

Medyka dnia: 2025-06-18

Gmina Medyka**Medyka 288****37-732 Medyka**.....
[nazwa zamawiającego, adres]**WYKONAWCY****ubiegający się o zamówienie**

Dotyczy: postępowania o udzielenie zamówienia publicznego:

Nazwa zamówienia: **Poprawa poziomu Cyberbezpieczeństwa w Gminie Medyka**
Numer referencyjny: **BiD.ZP.271.2.2025****WYJAŚNIENIA TREŚCI SWZ**

Zamawiający, Gmina Medyka, działając na podstawie art. 284 ust. 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r., poz. 1320), udostępnia poniżej treść zapytań do Specyfikacji Warunków Zamówienia (zwanej dalej "SWZ") wraz z wyjaśnieniami:

Pytanie nr 1

Zamawiający w załączniku nr 2 do SWZ – Szczegółowy opis przedmiotu zamówienia, tabela 4 System zasilania gwarantowanego UPS 1 szt., nie wskazuje okresu gwarancji producenta wymaganej dla urządzenia.

Prosimy o podanie okresu gwarancji jaki wymaga Zamawiający. Bez podania okresu, Wykonawca przedstawi ofertę ze standardowym okresem gwarancji dla specyfikowanego urządzenia.

Stanowisko (wyjaśnienie) Zamawiającego:**Zamawiający wymaga na urządzenie 36 miesięcznego okresu gwarancji.****Pytanie nr 2**

Zamawiający w załączniku nr 2 do SWZ – Szczegółowy opis przedmiotu zamówienia, tabela 6 Urządzenie UTM - analiza logów z podwójną autentykacją, nie wskazuje okresu gwarancji i subskrypcji licencji dla wymaganych funkcjonalności. Wykonawca podkreśla, że podanie okresu jest kluczowym czynnikiem cenotwórczym dla urządzeń UTM.

Prosimy o podanie okresu gwarancji producenta oraz okresu subskrypcji licencji dla urządzenia. Bez podania ww. wartości Wykonawca przedstawi ofertę ze standardowym okresem gwarancji i okresem

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający wymaga na urządzenie 36 miesięcznego okresu gwarancji producenta oraz okresu subskrypcji licencji

Pytanie nr 3

Zamawiający w załączniku do SWZ – Szczegółowy opis przedmiotu zamówienia, pozycja 2. Serwer (1 szt.), określa wymóg

„Obudowa - Możliwość zainstalowania dedykowanego wewnętrznego napędu Blu-ray”.

Wskazany parametr znacząco ogranicza konkurencyjność postępowania, ponieważ wyłącznie serwery Fujitsu spełniają to wymaganie, co może prowadzić do preferowania jednego producenta naruszenia zasad równego traktowania wykonawców oraz uczciwej konkurencji, wynikających z przepisów dotyczących zamówień publicznych. W związku z powyższym, w celu zapewnienia konkurencyjności oferty oraz optymalnego wykorzystania środków publicznych, prosimy o potwierdzenie, czy Zamawiający dopuści zastosowanie zewnętrznego napędu DVD, który pozwoli na zwiększenie liczby potencjalnych wykonawców i zapewni zgodność z zasadami przejrzystości i konkurencyjności w postępowaniu publicznym.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający dopuszcza zastosowanie zewnętrznego napędu Blu-ray.

Pytanie nr 4

Zamawiający w załączniku do SWZ – Szczegółowy opis przedmiotu zamówienia, pozycja 2. Serwer (1 szt.), określa wymóg

„Płyta główna - 4 złącza PCI Express x16 w tym minimum 3 złącza generacji 5;

Opcjonalnie możliwość uzyskania złącza typu pełnej wysokości tzw. FH”

a jednocześnie wymaga dostarczenia następujących kontrolerów LAN

„Kontrolery LAN Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:

Min 5x 1G Base-T;

Min 2x 10Gbit SFP+, porty obsadzone modułami SR LC;

Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

Kontrolery I/O

Kontroler SAS RAID dla dysków wewnętrznych obsługujący RAID 0,1,10 5;

Wymóg zapewnienia możliwości uzyskania czterech interfejsów 100Gbit QSFP28, przy jednoczesnym wymaganiu portów 1Gbit i 10Gbit, jest nieproporcjonalny do skali rozwiązania, jakim jest pojedynczy serwer o wysokości 1U. Tego typu interfejsy o ultrawysokiej przepustowości są charakterystyczne dla zaawansowanych infrastruktur o dużej skali, co znacząco zwiększa koszty rozwiązania i ogranicza konkurencyjność postępowania. Może to prowadzić do preferowania wąskiego grona producentów oraz nieoptymalnego wykorzystania środków publicznych, co stoi w sprzeczności z zasadami równego traktowania wykonawców i uczciwej konkurencji wynikającymi z przepisów o zamówieniach publicznych.

