Warszawa, dnia 03.03.2023 r.

Dotyczy postępowania nr IBE/82/2023

PYTANIA I ODPOWIEDZI – ZESTAW NR 1

W związku z pytaniami, które wpłynęły do Zamawiajacego od uczestników postępowania poniżej zamieszczamy ich treść wraz z odpowiedziami

Pytanie nr 1
Dotyczy treści załącznika nr 1- treść ogłoszenia:
„Do udziału w postępowaniu może przystąpić Ekspert/zespół Ekspertów dysponujący poniższym doświadczeniem lub Podmiot, który dysponuje Ekspertem/zespołem Ekspertów, posiadającym poniższe doświadczenie, którzy spełniają łącznie wszystkie poniższe warunki udziału w postępowaniu: posiadają certyfikaty z zakresu cyberbezpieczeństwa: CISM (Certified Information
Security Manager), OSCP (Offensive Security Certified Professional). Warunkiem udziału w postępowaniu jest posiadanie każdego z wymienionych certyfikatów. Imienne przedmiotowe certyfikaty zostaną załączone do oferty. Podmiot dysponujący Ekspertami lub Zespół Ekspertów - wszystkie powyższe warunki udziału w postępowaniu mogą zostać spełnione łącznie przez zespół”.
Czy Zamawiający potwierdza, iż Wykonawca spełni warunek dotyczący udziału w postępowaniu jeśli zaproponuje zespół, których będzie się składać np. z 2 konsultantów i jeden Konsultant będzie posiadał certyfikat **CISM**, a drugi konsultant **OSCP**?

Opowiedź do pytania nr 1
Tak, zespół łącznie spełnia określony warunek udziału.

Pytanie nr 2
Szczegółowy OPZ , Pkt 4 zakres prac

"Dokonanie analizy konfiguracji serwerów, na których została umieszczona aplikacja, pod kątem bezpieczeństwa. Analiza będzie obejmowała”
Prosimy o informacje nt. Ilości komponentów podlegających audytowi konfiguracji

Opowiedź do pytania nr 2
1x Debian, 1x MariaDB/MySQL, 1x Apache HTTPD

Pytanie nr 3
Szczegółowy OPZ , Sposób realizacji zamówienia pkt 1

Proponujemy etapowe rozliczenie projektu.
Po fazie testów i raportu etap 1 oraz po fazie retestów.

W przypadku nie niedostępności środowiska do retestu, Wykonawca powinien mieć możliwość rozliczenia, odebranej fazy.

Opowiedź do pytania nr 3

Rozliczenie nastąpi zagodnie z zapisami w OPZ po ostatecznym zaakceptowaniu raportu z re-testów oraz podpisaniu protokołu zdawczo-odbiorczego.

Pytanie nr 4
Szczegółowy OPZ , Warunki realizacji zamówienia pkt 5

"Realizując zlecenie, Wykonawca zweryfikuje całość udostępnionego kodu, nie stosując próbkowania."

Prosimy o wyjaśnienie. Czy projekt ma uwzględniać analizę kodu? Nie zostało to zdefiniowane w zakresie prac.
Jeśli tak to prosimy o dodatkowe dane:
- ile lini kodu podlega analizie
- w jakim języku została napisana aplikacja
- czy kod napisany został z wykorzystaniem bibliotek / jakich ?

Opowiedź do pytania nr 4
Tak, projekt ma uwzględnić analizę kodu źródłowego. Zamawiający nie jest w stanie określić ilośći linijek kodu, php z laravel wraz z obsługą mysql, HTML CSS,

Pytanie nr 5
Załącznik nr 1 - Ogłoszenie

Warunki udziału w postępowaniu pkt 3 b)

Uprzejmie prosimy o możliwość przedstawienia certyfikatu CISSP jako równoważnego / wyższego dla certyfikatu CISM lub prosimy o usunięcie niniejszego wymagania.
Należy mieć na względzie, iż certyfikat CISM nie odnosi się bezpośrednio do usług testów i audytów, które stanowią przedmiot zapytania. Ten certyfikat charakterystyczny jest dla usług audytów miękkich (procesów / procedur).

Prosimy także o dopuszczenie jako równoważne certyfikatów OSWE który jest wyższym od OSCP a także certyfikatu eWPTX który jest jednym z najwyższych w zakresie testów aplikacji webowych.

Opowiedź do pytania nr 5
Tak, certyfikaty zostaną dopuszczone jako równoważne.

Pytanie nr 6
Załącznik nr 1 - Ogłoszenie
Kryteria oceny oferty, ad 2 doświadczenie
Poproszę o wyjaśnienie prawidłowości zrozumienia.
Wykonawca musi przedstawić minimum 6 projektów referencyjnych dla zespołu ekspertów.
Jednakże za każdy dodatkowy dostaje 5 punktów. Dla uzyskania 25 punktów musi przedstawić 5 dodatkowych projektów.
Prosimy o potwierdzenie.

Prosimy także o informacje, jak należy liczyć jeśli w ramach 1 kontraktu dla klienta, realizowane było kilka projektów przez różnych audytów.
Rozumiem, iż możemy je wykazać dla każdego Eksperta o ile opiewał na 20 tyś brutto.

