Numer sprawy DL-271-41/24- załącznik numer 3 **PAKIET NUMER 1**

**Wykonawca:**

……………………………………………………………

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/ CEiDG)

**FORMULARZE:**

**FORMULARZ CENOWY**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Lp. | Pozycja oferty | Producent | Nazwa, model i wersja produktu lub oprogramowania | Liczba szt / zestaw | Cena jednostkowa netto w PLN | Wartość zamówienia netto w PLN | Stawka podatku VAT  Kwota podatku VAT | Wartość zamówienia brutto w PLN |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 (5x 6) | 8 | 9 (7+8) |
| 1 | System przestrzeni dyskowej wraz z usługą wdrożenia |  |  | 1 |  |  |  |  |
| 2 | Rozbudowa macierzy dyskowej wraz z usługą wdrożenia |  |  | 1 |  |  |  |  |
| 3 | Rozbudowa serwerów wraz z usługą wdrożenia |  |  | 1 |  |  |  |  |
| 4 | Rozbudowania oprogramowania HPE Aruba Clear Pass Policy Manager wraz z usługą wdrożenia |  |  | 1 |  |  |  |  |
| 5 | Oprogramowanie do wieloskładnikowego uwierzytelnienia wraz z usługą wdrożenia |  |  | 1 |  |  |  |  |
| xx | RAZEM | xxxxxxx | xxxxxx | xxxx | xxxxxxxxxxx |  |  |  |

**FORMULARZE- PARAMETRY WYMAGANE**

System przestrzeni dyskowej – 1szt.