W celu zapewnienia większej konkurencyjności oferty oraz racjonalnego wydatkowania środków publicznych, prosimy o potwierdzenie, czy Zamawiający dopuści rezygnację z wymogu uzyskania czterech interfejsów 100Gbit QSFP28, pozostawiając wymagania dotyczące portów 1Gbit Base-T oraz 10Gbit SFP+, które są wystarczające dla większości zastosowań serwera o podanej specyfikacji.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający rezygnuje z wymogu z Możliwość uzyskania czterech interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

Pytanie nr 5

Zamawiający w załączniku do SWZ – Szczegółowy opis przedmiotu zamówienia, pozycja 2. Serwer (1 szt.), określa następujące wymagania dla procesorów:

„Procesory - Min Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86_64; osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_fp_base 258 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <http://spec.org/cpu2017/results/cpu2017.html> dla dowolnego serwera z oferty producenta.”

Wskazany wymóg dotyczący publikacji wyniku testu SPECrate2017_fp_base na stronie <http://spec.org/cpu2017/results/cpu2017.html> dla dowolnego serwera z oferty producenta, a nie dla konkretnego modelu dostarczanego serwera, jest nieprecyzyjny i nieadekwatny, ponieważ nie gwarantuje, że oferowany serwer osiągnie wymagany wynik wydajności. Tego typu zapis może prowadzić do niejednoznaczności w ocenie zgodności oferty z wymaganiami oraz

ograniczać konkurencyjność postępowania. Ponadto, wymóg uzyskania wyniku dokładnie 258 pkt w teście SPECrate2017_fp_base znacząco zawęży liczbę dostępnych procesorów, co może preferować określonego producenta i zwiększać koszty rozwiązania, sprzecznie z zasadami optymalnego wykorzystania środków publicznych. Obniżenie wymaganego wyniku bazowego do 255 pkt w teście SPECrate2017_fp_base, przy jednoczesnym zapewnieniu wyniku szczytowego (peak) na poziomie minimum 260 pkt w teście SPECrate2017_fp_peak, nie wpłynie znacząco na wydajność rozwiązania, a pozwoli na zwiększenie konkurencyjności oferty.

W związku z powyższym, prosimy o wyjaśnienie, czy Zamawiający wymaga, aby wynik SPECrate2017_fp_base 258 pkt był osiągnięty dla konkretnego modelu serwera oferowanego w postępowaniu, oraz czy dopuści wynik bazowy na poziomie minimum 255 pkt w teście SPECrate2017_fp_base przy jednoczesnym zapewnieniu wyniku szczytowego na poziomie minimum 260 pkt w teście SPECrate2017_fp_peak. Takie podejście zapewni większą konkurencyjność postępowania przy zachowaniu wysokiej wydajności procesorów i zgodności z zasadami równego traktowania wykonawców.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający podtrzymuje wymagania

Pytanie nr 6

Zamawiający w załączniku do SWZ – Szczegółowy opis przedmiotu zamówienia, pozycja 2. Serwer (1 szt.), określa następujące wymagania dla portów:

„Porty - Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;

minimum 2 porty USB 3.0 dostępne z tyłu serwera;

minimum 2 porty USB 3.0 na panelu przednim;

opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem; ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgąłęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.”

