GTL/DZM/2122/2026

Pyrzowice, 30. 10. 2026

Zamieszczono na stronie internetowej Zamawiającego

Dot. postępowania prowadzonego w trybie przetargu nieograniczonego, którego przedmiotem zamówienia jest ***„Wybór dostawcy usługi Security Operations Center (SOC) polegającej na monitorowaniu w trybie ciągłym systemów teleinformatycznych oraz sieci informatycznych Górnośląskiego Towarzystwa Lotniczego S.A., a także reagowanie na pojawiające się incydenty bezpieczeństwa”***
nr sprawy: ***U/47/DTI/2026.***

Zamawiający – Górnośląskie Towarzystwo Lotnicze S.A., na podstawie art. 135 ust 2, art. 137 ust 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2026.793 ze zm), udziela wyjaśnień oraz zmienia treść SWZ.

Pytanie nr 1
Prosimy o podanie liczby urządzeń objętych usługą, w podziale na:

- stacje robocze Windows, macOS i Linux
- serwery Windows i Linux,
- urządzenia mobilne,
- urządzenia sieciowe,
- urządzenia i systemy OT/SCADA,
- pozostałe urządzenia specjalistyczne.

Odpowiedź nr 1
Liczba urządzeń objętych usługą:

- stacje robocze Windows – 340 szt.
- serwery Windows – 60 szt.
- urządzenia mobilne – 10 szt.
- urządzenia sieciowe – 100 szt.
- urządzenia i systemy OT/SCADA – 20szt.

Pytanie nr 2
Prosimy o wskazanie rodzajów i liczby źródeł logów, które mają zostać podłączone do monitoringu SOC.
Odpowiedź nr 2
Do monitoringu SOC mają być podłączone Systemy EDR (4 konsole) oraz system SIEM.

Pytanie nr 3
Prosimy o podanie wymaganego okresu retencji logów.
Odpowiedź nr 3
Zamawiający wymaga retencji logów przez okres 2 lat.

Pytanie nr 4
Prosimy o wskazanie producenta, nazwy i wersji obecnie wykorzystywanego rozwiązania EDR/XDR oraz liczby urządzeń objętych tym rozwiązaniem.
Odpowiedź nr 4
Liczba urządzeń objętych rozwiązaniem EDR/XDR wynosi 400 szt. Nazwa producenta, nazwa i wersja obecnie wykorzystywanego rozwiązania nie mają wpływu na wycenę oferty.

Pytanie nr 5
Czy Zamawiający korzysta obecnie z systemu SIEM lub SOAR? Jeśli tak, prosimy o wskazanie producenta, nazwy, wersji oraz modelu licencjonowania.
Odpowiedź nr 5
Zamawiający korzysta obecnie z systemu SIEM. Nazwa producenta, nazwa, wersje oraz model licencjonowania nie mają wpływu na wycenę oferty.

Pytanie nr 6
Prosimy o wskazanie wykorzystywanych rozwiązań w zakresie:
- ochrony poczty elektronicznej,
- firewalli i zabezpieczeń sieciowych,
- VPN i dostępu zdalnego,
- zarządzania podatnościami,
- zarządzania aktualizacjami,
- ochrony środowisk chmurowych,
- monitorowania środowisk OT/SCADA.

Odpowiedź nr 6
Zamawiający posiada rozwiązania umożliwiające realizację zadań w zakresie, o którym mowa w pytaniu.

Pytanie nr 7
Prosimy o wskazanie wykorzystywanych środowisk chmurowych oraz orientacyjnej liczby objętych usługą subskrypcji, tenantów, kont lub projektów.
Odpowiedź nr 7
Przedmiotem zamówienia nie są objęte rozwiązania chmurowe.

Pytanie nr 8
Prosimy o podanie liczby serwerów Windows objętych usługą Patch Management, wraz ze wskazaniem wersji systemów operacyjnych oraz liczby klastrów i systemów wysokiej dostępności.
Odpowiedź nr 8
Usługą Patch Management objętych jest 60 serwerów Windows.