|  |  |  |
| --- | --- | --- |
| **lp.** | **WYMAGANIA MINIMALNE** | **Spełnia**  **Tak/Nie**  Wypełnia wykonawca |
| 1 | **Obudowa i komponenty**  System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''. Podzespoły systemu przestrzeni dyskowej tj. wentylatory, zasilacze muszą być w pełni redundantne, żeby zapewnić odpowiedni poziom bezpieczeństwa. |  |
| 2 | **Pojemność**  System musi zostać dostarczony w konfiguracji zawierającej minimum:  42 fizyczne dyski 15,3TB NVME na pętli 100GbE  oraz posiadać możliwość rozbudowy o kolejne dyski w ramach pary dwukontrolerowej do minimum 240 fizycznych dysków.  System musi wspierać dyski NVMe o wielkościach w zakresie od 1900GB do co najmniej 30 000GB |  |
| 3 | **Parametry kontrolerów**  Dwa kontrolery wyposażone w co najmniej 512GB pamięci cache każdy.  Zamawiający dopuszcza zaoferowanie rozwiązania z mniejszą ilością cache na kontroler, jeżeli zostanie zaoferowane rozwiązanie wielokontrolerowe z sumaryczną ilością cache 1280GB. System wielokontrolerowy musi pozwalać na utworzenie jednej przestrzeni na wszystkich kontrolerach.  W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub za pomocą zrzutu danych na pamięć nie ulotną.  Procesory systemu przestrzeni dyskowej powinny być wykonane w technologii x86 wielordzeniowej z przynajmniej 92 rdzeniami na klaster kontrolerów. Zamawiający dopuszcza procesory wykonane w innej technologii z min 112 rdzeniami na każdy kontroler.  System przestrzeni dyskowej musi pozwalać na rozbudowę do klastra 24 kontrolerów lub musi pozwalać na obsługę przynajmniej 1152 dysków w obrębie pary kontrolerów lub klastra w szczególności rozbudowę w technologii NVMe z obsługą min 1152 dysków w technologii NVME. | Dodatkowo podać: parametry kontrolerów |
| 4 | **Parametry interfejsów sieciowych**  Oferowany system przestrzeni dyskowej musi posiadać minimum:   * 4 porty 1Gb RJ45 * 8 portów 100GbE QSFP28 * 8 portów 25Gb SFP28 * 2 porty konsolowy ze złączem RJ45   System przestrzeni dyskowej musi pozwalać na rozbudowę lub zamianę na dodatkowe porty:   * 4 porty 100GbE QSFP28 * 4 porty 32Gb FC   Urządzenie ma zostać dostarczone z następującym zestawem kabli i akcesoriów:   * 8 modułów SFP28 * 4 kable DAC QSFP28 o długości minimum 0,5 metra. |  |
| 5 | **Funkcjonalność RAID**  System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID. |  |
| 6 | **Funkcjonalność kopii migawkowych**  System przestrzeni dyskowej musi być wyposażony w funkcjonalność kopii migawkowych, dostępną dla wszystkich rodzajów danych przechowywanych na systemie przestrzeni dyskowej. Działanie funkcjonalności kopii migawkowych nie może powodować spadku wydajności przy odczycie więcej niż 5%. |  |
| 7 | **Obsługiwane protokoły**  System przestrzeni dyskowej musi obsługiwać jednocześnie następujące protokoły: FC; iSCSI; NFS (v3, v4, v4.1), NVMe/FC, NVMe/TCP, CIFS/SMB (3,0; 3.1.1). |  |
| 8 | **Pozostałe funkcjonalności**  System przestrzeni dyskowej musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych in-line. System przestrzeni dyskowej musi posiadać także funkcjonalność kompresji danych in-line.  Jeżeli oferowane rozwiązanie nie pozwala na deduplikację i kompresję działającą w trybie in-line (w locie) lub nie posiada możliwości deduplikacji i kompresji, zamawiający wymaga dostarczenia 4 krotnej pojemności wyspecyfikowanej w punkcie 2.  Zamawiający wymaga by dostarczona licencja na funkcjonalność deduplikacji i kompresji nie miała żadnych ograniczeń pojemnościowych, a także została dostarczona na najwyższy możliwy stopień deduplikacji/kompresji, jeżeli istnieje takie licencjonowanie.  System przestrzeni dyskowej musi posiadać wsparcie dla wielościeżkowości dla systemów Microsoft Windows Server 2019 i nowszych, Linux, VMware vSphere,  System przestrzeni dyskowej musi posiadać funkcjonalność priorytetyzacji zadań w tym ustawienie max parametrów (I/Ops i Mbps) dla poszczególnych LUN.  