Opowiedź do pytania nr 6

Tak, dla uzyskania 25 punktów należy przedstawić 5 projektów, innych niż wskazane w warunkach udziału w postępowaniu. Ponadto nie jest możliwe przyznanie punktów przy wskazaniu tego samego projektu kilkukrotnie, w przypadku realizowania go przez różnych audytorów (1 projekt spełniający warunki = 5 punktów)

Pytanie nr 7
Załącznik 4

Wartość zamówienia brutto

Uprzejmie prosimy o możliwość wpisania kwoty w formacie „powyżej 20 tyś / powyżej 30 tyś”
Dokładne kwoty mogą stanowić tajemnice kontraktu.
Ponadto jasnym jest, iz opiewać muszą minimum na 20 tyś.
Wykonawca potwierdza prawdziwość oraz zgodność, składanych danych.

Opowiedź do pytania nr 7

Nie ma konieczności wpisywania dokładnej kwoty brutto, można zastosować zapis 'powyżej 20 tys.'

Pytanie nr 8
Załącznik nr 5

a) Wartość zamówienia brutto

Uprzejmie prosimy o możliwość wpisania kwoty w formacie „powyżej 20 tyś / powyżej 30 tyś”
Dokładne kwoty mogą stanowić tajemnice kontraktu.
Ponadto jasnym jest, iz opiewać muszą minimum na 20 tyś.
Wykonawca potwierdza prawdziwość oraz zgodność, składanych danych.
Z wyrazami szacunku

b) Miejsce i data publikacji
(jeśli dotyczy)

Prosimy o dodatkowe wyjaśnienie o jaką publikacje chodzi.

Uprzejmie prosimy o dodatkowe wyjaśnienie i pozytywne rozpatrzenie naszych wniosków.

Opowiedź do pytania nr 8

a) Nie ma konieczności wpisywania dokładnej kwoty brutto, można zastosować zapis 'powyżej 20 tys.'

b) Zamawiajcy informuje, że dokona zmiany zapisu w załączniku nr 5 w nastepujący sposób: z "Miejsce i data publikacji (jeśli dotyczy)" na "Data realizacji projektu (od-do)".

Pytanie nr 9

Prosimy o podanie informacji jakie elementy zostać poddane analizie konfiguracji – serwer HTTP (ile, jakie), baza danych (ile, jakie), system operacyjny (ile, jakie), np. 2 x Debian, 1 x MySQL, 3 x Apache HTTPD

Opowiedź do pytania nr 9

1x Debian, 1x MariaDB/MySQL, 1x Apache HTTPD

Pytanie nr 10

Zwracamy się z uprzejmą prośbą o uznanie certyfikatu CISSP jako równoważny do wymaganego w postępowaniu certyfikatu CISM. Zwracamy uwagę, że uzyskanie certyfikatu CISSP wymaga posiadania kompetencji zarówno technicznych jak i menadżerskich (które są w zakresie certyfikatu CISM).

Opowiedź do pytania nr 10

Tak. Zamawiajacy dopuszcza przedmitowy certyfikat.

Pytanie nr 11

Zamawiający wymaga spełnienia następującego warunku udziału w postępowaniu: posiadają certyfikaty z zakresu cyberbezpieczeństwa: CISM (Certified Information Security Manager), OSCP (Offensive Security Certified Professional). Warunkiem udziału w postępowaniu jest posiadanie każdego z wymienionych certyfikatów. Imienne przedmiotowe certyfikaty zostaną załączone do oferty. Tak sformułowany warunek stanowi ograniczenie konkurencyjności i ma na celu dopuszczeni tylko jednego wykonawcę. Wnosimy o dopuszczenie równoważności certyfikatów.

Opowiedź do pytania nr 11

Tak, zostaną dopuszczone certyfikaty równoważne.

Pytanie nr 12

Czy Zamawiający uzna za równoważny do certyfikatu CISM certyfikat CISA (Certified Information Systems Auditor)?

Opowiedź do pytania nr 12

Tak.

Pytanie nr 13

Czy Zamawiający uzna za równoważny do certyfikatu OSCP certyfikat CEH (Certified Ethical Hacker)?

Opowiedź do pytania nr 13

Tak.

Pytanie nr 14

W OPZ znajduje się zdanie „Realizując zlecenie, Wykonawca zweryfikuje całość udostępnionego kodu, nie stosując próbkowania”, proszę o potwierdzenie, że należy je rozumieć jako weryfikację całości oprogramowania. Opisany zakres prac nie zawiera

zapisów o audycie kodu źródłowego oprogramowania. Proszę o potwierdzenie, że w zakresie prac nie ma audytu kodu źródłowego.

Opowiedź do pytania nr 14

W zakresie prac znajduje się audyt działania aplikacji oraz sprawdzenie kodu źródłowego aplikacji.

Pytanie nr 15

Zgłaszam się z uprzejmą prośbą o akceptację zapisu aby móc sporządzić ofertę „by kod weryfikować z pomocą pół-automatyczną weryfikacją kodu". W takim przypadku weryfikacja większości kodu zostanie przeprowadzona z wykorzystaniem narzędzia SAST. Biorąc pod uwagę, że aplikacja korzysta z frameworku Laravel wykonując analizy manualne zajmie to niewspółmiernie dużo czasu, a efekt będzie podobny.

Opowiedź do pytania nr 15

Zamawiajacy akceptuje przedmitowy zapis.