

Prosimy o doprecyzowanie czy wszystkie obiekty związane ze świadczeniem usługi SOC tj. miejsce pracy analityków oraz obiekt Data Center - gdzie zainstalowany jest system SIEM - winny spełniać wymagania „Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia w sprawie warunków organizacyjnych i technicznych...” ?

Zamawiający wymaga, aby wszystkie obiekty, w których świadczona będzie usługa, spełniały wymagania „Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo”. Zatem wymagania rozporządzenia muszą spełniać zarówno miejsce pracy analityków, jak i obiekt DataCenter, gdzie zainstalowany jest system SIEM.

2. Wykonawca prosi o informację czy w wypadku oferty złożonej elektronicznie poprzez platformę OpenNexus podpisanej kwalifikowanym podpisem elektronicznym Zamawiający dopuszcza aby poszczególne strony oferty nie były kolejno ponumerowane ? W odpowiedzi na uprzednio zadane pytanie Zamawiający wyraził już zgodę aby strony oferty nie ze sobą połączone.

Zamawiający dopuszcza odstępstwo od wymogu, aby poszczególne strony ofert były kolejno ponumerowane, w przypadku złożenia oferty w formie elektronicznej przez platformę OpenNexus.

3. W związku z trwającą weryfikacją techniczną oraz procedurami Wykonawcy dla zatwierdzania ofert niestandardowych aby móc złożyć ofertę w postępowaniu Wykonawca prosi o przedłużenie terminu składania ofert do dnia 16.10.2023 roku do godz. 15:00. Czy Zamawiający wyrazi zgodę na przedłużenie terminu składania ofert ?

Zamawiający wyraża zgodę na przedłużenie terminu składania ofert do dnia 16.10.2023 do godz. 15:00.

Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga złożenia wraz z ofertą Świadectwa Bezpieczeństwa Przemysłowego. Czy Zamawiający dopuści możliwość złożenia oferty przez Wykonawcę, który 2 sierpnia 2023 roku złożył wniosek o wydanie świadectwa bezpieczeństwa przemysłowego, o którym mowa w art. 56 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. 2023, poz. 756, z późn. zm.), który posiada Pion Ochrony Informacji Niejawnych, a także który zatrudnia 4 osoby posiadające ważne poświadczenie bezpieczeństwa w zakresie dostępu do informacji niejawnych oznaczonych co najmniej klauzulą „tajne”.

Zamawiający dopuści ofertę Wykonawcy posiadającego Pion Ochrony Informacji Niejawnych oraz zatrudnia minimum 3 osoby posiadające ważne poświadczenie bezpieczeństwa w zakresie dostępu do informacji niejawnych oznaczonych co najmniej klauzulą „tajne”.

Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga złożenia wraz z ofertą posiadanych i ważnych certyfikatów ISO 27001 dla świadczenia usług z zakresu cyberbezpieczeństwa, ISO 9001.

Czy Zamawiający jako równoważne uzna certyfikaty:

- ISO/IEC 27001:2013 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji (Zakres certyfikacji: świadczenie usług doradztwa, sprzedaży, wdrożenia, utrzymania infrastruktury oraz oprogramowania; outsourcing usług IT; usługi cyberbezpieczeństwa w obszarze bezpiecznej konfiguracji, usuwania podatności oraz analizy

- powłamaniowej; usługi świadczone w chmurze obliczeniowej, w tym usługi bezpiecznego przechowywania danych - zgodnie z Deklaracją Stosowania wydanie 2.0 z 3.04.2023r.);
- ISO 22301:2019 Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania (Zakres certyfikacji: świadczenie usług doradztwa, sprzedaży, wdrożenia, utrzymania infrastruktury oraz oprogramowania; outsourcing usług IT; usługi cyberbezpieczeństwa w obszarze bezpiecznej konfiguracji, usuwania podatności oraz analizy powłamaniowej; usługi świadczone w chmurze obliczeniowej, w tym usługi bezpiecznego przechowywania danych - zgodnie z Deklaracją Stosowania wydanie 2.0 z 3.04.2023r.);
 - ISO/IEC 27018:2019 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady ochrony informacji o identyfikowalnych osobach (PII) w chmurach publicznych działających jako przetwarzający PII (Zakres certyfikacji: świadczenie usług doradztwa, sprzedaży, wdrożenia, utrzymania infrastruktury oraz oprogramowania; outsourcing usług IT; usługi cyberbezpieczeństwa w obszarze bezpiecznej konfiguracji, usuwania podatności oraz analizy powłamaniowej; usługi świadczone w chmurze obliczeniowej, w tym usługi bezpiecznego przechowywania danych zgodnie z Deklaracją Stosowania wydanie 2.0 z 3.04.2023r.);
 - ISO/IEC 27017:2015 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze (Zakres certyfikacji: świadczenie usług doradztwa, sprzedaży, wdrożenia, utrzymania infrastruktury oraz oprogramowania; outsourcing usług IT; usługi cyberbezpieczeństwa w obszarze bezpiecznej konfiguracji, usuwania podatności oraz analizy powłamaniowej; usługi świadczone w chmurze obliczeniowej, w tym usługi bezpiecznego przechowywania danych - zgodnie z Deklaracją Stosowania wydanie 2.0 z 3.04.2023r.).

