PKP INTERCITY S.A.
Biuro Teleinformatyki
02-305 Warszawa
Aleje Jerozolimskie 142A

Warszawa, dnia 2023-06-20

Odpowiedzi do RFI nr BST-P5/076/33/2023

Szanowni Państwo,

Poniżej przekazujemy odpowiedzi na zadane w toku RFI pytania:

Pytanie nr 1:

Czy Zamawiający miał na myśli różne audyty bezpieczeństwa teleinformatycznego czy jest to pomyłka w redagowaniu dokumentu?

Odpowiedź:

Zgodnie z założeniami zapisy w punkcie 3 zapytania o informację cenową dotyczą badania różnych aspektów bezpieczeństwa teleinformatycznego wymienionych w p. 3.2. Podobnie w punkcie 5 zapytania audyty rozumiane są zgodnie ze wskazanymi zapisami zarówno w kontekście bezpieczeństwa teleinformatycznego jak i bezpieczeństwa informacji.

Pytanie nr 2:

Zamawiający w RFI wyszczególnił szereg usług, w ramach których niektóre działania będą trudne do dokładnego zwymiarowania liczby roboczogodzin (np.:"uzyskaniu od Zamawiającego akceptacji strategii mitygacji podatności z odpowiednim właścicielem systemu", „wsparciu w zakresie mitygacji", „Wykonawca odpowiada za nadzór nad planowaniem i realizacją działań dotyczących materializacji ryzyka oraz oceny skuteczności prowadzonych działań" czy „Wykonawca ma wspierać proces analizy ryzyka poprzez identyfikację oraz aktualizację mapy ryzyka i monitorowania realizacji planu postępowania z ryzykiem" itd.) W związku z powyższym prosimy o rozważenie modyfikacji zapisu punktu 2.8. w taki sposób, aby możliwe były uaktualnienia liczby roboczogodzin przez Wykonawcę po uzgodnieniu z Zamawiającym.

Odpowiedź:

Zamawiający nie wyraża zgody na proponowaną zmianę. Wszystkie niezbędne informacje do formalnej wyceny w ramach Oferty, o której mowa w pkt. 2.4 zapytania, przekazane będą przed podpisaniem przez Strony dokumentu Zamówienia.

Pytanie nr 3:

II. Brzmienie oryginalne: 3.2. Wykonawca realizować będzie audyty bezpieczeństwa teleinformatycznego dla systemów IT oraz OT Zamawiającego, polegające m.in. na:

a) wykonaniu analizy architektury bezpieczeństwa,

b) przeglądów konfiguracji rozwiązań,

c) analiz ruchu sieciowego (pakiety sieciowe),

d) analiz zasad filtracji ruchu sieciowego,

e) analizy pod kątem obecności niepożądanych usług,

f) analizy mechanizmów logowania zdarzeń,

g) weryfikacji sposobów kontroli dostępu do sieci,

h) weryfikacji stosowania zabezpieczeń i mechanizmów kryptograficznych,

i) weryfikacji sprawności działania systemów protekcji,

j) weryfikacji zabezpieczeń pomieszczeń specjalnych wykorzystywanych do przetwarzania danych,

k) analiza kodu źródłowego

l) weryfikacji sprawności wdrożonych polityk, procedur i instrukcji bezpieczeństwa.

Zamawiający zapisał wymóg przeprowadzania audytów bezpieczeństwa teleinformatycznego dla systemów IT oraz OT. Czy Zamawiający mógłby uszczegółowić, jakie systemy OT podlegałyby procesowi audytu oraz czy dla tych systemów Zamawiający udostępni kod źródłowy do analizy? Informacja o systemach OT, które będą podlegały procesowi audytu pozwoli właściwie oszacować koszt roboczogodziny.

