez mail. System musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych przy spełnieniu minimum kryterii:
  ◦ Czas zadania dłuższy niż zadany
  ◦ Ilość danych większa niż ….
  ◦ Ilość danych mniejsza niż ….
  ◦ Ilość nie zbackupowanych plików większa niż
  ◦ Ilość nie zbackupowanych plików większa niż …%
  ◦ Wielkość backupowanych danych większa niż …
6. Skalowalność i elastyczność
• Skalowalność: Oprogramowanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych.
• Wsparcie dla różnych środowisk: 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. Musi być kompatybilne z różnymi systemami operacyjnymi, takimi jak Windows, macOS, oraz Linux.
• Integracja z mechanizmami kopii migawkowych: System musi umożliwiać integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum:

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).

Dell, HPE, Huawei, NetApp, IBM, Pure Storage z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych ale i aplikacji.
• Integracja zewnętrznych repozytoriów: Oprogramowanie musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym zgodnymi z KMIP – minimum dla:
  ◦ AWS CloudHSM
  ◦ Fortanix Data Security Manager
  ◦ HashiCorp Vault
  ◦ IBM Security Key Lifecycle Manager (SKLM)
  ◦ Safenet
  ◦ StorMagic SvKMS
  ◦ Thales CipherTrust Manager
  ◦ Vormetric
  ◦ Amazon Web Services (AWS) key management service
  ◦ Microsoft Azure Key Vault

Wymagania techniczne
1. Kompatybilność sprzętowa: Oprogramowanie musi być kompatybilne z istniejącym sprzętem i infrastrukturą IT zamawiającego, w tym stacjami roboczymi, serwerami oraz systemami pamięci masowej.
2. Wsparcie techniczne: Wykonawca musi zapewnić wsparcie techniczne dla dostarczonego oprogramowania na minimum 24 miesiące, obejmujące pomoc przy konfiguracji oraz użytkowaniu, a także dostęp do aktualizacji i poprawek.
3. Dokumentacja: Oprogramowanie musi być dostarczone z pełną dokumentacją w języku polskim lub angielskim, obejmującą instrukcje instalacji, konfiguracji oraz zarządzania systemem backupu.

Warunki dostawy
1. Forma dostawy: Licencje oprogramowania powinny być dostarczone w formie elektronicznej, w postaci kodów aktywacyjnych lub plików licencyjnych.
2. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

Wdrożenie
1. Analiza przedwdrożeniowa:
• Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia oprogramowania do backupu wskazanych 33 szt. stacji roboczych.
• Opracowanie szczegółowego planu wdrożenia.
2. Instalacja i konfiguracja:
• Instalacja i konfiguracja oprogramowania do backupu wskazanych 33 szt. stacji roboczych.
• Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
• Testy funkcjonalne systemu.
3. Dokumentacja:
• Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.

Gwarancja

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. 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.
2. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

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 miesiące. Oprogramowanie ma zapewniać niezawodność, skalowalność oraz pełną integrację z istniejącą infrastrukturą wirtualną zamawiającego. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania podstawowe

1. Oprogramowanie powinno umożliwiać kompleksowe zarządzanie procesami tworzenia kopii zapasowych oraz przywracania danych na maszynach wirtualnych. Zakres zamówienia obejmuje funkcjonalności związane z ochroną danych, zarządzaniem kopiami zapasowymi, a także monitorowaniem i raportowaniem stanu zabezpieczeń. System musi być skalowalny i kompatybilny z popularnymi platformami wirtualizacji.

2. Oprogramowanie musi zapewniać niezawodność, bezpieczeństwo oraz skalowalność, umożliwiając ochronę danych na poziomie pojedynczych plików, katalogów, a także całych systemów operacyjnych.

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. Proces przełączenia serwera zarządzającego musi umożliwiać:

• Przełączenie automatyczne inicjalizowane przez administratora

• 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)

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).

5. Mechanizm przełączania serwera zarządzającego musi pozwalać (minimum) na wybór trybu:

• Test failover (testowanie mechanizmu przełączania)

• Failover (produkcyjne przełączenie działania na serwer standby)

• Maintenance failover (przełączenie w celu np. aktualizacji oprogramowania)

5. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji w języku polskim lub angielskim.

6. 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.

7. 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.

8. 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

9. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja) z jednej konsoli administracyjnej oraz także z konsoli webowej

10. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ

11. 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

12. 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).

13. 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

14. 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.

15. 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.

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).

16. System musi pozwalać na zarządzanie z poprzez „cmd” z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH.

17. System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix

18. System musi wspierać backup całych maszyn wirtualnych / kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:

- Alibaba Cloud
- Amazon
- Citrix Xen
- Google Cloud Platform
- Huawei FusionCompute
- Microsoft Azure
- Microsoft Azure Stack Hub
- Microsoft Azure Stack HCI
- Microsoft Hyper-V
- Kubernetes
- Nutanix Acropolis Hypervisor (AHV)
- OpenStack
- Oracle Cloud Classic
- Oracle Cloud Infrastructure
- Oracle VM
- Red Hat OpenShift
- Red Hat Virtualization
- vCloud Director
- 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. 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.

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).

19. 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

20. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.

21. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla Vmware i Hyper-V.

22. System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:

• Vmware do: Hyper-V, Azure, Amazon, Google Cloud Platform, Openstack, Oracle Cloud Infrastructure

• Hyper-V do: Azure, Amazon, Vmware

• Amazon do: Azure, Vmware

• Azure do: Amazon, Hyper-V, Vmware

23. System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V

24. System musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku:

• Hyper-V

• Vmware

25. 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

26. Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na:

• nielimitowana ilość bibliotek taśmowych i napędów fizycznych

• nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google)

27. W przypadku wielu lokalizacji licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami.

28. Zaoferowane licencje nie mogą mieć żadnych ograniczeń czasowych (muszą być wieczyste) dla wszystkich wymaganych funkcjonalności backupowych

29. Do dostarczonych licencji jest wymagane 24 miesięczne wparcie producenta lub autoryzowanego partnera serwisowego (pierwsza i druga linia wsparcia świadczona w języku

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).

polskim lub angielskim) zapewniające wsparcie techniczne w trybie9x5 oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień.

30. Zaoferowane licencje na system muszą zapewnić backup danych ze środowiska o wielkości 10 szt. maszyn wirtualnych.

31. Zaoferowane oprogramowania musi pochodzić od tego samego producenta co oprogramowania do backupu stacji roboczych, będące przedmiotem tego postępowania.

Wymagania funkcjonalne

1. Tworzenie kopii zapasowych

• Automatyczne kopie zapasowe: Oprogramowanie powinno umożliwiać automatyczne tworzenie kopii zapasowych maszyn wirtualnych zgodnie z ustalonym harmonogramem, z możliwością dostosowania harmonogramów do specyficznych potrzeb każdej maszyny wirtualnej.

• Ochrona całych maszyn wirtualnych: System musi umożliwiać tworzenie pełnych kopii zapasowych, obejmujących wszystkie dane na maszynie wirtualnej, w tym dyski wirtualne, konfiguracje i metadane. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego oraz syntetycznego.

• Backupy różnicowe i przyrostowe: Oprogramowanie powinno wspierać tworzenie kopii różnicowych i przyrostowych, aby optymalizować zużycie przestrzeni dyskowej i czas tworzenia kopii zapasowych.

• Szyfrowanie danych: Kopie zapasowe muszą być szyfrowane zarówno podczas przesyłania, jak i przechowywania, zapewniając ochronę przed nieautoryzowanym dostępem.

• Kompresja i deduplikacja: System powinien obsługiwać kompresję oraz deduplikację danych, aby zminimalizować zapotrzebowanie na przestrzeń dyskową i zwiększyć efektywność procesu backupu. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i MacOS. 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.

• Logiczna Globalna deduplikacja: System musi oferować deduplikację globalną co oznacza iż niezależnie z jakich klientów dane będą deduplikowane, deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej.

• Weryfikacja: System musi realizować funkcjonalność weryfikacji wykonanych kopii

2. Przywracanie danych

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).

• Elastyczne przywracanie: Oprogramowanie musi umożliwiać przywracanie danych na różne sposoby, w tym przywracanie całych maszyn wirtualnych, poszczególnych dysków wirtualnych, a także pojedynczych plików lub katalogów.

• Przywracanie na poziomie plików: System powinien umożliwiać przywracanie pojedynczych plików i katalogów bez konieczności przywracania całej maszyny wirtualnej.

• Przywracanie w wybranym punkcie w czasie: Oprogramowanie musi umożliwiać przywracanie danych do określonego punktu w czasie, aby zminimalizować skutki awarii i przywrócić system do stanu sprzed zdarzenia.

• Przywracanie na inny sprzęt: Oprogramowanie powinno wspierać przywracanie maszyn wirtualnych na inne hosty wirtualizacyjne, w tym do różnych środowisk wirtualizacyjnych.

3. Zarządzanie kopiami zapasowymi

• Centralne zarządzanie: Oprogramowanie musi oferować centralne zarządzanie procesem tworzenia i przywracania kopii zapasowych dla wszystkich obsługiwanych maszyn wirtualnych. Powinno pozwalać na konfigurację polityk backupu, monitorowanie procesów, oraz zarządzanie zasobami backupu z jednego panelu administracyjnego. System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane.