Wymóg dotyczący rozmieszczenia portów USB, tj. minimum 2 porty USB 3.0 z tyłu serwera oraz minimum 2 porty USB 3.0 na panelu przednim, ogranicza elastyczność konfiguracji serwera i może preferować rozwiązania wybranych producentów, co zmniejsza konkurencyjność postępowania. Proponowana alternatywa, zachowująca łączną liczbę 4 portów USB, ale z innym rozkładem

- 2 porty USB 2.0 na panelu przednim,
- 1 port USB 3.0 na panelu tylnym oraz,
- 1 port USB 3.0 wewnątrz serwera,

Takie podejście zwiększyłoby bezpieczeństwo podłączanych dedykowanych urządzeń (np. poprzez ograniczenie fizycznego dostępu do wewnętrznego portu USB) oraz umożliwiła zastosowanie szerszej gamy serwerów dostępnych na rynku. Tego typu rozwiązanie nie wpłynie negatywnie na funkcjonalność serwera, a przyczyni się do optymalnego wykorzystania środków publicznych oraz zgodności z zasadami równego traktowania wykonawców i uczciwej konkurencji wynikającymi z przepisów o zamówieniach publicznych.

W związku z powyższym, prosimy o potwierdzenie, czy Zamawiający dopuści rozwiązanie, w którym zachowana zostanie łączna liczba 4 portów USB, lecz w następującym rozkładzie: 2 porty USB 2.0 na panelu przednim serwera, 1 port USB 3.0 na panelu tylnym serwera oraz 1 port USB 3.0 wewnątrz serwera, co zwiększy bezpieczeństwo i konkurencyjność oferty.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający dopuszcza zmianę w następującym rozkładzie

**2 porty USB 3.0 na panelu przednim,
1 port USB 3.0 na panelu tylnym oraz,
1 port USB 3.0 wewnątrz serwera,**

Pytanie nr 7

Zamawiający w załączniku do SWZ – Szczegółowy opis przedmiotu zamówienia, pozycja 3. Macierz 1 szt, określa następujące wymagania:

„a. „Możliwość wyłączenia cache dla poszczególnych wolumenów.”

b. „Funkcjonalność partycjonowania pamięci cache.”

c. „Urządzenie musi mieć możliwość funkcjonalności wykonywania zdalnej kopii danych pomiędzy macierzami. Funkcjonalność ta powinna być realizowana w trybie synchronicznym lub asynchronicznym z możliwością przełączenia trybu pracy w sposób dynamiczny. Licencja na wykonywanie zdalnej kopii danych powinna obejmować całą przestrzeń dyskową oferowaną przez macierz. Licencja nie jest przedmiotem tego postępowania.”

d. „Zaoferowane rozwiązanie musi posiadać implementację klastra geograficznego. W ramach architektury klastra geograficznego musi być wspierane bezprzerwowe migrowanie maszyn wirtualnych pomiędzy ośrodkami. W przypadku awarii jednego z ośrodków nastąpi bezprzerwowe przełączenie do lokalizacji zapasowej.”

e. „Urządzenie musi obsługiwać co najmniej 200 dysków wewnętrznych. Możliwość podłączenia co najmniej 20 dodatkowych pól dyskowych. Możliwość podłączenia różnego rodzaju dysków w jednej obudowie tj. SAS, SSD, NL-HDD.”

f. „Macierz musi mieć możliwość kompresji sprzętowej i deduplikacji danych. Licencja na tę funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową.”

g. „Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych niż oferowane macierze dyskowe na potrzeby migracji danych. Migracja musi się odbyć w trybie bezprzerwowym.”

h. „Urządzenie musi mieć możliwość wykonywania natychmiastowej kopii danych (point-in-time copy). Funkcjonalność ta powinna być realizowana w trybie copy-on-write. Licencja powinna obejmować całą pojemność macierzy. Urządzenie musi umożliwiać stworzenie mirrorowanych LUN pomiędzy różnymi półkami macierzy, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta. Macierz musi posiadać funkcjonalność, która pozwala na wykonanie kopii migawkowych typu WORM. Licencja na tę funkcjonalność musi być zawarta w cenie i musi obejmować całą oferowaną pojemność macierzy.”

Wskazane wymagania, w szczególności dotyczące klastra geograficznego, wirtualizacji zasobów zewnętrznych macierzy, kopii migawkowych typu WORM, a także wysokiej skalowalności (200 dysków i 20 półek dyskowych), sugerują preferowanie zaawansowanych rozwiązań, takich jak macierz IBM 5045, co znacząco ogranicza konkurencyjność postępowania. Tego typu zapisy, wymagające kosztownych i złożonych funkcjonalności nieprzystających do skali rozwiązania (macierz o pojemności 14 TiB netto), mogą prowadzić do nieoptymalnego wykorzystania środków publicznych oraz naruszenia zasad równego traktowania wykonawców i uczciwej konkurencji wynikających z przepisów o zamówieniach publicznych.