System przestrzeni dyskowej musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych (blokowych i plikowych) bez przerywania pracy systemu przestrzeni dyskowej i bez przerywania dostępu do danych znajdujących się na danym wolumenie.  System przestrzeni dyskowej musi posiadać funkcjonalność replikacji danych z inny system przestrzeni dyskowej tego samego producenta w trybie synchronicznym i asynchronicznym. Funkcjonalność replikacji danych musi być natywnym narzędziem oferowanego systemu.  System przestrzeni dyskowej musi posiadać możliwość tworzenia zasobów typu WORM.  System musi posiadać moduł do zabezpieczenia przed atakiem ransomware, który w szczególności musi:   * informować administratora w przypadku niestandardowego zachowania systemu oraz danych * wykonywać automatycznie prewencyjną kopię migawkową „snapshot” w przypadku zagrożenia atakiem ransomware, * wykrywać z wyprzedzeniem potencjalnych zainfekowanych użytkowników/zasoby.   System przestrzeni dyskowej musi posiadać funkcjonalność klonowania danych bez potrzeby fizycznego kopiowania danych na nośnikach.  W celach bezpieczeństwa system przestrzeni dyskowej musi posiadać funkcjonalność wieloetapowej akceptacji wybranych operacji tj. operacje takie jak: Skasowanie LUN/Wolumeny, skasowanie Snapshotu, wyłączenie replikacji. System musi pozwalać by wykonanie w/w operacji było akceptowane przez przynajmniej dwóch administratorów w celu zwiększenia bezpieczeństwa i uniknięcia błędów ludzkich.  Zaoferowana konfiguracja systemu przestrzeni dyskowej musi osiągnąć wydajność do 620 000IOPS przy 8Kb bloku i stosunku 70/30% odczyt/zapis przy czasie opóźnienia maksymalnie 2 ms. **Zamawiający wraz z ofertą wymaga dostarczenia oficjalnego dokumentu producenta oferowanego rozwiązania z wymiarowaniem wydajności oraz dopuszcza możliwość sprawdzenia wydajności systemu przestrzeni dyskowej przy odbiorze.**  System przestrzeni dyskowej musi posiadać narzędzie umożliwiające generowanie raportu o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne systemu przestrzeni dyskowej.  System przestrzeni dyskowej musi być wyposażony w oprogramowanie do audytu zasobów plikowych, w szczególności umożliwiające:   * blokowanie zapisywania plików z określonym (do zdefiniowania przez administratora) rozszerzeniem, * monitorowanie operacji wykonywanych na plikach.   Zamawiający wymaga, by wraz z dostarczanym rozwiązaniem, dostarczono oprogramowanie producenta oferowanego rozwiązania pozwalające na:   * monitoring wykorzystania przestrzeni na systemie przestrzeni dyskowej, * monitoring grup RAIDowych, * monitoring wykonywanych backupów/replikacji danych między systemami przestrzeni dyskowej, * monitoring wydajności system przestrzeni dyskowej, * analizę i diagnozę spadku wydajności, * wykonanie spójnej kopii migawkowej (snapshot), minimum dla następujących aplikacji: VMware vSphere, MS SQL, MS Exchange, MS Hyper-V.   Oferowane rozwiązanie musi umożliwiać udostępnienie zasobów dyskowych w postaci minimum pojedynczego plikowego udziału sieciowego o pojemności co najmniej 400TB.  Oferowane rozwiązanie musi wspierać konfigurację klastra geograficznego. Przez klaster geograficzny zamawiający rozumie automatyczne przełączanie zasobów z jednego dwukontrolerowego systemu przestrzeni dyskowej na inny dwukontrolerowego system przestrzeni dyskowej w trybie:   * bez ingerencji administratora, * z ingerencją administratora.   Wszystkie funkcjonalności systemu przestrzeni dyskowej opisane w niniejszej tabeli muszą być dostarczone na dostarczaną pojemność urządzenia i pozwalać na wspólne(jednoczesne) działanie (żadna funkcjonalność nie może wykluczać działania innej funkcjonalności). |  |
| 9 | **Gwarancja i serwis**  5 lat serwisu z 2 godzinnym gwarantowanym czasem odpowiedzi i wymianą części na następny dzień roboczy po diagnozie problemu. W ramach serwisu musi być możliwość zgłaszania awarii w trybie 24x7.  Dostarczony system musi posiadać również 5 lat subskrypcji dla dostarczonego wraz z systemem przestrzeni dyskowej oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.  Uszkodzone dyski pozostają własnością zamawiającego |  |