Odpowiedź:

Zamawiający oczekuje gotowości do przeprowadzenia audytów bezpieczeństwa wg wymagań UKSC, uzależnionych od aktualnej potrzeby Zamawiającego, krytyczności systemów zarówno IT jak i OT wskazanych w trakcie obowiązywania umowy, stąd na etapie postępowania Zamawiający nie określi listy dedykowanych systemów, także ze względu na ich liczbę i wybór.

Pytanie nr 4:

Brzmienie oryginalne: 3.4. Wykonawca zobowiązany jest do niezwłocznego przekazywania informacji o wykrytych w toku realizacji audytu krytycznych niezgodnościach (w tym ryzykach o poziomie istotności minimum wysokim zgodnie z CVSS).

Chcielibyśmy zwrócić uwagę, że działania opisane w tym podpunkcie są działaniami typowanymi podczas wykonywania testów penetracyjnych. W związku z powyższym prosimy o rozważenie przeniesienia/ usunięcia tego podpunktu

Odpowiedź:

Zamawiający nie wyraża zgody na powyższą zmianę.

Pytanie nr 5:

Brzmienie oryginalne: 3.8. Wykonawca zobowiązany będzie do zapewnienia konsultacji w zakresie proponowanych rekomendacji.

Przez domniemanie przyjmujemy, że Zamawiający miał na myśli zapewnienie konsultacji w zakresie proponowanych rekomendacji określonych w umowie formie i zakresie. Prosimy o potwierdzenie naszych domniemań ewentualne uściślenie zapisów tego podpunktu.

Odpowiedź:

Zamawiający przewiduje realizację konsultacji każdorazowo w formie uzgodnionej z Wykonawcą.

Pytanie nr 6:

Brzmienie oryginalne: 3.10. Wykonawca ma wspierać proces analizy ryzyka poprzez identyfikację oraz aktualizację mapy ryzyka i monitorowania realizacji planu postępowania z ryzykiem.

Chcielibyśmy zwrócić uwagę, że działania opisane w tym podpunkcie nie są działaniami audytowymi. Prosimy o rozważenie usunięcie tego podpunktu.

Odpowiedź:

Zamawiający nie wyraża zgody na powyższą zmianę.

Pytanie nr 7:

Brzmienie oryginalne: 4.13. Wykonawca odpowiada za nadzór nad planowaniem i realizacją działań dotyczących materializacji ryzyka oraz oceny skuteczności prowadzonych działań.

I 4.14. Wykonawca ma wspierać proces analizy ryzyka poprzez identyfikację oraz aktualizację mapy ryzyka i monitorowania realizacji planu postępowania z ryzykiem.

II

Pytanie:

Chcielibyśmy zwrócić uwagę, że działania opisane w tych podpunktach nie są działaniami realizowanymi w testach penetracyjnych. Prosimy o rozważenie przeniesienia/usunięcia tych podpunktów.

Odpowiedź:

Zamawiający nie wyraża zgody na powyższą zmianę.

Pytanie nr 8:

Brzmienie oryginalne:

7. Wsparcie procesu zarządzania podatnościami

7.1. Do realizacji wsparcia procesu zarządzania podatnościami Wykonawca przeznaczy osoby pełniące rolę inżyniera cyberbezpieczeństwa i architekta bezpieczeństwa teleinformatycznego oraz posiadające doświadczenie w zarządzaniu podatnościami technicznymi.

7.2. Wykonawca dostarczy sprawność analizy zidentyfikowanych podatności każdorazowo w momencie przekazania informacji o podatności przez Zamawiającego.

7.3. sprawność analizy zidentyfikowanych podatności polegać będzie na:

a) określeniu egzystencji podatności (false-positive, true-positive),

b) potwierdzeniu powagi (zgodnie z CVSS), opracowania strategii mitygacji, uzgodnienia strategii mitygacji z odpowiednim administratorem,

c) uzyskaniu od Zamawiającego akceptacji strategii mitygacji podatności z odpowiednim właścicielem systemu

d) wsparciu w zakresie mitygacji;

7.4. Wykonawca zapewni przekazanie wiedzy o braku możliwości zastosowania mitygacji do procesu analizy ryzyka poprzez przygotowanie technicznej analizy skutków braku mitygacji, ocenie prawdopodobieństwa i skutku wystąpienia ryzyka oraz wypełnienie karty ryzyka.

