***Znak sprawy* *Załącznik nr 1B do SWZ***

Szczegółowy opis przedmiotu zamówienia publicznego pn. **„Cyberbezpieczny Samorząd - Gmina Lubenia”** realizowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, w ramach projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23, zgodnie z udzielonym grantem o numerze FERC.02.02-CS.01-001/23/0551/ FERC.02.02-CS.01-001/23/2024.

Przedmiotem zamówienia jest dostawa licencji na oprogramowanie, nie aktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania oraz nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne zarówno od wad fizycznych jak i prawnych. Zamawiający zastrzega sobie możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów u Producenta w przypadku wystąpienia wątpliwości co do ich legalności.

Poniższe parametry należy traktować jako wymagania minimalne. Jeżeli wskazano producenta lub inne cechy charakterystyczne dla danego produktu oznacza to, że powyższe informacje są podane przykładowo i określają jedynie minimalne oczekiwane parametry jakościowe oraz wymagany standard. Potencjalni Wykonawcy korzystając z oficjalnych kanałów dystrybucyjnych mają możliwość zaoferowania produktów których cechy wyszczególniono poniżej i które z punktu widzenia Zamawiającego będą pożądane ze względu na zastosowane rozwiązania w swojej infrastrukturze, dotyczy to zarówno zasobów sprzętowych ale również zasobów ludzkich zaangażowanych w utrzymanie ciągłości działania urządzeń, systemów i sieci. Powyższe nie wyklucza możliwości zaoferowania rozwiązań równoważnych których cechy, funkcjonalność oraz późniejsza eksploatacja będą zgodne z wymaganiami Zamawiającego. Aby umożliwić Wykonawcom prawidłowe skalkulowanie oferty dla rozwiązań równoważnych, tam gdzie to konieczne przygotowano kryteria równoważności.

***Poz.1 Serwerowy system operacyjny wraz dostępem dla 25 użytkowników***

|  |  |
| --- | --- |
| Nazwa parametru | Wartość parametru |
| Ilość | **16 sztuk** |
| Producent  | Microsoft  |
| Klasa produktu | System operacyjny |
| Typ licencji  | Komercyjna |
| Rodzaj licencji | Nowa licencja |
| Okres licencji | Bezterminowa |
| Jednostka licencjonowania | 16 rdzeni procesora |
| Architektura | 64 bit |
| Seria/model | Microsoft Windows Server Standard 2022 64 Bit  |
| Język | Polski |
| Wymagania ogólne | Licencje systemu operacyjnego Microsoft Windows Server 2022 Standard 16-core lub oprogramowania równoważnego nie mogą posiadać ograniczeń czasowych, muszą pochodzić z oficjalnego kanału dystrybucji. Licencje nie mogą być dedykowane tylko do jednego producenta sprzętu serwerowego. |
| Cechy rozwiązania równoważnego | Ilość i rodzaj licencji pozwolą Zamawiającemu uruchomienie następującej konfiguracji środowiska serwerowego: klaster HA - dwie maszyny fizyczne posiadające łącznie 4 procesory 16 rdzeniowe (2 procesory na serwer), całość umożliwi uruchomienie sześciu maszyn wirtualnych. Zastosowane licencjonowanie nie może posiadać ograniczeń czasowych, powinno pochodzić z oficjalnego kanału dystrybucji. Licencje dostępowe nigdy nie aktywowane oraz zgodne z zaproponowanym systemem serwerowym. Zastosowane licencjonowanie powinno zapewnić legalny dostęp do opisanego powyżej środowiska serwerowego dla 25 użytkowników z dowolnej liczby punktów końcowych.1. Współpraca z procesorami o architekturze x86 – 64bit.
2. Instalacja i użytkowanie aplikacji 32-bit i 64-bit na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 16 rdzeni.
5. Praca w roli klienta domeny Microsoft Active Directory.
6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
8. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
9. Możliwość uruchomienia roli serwera stron WWW.
10. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
11. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania
12. oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
* pozwalają na zmianę rozmiaru w czasie pracy systemu,
* umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
* umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
* umożliwiają zdefiniowanie list kontroli dostępu (ACL)
1. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
2. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji
3. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
4. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
5. Możliwość wykorzystania standardu http/2.
6. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych
7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa,
8. pomoc, komunikaty systemowe.
9. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
10. Mechanizmy logowania w oparciu o: login i hasło, karty z certyfikatami (smartcard), wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM)
11. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych
12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play)
13. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
14. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
15. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
16. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach
17. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
* podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
* usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1
* zdalna dystrybucja oprogramowania na stacje robocze,
* praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
* Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: dystrybucję certyfikatów poprzez http, konsolidację CA dla wielu lasów domeny, automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509
* szyfrowanie plików i folderów,
* szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
* szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
* możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
* serwis udostępniania stron WWW,
* wsparcie dla protokołu IP w wersji 6 (IPv6),
* wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
* wbudowane mechanizmy wirtualizacji (Hypervisor)
* możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci
* możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności
* mechanizmy wirtualizacji mające wsparcie dla: dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, obsługi ramek typu jumbo frames dla maszyn wirtualnych, obsługi 4-KB sektorów dysków, nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego
* możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów
* możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet
* wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath)
* mechanizmy deduplikacji i kompresji na wolumenach
* mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty
* wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu
* mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów
* możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).
 |