• Polityki retencji danych: System musi umożliwiać definiowanie polityk retencji danych, określających, jak długo kopie zapasowe będą przechowywane przed ich automatycznym usunięciem.

• Integracja z chmurą: Oprogramowanie powinno wspierać integrację z różnymi dostawcami usług chmurowych, umożliwiając tworzenie i przechowywanie kopii zapasowych w chmurze oraz przywracanie danych z chmury.

4. Bezpieczeństwo

• Zaawansowane szyfrowanie: Wszystkie operacje związane z kopiami zapasowymi, w tym tworzenie, przesyłanie i przechowywanie danych, muszą być zabezpieczone przy użyciu zaawansowanych mechanizmów szyfrowania. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu. 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.

• Ochrona przed ransomware: Oprogramowanie powinno oferować funkcje ochrony przed atakami typu ransomware, takie jak:

  ◦ Monitorowanie nietypowych zachowań systemu backupowego obejmującego obszary:

    ▪ Czyszczenia bazy deduplikacyjnej (DDB)

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).

- Zadarzeń w Systemie (events)
- Ilości nieudanych zadań
- Ilości zadań czekających
- Ilości zadań zakończonych sukcesem
- Konsoli monitorującej zadania
- Czasu trwania zadań

◦ Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane.

◦ Monitorowanie nietypowych aktywności na serwerach za pomocą metody: Honeypot (plików pułapek/wabików).

◦ Monitorowanie klientów Systemu i alertowanie o tych którzy tracą komunikację z Systemem .

◦ 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.

◦ 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.

◦ Możliwość definiowania kierunku inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego.

◦ 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.

• Zarządzanie uprawnieniami: System powinien wspierać szczegółowe zarządzanie uprawnieniami, pozwalając na kontrolę dostępu do danych kopii zapasowych i narzędzi administracyjnych. 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).

• Autentykacja: 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.

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).

5. Monitorowanie i raportowanie

• Monitorowanie w czasie rzeczywistym: Oprogramowanie powinno umożliwiać monitorowanie stanu kopii zapasowych w czasie rzeczywistym, z możliwością natychmiastowego wykrywania i powiadamiania o problemach związanych z backupami.

• Generowanie raportów: System powinien oferować funkcje raportowania, umożliwiające tworzenie szczegółowych raportów na temat stanu kopii zapasowych, zgodności z politykami, użycia przestrzeni dyskowej oraz incydentów bezpieczeństwa. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:

◦ Raport zmian/wzrostu środowiska systemu

◦ Raport wykorzystania licencji

◦ Raport wykonanych zadań backupowych

◦ Raporty obciążenia serwerów backupowych – minimum monitorowanie użycia CPU i pamięci RAM

• Powiadomienia: Oprogramowanie musi obsługiwać konfigurację alertów, które będą informować administratorów o krytycznych zdarzeniach, takich jak błędy podczas tworzenia kopii zapasowych, zakończenie procesów, oraz inne istotne informacje. Notyfikacje alertów muszą być wysyłane minimum poprzez mail. System musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych przy spełnieniu minimum kryterii:

◦ Czas zadania dłuższy niż zadany

◦ Ilość danych większa niż ….

◦ Ilość danych mniejsza niż ….

◦ Ilość nie zbackupowanych plików większa niż

◦ Ilość nie zbackupowanych plików większa niż …%

◦ Wielkość backupowanych danych większa niż …

6. Skalowalność i elastyczność

• Skalowalność: Oprogramowanie musi być skalowalne, umożliwiając ochronę rosnącej liczby maszyn wirtualnych oraz większej ilości danych bez konieczności wprowadzania istotnych zmian w infrastrukturze.

• Wsparcie dla różnych platform wirtualizacji: Oprogramowanie musi być kompatybilne z głównymi platformami wirtualizacji, takimi jak VMware vSphere, Microsoft Hyper-V, oraz inne środowiska wirtualizacyjne stosowane przez zamawiającego.

• Obsługa wielu środowisk: Powinno umożliwiać ochronę maszyn wirtualnych działających w różnych środowiskach, zarówno on-premises, jak i w chmurze. Niedopuszczalne jest aby

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).

funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia. Musi być kompatybilne z różnymi systemami operacyjnymi, takimi jak Windows, macOS, oraz Linux.

• Integracja z mechanizmami kopii migawkowych: System musi umożliwiać integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: Dell, HPE, Huawei, NetApp, IBM, Pure Storage z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych ale i aplikacji.

• Integracja zewnętrznych repozytoriów: Oprogramowanie musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym zgodnymi z KMIP – minimum dla:

- AWS CloudHSM
- Fortanix Data Security Manager
- HashiCorp Vault
- IBM Security Key Lifecycle Manager (SKLM)
- Safenet
- StorMagic SvKMS
- Thales CipherTrust Manager
- Vormetric
- Amazon Web Services (AWS) key management service
- Microsoft Azure Key Vault

Wymagania techniczne

1. Kompatybilność sprzętowa i systemowa: Oprogramowanie musi być kompatybilne z istniejącym sprzętem i infrastrukturą IT zamawiającego, w tym z hostami wirtualizacyjnymi, systemami pamięci masowej oraz siecią.

2. Wsparcie techniczne: Wykonawca musi zapewnić wsparcie techniczne dla dostarczonego oprogramowania na minimum 24 miesiące, obejmujące pomoc przy konfiguracji oraz użytkowaniu, a także dostęp do aktualizacji i poprawek.

3. Dokumentacja: Oprogramowanie musi być dostarczone z pełną dokumentacją w języku polskim lub angielskim, obejmującą instrukcje instalacji, konfiguracji oraz zarządzania systemem backupu.

Warunki dostawy

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. Forma dostawy: Licencje oprogramowania powinny być dostarczone w formie elektronicznej, w postaci kodów aktywacyjnych lub plików licencyjnych.

2. 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.

Wdrożenie

1. Analiza przedwdrożeniowa:

• Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia oprogramowania do backupu wskazanych maszyn wirtualnych.

• Opracowanie szczegółowego planu wdrożenia.

2. Instalacja i konfiguracja:

• Instalacja i konfiguracja oprogramowania do backupu wskazanych maszyn wirtualnych.

• Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.

• Testy funkcjonalne systemu.

3. Dokumentacja:

• Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.

Gwarancja

1. 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.

2. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

6. Oprogramowanie do wirtualizacji – 1 kpl.

Przedmiotem zamówienia jest dostawa, wdrożenie i skonfigurowanie kompleksowego oprogramowania wirtualizacyjnego w licencji wieczystej, które obejmuje zarówno hypervisor jak również narzędzia do zarządzania chmurą, automatyzacji, orkiestracji oraz monitorowania, umożliwiające stworzenie i zarządzanie nowoczesnym, elastycznym środowiskiem infrastruktury IT.

Wymagania:
1. Zakres funkcjonalności:
a. Wirtualizacja zasobów:

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).

i. Możliwość tworzenia i zarządzania wirtualnymi maszynami (VM) na platformie x86.
ii. Obsługa różnych systemów operacyjnych na wirtualnych maszynach, w tym Windows i Linux.
iii. Funkcje dynamicznego przydzielania zasobów (CPU, RAM, dysk), umożliwiające optymalizację wykorzystania infrastruktury sprzętowej.
b. Zarządzanie zasobami i automatyzacja:
i. Centralne zarządzanie infrastrukturą wirtualną z poziomu intuicyjnego interfejsu użytkownika w języku polskim lub angielskim.
ii. Automatyzacja operacji związanych z tworzeniem, migracją oraz kopiowaniem maszyn wirtualnych.
iii. Funkcje automatycznego skalowania zasobów w odpowiedzi na zmieniające się obciążenie systemów.
c. Wysoka dostępność i niezawodność:
i. Mechanizmy zapewniające wysoką dostępność (HA) maszyn wirtualnych oraz automatyczne przywracanie usług po awarii.
ii. Wsparcie dla klastrów wirtualizacji, umożliwiających rozłożenie obciążeń oraz zminimalizowanie ryzyka przestojów.
iii. Możliwość tworzenia kopii zapasowych oraz przywracania wirtualnych maszyn.
d. Bezpieczeństwo i zgodność:
i. Rozbudowane funkcje zarządzania bezpieczeństwem, w tym izolacja zasobów, zarządzanie tożsamością oraz kontrola dostępu.
ii. Monitorowanie i audytowanie działań administracyjnych oraz operacji wirtualnych maszyn.
iii. Zgodność z międzynarodowymi standardami bezpieczeństwa IT.
e. Integracja i skalowalność:
i. Możliwość integracji z innymi rozwiązaniami chmurowymi oraz systemami zarządzania IT.
ii. Obsługa różnych modeli wdrożeń, w tym chmury prywatnej, publicznej oraz hybrydowej.
iii. Skalowalność rozwiązania pozwalająca na rozbudowę infrastruktury w miarę wzrostu potrzeb organizacji.
f. Monitorowanie i analiza:
i. Zaawansowane narzędzia do monitorowania wydajności i stanu wirtualnych zasobów.
ii. Analiza i raportowanie w czasie rzeczywistym, umożliwiające szybkie reagowanie na zmiany w środowisku IT.
iii. Optymalizacja wykorzystania zasobów poprzez analizę trendów i prognozowanie potrzeb.
2. Wymagania techniczne:
a. Kompatybilność z istniejącą infrastrukturą sprzętową i sieciową organizacji.
b. Możliwość łatwego wdrożenia i integracji z istniejącymi systemami zarządzania IT.
c. Dostarczenie pełnej dokumentacji technicznej w języku polskim lub angielskim.
3. Oprogramowanie objęte minimum 36 miesięcznym okresem gwarancyjnym w trybie online z gwarantowanym czasem reakcji najpóźniej Next Business Day godziny od momentu zgłoszenia usterki.
4. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
5. Wdrożenie oprogramowania wirtualizacyjnego i skonfigurowanie pięciu maszyn wirtualnych na serwerze będącym przedmiotem tego postępowania.