7.5. Wykonawca zapewni SLA dla opracowania strategii i mitygacji w zakresie maksymalnie 1 dnia roboczego od dnia pozyskania przez Wykonawcę lub od Zamawiającego informacji o podatności.

7.6. Wykonawca zobowiązany będzie do dostarczeniu raportu zbiorczego z analizy podatności do 10 dnia każdego miesiąca. W raporcie wykonawca ujmie min. listę podatności wraz z ich statusem, zastosowaną strategię mitygacji podatności, opis podjętych działań oraz uwagi.

1. Zapisy pkt 7. sugerują, że Zamawiający ma w ramach swojej infrastruktury informatycznej SOC lub korzysta z usługi SOCaaS lub zamierza korzystać z takich usług w trakcie realizacji usługi opisanej w RFI. Prosimy o informację czy trafnie odczytaliśmy intencje Zamawiającego?

Odpowiedź:

Tak.

Pytanie nr 9:

2. W przypadku gdy Zamawiający nie dysponuje własnym SOC lub SOCaaS to czy rozważyłby możliwość rozszerzenia RFI o świadczenie usługi SOCaaS? Takie rozwiązanie pozwoliłoby na zapewnienie poprawności realizacji zadań wyszczególnionych w podpunktach 7.1 do 7.6.

Odpowiedź:

Zamawiający nie rozważa takiej możliwości.

Pytanie nr 10:

3. W zapisach podpunktów pojawia się określenie „strategii mitygacji” i „strategii i mitygacji”, czy jest to niezamierzony błąd czy pod tymi określeniami kryją się różne pojęcia?

Odpowiedź:

Zamawiający wyjaśnia, iż w przytoczonych punktach chodzi o strategię mitygacji

Pytanie nr 11:

4. Co Zamawiający rozumie pod pojęciem „sprawność analizy zidentyfikowanych podatności”?

Odpowiedź:

Zamawiający określił w pkt. 7.3 a-d pojęcie „sprawność analizy zidentyfikowanych podatności”.

Pytanie nr 12:

Brzmienie oryginalne: 8.2. Wykonawca opracuje i uzgodni z Zamawiającym program szkoleń wewnętrznych dla wybranych grup pracowników Zamawiającego. Program szkoleń wewnętrznych zostanie opracowany do 30 dnia od przekazania przez Zamawiającego zlecenia. W programie szkoleń zawarta zostanie lista szkoleń w raz z ich wstępną agendą, czas trwania szkolenia, adresowane audytorium (np.

kadra zarządcza, pracownicy księgowości), szczegóły dotyczące szkoleń (wskazane w zleceniu) oraz planowany termin realizacji szkolenia. Program szkoleń podlega akceptacji Zamawiającego.

Do prawidłowej wyceny kosztów szkoleń niezbędna jest wiedza nt. ilości uczestników. Szkolenia. Proponujemy dopisanie takiej informacji w „Programie szkoleń wewnętrznych”.

Odpowiedź:

Zamawiający oczekuje gotowości do realizacji szkoleń w ramach prawa OPCJI w różnym zakresie i zależnie od potrzeb dla różnej liczby uczestników i różnej formie.

Pytanie nr 13:

Brzmienie oryginalne: 9.3. Wykonawca zapewni możliwość zdalnej konsultacji cyberbezpieczeństwa w zakresie:

a) Incydentów bezpieczeństwa teleinformatycznego

b) Zagrożeń, błędów bezpieczeństwa i podatności oraz form ich mitygacji

c) Architektury zabezpieczeń systemów teleinformatycznych, technologicznych oraz sieci

d) Konfiguracji wybranych systemów teleinformatycznych

Brzmienie oryginalne: 9.4. Konsultacja zdalna realizowana będzie na zlecenie Zamawiającego z zapewnieniem SLA 8h od momentu zlecenia konsultacji. Wykonawca zapewni możliwość konsultacji w trybie 24/7/365.

