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

RFI nr BST-P5/076/33/2023

Warszawa, dnia 2023-05-29

Z A P Y T A N I E O I N F O R M A C J Ę

Dot.: świadczenia usług konsultacji cyberbezpieczeństwa przez okres 3 lat.

Zwracamy się do Państwa z prośbą o udzielenie informacji cenowej dotyczącej świadczenia usług konsultacji cyberbezpieczeństwa, zgodnie z poniższymi wymaganiami, w tym z compliance zwłaszcza poprzez:

1. realizację audytów bezpieczeństwa teleinformatycznego;
2. realizację testów penetracyjnych i testów badania podatności;
3. realizację audytów podmiotów trzecich;
4. badanie i identyfikację wycieków danych, w tym ”Threat intelligence” ustalanie, czy infrastruktura została już „skompromitowana” i w jakim stopniu (według wskaźników IOC – Indicators of Compromise);
5. wsparcie procesu zarządzania podatnościami;
6. 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;
7. realizację programu szkoleń wewnętrznych **(opcja)**;
8. mentoring kluczowych pracowników Zamawiającego odpowiedzialnych za bezpieczeństwo teleinformatyczne.

I. Szczegółowy opis przedmiotu zamówienia

1. Podstawowym celem usługi jest spełnienie wymagań wynikających z 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) oraz dobrych praktyk w zakresie cyberbezpieczeństwa.
2. Metoda rozliczenia pracy
   - 2.1. Usługi objęte przedmiotem zapytania realizowane są na podstawie zleceń, składanych przez Zamawiającego, zgodnie z procedurą opisaną poniżej (Zlecenie).
   - 2.2. Zamawiający przekazuje Wykonawcy Wniosek na piśmie lub za pośrednictwem poczty elektronicznej.

2.3. Wykonawca w ciągu 5 (pięciu) Dni Roboczych od dnia otrzymania Wniosku przedstawi Koordynatorowi Zamawiającego ofertę wykonania Zlecenia opisanego we Wniosku („Oferta") wraz z kalkulacją wynagrodzenia.

2.4. Oferta będzie zawierać w szczególności:

2.4.1. szczegółowy opis i zakres usług;

2.4.2. pracochłonność usług w podziale na typy usług: analiza i projekt, budowa oprogramowania, testy, dokumentacja, prace wyjazdowe, szkolenia, warsztaty, instalacje itp.;

2.4.3. produkty Zlecenia;

2.4.4. termin rozpoczęcia realizacji Zlecenia oraz – jeśli to konieczne – miejsce wykonania Zlecenia;

2.4.5. wynagrodzenie z tytułu realizacji Zlecenia obliczone w oparciu o stawkę dzienną zgodną z Cennikiem oraz przewidywaną ilością roboczodni na wykonanie Zlecenia,;

2.4.6. termin związania Ofertą, nie krótszy niż 30 dni;

2.4.7. inne warunki realizacji Zlecenia.

2.5. Zamawiający jest uprawniony, lecz nie zobowiązany do przyjęcia Oferty. Zamawiającemu przysługuje prawo do zgłoszenia uwag do Oferty i w takim wypadku Wykonawca zobowiązany jest do złożenia aktualizacji Oferty zgodnie z postanowieniami powyższymi. W przypadku przyjęcia Oferty, Zamawiający poinformuje Koordynatora Wykonawcy o przyjęciu Oferty.

2.6. Niezwłocznie po zawiadomieniu Wykonawcy o zaakceptowaniu jego Oferty, Strony podpisują Dokument Zamówienia, określający warunki realizacji Zlecenia zgodnie z przyjętą Ofertą. Dokument Zamówienia winien zawierać pod rygorem nieważności:

2.6.1. unikalny numer Zlecenia;

2.6.2. szczegółowy opis i zakres Zlecenia;

2.6.3. cel realizacji Zlecenia;

2.6.4. tryb realizacji Zlecenia (on-site, zdalny)

2.6.5. pracochłonność wykonania Zlecenia w podziale na typy usług: analiza i projekt, testy, dokumentacja, prace wyjazdowe, szkolenia, instalacje, itp.;

2.6.6. termin wykonania lub czas wykonania Zlecenia w podziale na etapy;

2.6.7. harmonogram realizacji Zlecenia;

2.6.8. określenie przypadków, dla których Wykonawca zobowiązany jest przygotować scenariusze testów (jeśli dotyczy);

2.6.9. określenie niezbędnej dokumentacji, w tym instrukcji obsługi i dokumentacji technicznej (jeśli dotyczy);

2.6.10. określenie niezbędnych szkoleń, jeżeli są objęte przedmiotem Zlecenia (jeśli dotyczy);

2.6.11. wynagrodzenie za zrealizowanie kolejnych etapów lub wynagrodzenie za całość Zlecenia, w wysokości wynikającej z Oferty;

2.6.12. inne postanowienia istotne dla realizacji przedmiotu Zlecenia (jeżeli występują).