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).

7. Oprogramowanie do monitoringu infrastruktury IT – 1 kpl.

Przedmiotem zamówienia jest dostawa, instalacja, konfiguracja oraz wdrożenie oprogramowania do monitorowania i zarządzania infrastrukturą IT, który pozwoli na kompleksową kontrolę oraz nadzór nad zasobami IT, w tym urządzeniami sieciowymi, serwerami, stacjami roboczymi oraz aktywnością użytkowników. Oprogramowanie ma również zapewniać funkcjonalności związane z zarządzaniem bezpieczeństwem danych, kontrolą dostępu oraz zarządzaniem oprogramowaniem i zasobami sprzętowymi. Zamówienie obejmuje dostawę licencji wieczystej na 75 stacji roboczych ze wsparciem technicznym na minimum 24 miesiące. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania funkcjonalne systemu

1. Oprogramowanie musi posiadać budowę modułową oraz składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów.
2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami musi odbywać się przy użyciu szyfrowanego protokołu TLS w wersji 1.2 lub 1.3.
3. Program musi umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.
4. System musi umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.
5. Program nie może być objęty limitem ilości danych.
6. Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., muszą być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej.
7. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, musi być objęty kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników.
8. Główny Administrator musi mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów.
9. Działania administratorów muszą być logowane a program musi posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta.
10. Działania administratorów muszą być automatycznie eksportowane do zewnętrznego kolektora Syslog.
11. Lista kont użytkowników, w tym administratorów, musi mieć możliwość synchronizowana z Active Directory, również przez szyfrowane połączenie LDAPS.

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).

12. Program musi umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli.
13. Program musi zawierać mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA można skonfigurować okres, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera.
14. Monitorowanie infrastruktury bezagentowo musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:
a. wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
b. wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
c. wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
d. wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
e. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
f. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
g. wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
h. wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
i. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
j. zablokowania mapy urządzeń przed przypadkową edycją
k. serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
l. serwerów pocztowych:
   i. monitorowanie czasu logowania do serwisu odbierającego oraz czasu wysyłania poczty
   ii. możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
   iii. możliwość wykonywania operacji testowych
   iv. możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
m. monitorowania serwerów WWW i adresów URL
n. cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
o. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
p. obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
q. obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
r. monitoringu routerów i przełączników wg:
   i. zmian stanu interfejsów sieciowych

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).

ii. ruchu sieciowego
iii. podłączonych stacji roboczych – graficzna prezentacja panelu switcha
iv. ruchu generowanego przez podłączone do portów stacje robocze
s. serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
t. wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
u. monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
v. zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
w. wydajności systemów Windows: obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy
15. Program musi posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.
16. Program musi umożliwiać również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera.
17. Program musi mieć możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).
18. Program musi automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:
a. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
b. Umożliwiać odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
c. Obejmować zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
d. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
e. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
f. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
g. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
h. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
i. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników i harmonogramie zadań.
j. Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem

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).

metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
k. Umożliwiać wymianę plików do i ze stacji roboczej poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.
19. Inwentaryzacja zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:
a. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
b. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
c. tworzenia powiązań między zasobami a urządzeniami,
d. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
e. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
f. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
g. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
h. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
i. masową edycję atrybutów zasobów,
j. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
k. importu danych z zewnętrznego źródła (.CSV),
l. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
m. tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
n. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
o. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
p. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
q. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
r. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
s. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
t. archiwizacji i porównywania audytów zasobów,
u. tworzenia kodów kreskowych dla zasobów,
v. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,

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).

w. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
x. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
y. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
z. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja").
Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
i. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
ii. Informacje o aplikacjach używanych w organizacji.
iii. Tworzenie własnych wzorców aplikacji.
iv. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe.
v. Informacje o komputerach, na których aplikacja została wykryta.
vi. Zarządzanie posiadanymi licencjami.
vii. Wskazywanie osób odpowiedzialnych za licencję.
viii. Wskazanie użytkowników licencji.
ix. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
x. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
xi. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
xii. Zarządzanie posiadanymi licencjami: raport zgodności licencji.
xiii. Możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe posiadają możliwość filtrowania elementów per oddział.
20. Program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:
a. Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
b. Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
c. Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
d. Informacji o edytowanych przez użytkownika dokumentach,
e. Historii pracy (cykliczne zrzuty ekranowe),
f. Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
g. Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),

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).

h. Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
i. Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.
21. Program ponadto musi posiadać możliwość:
a. wykrywania podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy.
b. zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
c. wyszczególnienia podejrzanej aktywności w raportach.
d. wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
e. automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
f. blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
g. integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
h. skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
i. automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
j. blokowania ruchu na wskazanych portach TCP/IP,
k. blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
l. prowadzenia rejestru naruszeń blokad,
m. wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
n. przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
o. definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone.
22. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie.
23. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku.
24. Reguły w postaci listy blokowanych plików lub lokalizacji muszą być tworzone dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.
25. Program musi posiadać Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.
26. Program musi umożliwiać realizację zdalnej pomocy użytkownikom.

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).

27. W ramach kontroli stacji użytkownika musi być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla).
28. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator muszą widzieć ten sam ekran.
29. Administrator w trakcie zdalnego dostępu musi mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika.
30. Funkcja zdalnego dostępu musi umożliwiać równoczesne podłączenie do tego samego komputera kilku administratorom.
31. Program musi posiadać bazę zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.
32. Oprogramowanie musi pozwalać na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0.
33. Oprogramowanie musi umożliwiać również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawierać dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę.
34. Musi być umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron.
35. System musi umożliwiać użycie pośredniego statusu „zgłoszenie rozwiązane" przed ostatecznym zamknięciem zgłoszenia.
36. Program musi zawierać również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów).
37. Czat musi pozwalać na:
a. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
b. rozmowy również między „zwykłymi" użytkownikami
c. przesyłanie plików między rozmówcami w trybie online
d. tworzenie pokojów tematycznych, rozmów grupowych
e. oznaczanie kontaktów jako „ulubionych" na liście kontaktów
f. uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
g. może być wyświetlany w trybie jasnym lub ciemnym
38. Program musi zawierać również bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic).

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).

39. Program musi umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy.
40. Użytkownik musi mieć możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta.
41. Administrator musi mieć możliwość tworzenia szkiców i archiwizowania komunikatów.
42. Dostęp do systemu zgłoszeń oraz bazy wiedzy musi być realizowany przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.
43. Program musi umożliwiać również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.
44. Program musi umożliwiać również:
a. pobieranie listy użytkowników z Active Directory,
b. wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,
c. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
d. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
e. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
f. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
g. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
h. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
i. definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
j. przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
k. procesowanie zgłoszeń użytkowników z wiadomości e-mail,
l. eksportowania listy zgłoszeń do plików CSV i XLSX,
m. integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
n. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
o. wykonywanie operacji na wielu zgłoszeniach równocześnie,
p. dołączanie załączników do zgłoszeń,
q. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
r. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
s. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
t. zrzuty ekranowe (podgląd pulpitu),
u. zdalną modyfikację rejestrów,
v. dystrybucję oprogramowania przez Agenty,

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).

w. definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
x. przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
y. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
z. zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
aa. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
bb. możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
cc. planowanie nieobecności pracowników helpdesk,
dd. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
ee. generowanie raportów obsługi helpdesk,
ff. zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
gg. zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
hh. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.
45. Oprogramowanie musi mieć ochronę danych przed wyciekiem poprzez blokowanie urządzeń i nośników danych:
a. Program musi mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
b. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
c. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
d. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
e. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
f. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
g. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
h. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
i. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
j. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
k. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
l. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.
46. Oprogramowanie musi zarządzać prawami dostępu do urządzeń:

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).

a. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
b. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
c. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
d. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
e. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.
47. Audyt operacji na plikach na urządzeniach przenośnych:
a. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
b. Podłączenie/odłączenie urządzenia przenośnego.
48. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.
49. Definiowanie reguł monitorowanych folderów w postaci list.
50. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.)
51. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych.
52. Przydzielanie uprawnień również do kont użytkowników lokalnych.
53. Program musi umożliwiać prowadzenie rejestru naruszeń blokad podłączanych nośników.
54. Program musi analizować aktywności użytkowników poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu.
55. Każdy pracownik organizacji musi mieć możliwość oznaczenia sesji aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy.
56. Menedżerowie oraz przełożeni muszą mieć możliwość uzyskania automatycznego dostępu do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania.
57. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje.
58. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania.
59. Dostęp realizowany przez przeglądarkę internetową a strona może być wyświetlana w trybie jasnym lub ciemnym.
60. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
61. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.
62. Statystyki aktywności podwładnych widoczne dla przełożonego.
63. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.
64. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
65. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
66. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.

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).

67. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
68. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
69. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
70. Wskaźnik czasu poświęconego na aktywność produktywną.
71. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
72. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.
73. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.
74. Oprogramowanie musi posiadać również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, których nazwy można zmieniać wg potrzeb.
75. Na każdym z dashboardów widgety muszą być rozłożone na siatce o rozmiarze ustalonym przez administratora.
76. Zawartość każdego z paneli informacyjnych musi być automatycznie odświeżana oraz może być:
a. Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.
b. Wyświetlana w trybie jasnym lub ciemnym (nocnym). Oprogramowanie umożliwia zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego. Widgety prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania:
c. Mapa sieci,
d. Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,
e. Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,
f. Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW, naruszenia reguł blokad,
g. Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,
h. Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych,
i. Produktywność dla grupy, Statystyki czasu nieproduktywnego.
77. Program musi być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
78. Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.

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).

79. Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji.

Wymagania techniczne

1. System musi być kompatybilny z popularnymi systemami operacyjnymi (Windows, Linux, macOS).
2. Wsparcie dla baz danych SQL (np. MS SQL, MySQL).
3. Możliwość skalowania systemu w zależności od liczby monitorowanych urządzeń i użytkowników.
4. Obsługa protokołów sieciowych takich jak SNMP, WMI, SSH, itp.
5. Przyjazny interfejs użytkownika, dostępny z poziomu przeglądarki internetowej w polskiej wersji językowej.
6. Wysoka dostępność systemu (HA), z opcją klastrowania i replikacji danych.
7. Wykonawca zobowiązany jest do przeprowadzenia analizy przedwdrożeniowej, mającej na celu optymalne dostosowanie systemu do specyfiki infrastruktury Zamawiającego.
8. Przeprowadzenie instalacji i konfiguracji systemu zgodnie z najlepszymi praktykami.
9. Wdrożenie systemu w środowisku produkcyjnym.
10. Dostarczenie dokumentacji technicznej oraz użytkowej w języku polskim.
11. Wykonawca zapewni wsparcie techniczne przez okres minimum 24 miesięcy od daty odbioru systemu.
12. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
13. Wsparcie techniczne obejmuje pomoc w rozwiązywaniu problemów, aktualizacje oprogramowania, oraz dostęp do dokumentacji i baz wiedzy.
14. Możliwość przedłużenia wsparcia technicznego na kolejne lata.
15. Odbiór przedmiotu zamówienia nastąpi po zakończeniu wdrożenia.
16. Przed odbiorem, Wykonawca zobowiązany jest do przeprowadzenia testów funkcjonalnych oraz wydajnościowych, potwierdzających prawidłowe działanie systemu.
17. Pozytywny wynik testów oraz akceptacja Zamawiającego są warunkiem końcowego odbioru przedmiotu zamówienia.
18. Wdrożenie:

a. Analiza przedwdrożeniowa:
   i. Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia oprogramowania do monitorowania i zarządzania infrastrukturą IT.
   ii. Opracowanie szczegółowego planu wdrożenia.

b. Instalacja i konfiguracja:
   i. Instalacja i konfiguracja oprogramowania do monitorowania i zarządzania infrastrukturą IT.
   ii. Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
   iii. Testy funkcjonalne systemu.

c. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.

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).

19. Zamawiający wymaga licencji wieczystych na 75 stacji roboczych z gwarancją i serwisem na okres minimum 24 miesięcy, z możliwością przedłużenia. Serwis powinien obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.

8. Oprogramowanie do zbierania i analizy logów z całej infrastruktury IT – 1 kpl.

Przedmiotem zamówienia jest dostawa oprogramowania do zbierania i analizy logów z całej infrastruktury IT. Zamówienie obejmuje dostawę licencji wieczystej ze wsparciem technicznym na minimum 24 miesiące. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

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.

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).

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.

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).

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.

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).

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:

- Syslog,
- WEF,
- Flat file,
- Event log,
- WMI,
- SNMP trap,
- XML,
- JSON,
- JDBC/ODBC
- CSV,
- 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.

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).

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.

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).

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.

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).

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.

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).

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. Wdrożenie:

a. Analiza przedwdrożeniowa:

i. Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia oprogramowania do zbierania logów, skanowania podatności oraz analizy danych i incydentów z całej infrastruktury IT.

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).

ii. Opracowanie szczegółowego planu wdrożenia.

b. Instalacja i konfiguracja:

i. Instalacja i konfiguracja oprogramowania do zbierania logów, skanowania podatności oraz analizy danych i incydentów z całej infrastruktury IT.

ii. Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.

iii. Testy funkcjonalne systemu.

c. Dostarczenie pełnej dokumentacji powykonawczej w języku polskim.

114. 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.

115. Wykonawca musi dołączyć do oferty oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

116. 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.

9. Oprogramowanie do wykrywania i reagowania na zagrożenia i incydenty – 1 kpl.

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja kompleksowego oprogramowania do wczesnego wykrywania i szybkiego reagowania na zagrożenia, które ma na celu automatyzację, orkiestrację i poprawę skuteczności procesów związanych z zarządzaniem incydentami bezpieczeństwa IT w organizacji. Oprogramowanie będzie musiało spełniać wymogi operacyjne i technologiczne Zamawiającego, zapewniając pełną integrację z istniejącą infrastrukturą oraz optymalizację działań związanych z cyberbezpieczeństwem. Rozwiązanie musi być w pełni kompatybilne z oprogramowaniem do zbierania logów, skanowania podatności oraz analizy danych i incydentów z całej infrastruktury IT, które również są przedmiotem tego postępowania. Zamówienie obejmuje dostawę licencji wieczystej ze wsparciem technicznym na minimum 24 miesiące. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania funkcjonalne

1. Wsparcie dla zespołów reagowania na incydenty komputerowe: Oprogramowanie musi wspomagać procesy monitorowania bezpieczeństwa teleinformatycznego, reagowania na

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).

incydenty, zarządzania podatnościami oraz standaryzację i automatyzację działań analityków cyberbezpieczeństwa w ramach zespołów SOC, CERT, CSIRT, IRT itp.

2. Integracja z systemem SIEM: Oprogramowanie musi natywnie integrować się z dostarczanym systemem klasy SIEM, będącym przedmiotem tego postępowania, z oficjalnym wsparciem producenta SOAR dla tej integracji.

3. Automatyczne tworzenie incydentów: Oprogramowanie musi umożliwiać automatyczne tworzenie incydentów na podstawie powiadomień z SIEM, zgłoszeń e-mail, zgłoszeń z systemów typu helpdesk, takich jak RTIR lub Jira, oraz automatyczne zamykanie obsłużonych zgłoszeń.

4. Ręczne tworzenie incydentów: Oprogramowanie musi umożliwiać ręczne tworzenie incydentów na podstawie:

a. Typów incydentów

b. Pól/etykiet incydentów

c. Typów wskaźników (ang. indicator)

d. Pól/etykiet wskaźników (ang. indicator)

e. Raportów

f. Dashboardów.

5. Klasyfikacja incydentów: Oprogramowanie musi umożliwiać automatyczną i ręczną klasyfikację incydentów według krytyczności oraz tworzenie własnych definicji klasyfikacji. W ramach wdrożenia Wykonawca wraz z Zamawiającym ustali oraz zaimplementuje właściwą klasyfikację incydentów w systemie.

6. Śledzenie i raportowanie incydentów: Oprogramowanie musi umożliwiać śledzenie czasu i działań związanych z incydentami, raportowanie wskaźników takich jak Time-to-detect i Time-to-mitigate oraz posiadać zestaw przygotowanych raportów takich jak:

a. Raport na temat incydentów: dzienny, 7- i 30-dniowy

b. Raport na temat średniego czasu rozwiązania incydentu.

7. Łączenie incydentów: Oprogramowanie musi umożliwiać zarówno ręczne, jak i automatyczne łączenie incydentów, w tym inteligentne łączenie automatyczne.

8. Przydzielanie zadań: Oprogramowanie musi umożliwiać automatyczne przydzielanie predefiniowanych zadań dla danych typów incydentów oraz ręczne przydzielanie incydentów do pracowników.

9. Tworzenie i edycja procedur: Oprogramowanie musi umożliwiać tworzenie i edytowanie procedur reagowania na incydenty w formie graficznej z użyciem podstawowych operatorów logicznych i matematycznych.

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).

10. Weryfikacja incydentów: Oprogramowanie musi umożliwiać automatyczną i ręczną weryfikację atrybutów incydentów w wewnętrznych i zewnętrznych źródłach informacji oraz pozwalać na sprawdzenie, które incydenty nie zostały obsłużone.

11. Wyszukiwanie incydentów: Oprogramowanie musi pozwalać na proste wyszukiwanie incydentów na podstawie ich cech (np. przy użyciu dedykowanego języka zapytań) oraz podobieństwa do innych incydentów (related incidents).

12. Automatyczne działania reagowania: Oprogramowanie musi umożliwiać projektowanie i wdrażanie automatycznych działań reagowania na dane typy incydentów oraz edycję kodu źródłowego tych działań w języku skryptowym takim jak Python 3.