Chcielibyśmy zwrócić uwagę, że jeżeli Zamawiający nie dysponuje własnym SOC lub nie korzysta z usługi SOCaaS to wskazane SLA (24/7/365) jest wymaganiem zawyżonym podnoszącym koszty usługi. Prosimy również o rozważenie czy SLA o takich parametrach dla podpunktów c) i d) jest rzeczywiście wymagane?

Odpowiedź:

Zamawiający dysponuje własnym SOC, terminy SLA dla podpunktów c) i d) będą każdorazowo uzgadniane z Wykonawcą.

Pytanie nr 14:

"consulting w zakresie compliance oraz cyberbezpieczeństwa zwłaszcza w obrębie Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560), Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000), standardów ISO/IEC 27001, ISO/IEC 22301, ISO 31000, ISO20000 oraz architektury bezpieczeństwa;"

Prosimy usunięcie za zakresu współpracy, obowiązku świadczenia.

Rekomendujemy rozdzielenie usług testów, audytów, szkoleń i mentorstwa od części procesowej, procedur i działań SOC.

Odpowiedź:

Zamawiający podtrzymuje zapisy

Pytanie nr 15:

"2.8. Wynagrodzenie, wynikające ze wskazanej w Dokumencie Zamówienia liczby roboczodni oraz wysokości stawki, jest stałe i nie może ulec podwyższeniu, niezależnie od liczby roboczodni faktycznie wykorzystanych na realizację Zlecenia."

Prosimy o usunięcie zapisu.

Wykonawca nie może zgodzić się na wskazany zapis w przypadku braku gotowości/ niedostępności środowiska czy zasobów, gdy ta niedostępność jest od niego niezależna.

Jeśli dłuższy czas realizacji jest zawiniony w całości przez Wykonawcę to zapis jest uzasadniony. Inaczej albo czas ewentualnej niedostępności zezwala wykonawcy na wyłączenia części zakresu prac albo strony dokonują modyfikacji zamówienia.

Odpowiedź:

Wykonawca nie będzie ponosił odpowiedzialności za działania od niego niezależne.

Pytanie nr 16:

Procedura odbioru

"Wykonawca przedłoży Zamawiającemu do podpisu raport za realizację danego Zlecenia/ etapu Zlecenia, który zawierać będzie listę zrealizowanych zadań oraz ilość przeznaczonych

na realizację godzin po stronie Wykonawcy. Podpisany przez Zamawiającego protokół będzie podstawą do wystawienia FV za zrealizowane prace."

Prosimy o modyfikacje / usunięcie zapisu.

Oferta i zamówienie definiuje ilość dni na realizacje prac. Klient akceptując ofertę przejmuje dni i powiązany z tym koszt.

Wykonawca nie zgadza się na ponowną rewizje czy negocjacje dni.

Odpowiedź:

Opisany w zapytaniu model zamawiania usług nie przewiduje rewizji lub negocjacji liczby roboczogodzin dla już złożonych Zleceń.

Pytanie nr 17:

Sposób realizacji

"Realizacja audytów bezpieczeństwa teleinformatycznego ma na celu zidentyfikowanie wszelkich luk i podatności w zabezpieczeniach, które mogą skutkować naruszeniem atrybutów bezpieczeństwa."

Prosimy o usunięcie / modyfikacje zapisu.

Nie zagwarantujemy, że znajdziemy wszystkie luki systemu czy środowiska. Trafnym byłoby użycie „w miarę możliwości”

Specyfika tego typu usług powoduje ze może zdarzyć się, że czegoś nie znajdziemy.

Choćby ze względu na odmienną konfiguracje między środowiskami.