Pytanie nr 9

Prosimy o podanie liczby zasobów objętych usługą Attack Surface Management, w szczególności:

- domen i subdomen,
- publicznych adresów IP lub klas adresowych,
- aplikacji webowych,
- publicznie dostępnych usług,
- certyfikatów SSL/TLS.

Odpowiedź nr 9

Usługą Attack Surface Management, objętych jest w szczególności:

- 35 domen i 8 subdomen
- publicznych adresów IP – 20 szt.
- aplikacji webowych – 6 szt.
- certyfikat SSL/TLS poczty elektronicznej – 1szt.

Pytanie nr 10

Czy Zamawiający posiada obecnie rozwiązania SPAN, TAP, NDR lub inne mechanizmy umożliwiające przekazywanie i analizę ruchu sieciowego? Jeśli tak, prosimy o wskazanie ich rodzaju i liczby.

Odpowiedź nr 10

W ramach usługi SOC Wykonawca zobowiązany jest dostarczyć rozwiązania, o których mowa w pytaniu.

Pytanie nr 11

Prosimy o wskazanie, które rozwiązania i licencje niezbędne do realizacji usługi SOC zostaną zapewnione przez Zamawiającego, a które powinny zostać dostarczone i uwzględnione w cenie przez wykonawcę.

Odpowiedź nr 11

Zamawiający posiada licencje na oprogramowanie EDR/XDR oraz SIEM. Pozostałe licencje wymagane do realizacji usługi SOC są po stronie Wykonawcy.

Pytanie nr 12

Zgodnie z art. 16 pkt 1 i 3 ustawy Pzp zamawiający przygotowuje i przeprowadza postępowanie w sposób zapewniający uczciwą konkurencję i proporcjonalny, a zgodnie z art. 91 ust. 1 ustawy Pzp zamawiający może udzielić zamówienia w częściach. Rozdział IV SWZ nie dopuszcza ofert częściowych. Zamówienie łączy usługę SOC (Załącznik nr 2 do SWZ, pkt 1-10, 12, 14-15), informatykę śledczą wraz z analizami urządzeń mobilnych i badaniem incydentów III linii (pkt 6 lit. c i pkt 13; Rozdział XIII pkt 1.4.2 lit. G i H SWZ) oraz zarządzanie poprawkami serwerów Windows Server (pkt 11; lit. I). Są to usługi świadczone na rynku przez różne grupy wykonawców, a łączne warunki dla wszystkich trzech zakresów ograniczają krąg wykonawców zdolnych złożyć ofertę, co przy cenie jako jedynym kryterium oceny (Rozdział XXVII SWZ) ogranicza konkurencję cenową. Czy Zamawiający podzieli zamówienie na części: Część 1 usługa SOC, Część 2 informatyka śledcza i badanie incydentów (III linia SOC), Część 3 zarządzanie poprawkami Windows Server, z przypisaniem do każdej części odpowiednich warunków udziału? Jeżeli nie, czy Zamawiający wskaże, z jakich powodów łączne wymaganie warunków dla trzech zakresów jest proporcjonalne do przedmiotu zamówienia i zapewnia uczciwą konkurencję?

Odpowiedź nr 12

Zamawiający nie wyraża zgody na podział zamówienia na części.