13. Raportowanie i dashboardy: Oprogramowanie musi umożliwiać tworzenie zbiorczych raportów z obsłużonych incydentów, integrację z systemami threat intel/threat hunting/threat share za pomocą API, generowanie dashboardów security, pozwalać na tworzenie własnych raportów oraz dashboardów za pomocą predefiniowanych komponentów umożliwiających wizualizację pożądanych danych (np. wykres kołowy, słupkowy, liniowy, tabela itp.) oraz pozwalać na eksport raportów w formacie:

a. PDF

b. DOCX

14. Dwustronna komunikacja: Oprogramowanie musi umożliwiać dwustronną komunikację z użytkownikami i operatorami systemu SOAR, np. za pomocą interaktywnych formularzy.

15. Gotowe integracje: System musi posiadać co najmniej 250 gotowych integracji z zewnętrznymi systemami.

16. Automatyzacja analizy i działań naprawczych: Oprogramowanie musi automatyzować analizę danych oraz podejmować działania naprawcze, takie jak analiza plików w chmurze sandbox, wysyłanie e-maili do użytkowników oraz blokada dostępu do usług.

17. Biblioteka typów incydentów: Oprogramowanie musi posiadać wbudowaną bibliotekę co najmniej 5 typów incydentów oraz umożliwiać ich edycję i kopiowanie.

18. Obsługa skryptów i integracji: Oprogramowanie musi umożliwiać wykorzystanie zewnętrznych bibliotek oraz programów w skryptach, a także możliwość wglądu w kod integracji oraz jego klonowanie pod kątem wprowadzania modyfikacji lub napisania własnej wersji integracji.

19. Zarządzanie scenariuszami: System musi pozwalać na automatyczne i ręczne wykonywanie dostępnych scenariuszy oraz umożliwiać tworzenie, edycję i uruchamianie scenariuszy (playbooków) za pomocą graficznego interfejsu, w tym tworzenie zadań warunkowych i scenariuszy zagnieżdżonych (tzn. scenariusz nadrzędny może zawierać scenariusze podrzędne uruchamiane na zasadzie pod-scenariuszy, edycja/zmiana pod-scenariusza wpływa automatycznie na wszystkie scenariusze, które go wykorzystują, co ułatwia administrację) zawierających:

a. zadania ręczne

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).

b. zadania zautomatyzowane

c. zadania warunkowe automatyczne

d. zadania warunkowe ręczne

e. akwizycję danych przy użyciu formularzy

f. filtry danych

g. pod-scenariusze.

20. Uruchamianie i zatrzymanie scenariuszy: Oprogramowanie musi pozwalać na uruchomienie scenariusza w trybie krokowym w celu analizy jego poprawności i usunięcia ewentualnych błędów, pozwalać na okresowe uruchamianie scenariuszy w zdefiniowanym czasie i wedle harmonogramu, pozwalać na ponowne uruchomienie scenariusza na konkretnym incydencie, jeżeli zajdzie taka potrzeba, pozwalać na zatrzymanie scenariusza w trakcie jego wykonania, pozwalać na doraźne wykonanie dowolnego zadania automatyzacyjnego przez operatora SOC, bez konieczności tworzenia nowych / modyfikacji istniejących scenariuszy (np. przy użyciu wiersza poleceń) oraz pozwalać na przydzielanie zadań pojedynczego scenariusza różnym członkom zespołu SOC.

21. Dokumentowanie i monitorowanie scenariuszy: Oprogramowanie musi umożliwiać dokumentowanie uruchomionych scenariuszy wraz z wynikami jego działania, wizualizacje przebiegu wykonania scenariusza (wizualizacje rezultatu wszystkich wykonanych oraz pominiętych zadań, operacji warunkowych, decyzji itp.), monitorowanie ich stanu (w przypadku wystąpienia jakichkolwiek anomalii w trakcie wykonania scenariusza, osoby odpowiedzialne za incydent powinny zostać natychmiast o tym poinformowane) oraz sterowanie ich wykonaniem przez operatorów drogą korespondencyjną (m.in. z poziomu wiadomości email oraz wiadomości w komunikatorze takim jak np. Microsoft Teams, Slack, Mattermost itp.).

22. Współpraca i transfer wiedzy: System musi wspierać współpracę pomiędzy członkami zespołu SOC, pozwalać na delegowanie zadań innym członkom zespołu SOC w ramach oceny danego incydentu, pozwalać na odczytywanie wyników analizy i wykorzystaniu ich w kolejnych zadaniach uruchomionego scenariusza, pozwalać na sprawdzenie historycznych danych na temat uruchomionych scenariuszy / zadań oraz umożliwiać zapisywanie historycznych incydentów do celów szkoleniowych i transferu wiedzy.

23. Podłączanie innych jednostek: System musi mieć możliwość działania jako platforma SOAR dla wielu instytucji/jednostek z całkowitą separacją zasobów i przetwarzanych danych (tzw. wsparcie dla trybu multi-tenant).

24. Wsparcie dla MISP: Oprogramowanie musi umożliwiać eksport i import danych z/do serwerów MISP oraz eksport incydentów w formatach STIX 1/2, CSV, DOCX, PDF.

25. Definicja wskaźników i enrichment: Oprogramowanie musi posiadać repozytorium wskaźników (ang. indicators), które kolekcjonuje i koreluje wskaźniki w ramach wszystkich incydentów, alertów i feedów dostarczanych do rozwiązania, umożliwiać definiowanie własnych wskaźników, automatyczną weryfikację wskaźników (enrichment), obsługę

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).

formatów takich jak JSON, CSV, STIX 1.X i STIX 2.X oraz wspierać minimum następujące typy wskaźników:

a. numery kart płatniczych

b. IBAN

c. adres email

d. konto użytkownika

e. wyniki CVE

f. domena

g. FQDN

h. nazwy hosta

i. IP (v4 oraz v6)

j. klucz i ścieżka rejestru

k. URL

l. CIDR.

26. Integracja z MITRE ATT&CK: System musi natywnie integrować się z MITRE ATT&CK i przypisywać odpowiednie techniki i taktyki do incydentów.

27. Dostępność interfejsu w dwóch językach: Interfejs użytkownika musi być dostępny w polskiej wersji językowej.

Wymagania Techniczne

1. Skalowalność: System musi być skalowalny i umożliwiać łatwą rozbudowę o dodatkowe serwery/urządzenia bez konieczności wprowadzania zmian programistycznych.

2. Wysoka dostępność: System musi zapewniać mechanizmy klastrowe, redundancję elementów oraz być odporny na awarie poszczególnych komponentów.

3. Wydajność: System musi oferować wysoką wydajność wszystkich komponentów, z możliwością skalowania przez dodanie kolejnych serwerów aplikacyjnych/web.

4. Ograniczenie bezpośredniej komunikacji: Aplikacje klienckie nie mogą komunikować się bezpośrednio z bazą danych.

5. Wsparcie dla infrastruktury Zamawiającego: Wykonawca, przy współpracy z Zamawiającym, musi określić wymagania dotyczące środowiska sprzętowego, które będzie bezpieczne, wydajne i stabilne, oraz dostarczyć system możliwy do zainstalowania na Red Hat Enterprise Linux 8 lub nowszym, lub Windows Server 2019 Datacenter lub nowszym.

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).

6. Opcja wirtualnego appliance: System może być dostarczony jako wirtualny appliance pod warunkiem, że obraz appliance jest dostępny na oficjalnej stronie producenta z dedykowanym systemem operacyjnym i regularnymi poprawkami bezpieczeństwa.

7. Aktualizacje: Wszystkie komponenty systemu, w tym również systemy operacyjne oraz bazy danych, muszą być regularnie aktualizowane, a ich instalacja musi umożliwiać wprowadzanie poprawek oraz nowych wersji udostępnianych przez producenta (w szczególności dotyczących bezpieczeństwa).

8. Uwierzytelnianie: System musi integrować się z Active Directory na Windows Server, zapewniając uwierzytelnianie użytkowników i administratorów poprzez logowanie z użyciem loginu i hasła AD. Zamawiający nie dopuszcza możliwości instalowania żadnych zabezpieczeń fizycznych w postaci kart, kluczy USB, fizycznych sieciowych serwerów licencyjnych.

9. Autoryzacja: Autoryzacja administratorów Systemu musi bazować na rolach użytkowników. Rozwiązanie musi udostępniać mechanizm wielopoziomowego hierarchizowania uprawnień do jego zasobów z możliwością przydzielania i odbierania uprawnień przez administratora Systemu lub domeny Active Directory.

10. Administratorzy: Każdy Administrator rozwiązania musi posiadać indywidualne konto, pozwalające na jego jednoznaczną identyfikację. Identyfikator Administratora musi pokrywać się kontem Użytkownika w domenie Active Directory.

11. Użytkownicy: System musi zapewniać obsługę co najmniej 15 jednoczesnych użytkowników o różnych rolach. Niniejszy wymóg stanowi wymaganie wydajnościowe dla systemów.

12. Dostęp do Systemu: Dostęp musi być realizowany za pomocą przeglądarki internetowej, przy czym akceptowanym sposobem transmisji danych do przeglądarki WWW jest szyfrowanie przepływu danych, w szczególności należy wykorzystać szyfrowanie danych protokołem TLS. System musi być wyposażony w certyfikaty SSL (dostarczone przez Zamawiającego z wewnętrznego lub komercyjnego CA) dla serwerów WWW, a transmisja danych musi odbywać się z wykorzystaniem do tego celu protokołu HTTPS.