Rozbudowa Macierzy Dyskowej – 1 zestaw

|  |  |  |
| --- | --- | --- |
| **lp.** | **WYMAGANIA MINIMALNE** | **Spełnia**  **Tak/Nie**  Wypełnia Wykonawca |
| 1 | Rozbudowa macierzy dyskowej Unity XT 380 o następujący zestaw dysków:  Dysk 1.8TB SAS – 24 szt.  Dysk 4TB NL-SAS – 12szt.  Wraz z dostarczanymi dyskami należy dostarczyć moduły dyskowe kompatybilne z macierzą umożliwiające montaż wszystkich dostarczanych dysków.  Zamawiający dopuszcza dostarczenie dysków odnawianych (Refurbished)  Gwarancja 2 lata |  |

Rozbudowa Serwerów – 1 zestaw

|  |  |  |
| --- | --- | --- |
| **lp.** | **WYMAGANIA MINIMALNE** | **Spełnia**  **Tak/Nie**  Wypełnia Wykonawca |
| 1 | Rozbudowa serwerów Dell PowerEdge R740 o następujący zestaw pamięci RAM:  Pamięć RAM: 32GB 2Rx4 2993Y – 24szt.  Zamawiający dopuszcza dostarczenie pamięci RAM odnawiane (Refurbished)  Gwarancja 2 lata |  |

Rozbudowa oprogramowania HPE Aruba ClearPass Policy Manager– 1 szt

|  |  |  |
| --- | --- | --- |
| **lp.** | **WYMAGANIA MINIMALNE** | **Spełnia**  **Tak/Nie**  Wypełnia Wykonawca |
| 1 | Rozbudowa systemu do autoryzacji dostępu do sieci HPE Aruba Clear PassPolicy Manager o funkcjonalność klastra wysokiej dostępności.  Obecnie Zamawiający posiada licencje: Aruba ClearPass Cx000V VM Appl E-LTU  Wsparcie producenta na okres 5 lat. |  |