Tym bardziej, iż typowy test ma ograniczone ramy czasowe. Zwykle nie ma możliwości realizacji badania przez 3 miesiące (uwzględniające wszelkie powiązane komponenty) celem upewnienia się, że na obecny dzień nie znajdują się w danym środowisku, żadne luki.

Odpowiedź:

Zamawiający oczekuje zidentyfikowania luk i podatności na czas wykonywania audytu.

Pytanie nr 18:

Termin realizacji

"Przystąpienie Wykonawcy do testów będzie na wezwanie Zamawiającego w terminie, miejscu, formie i czasie wskazanym przez Zamawiającego."

Wykonawca nie może zgodzić się na powyższy zapis.

Powinno być to uzgodnione za porozumienie stron. Może być to zawarte w ofercie / zamówieniu.

Umowa nie przewiduje jak rozumiemy płacenia wykonawcy za określoną ilość dni stand by?

Odpowiedź:

Zamawiający wskazał w pkt. 4.5 wymogi dotyczące realizacji testów bezpieczeństwa.

Pytanie nr 19:

Zakres usług

Prosimy o rozdzielenie usług testów, audytów, szkoleń i mentorstwa od działań na procedurach, procesach i usług soc

Odpowiedź:

Zamawiający nie wyraża zgody.

Pytanie nr 20:

Czy Zamawiający planuje podpisać umowę z 1 wykonawcą czy z większą grupą?

Wykonawcę powinien mieć prawo odmowy złożenia oferty w ramach umowy.

Umowa łączy w sobie szeroki wachlarz usług, których pokrycie przez 1 wykonawcę jest trudne czy nie możliwe.

Zwykle rozwiązywane będzie to podwykonawstwem na część usług co stanowi dla Klienta ryzyko w kontekście jakości ich świadczenia oraz docelowej rozliczności prac.

Według nas warto kategorie usług podzielić na dwie umowy.

Testy, audyty, osint, szkolenia w jednym natomiast procesy, procedury, soc w drugiej.

Odpowiedź:

Zamawiający nie przewiduje podziału zakresu zamówienia. Zamawiający dopuszcza zawarcie umowy zarówno z konsorcjum, jak i z Wykonawcą, który będzie mógł skorzystać z podwykonawców

Pytanie nr 21:

Prosimy o usunięcie wymagania

• Konsultacja zdalna realizowana będzie na zlecenie Zamawiającego z zapewnieniem SLA 8h od momentu zlecenia konsultacji. Wykonawca zapewni możliwość konsultacji w trybie 24/7/365.

Odpowiedź:

Zgodnie z odpowiedzią udzieloną na pytanie nr 13 , terminy SLA dla podpunktów c) i d) będą każdorazowo uzgadniane przez Zamawiającego z Wykonawcą.

Pytanie nr 22:

certyfikaty

a) Jako zespół łącznie posiadają następujące certyfikaty: CISM lub równoważny, CISA lub równoważny, CRISK lub równoważny, CEH lub równoważny, CISSP lub równoważny.

Prosimy o pozostawienie w wymaganiach zespołu jednego z opisanych certyfikatów.

Dodatkowo według nas w wymaganiach brakuje certyfikatów, które dotyczą docelowo przedmiotu planowanej współpracy tj: osint, testy, audytów, threat modeling jak np. LPT, GIAC GXPN, GMOB, GPEN, EWPTX, OSCE, OSWE, OSCP, CPT, CEPT

To właśnie takie certyfikaty oddają kompetencje wymagane dla celów niniejszej umowy. "

Odpowiedź:

Zamawiający podtrzymuje dotychczasowe zapisy.

Pytanie nr 23:

Każdy z członków zespołu posiada certyfikat audytora wiodącego Systemu Zarządzania Bezpieczeństwem Informacji lub równoważny oraz certyfikat audytora wiodącego Systemu Zarządzania Ciągłością Działania lub równoważny wydany przez akredytowaną jednostkę.