1. Wymóg możliwości wyłączenia cache dla poszczególnych wolumenów oraz partycjonowania pamięci cache jest specyficzny i może ograniczać wybór dostępnych macierzy. Dopuszczenie rozwiązań bez tych funkcjonalności, przy zachowaniu standardowego zarządzania cache, zapewniłoby porównywalną wydajność przy niższych kosztach.

Stanowisko (wyjaśnienie) Zamawiającego:

Funkcjonalność od lat jest dostępna u różnych producentów. Urządzenie będzie użytkowane przez wiele systemów i wiele lat. Zakup ma sprostać obecnym i przyszłym potrzebom Zamawiającego. Zamawiający podtrzymuje wymóg opisany w SWZ.

2. Wymóg zdalnej kopii danych w trybie synchronicznym lub asynchronicznym z dynamicznym przełączaniem oraz implementacja klastra geograficznego z bezprzerwowym migrowaniem maszyn wirtualnych są nieproporcjonalne do skali rozwiązania (pojedyncza macierz o pojemności 14 TiB). Tego typu funkcjonalności są charakterystyczne dla dużych infrastruktur enterprise i znacząco zwiększają koszty, nie przynosząc proporcjonalnych korzyści w kontekście obecnych potrzeb Zamawiającego. Dopuszczenie rozwiązań bez tych funkcjonalności lub z podstawową replikacją asynchroniczną zwiększyłoby konkurencyjność.

Stanowisko (wyjaśnienie) Zamawiającego:

Wielkość, ilość danych nie determinuje potrzeb wysokiej dostępności. Synchroniczna replikacja z mechanizmem HA jest dostępna obecnie w wielu renomowanych rozwiązaniach na rynku we wszystkich segmentach cenowych. Zamawiający podtrzymuje wymóg opisany w SWZ.

3. Wymóg skalowalności do 200 dysków wewnętrznych i 20 dodatkowych półek dyskowych jest nadmiarowy dla macierzy o pojemności 14 TiB. Proponujemy dopuszczenie skalowalności do 2 dodatkowych półek dyskowych, każda na minimum 24 dyski 2,5" lub 12 dysków 3,5", co jest wystarczające dla potrzeb Zamawiającego i bardziej adekwatne do skali rozwiązania.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający zmienia treść – wymóg na 10 półek dyskowych i 140 dysków. Zamawiający podtrzymuje wymóg opisany w SWZ.

4. Wymóg kompresji sprzętowej i deduplikacji danych w macierzach hybrydowych jest kosztowny i oferuje ograniczoną efektywność w porównaniu do macierzy opartych wyłącznie na SSD. Dopuszczenie rozwiązań bez tych funkcjonalności lub z opcjonalną kompresją/deduplikacją obniżyłoby koszty przy zachowaniu wysokiej wydajności.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający nie ogranicza zaoferowania macierzy opartej o dyski SSD i wyposażonego w funkcję deduplikacji i kompresji. Mechanizmy redukcji danych są obecnie standardem na rynku i pozwalają na ograniczenie kosztów utrzymania systemu. Zamawiający podtrzymuje wymóg opisany w SWZ.

5. Wymóg wirtualizacji zasobów zewnętrznych macierzy na potrzeby bezprzerwowej migracji danych jest kosztowny i nieproporcjonalny do skali rozwiązania. Proponujemy rezygnację z tej funkcjonalności lub dopuszczenie standardowych metod migracji danych, co zwiększyłoby dostępność rozwiązań.

Stanowisko (wyjaśnienie) Zamawiającego:

Mechanizm bezprzerwowej migracji danych jest dostępny u renomowanych producentów. Zamawiający podtrzymuje wymóg opisany w SWZ.

6. Wymóg kopii migawkowych typu WORM, obok standardowych kopii point-in-time i mirrorowanych LUN, jest specyficzny i może preferować wybrane rozwiązania, zwiększając koszty. Dopuszczenie standardowych kopii migawkowych bez funkcjonalności WORM zapewniłoby wystarczającą ochronę danych przy niższych kosztach.

Stanowisko (wyjaśnienie) Zamawiającego:

W dobie powszechnych ataków typu ransomware możliwość szybkiego przywrócenia środowiska/danych jest kluczowa dla obsługi ludności. Zamawiający podtrzymuje wymóg opisany w SWZ.