Oprogramowanie do wieloskładnikowego uwierzytelnienia – 1 szt

|  |  |  |
| --- | --- | --- |
| **lp.** | **WYMAGANIA MINIMALNE** | **Spełnia**  **Tak/Nie**  Wypełnia Wykonawca |
| 1 | System musi być dostępny jako aplikacja mobilna lub fizyczny token. |  |
| 2 | System musi wspierać uwierzytelnianie wieloskładnikowe na stacje robocze, VPN, serwisy chmurowe dla co najmniej 10 użytkowników równolegle. |  |
| 3 | System musi posiadać własne repozytorium tożsamości tak, aby mógł działać bez zewnętrznych źródeł danych, jeśli będzie taka konieczność. |  |
| 4 | System musi mieć możliwość podłączenia do następujących repozytoriów tożsamości: baza danych na urządzeniu typu firewall (minimum producenta), RADIUS Client, SAML, ADFS, RD Web, RESTful API Client. |  |
| 5 | System musi zapewniać obsługę i mieć możliwość uwierzytelnienia wieloskładnikowego dla stacji roboczych Microsoft Windows, które nie są w domenie. |  |
| 6 | System musi posiadać scentralizowaną bazę reguł uwierzytelniających dla użytkowników. |  |
| 7 | System musi działać, zanim użytkownik zaloguje się na urządzenie. |  |
| 8 | System musi zawierać różne metody uwierzytelniania: notyfikacja push, kod QR, OTP. |  |
| 9 | System musi wspierać uwierzytelnianie wieloskładnikowe również offline. |  |
| 10 | System musi być dostępny przez konsole webową, hostowaną przez producenta rozwiązania. |  |
| 11 | System musi mieć podział w zarządzaniu na: użytkowników, grupy, źródła (punkty dostępu), tożsamość zewnętrzną (uzyskanie informacji o kontach użytkowników i zatwierdzanie haseł), Gateway producenta. |  |
| 12 | Aplikacja mobilna musi być darmowa. |  |
| 13 | Aplikacja mobilna musi pozwalać na zarządzanie i zapisywanie poświadczeń. |  |
| 14 | Aplikacja mobilna musi posiadać możliwość zabezpieczenia tokenów przez PIN lub biometryczne ID. |  |
| 15 | Aplikacja mobilna musi wspierać: iOS 12.0 lub nowsza, iPadOS 12.0 lub nowsza, Android 7.0 lub nowszy. |  |
| 16 | System musi mieć możliwość instalacji Gateway producenta, aby uwierzytelnianie mogło komunikować się z klientami RADIU i bazami danych LDAP. |  |
| 17 | Gateway musi być dostępny do pobrania na stronie producenta. |  |
| 18 | System musi posiadać agenta, który zostanie zainstalowany na stacji roboczej. |  |
| 19 | System musi obejmować ochronę również RDP i RD Gateway. |  |
| 20 | Agent musi wspierać systemy operacyjne Windows (Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 11, Windows 10, Windows 8.1) oraz macOS (Monterey (12.x), Big Sur (11.x), Catalina (10.15), Mojave (10.14), High Sierra (10.13), Sierra (10.12), El Capitan (10.11)) |  |
| 21 | Gateway musi wspierać: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Amazon Corretto 8 do Amazon Coretto 15, Oracle JRE 8 (update 162) do Oracle JDK 15. |  |
| 22 | ADFS musi wspierać: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, .Net Framework 4.5 |  |
| 23 | RD Web musi wspierać: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, .NET Framework 4.8 |  |
| 24 | W celu działania uwierzytelniania wieloskładnikowego dla ADFS, system może korzystać z Gateway’a producenta. |  |
| 25 | Konsola webowa musi zawierać monitorowanie systemu, minimum dla: aktywności użytkowników, uwierzytelniania (udanego, nieudanego, użytkownika, tokenu, daty, metody), danych o danym źródle, ilości notyfikacji push odrzuconych przez użytkowników, tokenów (które nie zostały aktywowane), synchronizacji z LDAP (jeżeli została użyta). |  |
| 26 | System musi posiadać możliwość zarządzania hasłami. |  |
| 27 | Zarządzanie hasłami musi posiadać dostępny skarbiec dla minimum aplikacji mobilnej od tego samego producenta oraz rozszerzeniu przeglądarki również od tego samego producenta. |  |
| 28 | System pozwala na udostępnienie hasła ze skarbca dla innych użytkowników firmy przypisanych przez administratora. |  |
| 29 | System musi posiadać funkcję generowania bezpiecznego hasła. |  |
| 30 | Generator musi mieć możliwość określenia wymagań dotyczących długości i znaków dla wygenerowanego hasła. |  |
| 31 | System musi posiadać funkcję raportowania ocen siły haseł. |  |
| 32 | Raporty w menedżerze haseł muszą również wyświetlać podane informacje: - ujawnione hasła – liczba używanych haseł, które zostały ujawnione w wyniku naruszenia bezpieczeństwa danych. - słabe hasła – liczba haseł, które nie są uważane za złożone. - zduplikowane hasła – liczba haseł używanych do więcej niż jednego konta. - stare hasła – liczba haseł, które nie były zmieniane od dłuższego czasu. |  |
| 33 | System musi pozwalać na dodawanie prywatnych haseł użytkownikom. |  |
| 34 | System musi pozwalać na dodawanie przez administratora haseł firmowych, dostępnych dla wydzielonej grupy użytkowników. |  |
| 35 | System musi pozwalać na automatyczne logowanie z użyciem podanych poświadczeń dla danych adresów URL/domen. |  |
| 36 | System musi oddzielać hasła prywatne od haseł firmowych minimum w formie różnych zakładek w aplikacji lub rozszerzeniu przeglądarki. |  |
| 37 | System musi wspierać import zapisanych haseł z zewnętrznych menedżerów haseł, takich jak Google Chrome, do magazynu haseł. |  |
| 38 | System musi mieć możliwość eksportu hasła z prywatnego skarbca do pliku .CSV. |  |
| 39 | System musi posiadać możliwość ręcznego wymuszenia synchronizacja urządzenia z kontem, w celu pobrania haseł. |  |
| 40 | Użytkownik musi mieć możliwość przypomnienia hasła za pomocą specjalnego klucza odzyskiwania. |  |
| 41 | Po wykonaniu akcji przypomnienia hasła, system musi wygenerować nowy klucz odzyskiwania. |  |
| 42 | System musi nie pozwalać na przywrócenie hasła bez użycia klucza odzyskiwania. |  |
| 43 | **Wsparcie**  Wsparcie producenta na okres 5 lat. |  |