Przedmiot zamówienia obejmuje kompleksową usługę Security Operations Center (SOC), której prawidłowa realizacja wymaga zapewnienia pełnej integracji procesów monitorowania, wykrywania, analizy i obsługi incydentów bezpieczeństwa teleinformatycznego.
Podział zamówienia na części skutkowałby koniecznością angażowania wielu wykonawców realizujących wzajemnie zależne zadania, co mogłoby prowadzić do rozproszenia odpowiedzialności za bezpieczeństwo systemów Zamawiającego, wydłużenia czasu reakcji na incydenty, utrudnień w wymianie informacji oraz zwiększenia ryzyka wystąpienia luk organizacyjnych i technicznych.
Ze względu na charakter usługi SOC niezbędne jest zapewnienie jednolitych procedur operacyjnych, spójnego systemu raportowania, centralnego zarządzania incydentami oraz jednoznacznej odpowiedzialności wykonawcy za realizację wszystkich elementów usługi. Realizacja zamówienia przez jednego wykonawcę gwarantuje zachowanie ciągłości procesów bezpieczeństwa, skuteczną koordynację działań oraz ograniczenie ryzyk związanych z cyberbezpieczeństwem.
Brak podziału zamówienia na części nie ogranicza konkurencji w sposób nieuzasadniony, ponieważ na rynku funkcjonuje znaczna liczba podmiotów zdolnych do kompleksowego świadczenia usług SOC. Wykonawcy mogą również korzystać z potencjału podmiotów trzecich lub realizować zamówienie wspólnie w ramach konsorcjów.

Pytanie nr 13

Zgodnie z art. 16 pkt 3 ustawy Pzp postępowanie prowadzi się w sposób proporcjonalny, a zgodnie z art. 112 ust. 1 ustawy Pzp (Rozdział XIII pkt 1 SWZ określa warunki na podstawie art. 112) warunki udziału określa się w sposób proporcjonalny do przedmiotu zamówienia, umożliwiający ocenę zdolności wykonawcy do należytego wykonania zamówienia. Rozdział XIII pkt 1.4.2 lit. A SWZ wymaga od Kierownika Usługi SOC „minimum 10 lat doświadczenia w obszarze cyberbezpieczeństwa" (ppkt 1) i „minimum 10 lat doświadczenia we współpracy z organami ścigania" (ppkt 2), łącznie z 5 latami zarządzania usługami SOC lub CSIRT (ppkt 3) i udziałem w co najmniej 10 usługach SOC (ppkt 4). Staż liczony bez odniesienia do okresu, w którym został zdobyty, nie potwierdza aktualności wiedzy: Zamawiający sam w lit. H ppkt 1 wymaga doświadczenia, które zostało „zdobyte w okresie ostatnich 5 lat", a usługa ma być świadczona z użyciem obecnych rozwiązań klasy EDR/XDR (Załącznik nr 2 pkt 7) i w ramach ustawy o krajowym systemie cyberbezpieczeństwa w brzmieniu obowiązującym od 3 kwietnia 2026 r. Współpraca z organami ścigania występuje w OPZ jako wsparcie Zamawiającego (Załącznik nr 2 pkt 13 ppkt 11), obok wsparcia przy komunikacji z właściwym zespołem CSIRT (pkt 12 ppkt 16). Czy Zamawiający nada lit. A ppkt 1 brzmienie: „minimum 5 lat doświadczenia w obszarze cyberbezpieczeństwa", a ppkt 2 brzmienie: „doświadczenie we współpracy z zespołami CSIRT lub organami ścigania w zakresie obsługi incydentów bezpieczeństwa"? Jeżeli nie, czy Zamawiający wskaże, jakie kompetencje potwierdza staż dłuższy niż 5 lat i które zadania Kierownika Usługi SOC opisane w OPZ wymagają 10 lat współpracy z organami ścigania?

Odpowiedź nr 13

Zamawiający nie wyraża zgody.
Zamawiający określił warunki udziału w postępowaniu w sposób proporcjonalny do przedmiotu zamówienia, zgodnie z art. 112 ust. 1 ustawy Prawo zamówień publicznych. Przy formułowaniu warunków uwzględniono charakter, zakres, złożoność oraz znaczenie usługi Security Operations Center (SOC) dla zapewnienia bezpieczeństwa teleinformatycznego Zamawiającego.
Warunki dotyczące zdolności technicznej i zawodowej, doświadczenia wykonawcy oraz kwalifikacji personelu zostały ustalone wyłącznie w zakresie niezbędnym do potwierdzenia, że wykonawca posiada odpowiednie