Pytanie nr 8

Zamawiający w załączniku do SWZ – Szczegółowy opis przedmiotu zamówienia, pozycja 1. System monitorowania sieci i użytkowników 50 USER (SIEM), określa następujące wymagania:

„a. „System musi posiadać własny moduł EDR/XDR, czyli zintegrowane rozwiązanie bezpieczeństwa, którego główne funkcje to: monitorowanie i gromadzenie danych o aktywnościach użytkowników i oprogramowania na urządzeniach końcowych, analiza tych danych w celu identyfikacji wzorców zagrożeń, automatyczne reagowanie na zidentyfikowane zagrożenia w celu ich usunięcia lub powstrzymania, powiadamianie personelu bezpieczeństwa o zidentyfikowanych anomaliach. System musi być otwarty, tj. posiadać możliwość integracji z rozwiązaniami EDR/XDR innych producentów (co najmniej ESET, WithSecure, Bitdefender).”
b. „Integracja ze stale aktualizowaną bazą danych CVE oraz MITRE ATT&CK, z codzienną synchronizacją i automatycznym sprawdzaniem podatności w infrastrukturze sieciowej.”
c. „Treści pojawiające się w interfejsie użytkowników CSB będą spełniać standardy WCAG 2.1 na poziomie AA, z zapewnieniem dostępności dla osób z niepełnosprawnościami.”
d. „System musi obsługiwać co najmniej 100 urządzeń i metryk w zakresie skalowalności.”
e. „Moduł analizy logów musi umożliwiać przeglądanie i analizę logów z systemów operacyjnych, aplikacji i systemów dziedzinowych, z zaawansowanym filtrowaniem i korelacją z problemami w module monitoringu zasobów.”

Wskazane wymagania, w szczególności dotyczące zintegrowanego modułu EDR/XDR, integracji z bazami CVE i MITRE ATT&CK, szczegółowych funkcjonalności wizualizacji zgodnych z WCAG 2.1 AA oraz wysokiej skalowalności, mogą sugerować preferowanie zaawansowanego rozwiązania, takiego jak SecureVisio, co znacząco ogranicza konkurencyjność postępowania. Tego typu zapisy, wymagające kosztownych i złożonych funkcjonalności, mogą nie być w pełni uzasadnione dla systemu obsługującego 50 użytkowników i 100 urządzeń, co prowadzi do nieoptymalnego wykorzystania środków

publicznych oraz potencjalnego naruszenia zasad równego traktowania wykonawców i uczciwej konkurencji wynikających z przepisów o zamówieniach publicznych.

1. Wymóg posiadania zintegrowanego modułu EDR/XDR w systemie SIEM znacząco zwiększa koszty i ogranicza wybór dostawców, szczególnie w kontekście stosunkowo niewielkiej skali rozwiązania (50 użytkowników, 100 urządzeń). Funkcjonalności EDR/XDR, takie jak monitorowanie, analiza i automatyczne reagowanie na zagrożenia, mogą być efektywnie realizowane przez osobne, dedykowane rozwiązania EDR/XDR, co zwiększyłoby konkurencyjność i pozwoliło na wybór bardziej kosztowo efektywnych systemów SIEM.
2. Wymóg integracji z bazami CVE i MITRE ATT&CK z codzienną synchronizacją i automatycznym wykrywaniem podatności jest zaawansowany i może preferować konkretnych dostawców. Dopuszczenie rozwiązań z okresową (np. cotygodniową) synchronizacją lub manualnym importem danych CVE i MITRE ATT&CK zapewniłoby porównywalną funkcjonalność przy niższych kosztach.
3. Wymóg zgodności z WCAG 2.1 AA dla całego interfejsu użytkownika, w tym multimediów, jest kosztowny i może być nieproporcjonalny do skali systemu. Dopuszczenie zgodności z podstawowymi standardami dostępności (np. WCAG 2.1 A) dla kluczowych elementów interfejsu zwiększyłoby dostępność rozwiązań.
4. Wymóg zaawansowanej korelacji logów z systemów dziedzicznych i automatycznego przekierowania do logów w module analizy logów może ograniczać wybór systemów SIEM. Dopuszczenie podstawowej agregacji i filtrowania logów bez konieczności ścisłej korelacji z problemami w module monitoringu zasobów zwiększyłoby konkurencyjność.