***Poz.2 Oprogramowanie do wykonywania kopii zapasowych***

|  |  |
| --- | --- |
| Nazwa parametru | Wartość parametru |
| Ilość | 1 sztuka |
| Producent  | Nakivo |
| Klasa produktu | System bakcupu  |
| Typ licencji  | Komercyjna |
| Rodzaj licencji | Nowa licencja, bezterminowa |
| Okres wsparcia | 24 miesiące |
| Jednostka licencjonowania | socket, workstations |
| Zastosowanie | Oprogramowanie wspomagające wykonywanie kopii zapasowych  |
| Seria/model | Nakivo Pro Essentials perpetual, 4 socket,25 workstations, 2y support |
| Język | Polski lub Angielski |
| Wymagania ogólne | Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk serwerowych oraz znajdować się na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 400, - minimalna ocena z referencji 4,8 |
| Cechy rozwiązania równoważnego | 1. Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji:
* Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
* Vmware vSphere min. w wersjach v5.5-7.0.3
* Nutanix AHV 5.15, 5.20 (LTS)
* Maszyny fizyczne: Windows Server 2022, 2019, 2016
* Microsoft 365 (Exchange online, One Drive for Business, Sharepoint)
1. Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
2. Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
* na serwerze Windows lub Linux
* jako maszyna wirtualna Vmware
* jako maszyna wirtualna Amazon
* na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
1. Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
2. Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
3. Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
4. Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności
5. W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 2 lat wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania
6. W ramach dostawy wymagane jest dostarczenie licencji na ochronę 4 gniazd procesorów w hostach Vmware lub Hyper-V
7. W ramach dostawy wymagane jest dostarczenie licencji na ochronę 25 maszyn fizycznych z systemem operacyjnym Windows 10/11 Pro lub Ubuntu Desktop
8. Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
9. Oprogramowanie musi posiadać funkcje backupu i replikacji
* Backup maszyn wirtualnych Vmware
* Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
* Backup maszyn wirtualnych Hyper-V
* Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
* Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
* Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
* Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
* Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
* Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych. Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
* Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
1. Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych
* Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
* Kompresja backupu, w tym konfigurowalny stopień kompresji
* Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
1. Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych
* Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
* Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
* Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji: Microsoft Exchange 2013, 2016, 2019 oraz Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
* Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
* Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
* Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
* Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
1. Oprogramowanie musi posiadać poniższe funkcje
* Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
* Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
* Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
* Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu): Microsoft Exchange, Active Directory, MS SQL
* Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.
1. Oprogramowanie do backupu musi pozwalać na
* Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
* Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
* Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
* Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
1. Oprogramowanie musi pozwalać na następujące formy zarządzania
* Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
* Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
* Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
* Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
* Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
 |
| Dla rozwiązania równoważnego Wykonawca zapewni | Wdrożenie rozwiązania przeprowadzone przez certyfikowanego technika producenta oprogramowania.Szkolenie dla pracownika IT Zamawiającego (min. 4h w siedzibie Zamawiającego) zakres szkolenia powinien obejmować:* Instalację konsoli zarządzającej,
* Konfigurację repozytoriów,
* Konfigurację węzłów,
* Konfigurację zadań backupu,
* Konfigurację zadań replikacji,
* Weryfikację poprawności działania rozwiązania
 |

***Poz.3 Licencja analizator logów***

|  |  |
| --- | --- |
| Nazwa parametru | Wartość parametru |
| Ilość | 1 sztuka |
| Producent  | Fortinet |
| Klasa produktu | Analizator logów |
| Kod producenta | FAZ-VM-GB5, FC1-10-LV0VM-248-02-DD |
| Typ licencji  | Komercyjna |
| Rodzaj licencji | Nowa licencja |
| Okres wsparcia | 24 miesiące |
| Jednostka licencjonowania | UNIT |
| Zastosowanie | Zbieranie informacji z sieci, analizę informacji, także raportowanie, zapewnia szeroki zakres danych na temat działania sieci i urządzeń  |
| Seria/model | FortiAnalyzer-VM Support 2 Year 24x7 FortiCare Contract (for 1-6 GB/Day of Logs), Upgrade license for adding 5 GB/Day of Logs and 3 TB storage capacity. |
| Język | Polski |
| Wymagania ogólne | W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer, Microsoft Azure, Google Cloud. |
| Wymagania dodatkowe | Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent/wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań – dołączyć do oferty |
| Cechy rozwiązania | 1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.
2. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów
4. W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:
5. Podgląd logowanych zdarzeń w czasie rzeczywistym
6. Możliwość przeglądania logów historycznych z funkcją filtrowania.
7. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: listę najczęściej wykrywanych ataków, listę najbardziej aktywnych użytkowników, listę najczęściej wykorzystywanych aplikacji, listę najczęściej odwiedzanych stron www, listę krajów do których nawiązywane są połączenia, listę najczęściej wykorzystywanych polityk Firewall, informacje o realizowanych połączeniach IPSec
8. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów
9. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514
10. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy
11. W zakresie raportowania system musi zapewniać: generowanie raportów co najmniej w formatach: PDF, CSV. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników, funkcję definiowania własnych raportów, możliwość spolszczenia raportów, generowanie raportów w sposób cykliczny lub na żądanie z możliwością automatycznego przesłania wyników na określony adres lub adresy email
12. W zakresie korelacji zdarzeń system musi zapewniać: korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany, konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System musi korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: malware, aplikacje sieciowe, email, IPS, traffic, systemowe (utracone połączenie vpn, utracone połączenie sieciowe). System musi zapewniać funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
13. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
14. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
15. System musi być objęty serwisem producenta przez okres 24 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
 |