Urząd Miasta Bydgoszczy
Wydział Zamówień Publicznych
ul. Grudziądzka 9-15
85-130 Bydgoszcz

Bydgoszcz, dnia 28.06.2024r.

Nr sprawy: WZP.271.31.2024.B

Oznaczenie postępowania: **Świadczenie usługi cyberbezpieczeństwa opartej o Security Operations Center (SOC) działającej w reżimie 24 H/7 dni w tygodniu**

Na podstawie art. 284 ust. 2 ustawy z dnia 11.09.2019r. Prawo zamówień publicznych (dalej uPzp - tekst jedn. Dz. U. z 2023 r., poz. 1605 ze zm.) Zamawiający przedstawia zadane pytania i udziela odpowiedzi:

Pytanie nr 16:
W zakresie § 4 ust. 6 Wzoru Umowy – Załącznik nr 1 e do SWZ jest zastrzeżenie, że jeżeli przy wykonywaniu przedmiotu umowy konieczne będzie używanie pojazdów, Wykonawca będzie musiał spełnić wymagania wynikające z ustawy o elektromobilności i paliwach alternatywnych. Wykonawca nie widzi związku pomiędzy wykonaniem umowy i koniecznością dostosowania się do powołanej ustawy. Proszę wskazanie związku pomiędzy przedmiotem Umowy a obowiązkiem dostosowania się do ustawy o elektromobilności i paliwach alternatywnych oraz podstawę prawną zastosowania ustawy do przedmiotowej Umowy. Dodatkowo w treści postanowienia użyto sformułowania umowa z małej litery, zgodnie ze §1 zdefiniowane terminy będą w treści Umowy użyte w wielkiej litery. W związku z czym prosimy o wyjaśnienie o jaką umowę chodzi Zamawiającemu w postanowieniu §4 ust. 6?

Odpowiedź:

Zamawiający wykreśla ust. 6 w § 4 Wzoru Umowy.

Pytanie nr 17:

W zakresie §10 ust. 3 pkt. 8) Wzoru Umowy – Załącznik nr 1 e do SWZ wskazano, iż:
1) niezłożenie oświadczenia, o którym mowa w § 5 ust. 6 pkt 2 umowy w terminie wyznaczonym przez Zamawiającego w wysokości 3 000,00 zł.
Trudno stwierdzić za co jest zastrzeżona kara umowna, gdyż Umowa nie zawiera §5 ust. 6. Prosimy w

związku z tym o wyjaśnienie do czego odnosi się kara umowna zawarta w §10 ust. 3 pkt. 8) Umowy, gdyż umowa nie zawiera w §5 ust. 6 pkt 2.

Odpowiedź:

Wzór Umowy nie zawiera treści wskazanej przez Wykonawcę w §10 ust. 3 pkt. 8).

Jeśli Wykonawca miał na myśli §10 ust. 2 pkt. 8) wzoru umowy, to Zamawiający informuje, że wykreśla wskazany pkt. 8), a §10 ust. 2 przyjmuje następujące brzmienie:

Kary:

1) Zamawiającemu przysługuje prawo naliczania kar umownych za nieterminową realizację Umowy, nie zrealizowanie elementów Umowy oraz niedochowanie ustalonych parametrów świadczenia usługi zgodnie z poniższą tabelą:

Zadanie	**Czas reakcji / podjęcia**	**Czas realizacji**	**Zwłoka**	**Wysokość kary**
SOC L1, całodobowe 24/7/365, podjęcie działań związanych z incydentem, rozwiązanie incydentu polegające na zatrzymaniu zagrożenia (obejście) i/lub przekazanie do SOC L2	30 minut	2h	każda kolejna godzina	kwota 100,00 zł
SOC - L2, 8/5 w dni robocze w godzinach roboczych 8:00 – 16:00, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie reakcji	1h	8h	każda kolejna godzina	kwota 100,00 zł
SOC L2 SOAR 24/7/365, zautomatyzowane podjęcie incydentu i aplikacja rozwiązania zatrzymującego zagrożenie w czasie realizacji	15 min	1h	Każdy kolejny godzina	kwota 100,00 zł
SOC L3, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie realizacji	8h	40h	każda kolejna godzina	kwota 100,00 zł

2) Zamawiający naliczy karę w wysokości 300,00 zł za każdy dzień roboczy zwłoki w stosunku do każdego z zadań określonych w Załączniku nr 1 do Umowy – harmonogram, niezależnie i określonych w pkt 2 podpunkt 1-6, pkt 4, pkt 5, pkt 6 podpunkt 1-3.