2.7. Dokument Zamówienia wymaga formy pisemnej pod rygorem nieważności.

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.

2.9. 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.

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

3.1. Do realizacji audytów bezpieczeństwa teleinformatycznego Wykonawca zapewni osoby pełniące rolę audytora bezpieczeństwa oraz posiadające doświadczenie w wykonywaniu audytów bezpieczeństwa systemów IT oraz OT.

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.

3.3. Wykonawca przed realizacją zleconego audytu bezpieczeństwa opracuje i uzgodni z Zamawiającym tryb (on-site, zdalny), cel, plan i harmonogram audytu oraz wzór raportu z audytu.

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).

3.5. Wykonawca zobowiązany będzie do dostarczeniu raportu z audytu w terminie do 10 dni od zakończenia działań audytowych. W raporcie z audytu wykonawca ujmie min. informacje o celu, zakresie, podjętych działaniach, opisie podjętych działań, niezgodnościach i innych naruszeniach, obserwacjach oraz rekomendacjach.

3.6. Wykonawca zobowiązany będzie do opracowania listy ryzyk wraz z rekomendacjami mitygującymi ryzyka wynikających z wniosków z audytu, które stanowić będą załączniki raportu.

3.7. Wykonawca zobowiązany będzie do realizacji spotkania zamykającego w terminie do 10 dni od zakończenia działań audytowych.

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

3.9. Wykonawca odpowiada za nadzór nad planowaniem i realizacją działań dotyczących materializacji ryzyka oraz oceny skuteczności prowadzonych działań.

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

4. Realizacja testów penetracyjnych oraz badania podatności ma na celu ocenę odporności na ataki zasobów Zamawiającego.

4.1. Do realizacji testów Wykonawca przeznaczy osoby pełniące rolę testera penetracyjnego oraz posiadające doświadczenie w wykonywaniu testów penetracyjnych systemów IT, oraz OT oraz posiadający doświadczenie w zakresie tworzenia scenariuszy testów bezpieczeństwa.

4.2. Wykonawca realizować będzie testy typu white-box, gray-box oraz black-box.

4.3. Wykonawca realizować będzie testy penetracyjne dla infrastruktury, systemów operacyjnych, aplikacji web, aplikacji klienckich (desktop), aplikacji mobilnych (OWASP MASVS), interfejsów programowania aplikacji (API) oraz protokołów komunikacyjnych.

4.4. Dla realizacji usługi Wykonawca zobowiązany będzie do zastosowania odpowiednio standardów OWASP Top 10 , OWASP Testing Guide, OWASP, ASVS, OSSTMM, PTES oraz NIST Special Publication 800-115.

4.5. Wykonawca przed realizacją zleconego testu opracuje i uzgodni z Zamawiającym tryb (on-site, zdalny), cel, plan i harmonogram testu, scenariusze testowe, wzór raportu z testu oraz narzędzia, które będą wykorzystane do realizacji testu.

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

4.7. Testy będą realizowane przez Wykonawcę w oparciu o narzędzia bezpieczeństwa, do których licencje zapewnia Wykonawca.

4.8. Wykonawca zobowiązany jest do niezwłocznego przekazywania informacji o wykrytych w toku realizacji testu krytycznych niezgodnościach (w tym ryzykach o poziomie istotności minimum wysokim zgodnie z CVSS).

4.9. Wykonawca zobowiązany będzie do dostarczeniu raportu z testów w terminie do 10 dni od zakończenia działań testowych. W raporcie wykonawca ujmie min. informacje o celu, zakresie, zrealizowanych scenariuszach, opisie podjętych działań, niezgodnościach i innych naruszeniach, obserwacjach oraz rekomendacjach. W załącznikach do raportu Wykonawca dostarczy materiały dokumentujące zrealizowane scenariusze testowe w postaci danych maszynowych / logów z wykorzystywanego do realizacji scenariusza oprogramowania.

4.10. Wykonawca zobowiązany będzie do opracowanie listy ryzyk wraz z rekomendacjami mitygującymi ryzyka, wynikających z wniosków z audytu; które stanowić będą załączniki raportu.

4.11. Wykonawca zobowiązany będzie do realizacji spotkania zamykającego w terminie do 10 dni od zakończenia działań testowych, w toku którego omawiane będą wyniki przeprowadzonego testu, opisane w raporcie.