kompetencje i zasoby umożliwiające prawidłową realizację zamówienia. Wymagania te pozostają w bezpośrednim związku z przedmiotem zamówienia i odpowiadają ryzyku związanemu ze świadczeniem usług monitorowania, wykrywania oraz obsługi incydentów bezpieczeństwa.
Zamawiający nie wprowadził warunków wykraczających poza potrzeby wynikające z charakteru zamówienia ani takich, które mogłyby w sposób nieuzasadniony ograniczać konkurencję lub utrudniać dostęp do zamówienia wykonawcom zdolnym do jego należytego wykonania. Poziom wymaganych referencji, doświadczenia i kwalifikacji został ustalony w sposób zapewniający wybór wykonawcy gwarantującego odpowiednią jakość usług przy jednoczesnym zachowaniu uczciwej konkurencji i równego traktowania wykonawców.
W ocenie Zamawiającego określone warunki udziału są adekwatne do wartości i stopnia skomplikowania zamówienia, służą wyłącznie weryfikacji zdolności wykonawcy do należytej realizacji usługi SOC oraz pozostają zgodne z zasadą proporcjonalności wyrażoną w ustawie Prawo zamówień publicznych.

Pytanie nr 14
Zgodnie z art. 16 pkt 3 i art. 112 ust. 1 ustawy Pzp warunki udziału określa się w sposób proporcjonalny do przedmiotu zamówienia. Rozdział XIII pkt 1.4.2 lit. B SWZ wymaga, aby co najmniej jeden Lider Operacyjny SOC posiadał „certyfikat bezpieczeństwa CEH lub OSCP lub równoważny". Wskazane certyfikaty potwierdzają kompetencje w testach penetracyjnych, a doświadczenie wymagane od lidera dotyczy koordynacji obsługi incydentów bezpieczeństwa oraz budowy polityk i procedur (lit. B ppkt 2 i 3); wsparcie eksperckie w zakresie testów penetracyjnych Załącznik nr 2 do SWZ przypisuje III linii SOC (pkt 6 lit. c). SWZ nie określa kryteriów równoważności. Czy Zamawiający potwierdza, że za równoważny uzna certyfikat potwierdzający kompetencje w zakresie obsługi incydentów bezpieczeństwa, analizy zagrożeń lub monitorowania bezpieczeństwa, wydany przez producenta rozwiązań bezpieczeństwa lub przez niezależną organizację certyfikującą? Jeżeli nie, czy Zamawiający wskaże, które zadania Lidera Operacyjnego SOC opisane w OPZ wymagają kompetencji z zakresu testów penetracyjnych?
Odpowiedź nr 14
Zgodnie z odpowiedzią na pytanie nr 13.

Pytanie nr 15
Zgodnie z art. 16 pkt 1 i 3 oraz art. 112 ust. 1 ustawy Pzp warunki udziału określa się w sposób proporcjonalny i zapewniający równe traktowanie wykonawców. Rozdział XIII pkt 1.4.2 lit. D ppkt 1 SWZ wymaga od Analityka SOC Linia 2 „minimum 2 lata doświadczenia na stanowisku analityka SOC Linia 2", a lit. E ppkt 1 od Analityka SOC Linia 3 „minimum 10 lat doświadczenia na stanowisku analityka SOC Linia 3 (projekty/ zadania)". Wymagane czynności opisują lit. D ppkt 2-5 i lit. E ppkt 2-5, a nazwy stanowisk w zespołach SOC różnią się między organizacjami. Czy Zamawiający potwierdza, że warunek z lit. D ppkt 1 oraz, w zakresie, w jakim Zamawiający nie zmieni lit. E zgodnie z pytaniem 5, warunek z lit. E ppkt 1 spełnia osoba, która przez wymagany okres wykonywała czynności odpowiadające wymaganiom odpowiednio z lit. D ppkt 2-5 albo lit. E ppkt 2-5, niezależnie od nazwy zajmowanego stanowiska i od organizacji zespołu, w którym je wykonywała? Jeżeli nie, czy Zamawiający wskaże, z którego zadania opisanego w OPZ wynika wymóg określonej nazwy stanowiska?