Usługa wdrożenia.

1. Usługi w zakresie dostawy systemu przestrzeni dyskowej
   1. Instalacja urządzeń w szafie RACK w miejscu wyznaczonym przez Zamawiającego
   2. Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
   3. Okablowanie sieciowe urządzeń
   4. Podłączenie systemu przestrzeni dyskowej do przełączników rdzeniowych Zamawiającego Dell S5224F-ON
   5. Konfiguracja na przełączniki Dell S5224F-ON wymaganych portów typu SFP28,
   6. Konfiguracja dedykowanej sieci VLAN na przełącznikach Dell S5224F-ON w celu wystawienia przestrzeni dyskowej,
   7. Konfiguracja na przełączniki Dell S5224F-ON funkcjonalności jumbo frames dla podłączanych portów,
   8. Konfiguracja połączeń agregowanych z wykorzystaniem protokołu LACP na przełącznikach sieciowych Dell S5224F-ON,
   9. Konfiguracja protokołu RDMA, na przełącznikach sieciowych S5224F-ON.
   10. Uruchomienie i weryfikacja poprawności działania urządzeń
   11. Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
   12. Konfiguracja adresacji IP interfejsów zarządzania
   13. Konfiguracja protokołu synchronizacji czasu NTP
   14. Konfiguracja protokołu rozwiązywania nazw DNS
   15. Konfiguracja agregacji połączeń z wykorzystaniem protokołu LACP i podłączenie systemu przestrzeni dyskowej do przełączników Dell S5224F-ON
   16. Instalacje niezbędnych licencji do uruchomienia wymaganych funkcjonalności
   17. Integracja uwierzytelniania systemu przestrzeni dyskowej z domeną MS Active Directory
   18. Migracja danych na nowy system
   19. Integracja z domeną MS Active Directory w celu konfiguracji uprawnień dostępowych dla poszczególnych usług oraz użytkowników.
   20. Konfiguracja przestrzeni dyskowych zgodnie z wymaganiami Zamawiającego
   21. Konfiguracja interfejsów Front-End zgodnie z wymaganiami Zamawiającego
   22. Konfiguracja mechanizmów zabezpieczeń przestrzeni dyskowych (snapshot)
   23. Konfiguracja mechanizmów deduplikacji oraz kompresji,
   24. Konfiguracja przestrzeni dyskowej wraz z jej zabezpieczeniem,
   25. Wystawienie przestrzeni dyskowej do systemów IT wskazanych przez Zamawiającego,
   26. Wykonanie testów działania nadmiarowości komponentów i poprawności konfiguracji w zakresie połączeń Front-End i odporności na zanik napięcia w jednym źródle zasilania
2. Usługi w zakresie rozbudowy macierzy dyskowej o dyski
   1. Instalacja dostarczanych dysków w macierzach dyskowych Dell EMC Unity XT 380 wskazanych przez Zamawiającego,
   2. Instalacja oprogramowania układowego dostarczanych dysków twardych,
   3. Weryfikacja poprawności działania dysków twardych.
   4. Rekonfiguracja przestrzeni dyskowej dyskowej,
   5. Rekonfiguracja polityk snapshotowych,
   6. Rekonfiguracja polityk replikacji danych,
   7. Aktualizacja wystawianej przestrzeni dyskowej do systemów IT Zamawiającego,
3. Usługi w zakresie rozbudowy serwerów o pamięć ram
   1. Instalacja dostarczanych pamięci RAM w serwerach Dell PowerEdge R740 Zamawiającego,
   2. Migracja wirtualnych maszyn z serwera, który będzie podlegał dodaniu kości RAM,
   3. Wyłączenie systemu VMware ESXi,
   4. Wyłączenie serwera Dell PowerEdge R740
   5. Instalacja nowych pamięci RAM,
   6. Uruchomienie serwera i weryfikacja poprwności działnia zainstslownych pamięci RAM,
   7. Uruchomienie systemu VMware ESXi,
   8. Migracja powrotna wirtualnych maszyn,
   9. Weryfikacja poprawności działania środowiska wirtualnego,
   10. Powyższą rozbudowę należy wykonać dla trzech serwerów R740 pracujących w klastrze wysokiej dostępności opartego o środowisku wirtualizacyjnego VMware vSphere
4. Usługi w zakresie rozbudowy oprogramowania HPE Aruba ClearPass Policy Manager
   1. Wdrożenie wirtualnej maszyny HPE Aruba ClearPass Policy Manager VM w środowisku wirtualizacyjnym Zamawiającego VMware vSphere,
   2. Konfiguracja paramentów wirtualnej maszyny w tym wirtualnej przestrzeni dyskowej, wirtualnych procesorów oraz wirtualnej pamięci RAM,
   3. Konfiguracja parametrów wirtualnej maszyny zgodnie z najlepszymi praktykami producenta,
   4. Konfiguracja parametrów wirtualnej sieci LAN,
   5. Instalacja oprogramowania Aruba ClearPass Policy Manager,
   6. Rozbudowa obecnego systemu Aruba ClearPass Policy Manager o nadmiarową konsole do zarządzania,
   7. Konfiguracja klastra wysokiej dostępności,
   8. Przeprowadzenie testów poprawności dziania klastra,
   9. Weryfikacja poprawności autoryzacji użytkowników.
5. Usługi w zakresie wieloskładnikowego uwierzytelnienia
   1. Wdrożenie wirtualnej maszyny w środowisku Zamawiającego VMware vSphere, z systemem operacyjnym Microsoft Windows Serwer 2022,
   2. Integracja systemu z domeną Zamawiającego Microsoft Active Directory,
   3. Konfiguracja systemu operacyjnego wirtualnej maszyny zgodnie z najlepszymi praktykami producenta,
   4. Instalacja i wdrożenie Gateway systemu do wieloskładnikowego uwierzytelniania,
   5. Weryfikacja poprawności działania,
   6. Konfiguracja polityk bezpieczeństwa na klastrze UTM WatchGuard Firebox posiadanym przez Zamawiającego w celu dostosowania do wymagania dostarczanego systemu do wieloskładnikowego uwierzytelniania.
   7. Integracja klastra UTM WatchGuard Firebox posiadanego przez Zamawiającego z systemem do wieloskładnikowego uwierzytelnienia,
   8. Konfiguracja usługi VPN realizowanego przez klaster UTM WatchGuard Firebox w celu integracji z systemem do wieloskładnikowego uwierzytelniania,
   9. Konfiguracja dodatkowych usług wskazanych przez Zamawiającego w celu integracji z systemem do wieloskładnikowego uwierzytelniania.
   10. Przygotowanie procedury generowania tokenów dla nowych użytkowników.
6. Przeprowadzenie testów akceptacyjnych
   1. Opracowanie scenariuszy testów akceptacyjnych wraz z Zamawiającym
   2. W ramach zakończonych testów akceptacyjnych, Wykonawca sporządzi protokół zawierający listę wraz z wynikiem przeprowadzonych testów.
7. Przygotowanie dokumentacji powykonawczej,
   1. Opracowanie dokumentacji powykonawczej wdrożonego rozwiązania, zawierającej minimum:
   2. Topologia fizyczna sieci LAN oraz SAN,
   3. Topologia logiczna sieci LAN oraz SAN,
   4. Adresacja IPv4,
   5. Konfiguracje protokołów sieciowych,
   6. Konfiguracje sieci VLAN,
   7. Konfiguracje dostarczonego systemu przestrzeni dyskowej
   8. Konfiguracje dostarczanego oprogramowania do wieloskładnikowego uwierzytelniania