4.12. Wykonawca zobowiązany będzie do zapewnienia konsultacji w zakresie proponowanych rekomendacji.

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

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

5. Wykonawca realizować będzie audyty bezpieczeństwa teleinformatycznego dla systemów IT oraz OT Zamawiającego, polegające na:

a) badaniu OSINT wskazanych artefaktów,

b) audycie w zakresie RODO,

c) audycie w zakresie Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560),

d) audycie w zakresie wymagań standardów ISO/IEC 27001 oraz ISO 22301, TIER, ISO 31000.

5.1. Wykonawca przed realizacją zleconego audytu bezpieczeństwa opracuje i uzgodni z Zamawiającym tryb (on-site, zdalny), cel, plan i harmonogram audytu oraz wzór raportu z audytu.

5.2. Wykonawca zobowiązany będzie do dostarczeniu raportu z audytu w terminie do 10 dni od zakończenia działań audytowych. W raporcie z audytu wykonawca ujmie min. informacje o celu, zakresie, podjętych

działaniach, opisie podjętych działań, niezgodnościach i innych naruszeniach, obserwacjach oraz rekomendacjach.

5.3. Wykonawca zobowiązany będzie do opracowanie listy ryzyk wynikających z wniosków z audytu; lista ryzyk stanowić będzie załącznik raportu.

5.4. Wykonawca zobowiązany będzie do realizacji spotkania zamykającego w terminie do 10 dni od zakończenia działań audytowych.

6. Identyfikacja wycieków danych

6.1. Do realizacji identyfikacji wycieków danych Wykonawca przeznaczy osoby pełniące rolę inżyniera cyberbezpieczeństwa oraz posiadające doświadczenie w wykonywaniu audytów bezpieczeństwa oraz testów OSINT.

6.2. Wykonawca realizować będzie monitorowanie wycieków danych poprzez narzędzia threat intelligence dla takich artefaktów jak nazwa domenowa, adresy e-mail, adresacja IP, sumy kontrolne plików.

6.3. Wykonawca realizować będzie na żądanie Zamawiającego monitorowanie zmian w zakresie eksponowanych publicznie usług.

6.4. Wykonawca realizować będzie monitorowanie domen phishingowych leksykalnie zbliżonych do domen wskazanych przez Zamawiającego; liczba wskazanych domen: trzy.

6.5. Wykonawca do 10 dni od zakończenia działań przygotuje oraz omówi raport otwarcia zawierający wyniki monitorowania. Następnie każdorazowo w przypadku zaistnienia zmiany wykonawca poinformuje Zamawiającego w wystąpieniu zmiany.

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.

8. Realizacja programu szkoleń wewnętrznych **(opcja)**:

8.1. Do realizacji programu szkoleń wewnętrznych Wykonawca przeznaczy osoby pełniące rolę trenera cyberbezpieczeństwa oraz posiadające doświadczenie w realizacji szkoleń w obszarze bezpieczeństwa prawnego, organizacyjnego oraz cyberbezpieczeństwa.

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.

8.3. Zamawiający zastrzega sobie prawo do weryfikacji szkolenia przed przeprowadzeniem właściwego szkolenia. Weryfikacja szkolenia musi nastąpić min. 10 dni roboczych przed realizacją szkolenia. Weryfikacja polegać będzie na dostarczeniu prezentacji multimedialnej wraz z materiałami pomocniczymi (quizy, testy, ect.) oraz wykonaniu testowej prezentacji przed wybranymi pracownikami Zamawiającego. Zamawiający zastrzega prawo do wprowadzenia zmian merytorycznych w zakresie treści prezentacji oraz wystąpienia.

8.4. Szkolenia realizowane będą on-site w siedzibie Zamawiającego, w trybie zdalnym lub w miejscu wskazanym przez Zamawiającego.

9. Consulting w zakresie compliance oraz cyberbezpieczeństwa

9.1. Do realizacji usługi consultingu w zakresie compliance oraz cyberbezpieczeństwa Wykonawca przeznaczy osoby pełniące rolę audytora bezpieczeństwa i architekta bezpieczeństwa teleinformatycznego oraz posiadające doświadczenie w wdrażaniu systemów zarządzania bezpieczeństwem informacji, ciągłości działania oraz praktykę w zakresie zapewnienia spełnienia wymagań prawnych w obszarze bezpieczeństwa i cyberbezpieczeństwa.

9.2. Wykonawca zapewni zdolność zdalnej konsultacji compliance w zakresie:

a) Wymagań standardów ISO/IEC 27001, ISO 22301, ISO/IEC 20000, ISO31000

b) Ustawy o ochronie danych osobowych

c) Ustawy o krajowym systemie cyberbezpieczeństwa

d) Dobrych praktyk w przedmiotowym zakresie

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

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.