3) Zamawiający naliczy karę umowną w wysokości 5% łącznej wartości Umowy w przypadku niezrealizowania przez Wykonawcę wymaganych szkoleń.
4) Zamawiający naliczy karę umowną w wysokości 25% łącznej wartości Umowy w przypadku nie przekazania na wniosek Zamawiającego reguł korelacyjnych w standardzie Sigma Rules opartym o YAML, scenariuszy działań i playbooków pozwalających na wykorzystanie przez innego dostawcę cyberbezpieczeństwa.
5) Zamawiający naliczy karę umowną w wysokości 20% łącznej wartości Umowy w przypadku wypowiedzenia Umowy z powodu okoliczności leżących po stronie Wykonawcy.
6) Zamawiający naliczy karę umowną w przypadku ujawnienia przez Wykonawcę Informacji Poufnych, dotyczących Zamawiającego, w sposób naruszający postanowienia Umowy i narażający Zamawiającego na incydent cyberbezpieczeństwa wynikający z ujawnionych danych w wysokości 50 000 złotych chyba, że Wykonawca naprawi swój błąd i doprowadzi do usunięcia skutków tego faktu.
7) w wysokości 200 zł za każdy dzień zwłoki w złożeniu oświadczenia lub któregokolwiek z dokumentów, o których mowa w § 4 ust. 4 i 5 umowy.

Pytanie nr 18:

W zakresie § 11 ust. 6 Wzoru Umowy – Załącznik nr 1 e do SWZ wskazano, iż Wykonawca ponosi odpowiedzialność za wszelkie szkody wyrządzone Zamawiającemu w związku z niewykonaniem lub nienależytym wykonaniem umowy, w tym szkody wyrządzone przez osoby pozostające pod jego kierownictwem. Wykonawca ponosi także pełną odpowiedzialność odszkodowawczą za wszelkie szkody poniesione przez Zamawiającego lub osoby trzecie przy wykonywaniu niniejszej umowy. W zdaniu pierwszym Zamawiający zawarł, że Wykonawca ponosi odpowiedzialność za szkody związane z niewykonaniem lub nienależytym wykonaniem umowy wyrządzone z winy Wykonawcy lub osób pozostających pod jego kierownictwem., w związku z tym prosimy o wyjaśnienie o jakie więc szkody wyrządzone Zamawiającemu chodzi w zdaniu drugim?

Odpowiedź:

Wzór Umowy nie zawiera ust. 6 w § 11.

Jeśli Wykonawca miał na myśli § 10 ust. 6, to Zamawiający informuje, że zmienia treść tego ust., który przyjmuje następujące brzmienie:

6. Wykonawca ponosi odpowiedzialność za wszelkie szkody wyrządzone Zamawiającemu w związku z niewykonaniem lub nienależytym wykonaniem umowy, w tym szkody wyrządzone przez osoby pozostające pod jego kierownictwem.

Pytanie nr 19:

Zgodnie z §10 ust. ust. 2 pkt 1) Umowy wskazano, że w zakresie SOC L3 czas reakcji to 8h, natomiast w OPZ pkt 2) SOC-12 czas reakcji to 1 dzień roboczy, prosimy więc o wyjaśnienie, które z tych parametrów są poprawne?

Odpowiedź:

Zgodnie z definicją określoną w umowie Dzień Roboczy odpowiada 8h roboczym. Zgłoszenia zgłoszone przez Zamawiającego o godzinie 14:00 w piątek, powinny być podjęte do godziny 14:00 w poniedziałek.

Zamawiający zmienia treść Wzoru Umowy w §10 ust. ust. 2 pkt 1), który przyjmuje następujące brzmienie:

Kary:
Zamawiającemu przysługuje prawo naliczania kar umownych za nieterminową realizację Umowy, nie zrealizowanie elementów Umowy oraz niedochowanie ustalonych parametrów świadczenia usługi zgodnie z poniższą tabelą:

Zadanie	**Czas reakcji / podjęcia**	**Czas realizacji**	**Zwłoka**	**Wysokość kary**
SOC L1, całodobowe 24/7/365, podjęcie działań związanych z incydentem, rozwiązanie incydentu polegające na zatrzymaniu zagrożenia (obejście) i/lub przekazanie do SOC L2	30 minut	2h	każda kolejna godzina	kwota 100,00 zł
SOC - L2, 8/5 w dni robocze w godzinach roboczych 8:00 – 16:00, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie reakcji	1h	8h	każda kolejna godzina	kwota 100,00 zł
SOC L2 SOAR 24/7/365, zautomatyzowane podjęcie incydentu i aplikacja rozwiązania zatrzymującego zagrożenie w czasie realizacji	15 min	1h	Każdy kolejny godzina	kwota 100,00 zł
SOC L3, podjęcie działań związanych z incydentem i rozwiązanie incydentu w czasie realizacji	8h	40h	każda kolejna godzina	kwota 100,00 zł

Pytanie nr 20:

W zakresie pkt. 3 ppkt 2 XXI Rozdziału SWZ Zamawiający wymaga spełnienia następującego warunku:
2)dysponuje osobami zdolnymi do wykonania zamówienia, które będą uczestniczyć w wykonywaniu zamówienia, tj. minimum 8-osobowym zespołem analityków bezpieczeństwa, w tym:
a) 4 osoby posiadające poświadczenie bezpieczeństwa osobowego na poziomie „poufne”,
b) 2 osoby posiadające specjalistyczną wiedzę w zakresie cyberbezpieczeństwa z użyciem rozwiązań Fortinet potwierdzoną certyfikacją Fortinet Network Security Expert (NSE) Enterprise Firewall lub równoważnym,
c) 2 osoby posiadające specjalistyczną wiedzę w zakresie cyberbezpieczeństwa potwierdzoną certyfikacją Offensive Security Certified Professional – OSCP lub równoważnym,
d) 2 osoby posiadające specjalistyczną wiedzę w zakresie cyberbezpieczeństwa potwierdzoną certyfikacją CompTIA Security lub równoważnym,
e) 2 osoby posiadające specjalistyczną wiedzę w zakresie cyberbezpieczeństwa potwierdzoną certyfikacją Certified Ethical Hacker - CEH lub równoważnym,
f) 2 osoby posiadające specjalistyczną wiedzę w zakresie cyberbezpieczeństwa potwierdzoną certyfikacją Certified Incident Handling Engineer – CIHE lub równoważny
Prosimy o wyjaśnienie:
1) czy 4 osoby posiadające poświadczenie bezpieczeństwa osobowego na poziomie „poufne” to mają być osoby z poniżej wymienionych z certyfikatami z obszaru cyberbezpieczeństwa czy dodatkowe 4 osoby oprócz osób wymienionych w lit. b-f?
2) ile minimalnie osób powinien wskazać wykonawca w wykazie, gdyż wymagane jest min. 8 osobowy zespół, podczas gdy po zsumowaniu ilości z lit a-f wychodzi 14 osób? Jakie są prawidłowe wartości łącznie i jednostkowo, mając również na uwadze pytanie z pkt. 1) powyżej?

Odpowiedź:

Zamawiający zakłada, że jedna osoba może dysponować wieloma certyfikatami i poświadczeniami. Zamawiający wymaga, aby zespół wykonujący zamówienie składał się z minimum 8 osób, z czego minimum wskazana liczba osób w punktach a) f) musi posiadać wymienione certyfikaty.

Osoby tworzące zespół powinny spełniać wymagania od a) do f), z zastrzeżeniem, że zespół powinien liczyć nie mniej niż 8 osób.

Pytanie nr 21:
W zakresie pkt. 3 ppkt. 1 XXI Rozdziału SWZ Zamawiający wymaga spełnienia warunku posiadania doświadczenia w postaci wykonania (a w przypadku świadczeń powtarzających się lub ciągłych również wykonywania) w okresie ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie co najmniej 2 (dwóch) zamówień polegających na świadczeniu usług cyberbezpieczeństwa w oparciu o systemy SIEM i SOAR w organizacji posiadającej minimum 1500 użytkowników lub minimum 1500 stacji roboczych, każde o wartości minimum 500 000,00 zł brutto.

Wskazujemy po pierwsze, iż na rynku jest mało podmiotów posiadających 1500 użytkowników lub 1500 stacji roboczych (liczba ograniczona) oraz należy zaznaczyć, iż podmiot, który zrealizował należycie co najmniej jedną umowę na taką skalę daje gwarancje właściwej realizacji przedmiotu zamówienia. Ponadto umowy na świadczenie usług cyberbezpieczeństwa w oparciu o systemy SIEM i SOAR o wartości ponad 500 000,00 zł brutto są zaliczane do dość dużych chociaż skalą ilości użytkowników czy stacji roboczych może być nieco mniejsza niż wymagana. W związku z powyższym prosimy o zmianę warunku na poniższe brzmienie:
„posiadania doświadczenia w postaci wykonania (a w przypadku świadczeń powtarzających się lub ciągłych również wykonywania) w okresie ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie co najmniej 2 (dwóch) zamówień polegających na świadczeniu usług cyberbezpieczeństwa w oparciu o systemy SIEM i SOAR albo każde o wartości minimum 500 000,00 zł brutto albo w organizacji posiadającej minimum 1500 użytkowników lub minimum 1500 stacji roboczych".