Powyższe zmiany zapewnią większą konkurencyjność postępowania, racjonalne wykorzystanie środków publicznych oraz zgodność z zasadami równego traktowania wykonawców.

W związku z powyższym, prosimy o potwierdzenie, czy Zamawiający:

- a. Dopuszcza rozdzielenie funkcji EDR/XDR na osobne rozwiązanie, zamiast wymagania zintegrowanego modułu EDR/XDR w systemie SIEM, z zachowaniem możliwości integracji z rozwiązaniami innych producentów (np. ESET, WithSecure, Bitdefender).

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający nie dopuszcza rozdzielania funkcji EDR/XDR na osobne rozwiązanie niezintegrowane z systemem SIEM. Wymaganie dotyczące zintegrowanego modułu EDR/XDR w ramach oferowanego rozwiązania SIEM pozostaje aktualne.

Celem Zamawiającego jest uzyskanie centralnego systemu bezpieczeństwa, w którym komponenty takie jak SIEM oraz EDR/XDR stanowią zintegrowaną całość, co zapewnia wyższą efektywność w zakresie wykrywania, korelacji i reagowania na incydenty

bezpieczeństwa. Dopuszczenie rozwiązań niezintegrowanych mogłoby wpłynąć na ograniczenie funkcjonalności, zwiększenie złożoności integracji oraz trudności w bieżącej eksploatacji systemu.

- b. Dopuszczenia okresową (np. cotygodniową) synchronizację z bazami CVE i MITRE ATT&CK lub manualny import danych, zamiast codziennej synchronizacji i automatycznego wykrywania podatności.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający nie dopuszcza okresowej synchronizacji ani ręcznego importu danych z baz CVE i MITRE ATT&CK w miejsce codziennej, automatycznej synchronizacji i wykrywania podatności.

Wymóg codziennej synchronizacji oraz automatycznego wykrywania podatności wynika z potrzeby zapewnienia możliwie najwyższego poziomu bezpieczeństwa systemów informatycznych. Aktualność danych o podatnościach oraz możliwość ich automatycznej analizy w czasie zbliżonym do rzeczywistego stanowi kluczowy element skutecznego systemu zarządzania ryzykiem. Rozwiązania wymagające interwencji manualnej lub operujące na nieaktualnych danych nie spełniają wymagań funkcjonalnych określonych przez Zamawiającego. Założona cotygodniowa integracja, stanowi wysokie ryzyko, dotyczące utracenia danych bądź włamania się cyberprzestępców do infrastruktury zamawiającego. Tygodniowa niewiedza na temat podatności systemów i oprogramowania jest niedopuszczalna wg. powszechnie znanych standardów dotyczących zakresu cyberbezpieczeństwa.

- c. Dopuszczenia zgodność z podstawowymi standardami dostępności (WCAG 2.1 A) dla kluczowych elementów interfejsu użytkownika, zamiast pełnej zgodności z WCAG 2.1 AA.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający nie dopuszcza ograniczenia zgodności interfejsu użytkownika wyłącznie do poziomu WCAG 2.1 A. Wymagana jest pełna zgodność z poziomem WCAG 2.1 AA dla całego interfejsu użytkownika.

Wymaganie zgodności z poziomem WCAG 2.1 AA wynika z obowiązujących przepisów prawa, w tym ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, oraz z dążenia do zapewnienia równego dostępu do oferowanych funkcjonalności wszystkim użytkownikom, w tym osobom ze szczególnymi potrzebami. Zgodność wyłącznie z poziomem A nie spełnia minimalnych standardów przyjętych przez Zamawiającego.

d. Dopuszcza podstawową agregację i filtrowanie logów z systemów dziedzinowych, bez konieczności ścisłej korelacji z problemami w module monitoringu zasobów.

Powyższe zmiany zapewnią większą konkurencyjność postępowania, racjonalne wykorzystanie środków publicznych oraz zgodność z zasadami równego traktowania wykonawców.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający nie dopuszcza ograniczenia funkcjonalności do podstawowej agregacji i filtrowania logów z systemów dziedzinowych bez ich ścisłej korelacji z problemami wykrywanymi w module monitoringu zasobów. Wymóg ścisłej korelacji logów z informacjami pochodzącymi z monitoringu zasobów stanowi istotny element koncepcji całościowego i proaktywnego zarządzania bezpieczeństwem IT. Tylko zintegrowane podejście umożliwia skuteczne wykrywanie incydentów, identyfikację przyczyn problemów oraz szybkie reagowanie na zagrożenia. Ograniczenie się wyłącznie do agregacji i filtrowania logów znacząco obniża efektywność działania systemu i nie spełnia założeń funkcjonalnych określonych w dokumentacji przetargowej.