10. Mentoring kluczowych pracowników Zamawiającego odpowiedzialnych za bezpieczeństwo teleinformatyczne

10.1. Do realizacji usługi mentoringu kluczowych pracowników Zamawiającego Wykonawca przeznaczy osobę posiadającą praktyczną wiedzę popartą min. dziesięcioletnim doświadczeniem w zakresie bezpieczeństwa organizacyjnego, teleinformatycznego, aspektów prawnych, cyberbezpieczeństwa oraz prowadzenia szkoleń i warsztatów.

10.2. Wykonawca w terminie uzgodnionym z Zamawiającym, ale nie później niż do 30 dni od przekazania zlecenia opracuje plan rozwoju kompetencji w zakresie cyberbezpieczeństwa dla pracowników Zamawiającego. W planie rozwoju kompetencji zostaną zawarte konkretne cele (perspektywa roczna), oczekiwany efekt realizacji, stopień ich realizacji oraz szczegóły określone w zleceniu.

10.3. Wykonawca na wniosek Zamawiającego ale nie rzadziej niż raz na kwartał opracuje listę konkretnych zadań, które umożliwią osiągnięcie wyznaczonego celu. Lista zadań zawierać będzie jednostkowe zagadnienia (np. budowa wiedzy w zakresie ataków wolumetrycznych), sposób ich realizacji oraz oczekiwany efekt realizacji. Do każdego z zadań zostanie wskazany jego typ (samokształcenie, trening wewnętrzny).

10.4. Wykonawca realizować będzie treningi wewnętrzny w cyklu miesięcznym. Celem treningu wewnętrznego jest zapewnienie realizacji określonego zadania (np. budowa wiedzy w zakresie ataków wolumetrycznych). Czas trwania treningu: min. 3 godziny, forma treningu: spotkanie zdalne lub spotkanie on-site.

10.5. Wykonawca raz na kwartał wykona ewaluację planu rozwoju kompetencji. W wyniku ewaluacji Wykonawca w porozumieniu z Zamawiającym zaktualizuje listę zadań.

II. Wymagania dla Wykonawcy

1. Wykonawca zapewni realizację usługi poprzez delegowanie i posiadanie min. sześcioosobowego zespołu pełniącego następujące role:

a) Architekt bezpieczeństwa teleinformatycznego

b) Audytor bezpieczeństwa

c) Inżynier cyberbezpieczeństwa
d) Mentor
e) Tester penetracyjny
f) Trener cyberbezpieczeństwa
g) Analityk w zakresie cyberbezpieczeństwa
h) Zamawiający dopuszcza łączenie powyższych ról.

2. Każda z osób delegowanych do zespołu posiadać będzie udokumentowane min. pięcioletnie doświadczenie w zakresie realizacji projektów w obszarach cyberbezpieczeństwa, bezpieczeństwa informacji oraz ciągłości działania.
3. Jako zespół łącznie posiadają następujące certyfikaty: CISM lub równoważny, CISA lub równoważny, CRISK lub równoważny, CEH lub równoważny, CISSP lub równoważny.
4. 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.
5. Jako certyfikat równoważny Zamawiający rozumie posiadanie certyfikatów analogicznych do zakresu wskazanych certyfikatów tj. dotyczących analogicznej dziedziny merytorycznej, analogicznego stopnia poziomu kompetencji, analogicznego poziomu doświadczenia zawodowego wymaganego dla otrzymania danego certyfikatu itp.
6. Wykonawca zobowiązany będzie do posiadania uprawnień do korzystania z oprogramowania narzędziowego niezbędnego do realizacji usług objętych przedmiotem zapytania.
7. Wykonawca posiada udokumentowaną niezbędną wiedzę i doświadczenie, tj. zrealizował w okresie ostatnich 3 lat przed upływem terminu składania informacji cenowych co najmniej umowy określone poniżej, w tym przynajmniej jedna na kwotę min. 150 000 zł netto:
   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);
   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.
8. 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.

III. ODPOWIEDŹ POWINNA ZAWIERAĆ:

1. Brak lub szczegółowe potwierdzenie spełnienia wymagań zgodnie z Załącznikiem nr 1 do RFI.
2. Uzupełnienie szacowanych kosztów według wariantów określonych w Załączniku nr 2 do RFI – Formularzu odpowiedzi.

IV. Terminy

Termin składania informacji upływa **w dniu 16 czerwca 2023r. o godzinie 10.00**

(ewentualne pytania prosimy kierować **do dnia 12 czerwca 2023 r. do godziny 10:00**).

Odpowiedź prosimy przesłać w formie e-mail na adres: it@intercity.pl

„PKP INTERCITY" S.A. zastrzega, że niniejsze zapytanie nie stanowi elementu jakiegokolwiek postępowania o udzielenie zamówienia, wobec czego PKP INTERCITY S.A. nie jest zobligowane do wyboru którejkolwiek oferty. Niniejsze pismo nie stanowi również oferty w rozumieniu Kodeksu Cywilnego.