13. Aplikacja kliencka: Aplikacja kliencka Systemu musi posiadać minimalne wymagania dla łącza przy pracy w sieci WAN lub Internet z przepustowością maksymalnie 1024 Kbps na jednego użytkownika oraz musi pracować w kontekście standardowego użytkownika Windows

14. Bezpieczeństwo transmisji: System musi szyfrować ruch sieciowy za pomocą bezpiecznych protokołów kryptograficznych, takich jak TLSv1.2, SSH 2 lub nowsze wersje, przy czym komunikacja z przeglądarką użytkowników musi wykorzystywać TLSv1.3. Nie jest dopuszczalne stosowanie protokołu IPSec oraz protokołów SSL 2.0, SSL 3.0, TLS 1.0 i TLS 1.1 i starszych.

15. Antywirus i hardening: Oprogramowanie antywirusowe musi być zainstalowane na wszystkich serwerach systemu, a konfiguracje komponentów muszą być zoptymalizowane pod kątem bezpieczeństwa zgodnie z zaleceniami producentów. Konfiguracje wszystkich komponentów w tym systemy operacyjne, bazy danych, serwery aplikacji i inne komponenty

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).

muszą podlegać procesowi optymalizacji działania i poprawy stanu zabezpieczeń (hardeningu) na podstawie zaleceń producentów wykorzystywanego oprogramowania, ogólnie uznanych za poprawne zasad i standardów bezpieczeństwa oraz ogólnodostępnymi benchmarkami np. CIS Benchmarks https://www.cisecurity.org/cisbenchmarks/. Wykonawca dostarczy szczegółowe wytyczne do utwardzania konfiguracji wszystkich elementów Systemu, w szczególności hardening powinien obejmować:

a. instalację wyłącznie niezbędnych pakietów oprogramowania (lub usunięcie zbędnych),

b. instalację i uruchamianie wyłącznie niezbędnych usług sieciowych (lub wyłączenie zbędnych),

c. ustalenie restrykcyjnych praw dostępu do wszystkich krytycznych obiektów w Systemie,

d. parametry udostępnionych usług sieciowych.

16. Wsparcie dla przeglądarek: Aplikacja webowa musi być zgodna z Microsoft Edge na platformie MS Windows oraz Google Chrome na MS Windows, bez korzystania z technologii, które nie są wspierane przez W3C. Wymagane jest, aby Wykonawca dopasowywał w ramach gwarancji technicznej rozwiązanie do poprawnej współpracy z aktualną wersją stabilną w/w przeglądarek w miarę udostępnianych przez producenta aktualnych wersji lub poprawek dla danej wersji. Aplikacja webowa nie może korzystać z komponentów ActiveX i wtyczek NPAPI oraz nie może wykorzystywać Flasha, Silverlighta, apletów Java ani innej technologii klienckiej, która nie jest natywnie wspierana przez standardy W3C w przeglądarkach;

17. Szyfrowanie danych: Wymagane jest stosowanie zaufanych certyfikatów X.509 dostarczonych przez Zamawiającego, które muszą być zgodne z infrastrukturą PKI lub zakupione komercyjnie.

18. System operacyjny i komponenty: System musi być oparty na wersji systemu operacyjnego, która jest wspierana przez producenta systemu oraz inne niezbędne komponenty. Wszystkie komponenty, aplikacje i usługi serwerowe muszą być uruchamiane jako usługi systemowe.

19. Audyt: Rozwiązanie musi posiadać wewnętrzny dziennik zdarzeń (audyt). Dziennik zdarzeń musi zawierać całą historię wszystkich operacji oraz składni realizowanych zapytań wykonywanych przez użytkowników Systemu. Rozwiązanie musi posiadać możliwość konfigurowalnego raportowania i automatycznego monitorowania i logowania aktywności Operatorów.

20. Kopie zapasowe: System musi być objęty systemem kopii zapasowych w ramach prowadzonego postępowania. Musi być zapewnione wykonywanie kopii zapasowej minimum konfiguracji Systemu.

21. Infrastruktura: System ma być w całości posadowiony w infrastrukturze Zamawiającego (ang. on-premises). Nie jest dopuszczalne aby System lub jakikolwiek jego komponent wymagał komunikacji z elementami posadowionymi poza infrastrukturą zamawiającego (np. zewnętrzne serwery licencji). Żaden z serwerów oraz aplikacja kliencka nie mogą wymagać do poprawnej pracy komunikacji z siecią Internet tj. komponentami posadowionymi poza

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).

infrastrukturą Zamawiającego przez sieć Internet. Wyjątkiem od tego wymogu są tylko ewentualne aktualizacje sygnatur.

22. Zgodność z wymaganiami: System musi spełniać wymagania, aby zapewnić poprawne działanie w infrastrukturze sieciowej Zamawiającego i być kompatybilny z funkcjonującą infrastrukturą.

23. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

Dokumentacja

1. Dostarczenie pełnej dokumentacji technicznej, w tym instrukcji instalacji, konfiguracji oraz użytkowania systemu w języku polskim lub angielskim.

2. Dokumentacja powykonawcza musi być w języku polskim.

Zakres wdrożenia

1. Analiza przedwdrożeniowa: Ocena obecnej infrastruktury bezpieczeństwa, identyfikacja potrzeb oraz opracowanie planu wdrożenia w języku polskim. Wykonawca określi szczegółowo niezbędne do działania Systemu wymagania w zakresie infrastruktury sieciowej i systemowej stosując zasadę przyznawania minimalnych, potrzebnych do poprawnej pracy uprawnień (np. wymagania w zakresie komunikacji sieciowej z dokładnością po portów TCP/UDP, uprawniania do usług katalogowych).

2. Dostawa licencji SOAR: Zapewnienie licencji na oprogramowanie zgodnie z potrzebami organizacji, w tym wersje testowe oraz produkcyjne.

3. Instalacja i konfiguracja: Instalacja oprogramowania w środowisku Zamawiającego, w tym konfiguracja na podstawie wcześniej zidentyfikowanych wymagań. Zamawiający zastrzega sobie prawo nadzoru i uczestnictwa w procesie instalacji Systemu. Wykonawca dostarczy procedury/instrukcje instalacji i konfiguracji dla wszystkich komponentów Systemu. Zamawiający nie dopuszcza dostępu zdalnego do produkcyjnego środowiska/Systemu zainstalowanej u Zamawiającego.

4. Integracja z istniejącą infrastrukturą: Połączenie rozwiązania SOAR z istniejącymi systemami SIEM, EDR, firewallami, bazami danych, systemami zgłoszeń oraz innymi narzędziami używanymi w organizacji.

5. Szkolenie administratorów: Przeprowadzenie szkolenia dla personelu technicznego w zakresie obsługi, konfiguracji oraz utrzymania systemu.

6. Wsparcie powdrożeniowe: Zapewnienie wsparcia technicznego przez okres co najmniej 24 miesiące od zakończenia wdrożenia, obejmującego pomoc techniczną, usuwanie usterek

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).

oraz dostarczanie aktualizacji. Wymagane oświadczenie producenta z potwierdzeniem zaoferowanego poziomu wsparcia technicznego.

Harmonogram realizacji

1. Etap 1: Analiza przedwdrożeniowa – do 4 tygodni od podpisania umowy.

2. Etap 2: Dostawa licencji i instalacja – do 6 tygodni od zakończenia analizy przedwdrożeniowej.

3. Etap 3: Konfiguracja i integracja z infrastrukturą – do 10 tygodni od zakończenia instalacji.

4. Etap 4: Szkolenia i uruchomienie produkcyjne – do 12 tygodni od zakończenia konfiguracji.

5. Etap 5: Wsparcie powdrożeniowe – przez 24 miesiące od zakończenia wdrożenia.

10. Oprogramowanie EDR – 1 kpl.

Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja oprogramowania EDR na minimum 75 stacji końcowych w formie agentów, które zapewnia zaawansowaną ochronę punktów końcowych (endpointów) w infrastrukturze informatycznej zamawiającego. Oprogramowanie ma na celu ochronę w zakresie minimum: ochrona przed oprogramowaniem ransomware, posiada zaawansowane techniki ochrony przed złośliwym oprogramowaniem malware, exploitami oraz atakami Advanced Persistent Threat (APT), posiada ochronę antytamperową, aktualizuje sygnatury i heurystykę. Zamówienie obejmuje zarówno licencje na oprogramowanie, jak i usługi wdrożeniowe, dlatego wymagane jest uwzględnienie obu elementów w ofercie. W celu weryfikacji funkcjonalności oferowanych przez proponowane oprogramowanie, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymagania

1. Ochrona przed zagrożeniami:

a. Ochrona przed znanym oraz nowo wykrytym (zero day) złośliwym oprogramowaniem, ransomware i exploitami.

b. Zabezpieczenie przed zagrożeniami pochodzącymi z różnych wektorów ataku, w tym z sieci, poczty elektronicznej, stron internetowych i urządzeń.

c. Ochrona przed zaawansowanymi zagrożeniami typu APT.

d. Automatyczne aktualizacje zapewniające najnowszą ochronę.

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).