Zamawiający podtrzymuje swoje wymagania, które wynikają z konieczności zapewnienia wysokiego poziomu bezpieczeństwa, spójności systemu oraz efektywnego wykorzystania infrastruktury monitorującej.

Pytanie nr 9

Zamawiający w załączniku do SWZ – Szczegółowy opis przedmiotu zamówienia, pozycja 6. Urządzenie UTM - analiza logów z podwójną autentykacją 1 szt, określa następujące wymagania:

- a. *„Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.”*
- b. *„Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu: Amazon Web Services (AWS), Microsoft Azure, Cisco ACI, Google Cloud Platform (GCP), OpenStack, VMware NSX, Kubernetes.”*
- c. *„W zakresie routingu rozwiązanie zapewnia obsługę: BFD (Bidirectional Forwarding Detection).”*

Wskazane wymagania, w szczególności dotyczące wysokiej wydajności szyfrowania IPSec VPN, integracji z zaawansowanymi rozwiązaniami SDN oraz wsparcia dla protokołu BFD, mogą wskazywać na preferowanie konkretnego rozwiązania, np. FortiGate 100F, co znacząco ogranicza konkurencyjność postępowania. Tego typu zapisy, wymagające kosztownych i złożonych funkcjonalności klasy enterprise, mogą nie być uzasadnione w kontekście skali rozwiązania (pojedyncze urządzenie UTM) i typowych potrzeb infrastruktury Zamawiającego,

co prowadzi do nieoptymalnego wykorzystania środków publicznych oraz potencjalnego naruszenia zasad równego traktowania wykonawców i uczciwej konkurencji wynikających z przepisów o zamówieniach publicznych.

1. Wymóg wydajności szyfrowania IPsec VPN na poziomie 6 Gbps jest nieproporcjonalny, zważywszy, że typowe połączenie WAN w infrastrukturze Zamawiającego prawdopodobnie nie przekracza 1 Gbps. Obniżenie tego parametru do 1,5 Gbps zapewniłoby wystarczającą wydajność dla większości zastosowań, jednocześnie zwiększając konkurencyjność oferty i obniżając koszty rozwiązania.
2. Wymóg integracji z rozwiązaniami SDN, takimi jak Cisco ACI, VMware NSX czy Kubernetes, jest nadmiarowy, jeśli Zamawiający nie wykorzystuje data center opartego na tych technologiach lub klastrów Kubernetes. Tego typu funkcjonalności znacząco zwiększają koszty i ograniczają wybór dostawców. Dopuszczenie rozwiązań bez konieczności integracji z tymi platformami SDN lub ograniczenie integracji do popularnych chmur publicznych (np. AWS, Azure) byłoby bardziej adekwatne do skali rozwiązania.
3. Wymóg wsparcia dla protokołu BFD jest charakterystyczny dla środowisk wykorzystujących zaawansowany routing dynamiczny (np. OSPF, BGP). Jeśli Zamawiający nie korzysta z takich protokołów, wymóg ten jest nieuzasadniony i ogranicza konkurencyjność. Dopuszczenie rozwiązań bez obsługi BFD zwiększyłoby dostępność urządzeń UTM.

W związku z powyższym, prosimy o potwierdzenie, czy Zamawiający:

- a. Dopuszcza rozwiązanie z wydajnością szyfrowania IPsec VPN protokołem AES z kluczem 128 na poziomie minimum 1,5 Gbps, zamiast 6 Gbps. \

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający podtrzymuje wymagania

- a. Dopuszcza rezygnację z wymogu integracji z rozw b. Dopuszcza rezygnację z wymogu integracji z rozwiązaniami SDN (Cisco ACI, VMware NSX, Kubernetes) lub ograniczenie integracji do chmur publicznych (AWS, Azure, GCP, OpenStack).