Pytanie nr 23:
Proszę o wyjaśnienie warunku doświadczenia wskazanego w SWZ w pkt. 3 ppkt. 1 XXI Rozdziału - czy Zamawiający dopuści, aby spełnienie warunku posiadania doświadczenia dotyczyło co najmniej 2 (dwóch) zamówień polegających na świadczeniu usług cyberbezpieczeństwa w oparciu o systemy SIEM lub SOAR w organizacji posiadającej minimum 1500 użytkowników lub minimum 1500 stacji roboczych, każde o wartości minimum 500 000,00 zł brutto. Wskazujemy, iż na rynku jest mało podmiotów posiadających1500 użytkowników lub 1500 stacji roboczych (liczba ograniczona), gdzie wykorzystywane są oba systemy - a zazwyczaj jest tylko jeden z nich.

Odpowiedź na pytanie 21 i 23:
Zamawiający zmienia Rozdz. XXI pkt 3 ppkt 1 swz, który przyjmuje brzmienie:

"posiada doświadczenie w postaci wykonania (a w przypadku świadczeń powtarzających się lub ciągłych również wykonywania) w okresie ostatnich trzech lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie co najmniej 2 (dwóch) zamówień polegających na świadczeniu usług cyberbezpieczeństwa w oparciu o systemy SIEM **lub** SOAR w organizacji posiadającej minimum 1500 użytkowników lub minimum 1500 stacji roboczych, każde o wartości minimum 500 000,00 brutto zł"

Pytanie nr 22:
Najnowsze rekomendacje organizacji Gartner dotyczące narzędzi używanych przez nowoczesne Security Operations Center opisują zunifikowane systemy SIEM+SOAR znane pod nazwą „Threat Detection Investigation Response Platform". Według organizacji Gartner dzięki zunifikowanym systemom SIEM+SOAR uzyskuje się zdecydowaną poprawę obsługi incydentu między innymi przez znaczące skrócenie czasu reakcji w stosunku do klasycznego modelu SIEM i SOAR funkcjonujących jako osobne instancje.

Zunifikowane systemy „Threat Detection Investigation Response Platform”, wielokrotnie były opisywane i porównywane przez organizację Gartner, ale nigdy nie został dla nich opracowany tzw. Gartner Magic Quadrant. W zawiązku z powyższym:

Czy Zamawiający dopuści ofertę Security Operations Center bazującą na technologii zunifikowanego systemu (SIEM+SOAR), który według organizacji Garnter posiada krótszy czas reakcji i obsługi incydentu niż opisany w OPZ klasyczny model (SIEM i SOAR jako osobne instancje), a który nie znajduje się w tzw. Gartner Magic Quadrant, gdyż takowy raport jeszcze nie został przez organizację Gartner opublikowany?

Odpowiedź:
Zamawiający pozostawia zapisy bez zmian.

Pytanie nr 24:
Jakie certyfikaty Zamawiający uznaje za równoważne do Offensive Security Certified Professional (OSCP)?

Odpowiedź:
Równoważność będzie badana jako certyfikat analogiczny co do zakresu z przykładowymi certyfikatami wskazanymi z nazwy, co jest rozumiane jako analogiczna dziedzina merytoryczna, której dotyczy certyfikat, analogiczny i nie niższy stopień poziomu kompetencji, analogiczny i nie niższy poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu po złożeniu oferty przez potencjalnego Wykonawcę. W przytoczonym przypadku za równoważny zamawiający uzna np. certyfikat Offensive Security Certified Expert (OSCE).

Pytanie nr 25:

Czy Zamawiający dopuszcza współdzielenie zasobów podmiotów polskich w ramach jednej grupy kapitałowej?

Odpowiedź:

Wykonawca zgodnie z art. 118. ust. 1 uPzp może w celu potwierdzenia spełniania warunków udziału w postępowaniu lub kryteriów selekcji, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych.

W związku z jw., zmianie ulegają:

1) Rozdz. XI pkt 1 swz, który przyjmuje brzmienie:
„Wykonawca będzie związany ofertą od dnia upływu terminu składania ofert do dnia 06.08.2024”

2) Rozdz. XIII pkt 1 swz, który przyjmuje brzmienie:
„Składanie ofert: Ofertę wraz ze wszystkimi wymaganymi oświadczeniami i dokumentami, należy złożyć za pośrednictwem strony Platforma zakupowa Bydgoszcz, w zakładce dedykowanej postępowaniu, **do 08.07.2024r. do godz. 11:00”.**

3) Rozdz. XIV pkt 1 swz, który przyjmuje brzmienie:
„Otwarcie ofert złożonych na Platformie nastąpi w dniu **08.07.2024r. o godz. 11.30.** Otwarcie ofert na Platformie dokonywane jest poprzez kliknięcie przycisku “Odszyfruj oferty”.

Kornelia Kwaczonek
Dyrektor WZP

Janusz Popielewski
Zastępca Przewodniczącego
komisji przetargowej

Maciej Szymczak
Członek komisji przetargowej

Rafał Kowalkowski
Członek komisji przetargowej