Zamawiający uzna podane certyfikaty za równoważne.

Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga złożenia wraz z ofertą co najmniej dwóch referencji na wdrożenie usługi SOC wystawionych przez podmioty kwalifikowane jako Operatorzy Usług Kluczowych na podstawie ustawy z dnia 5 lipca 2018 r, o krajowym systemie cyberbezpieczeństwa, na rzecz których usługa była świadczona przez Wykonawcę w ciągu ostatniego roku. Czy Zamawiający w celu wyrazi zgodę na przedłożenie referencji na wdrożenie usługi SOC/SIEM w podmiotach prywatnych lub placówkach administracji publicznej lub placówkach służby zdrowia.

Zamawiający wyrazi zgodę na przedłożenie co najmniej dwóch referencji na wdrożenie usługi SOC wystawionych przez placówki służby zdrowia.

Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga złożenia wraz z ofertą oświadczenia o zatrudnieniu na umowę o pracę minimum 8 analityków bezpieczeństwa. Branża IT jest branżą bardzo specyficzną, w której pracodawcy chcąc przyciągnąć najlepszych pracowników muszą niejako wychodzić naprzód oczekiwaniom osób, z którymi chcą nawiązać współpracę, a w większości najlepsi specjaliści preferują współpracę w formie umowy B2B. W związku z powyższym wnosimy o odstąpienie od wymogu zatrudnienia o umowę o pracę minimum 8 analityków bezpieczeństwa i modyfikację zapisu w sposób następujący:

3.4.Oświadczenia o skierowaniu do realizacji zadania minimum 8 analityków bezpieczeństwa.

Zamawiający nie wyraża zgody na zmianę zapisu punktu 3.4 Zapytania ofertowego.

Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga, aby wybrany w toku postępowania Wykonawca przedstawił posiadane przez zatrudnionych na umowę o pracę analityków bezpieczeństwa certyfikaty: OSCP, CEH, Comptia Security+. Ponadto w odpowiedziach na

pytania Zamawiający dopuścił drugi certyfikat CEH wydany przez EC-Council za równoważny certyfikatowi OSCP. Czy jako Zamawiający uzna, że Wykonawca spełni ww. warunek udziału w postępowaniu jeżeli wykaże, że wśród osób skierowanych do realizacji przedmiotu zamówienia skieruje osoby posiadające m.in. następujące certyfikaty: Microsoft SC-900, CEH, C)IHE: Certified Incident Handling Engineer, ISO 22301 IA, PRINCE2 Foundation, Pentester Academy CRTP, CCNA R&S/intro to Network.

Zamawiający uzna posiadanie przez osoby skierowane do realizacji przedmiotu zamówienia certyfikaty Microsoft SC-900, CEH, C)IHE: Certified Incident Handling Engineer, ISO 22301 IA, PRINCE2 Foundation, Pentester Academy CRTP, CCNA R&S/intro to Network za wystarczające.

Zamawiający w punkcie 3 Wymagania dla usługi określił, że:

3.2. Wykonawca musi posiadać kapitał zakładowy przynajmniej na poziomie wartości Usługi.

3.3. Wykonawca musi posiadać ubezpieczenie OC działalności gospodarczej na kwotę minimum 2 miliony zł.

W pierwszej kolejności należy podkreślić, iż kapitał zakładowy Wykonawcy może nie odzwierciedlać bieżącej sytuacji finansowej Wykonawcy. Ponadto wartość usługi stanowi kryterium oceny ofert, w związku z powyższym wymagana wysokość kapitału zakładowego nie będzie równa dla wszystkich Wykonawców.

W związku z powyższym oraz w celu ujednoczenia wymogów wnosimy o modyfikację ww. wymogu w sposób następujący:

„Wykonawca musi posiadać kapitał zakładowy przynajmniej na poziomie wartości Usługi 100 000,00 złotych.” oraz w celu zabezpieczenia interesów Zamawiającego podniesienia wysokości wymaganej polisy OC do wysokości 5 milionów złotych.

Zamawiający nie wyraża zgody na zmianę brzmienia zapisu punktu 3.2 Opisu Przedmiotu Zamówienia.