2. Monitorowanie i analiza:

a. Monitorowanie ryzyka na poziomie punktów końcowych.

b. Ciągłe monitorowanie aktywności procesów w chmurze.

c. Przechowywanie danych przez 12 miesięcy w celu retrospektywnej analizy ataków.

d. Graficzne przedstawienie incydentów oraz informacji o cyklu życia zagrożeń dostępne w konsoli webowej.

e. Możliwość eksportu danych dotyczących cyklu życia zagrożeń do analizy lokalnej.

f. System posiada możliwość wybrania jednej lub więcej stacji roboczej, która przeskanuje ich sieć w poszukiwaniu stacji, które nie są obecnie zarządzane przez System.

g. System posiada możliwość alertowania e-mail (z opcjami włącz/ wyłącz dany alert). W skład alertów muszą się znajdywać minimum: detekcja malware, detekcja exploitu, stacja robocza z problemami, stacja robocza bez licencji, znalezienie stacji roboczej nie zarządzanej przez system.

3. Zarządzanie i konfiguracja:

a. Intuicyjny interfejs administracyjny w języku polskim lub angielskim umożliwiający centralne zarządzanie politykami bezpieczeństwa oraz monitorowanie stanu ochrony wszystkich urządzeń w sieci.

b. Centralna, chmurowa konsola zarządzania z możliwością natychmiastowej izolacji zainfekowanych komputerów.

c. Dziedziczenie ustawień między grupami i punktami końcowymi.

d. Możliwość konfigurowania i stosowania ustawień zarówno na poziomie grup, jak i pojedynczych punktów końcowych.

e. Zarządzanie bezpieczeństwem oparte na widokach punktów końcowych oraz dynamicznych filtrach.

f. Przypisywanie ról użytkownikom konsoli zgodnie z predefiniowanymi ustawieniami.

g. Audytowanie aktywności użytkowników oraz dostosowywanie alertów lokalnych.

h. Instalacja oprogramowania za pomocą pakietów MSI, linków do pobrania oraz e-maili wysyłanych do użytkowników.

i. Deinstalacja agenta lokalnie jest chroniona hasłem.

j. Możliwość tymczasowego wyłączenia/ ochrony lokalnie po podaniu hasła.

k. System posiada możliwość wybrania jednej lub więcej stacji roboczej, które będą działać jako pamięć podręczna do przechowywania aktualizacji, instalatorów i wszelkich innych pakietów pobranych z Internetu. Wszystkie inne stacje robocze będą automatycznie korzystać ze stacji podręcznych, które znajdą w sieci. Jeśli znajdą więcej niż jedną stację podręczną, użyją jednej lub drugiej w zależności od ich dostępności.

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).

l. System posiada możliwość pracy minimum w 3 trybach operacyjnych dla systemów Windows:

◦ Śledzi aktywność każdego programu na komputerach. Nieznane programy mogą być uruchamiane. Złośliwe i potencjalnie złośliwe programy są usuwane.

◦ Śledzi aktywność każdego programu na komputerach. Złośliwe i potencjalnie złośliwe programy są usuwane. Nieznane programy z Internetu, innych komputerów w sieci lub z zewnętrznych dysków są blokowane do czasu ustalenia przez laboratorium producenta, czy są one złośliwym oprogramowaniem. Inne nieznane programy mogą być uruchamiane, gdy są analizowane przez laboratorium.

◦ Śledzi aktywność każdego programu na komputerach. Złośliwe i potencjalnie złośliwe programy są usuwane. Nieznane programy są blokowane, dopóki laboratorium producenta nie ustali, czy są złośliwe.

m. System posiada możliwość pracy w minimum 3 trybach dla systemów Linux:

◦ Śledzenie aktywności każdego programu na stacjach roboczych.

◦ Śledzenie aktywności każdego programu na stacjach roboczych i blokowanie złośliwych i potencjalnie złośliwych programów.

◦ Brak wykrywania złośliwych i potencjalnie złośliwych programów.

4. Integracja i raportowanie:

a. Integracja z narzędziami ConnectWise Automate, Kaseya VSA, N-able N-central oraz N-able N-sight.

b. Dostępność API do integracji zewnętrznej.

c. Generowanie raportów na żądanie oraz według harmonogramu, na różnych poziomach z różnym stopniem szczegółowości.

d. Udostępnienie kluczowych wskaźników wydajności (KPI) oraz dashboardów do zarządzania bezpieczeństwem.

e. Możliwość integracji z innymi narzędziami bezpieczeństwa IT oraz systemami SIEM.

f. Możliwość współpracy z każdym oprogramowaniem antywirusowym dostępnym na rynku

g. Wsparcie dla automatyzacji zadań administracyjnych i reagowania na incydenty.

5. Zgodność i obsługiwane platformy:

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

b. Technologia anty-exploitowa zapewniająca ochronę przed wykorzystaniem luk w zabezpieczeniach.

c. Automatyczne wykrywanie niechronionych punktów końcowych.

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).

d. Zabezpieczenie połączeń VPN (wymagana integracja z dostarczonym UTM w postępowaniu) oraz dostęp do sieci Wi-Fi przez punkty dostępu.

e. Usługa o wysokiej dostępności oraz zgodność z certyfikatami platform hosta.

6. Szybka reakcja na incydenty:

a. System musi umożliwiać automatyczne wykrywanie i eliminowanie zagrożeń w czasie rzeczywistym.

b. Powinien zapewniać narzędzia do szczegółowej analizy i raportowania incydentów bezpieczeństwa.

c. Funkcjonalność izolowania zainfekowanych urządzeń w celu zapobiegania dalszemu rozprzestrzenianiu się zagrożeń.

7. Zapewnienie automatycznych i regularnych aktualizacji oprogramowania oraz baz danych z zagrożeniami.

8. Wdrożenie:

a) Analiza przedwdrożeniowa:

- Przeprowadzenie analizy infrastruktury IT pod kątem wdrożenia EDR.
- Opracowanie szczegółowego planu wdrożenia.

b) Instalacja i konfiguracja:

- Instalacja i konfiguracja oprogramowania na wskazanych punktach końcowych.
- Konfiguracja polityk bezpieczeństwa zgodnie z wymaganiami zamawiającego.
- Testy funkcjonalne systemu.

c) Dostarczenie pełnej dokumentacji technicznej i użytkowej.

9. Gwarancja: Zamawiający wymaga licencji na okres minimum 24 miesięcy, z możliwością przedłużenia. Licencja powinna obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.

10. 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.

11. Przełącznik szkieletowy – 1 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 1 szt. przełącznika szkieletowego.

Wymagania

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. 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. Przełącznik musi posiadać system operacyjny (firmware) dostarczony przez producenta urządzenia; zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.

2. Wymagane parametry fizyczne:

a. montaż w stelażu/szafie 19”

b. maksymalna wysokość 1U

c. dwa redundantne zasilacze 230V AC typu hot-swap o mocy min. 1000W każdy

d. zakres temperatur pracy ciągłej co najmniej od -5 do +45 °C

e. zakres wilgotności pracy co najmniej 5% - 95%

f. ochrona przed przepięciami: ±6 kV

g. MTBF: minimum 370 000 h

h. minimum 2 moduły wentylatorów umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap)

3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:

a. 12 portów 10/25 Gbit/s SFP28

b. 12 portów 1/10 Gbit/s RJ45 z obsługą PoE++ (802.3bt 90W/port z jednoczesną obsługą pełnej mocy na min. 6 portach)

c. 12 portów 1 Gbit/s RJ45 z obsługą PoE++ (802.3bt 90W/port z jednoczesną obsługą pełnej mocy na wszystkich portach) z możliwością upgrade’u do 10Gbit/s

d. 2 porty 40/100 Gbit/s QSFP28

4. Dostępna łączna moc PoE na przełączniku: min. 1680W

5. Przełącznik musi posiadać następujące porty służące do zarządzania:

a. Port konsoli. Zamawiający dopuszcza port konsoli RS232 ze złączem RJ45

b. dedykowany port zarządzający out-of-band Ethernet 10/100Base-T

c. wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych

6. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:

a. Zarządzanie stosem poprzez jeden adres IP

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).

b. Do min. 9 jednostek w stosie

c. Magistrala stackująca o wydajności min. 800Gb/s

d. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)

e. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree

f. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia

g. Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink QSFP28.

7. Układ przełączający o wydajności min. 1.4 Tbps, wydajność przełączania przynajmniej 480 Mpps

8. Obsługa min. 128 000 adresów MAC

9. Wbudowana pamięć RAM min. 4 GB

10. Procesor min. czterordzeniowy. . Minimalne taktowanie procesora 1400MHz.

11. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 2 GB

12. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)

13. Możliwość skonfigurowania min. 1024 interfejsów vlan interface SVI działających równocześnie

14. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad

15. Obsługa LAG

16. Obsługa ramek jumbo o wielkości min. 9216 bajtów

17. Obsługa protokołu GVRP

18. Wsparcie dla G.8032 ERPS

19. Obsługa protokołu VRRP

20. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).

21. Wsparcie dla mechanizmu PVST+.

22. Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-ISv6, BGPv4, BGPv4+, RIP, RIPng, PIM-SM i PIM-DM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania

23. Obsługa min. 192 000 tras dla routingu IPv4

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).