Prosimy o usunięcie wymagania. Jest to trudne a nawet niemożliwe do wypełniania. Audytor wiodący niemal nigdy nie pełni funkcji architekta bezpieczeństwa czy pentestera. Są to odmienne ścieżki kompetencji adresując inne aspekty cyberbezpieczeństwa.

Odpowiedź:

Zamawiający oczekuje od Wykonawcy, aby w dedykowanym zespole jeden z pracowników posiadał wskazany certyfikat.

Pytanie nr 24:

a) 5 umów, przedmiotem których była realizacja audytów bezpieczeństwa w zakresie spełnienia wymagań Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

b) 5 umów, przedmiotem których była realizacja audytów bezpieczeństwa w zakresie spełnienia wymagań Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych);

Prosimy o usunięcie wymagania. Jego spełnienie nie jest wymagane dla potwierdzenia należytego doświadczenia czy kompetencji, które uprawniają do realizacji współpracy w ramach niniejszej umowy.

Odpowiedź:

Zamawiający zmienił warunek zgodnie z opublikowanymi odpowiedziami z dnia 2 czerwca 2023 r.

Pytanie nr 25:

referencje

c) 5 umów, przedmiotem których była realizacja testów penetracyjnych;

d) 5 umów, przedmiotem których była realizacja szkoleń w zakresie bezpieczeństwa informacji, socjotechniki lub cyberbezpieczeństwa

e) 3 umowy, przedmiotem których była realizacja analizy forensic / analizy śledczej / threat intelligence.

Prosimy o umożliwienie przedstawienie zamiennie 10 referencji z zamówień lub umów, które dotyczyły usług z powyższych punktów.

Czyli referencja może dotyczyć albo c albo d albo e.

W obecnym brzmieniu wymaganie jest istotnie nadmiarowe, Tym bardziej uwzględniając, iz mają być to referencje z ostatnich 3 lat.

Trudnym byłoby zebranie takiej ilości referencji nawet w przeciągu 6 lat.

Należy uwzględnić w tym czas przestoju podyktowany covidem.

Tak restrykcyjne wymagani ograniczą konkurencyjność postępowania. Zaś brak takiej ilości poświadczeń nie determinuje, że wykonawca nie jest kompetentny w realizacji usług.

Odpowiedź:

Zamawiający zmienił warunek zgodnie z opublikowanymi odpowiedziami z dnia 2 czerwca 2023 r.

Pytanie nr 26:

Wykonawca zobowiązany jest do kierowania do realizacji danego Zlecenia specjalistów określonych w Zleceniu w terminie 5 dni lub w terminie wskazanym w Zleceniu, w zależności od tego które nastąpi wcześniej.

Prosimy o usunięcie / modyfikacje zapisu. Oferta i zamówienie powinny definiować terminy i to one powinny być wiążące.

Odpowiedź:

Zamawiający nie wyraża zgody na proponowaną zmianę.

Pytanie nr 27:

Czy wykonawca uprawniony jest do przedstawienia oferty jeśli nie spełnia wszyskich wymagań?"

Odpowiedź:

Zamawiający nie wyraża zgody.

Pytanie nr 28:

Czy dopuszczą Państwo Certyfikat OSCP jako równoważny w stosunku do wymienionych w zapyta-niu

„Jako zespół łącznie posiadają następujące certyfikaty: CISM lub równoważny, CISA lub równoważny, CRISK lub równoważny, CEH lub równoważny, CISSP lub równoważny”

Odpowiedź:

Zamawiający wyraża zgodę.

Pytanie nr 29:

Na platformie Zakupowej termin składania ofert jest określony na dzień 16.06 do godziny 10:00, podczas gdy w odpowiedziach na pytania

„Zamawiający wyraża zgodę na wydłużenie terminu składania informacji cenowych do 19 czerwca 2023 r. do godz. 10:00.”

Proszę o informację, który z powyższych terminów jest obowiązujący?

Odpowiedź:

Termin przesyłania informacji cenowych został przedłużony do 23.06.2023