**FORMULARZ- PARAMETRY TECHNICZNE- OCENIANE**

|  |  |  |  |
| --- | --- | --- | --- |
| **lp.** | **Parametry techniczne- Oceniane (waga 40%)** | **Waga Punktu** | **Spełnia**  **Tak/Nie**  Wypełnia Wykonawca |
| 1 | **System przestrzeni dyskowej**  System przestrzeni dyskowej musi posiadać funkcjonalność „Tieringu” zimnych danych na:   * inny system przestrzeni dyskowej tego samego producenta (z wolnymi dyskami np. NL-SAS) * inny system przestrzeni dyskowej dowolnego producenta z protokołem S3. * na zasób S3 dostawcy usługi w chmurze   Funkcjonalność Tieringu musi być natywną funkcjonalnością systemu przestrzeni dyskowej i wykonywać się automatycznie.  System przestrzeni dyskowej umożliwia replikację asynchroniczną na dowolny zasób S3 dowolnego producenta  System przestrzeni dyskowej obsługuje następujące protokoły:   * NFS 4.2, * NFS Trunking, * NFS over RDMA * pNFS | 8 |  |
| 2 | **System przestrzeni dyskowej**  System przestrzeni dyskowej posiada moduł do audytu zasobów plikowych na wyspecyfikowanym systemie przestrzeni dyskowej pod kątem przechowywanych danych wrażliwych/osobowych.  W szczególności moduł musi posiadać:   * Możliwość przeszukiwania zasobów plikowych na wyspecyfikowanym systemie przestrzeni dyskowyej innych serwerach plików jak Windows File server, SYnology File sever, QnapFIle server, Google drive, Onedrive, Azure files, baz danych: Oracle, MySQL, MS SQL, PostgreSQL, Mongo DB, SAP HANA * tworzenie kategorii przeszukanych plików na:   + nie wrażliwe (ogólne informacje o pracowniku)   + dane osobiste (numer NIP, Pesel)   + dane wrażliwe (dane zdrowotne, informacje o wynagrodzeniu) * zgodność z europejskimi przepisami GDPR (RODO), w tym móc przeszukiwać i kategoryzować dane po:   + NIP/Regon   + Pesel   + Adresie Email   + Kontach bankowych | 8 |  |
| 3 | **System przestrzeni dyskowej**  System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum trzech dysków w grupie RAID | 6 |  |
| 4 | **System przestrzeni dyskowej**  System przestrzeni dyskowej musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych (blokowych i plikowych), w tym zwiększanie i zmniejszanie pojemności, bez przerywania pracy systemu przestrzeni dyskowej i bez przerywania dostępu do danych znajdujących się na danym wolumenie. | 8 |  |
| 5 | **System przestrzeni dyskowej**  Przed procesem replikacji system przestrzeni dyskowej musi umożliwiać włączenie procesu deduplikacji danych i kompresji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów. | 8 |  |
| 6 | **Oprogramowanie do wieloskładnikowego uwierzytelnienia**  System musi posiadać możliwość monitorowania domeny w Dark Web dla minimum 3 domen. Jeżeli okaże się, że naruszenie danych obejmuje dane adresy e-mail i domeny, administrator zostanie o tym natychmiast powiadomiony.  System musi pozwalać na ręczne sprawdzanie domen, adresów lub adresu e-mail w celu znalezienia wycieku danych w Dark Web. | 2 |  |

kwalifikowany podpis elektroniczny