24. Obsługa min. 80 000 tras dla routingu IPv6

25. Obsługa min. 80 000 IPv6 neighbor discovery (ND)

26. Obsługa protokołów związanych z obsługą ruchu typu multicast:

a. IGMP v1, v2 i v3

b. IGMP Snooping v1, v2 i v3

c. PIM-SM i PIM-DM

d. MSDP i MLD Snooping

e. minimum 64 000 tras multicast dla IPv4 i minimum 4 000 tras multicast dla IPv6

27. Obsługa VRF

28. Minimalny rozmiar tablicy ARP 140 000 wpisów

29. Obsługa protokołów LLDP i LLDP-MED

30. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP Relay, DHCP Client

31. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

a. min. 3 poziomy dostępu administracyjnego poprzez konsolę

b. autoryzacja użytkowników w oparciu o IEEE 802.1x, RADIUS oraz TACACS (lub równoważny)

c. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www

d. zarządzanie urządzeniem przez HTTPS, SNMPv3 i SSHv2 za pomocą protokołów IPv4 i IPv6 z możliwością podłączenia do oprogramowania chmurowego producenta oraz przez system zarządzania producenta instalowany na serwerach wirtualizacji

e. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP

f. obsługa mechanizmów MACsec, Dynamic ARP Inspection, Super-VLAN (min. 256), Sub-VLAN (min. 1000), MUX VLAN, Voice VLAN oraz private VLAN (lub równoważny)

g. Ochrona przed atakami typu UDP flood, TCP SYN flood oraz ICMP flood

h. możliwość synchronizacji czasu zgodnie z NTP

32. Obsługa MPLS wraz ze wsparciem dla L3VPN oraz VPLS. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania

33. Obsługa BPDU, Root oraz Loop protection

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).

34. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:

a. klasyfiacja 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 algorytmów: Priority Queuing (PQ), Weighted Deficit Round Robin (WDRR), PQ+WDRR, Weighted Round Robin (WRR) oraz PQ+WRR.

35. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP.

36. Wymagane opcje zarządzania:

a. możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN

b. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)

c. wsparcie dla skyptów python uruchamianych na urządzeniu

d. wsparcie dla RMON

37. 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

38. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 9 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.

39. Wsparcie dla funkcjonalności VXLAN. Jeżeli obsługa powyżej funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający nie wymaga jej dostarczenia.

40. Urządzenie musi posiadać funkcjonalności WLAN:

a. Przełącznik musi umożliwiać obsługę funkcjonalności kontrolera WLAN celem zarządzania punktami dostępowymi WiFi tego samego producenta.

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).

b. Obsługę punktów dostępowych (access-point) pracujących w standardzie: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 1, 802.11ac wave 2, 802.11ax.

c. Mechanizmów uwierzytelniania: WPA/WPA2 with PSK, EAP-MD5, EAP-TLS, PEAP.

d. Możliwość zarządzania minimum 1000 access-pointów. Jeżeli powyższa funkcjonalność wymaga licencji to w ramach niniejszego postępowania Zamawiający nie wymaga dostarczenia licencji.

41. Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego switcha, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.

42. Zamawiający wymaga, aby przełączniki posiadały 36 miesięczny serwis gwarancyjny świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. 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).

43. Usługa serwisu musi być świadczona w języku polskim.

44. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancyjny urządzeń.

45. Oświadczenie producenta lub Wykonawcy z potwierdzeniem zaoferowanego poziomu gwarancji.

46. Zakres prac wdrożeniowych:

a. Analiza przedwdrożeniowa:

i. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.

ii. Opracowanie planu wdrożenia.

b. Wdrożenie i konfiguracja:

i. Instalacja przełącznika oraz podłączenie do sieci.

ii. Konfiguracja przełącznika zgodnie z wymaganiami zamawiającego.

iii. Integracja z istniejącymi systemami IT zamawiającego.

c. Testy akceptacyjne:

i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.

ii. Weryfikacja poprawności działania przełącznika.

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).

12. Przełącznik dostępowe – 2 szt.

Przedmiotem zamówienia jest dostawa, instalacja oraz konfiguracja 2 szt. przełączników dostępowych .

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 35 cm

d. minimum jeden zasilacz 230V AC

e. zakres temperatur pracy ciągłej co najmniej od 0°C do +45 °C

f. zakres wilgotności pracy co najmniej 5% - 90%

3. Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:

a. 24 porty 100/1000BASE-T

b. 4 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC

4. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.

5. Przełącznik musi posiadać następujące porty służące do zarządzania:

a. Port konsoli. Zamawiający dopuszcza port konsoli ze złączem Micro-USB lub port konsoli RS232 ze złączem RJ45

6. 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 80Gb/s

e. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)

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).

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.

7. Układ przełączający o wydajności min. 128 Gbps, wydajność przełączania przynajmniej 95 Mpps

8. Obsługa min. 32 500 adresów MAC

9. Wbudowana pamięć RAM min. 1GB.

10. Procesor wielordzeniowy. Minimalne taktowanie procesora 1000MHz

11. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB

12. Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)

13. Możliwość skonfigurowania min. 32 interfejsów vlan interface SVI działających równocześnie

14. Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad

15. Obsługa minimum 120 grup LAG

16. Obsługa ramek jumbo o wielkości min. 9216 bajtów

17. Obsługa sFlow

18. Wsparcie dla G.8032 ERPS

19. Obsługa protokołu VRRP

20. Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).

21. Wsparcie dla mechanizmu PVST+.

22. Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania.

23. Obsługa min. 6 100 tras dla routingu IPv4

24. Obsługa min. 2 000 tras dla routingu IPv6

25. Obsługa min. 2 000 IPv6 neighbor discovery (ND)

26. Obsługa protokołów związanych z obsługą ruchu typu multicast:

a. IGMP v1, v2 i v3

b. IGMP Snooping v2 i v3

c. PIM-SM, PIM-SSM i PIM-DM

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).

d. MSDP i MLD Snooping

e. minimum 2000 tras multicast dla IPv4 i minimum 1000 tras multicast dla IPv6

27. Minimalny rozmiar tablicy ARP 4000 wpisów

28. Obsługa protokołów LLDP i LLDP-MED.

29. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client

30. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

a. min. 3 poziomy dostępu administracyjnego poprzez konsolę

b. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL

c. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC

d. obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1500 reguł ACL

e. zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2

f. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP

g. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard

h. możliwość synchronizacji czasu zgodnie z NTP lub SNTP

31. 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, WDRR, DRR, WFQ

32. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).

33. 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

34. Wraz z urządzeniami muszą zostać dostarczone:

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).

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

35. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 9 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy

36. Urządzenia i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanych switchy, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

37. Zamawiający wymaga, aby urządzenia posiadały 36 miesięczny serwis gwarancyjny świadczony przez Wykonawcę lub autoryzowany serwis producenta. Wymiana uszkodzonego elementu w trybie 9x5xNBD. 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).

38. Usługa serwisu musi być świadczona w języku polskim.

39. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.

40. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

41. Wraz z urządzeniem należy dostarczyć systemu centralnego zarządzania pochodzący od producenta oferowanych urządzeń.

42. 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.

43. 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.

44. 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.

45. System centralnego zarządzania musi umożliwiać:

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).

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

46. Zakres prac wdrożeniowych:

a. Analiza przedwdrożeniowa:

i. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.

ii. Opracowanie planu wdrożenia.

b. Wdrożenie i konfiguracja:

i. Instalacja przełączników oraz podłączenie do sieci.

ii. Konfiguracja przełączników zgodnie z wymaganiami zamawiającego.

iii. Integracja z istniejącymi systemami IT zamawiającego.

c. Testy akceptacyjne:

i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.

ii. Weryfikacja poprawności działania przełączników.

13. UPS – 1 szt.

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

Wymagania

1. MOC min. 6000VA/6000W

2. Obudowa Rack o wysokości maksymalnej 2U

3. Topologia On-line

4. Kształt napięcia w trybie bateryjnym: Czyste napięcie sinusoidalne

5. Czas ładowania akumulatorów: do 4 godzin

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).

6. UPS powinien posiadać zainstalowane wewnętrzne akumulatory

7. Czas podtrzymania systemu dla obciążenia 3300 W– min 17 min przy wykorzystaniu przestrzeni w szafie rack max. 4U dla UPSa i modułu bateryjnego łącznie.

8. Możliwość rozbudowy systemu do uzyskania podtrzymania 3 godzin dla w/w obciążenia

9. Ilość gniazd wyjściowych C13: co najmniej 4

10. Ilość gniazd wyjściowych C19: co najmniej 2

11. UPS musi posiadać wydzieloną grupę gniazd dla obciążeń kluczowych, krytycznych oraz dla pozostałych obciążeń.

12. Porty komunikacyjne: USB/S232/EPO

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. Gwarancja min. 24 miesiące

16. Oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.

17. Urządzenie i oprogramowanie muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi dołączyć do oferty oświadczenie producenta oferowanego UPSa, potwierdzające pochodzenie urządzenia i oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

18. Zakres prac wdrożeniowych:

a. Analiza przedwdrożeniowa:

i. Przeprowadzenie analizy potrzeb i wymagań zamawiającego.

ii. Opracowanie planu wdrożenia.

b. Wdrożenie i konfiguracja:

i. Instalacja UPS oraz podłączenie do wskazanych serwerów oraz urządzeń.

ii. Konfiguracja UPS zgodnie z wymaganiami zamawiającego.

iii. Integracja z istniejącymi systemami IT zamawiającego.

c. Testy akceptacyjne:

i. Przeprowadzenie testów funkcjonalnych i wydajnościowych wymaganych przez Zamawiającego potwierdzających zadeklarowane funkcjonalności. Wynik negatywny jakiejkolwiek funkcjonalności lub testu pozwala Zamawiającemu odrzucić proponowaną ofertę i odstąpić od umowy bez podania przyczyny.

ii. Weryfikacja poprawności działania UPS.

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).