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający podtrzymuje wymagania

- b. Dopuszcza rezygnację z wymogu obsługi protokołu BFD, jeśli Zamawiający nie wykorzystuje zaawansowanych protokołów routingu dynamicznego (OSPF, BGP).

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiający podtrzymuje wymagania

Powyższe zmiany zapewnią większą konkurencyjność postępowania, racjonalne wykorzystanie środków publicznych oraz zgodność z zasadami równego traktowania wykonawców

Pytanie nr 10

Zamawiający w załączniku do SWZ – Szczegółowy opis przedmiotu zamówienia, pozycja 7. Zakup usługi konfiguracyjnej pozwalającej wdrożyć nowe rozwiązania informatyczne, określa następujące wymagania:

„Wykonawca musi posiadać kompetencje w zakresie projektowania i wdrażania systemów informatycznych, potwierdzone certyfikatami ISO 9001 oraz 27001 lub inne równoważne. Zamawiający żąda złożenia dowodu potwierdzającego posiadanie certyfikatu ISO 9001 oraz/ 27001 lub równoważnych wraz z ofertą na potwierdzenie zgodności oferowanej usługi z wymaganiami określonymi w SZOPZ.”

Wskazany wymóg posiadania certyfikatów ISO 9001 oraz ISO 27001 (lub równoważnych) znacząco ogranicza konkurencyjność postępowania, ponieważ może wykluczać mniejszych wykonawców, którzy dysponują odpowiednimi kompetencjami i doświadczeniem w projektowaniu oraz wdrażaniu systemów informatycznych, ale nie posiadają tych konkretnych certyfikatów. Uzyskanie i utrzymanie certyfikatów ISO 9001 i ISO 27001 wiąże się z wysokimi kosztami, co może preferować większe podmioty i prowadzić do nieoptymalnego wykorzystania środków publicznych, sprzecznie z zasadami równego traktowania wykonawców i uczciwej konkurencji wynikającymi z przepisów o zamówieniach publicznych. Kompetencje w zakresie konfiguracji infrastruktury IT, w tym serwerów, macierzy, systemów SIEM, UTM oraz przełączników sieciowych, mogą być skutecznie potwierdzone innymi metodami, takimi jak referencje od poprzednich klientów, udokumentowane doświadczenie w realizacji podobnych projektów lub posiadanie certyfikatów branżowych wydanych przez producentów sprzętu i oprogramowania (np. certyfikaty VMware, Cisco, Microsoft lub Fortinet).

W związku z powyższym, prosimy o potwierdzenie, czy Zamawiający dopuści potwierdzenie kompetencji Wykonawcy w zakresie projektowania i wdrażania systemów informatycznych za pomocą alternatywnych form, takich jak:

- Referencje od co najmniej dwóch klientów potwierdzające pomyślne wdrożenie systemów informatycznych o podobnej skali i zakresie w ciągu ostatnich 3 lat.
- Udokumentowane doświadczenie w konfiguracji infrastruktury IT, w tym serwerów, macierzy, systemów SIEM, UTM i przełączników sieciowych, poparte szczegółowym opisem zrealizowanych projektów.

- c. Certyfikaty branżowe wydane przez producentów sprzętu lub oprogramowania (np. VMware, Cisco, Microsoft, Fortinet) potwierdzające kwalifikacje w zakresie konfiguracji oferowanych rozwiązań.

Stanowisko (wyjaśnienie) Zamawiającego:

Zamawiaczy jasno określił wymagania dotyczące

Norma ISO 9001 zawiera szczegółowe wymagania dotyczące systemu zarządzania jakością. Posiadanie ww. certyfikatu zwiększają zdolność firmy do konsekwentnego dostarczania produktów i usług, które spełniają wymagania klientów oraz ustawowe i wykonawcze.

Norma ISO 27001 – System Zarządzania Bezpieczeństwem Informacji, z kolei to międzynarodowy standard określający wymagania dotyczące Systemu Zarządzania Bezpieczeństwem Informacji. Wskazana norma skoncentrowana jest na identyfikacji, zarządzaniu i minimalizowaniu ryzyka związanego z bezpieczeństwem informacji. Obejmuje zarówno aspekty techniczne, organizacyjne, jak i proceduralne.

Zamawiający podtrzymuje wymagania

Zamawiający:



*na podstawie upoważnienia
Kierownik Referatu Inwestycji
i Ochrony Środowiska*