Odpowiedź nr 15
Zgodnie z odpowiedzią na pytanie nr 13.

Pytanie nr 16

Zgodnie z art. 16 pkt 3 i art. 112 ust. 1 ustawy Pzp warunki udziału określa się w sposób proporcjonalny do przedmiotu zamówienia. Rozdział XIII pkt 1.4.2 lit. E SWZ wymaga od Analityka SOC Linia 3 / Incident Responder 10 lat doświadczenia na tym stanowisku oraz łącznie czterech certyfikatów: dwóch z obsługi oprogramowania do analiz urządzeń mobilnych, jednego z oprogramowania do analizy dysków i jednego z testów penetracyjnych (lit. E, kwalifikacje zawodowe, ppkt 1-4). Analizy urządzeń mobilnych SWZ przypisuje odrębnie Specjalistom ds. analiz śledczych urządzeń mobilnych (lit. H). Wzór umowy w § 3 ust. 14 określa kompetencje wymagane od co najmniej jednej osoby w zespole zabezpieczającym materiał dowodowy: „aktualny certyfikat potwierdzający kompetencje w zakresie informatyki śledczej lub analizy śledczej urządzeń cyfrowych lub reagowania na incydenty bezpieczeństwa", wydany przez producenta oprogramowania do analiz śledczych lub niezależną organizację certyfikującą. Czy Zamawiający nada lit. E brzmienie: „DOŚWIADCZENIE: 1) minimum 5 lat doświadczenia w reagowaniu na incydenty bezpieczeństwa, informatyce śledczej lub analizie złośliwego oprogramowania oraz ppkt 2-5 bez zmian; KWALIFIKACJE ZAWODOWE: certyfikat potwierdzający kompetencje w zakresie informatyki śledczej lub reagowania na incydenty bezpieczeństwa, wydany przez producenta specjalistycznego oprogramowania do analiz śledczych lub przez niezależną organizację certyfikującą"? Jeżeli nie, czy Zamawiający wskaże, które zadania z pkt 6 lit. c i pkt 13 OPZ wymagają od jednej osoby łącznie certyfikatów z ppkt 1-4, skoro analizy urządzeń mobilnych przypisano lit. H, oraz jakie kompetencje potwierdza staż dłuższy niż 5 lat?

Odpowiedź nr 16

Zgodnie z odpowiedzią na pytanie nr 13.

Pytanie nr 17

Zgodnie z art. 16 pkt 3 i art. 112 ust. 1 ustawy Pzp warunki udziału określa się w sposób proporcjonalny do przedmiotu zamówienia. Rozdział XIII pkt 1.4.2 lit. F SWZ wymaga od Analityka bezpieczeństwa sieci minimum 10 lat doświadczenia „na stanowisku analityka bezpieczeństwa sieci", doświadczenia DFIR oraz certyfikatów OSWP i OSCP lub równoważnych. Oba certyfikaty potwierdzają kompetencje ofensywne (testy penetracyjne sieci bezprzewodowych i systemów), natomiast wymagane doświadczenie dotyczy analizy bezpieczeństwa sieci i DFIR, a Załącznik nr 2 do SWZ przewiduje w zakresie sieci analizę ruchu i wykrywanie ataków w ramach Threat Huntingu (pkt 8). Od Specjalistów ds. analiz śledczych urządzeń mobilnych Zamawiający wymaga doświadczenia 5-letniego, zdobytego w okresie ostatnich 5 lat (lit. H ppkt 1). SWZ nie określa kryteriów równoważności. Czy Zamawiający nada lit. F ppkt 1 brzmienie: „minimum 5 lat doświadczenia w analizie bezpieczeństwa sieci, niezależnie od nazwy zajmowanego stanowiska" oraz potwierdzi, że wymóg kwalifikacji z ppkt 1 i 2 łącznie spełnia jeden certyfikat potwierdzający kompetencje w zakresie bezpieczeństwa sieci, analizy ruchu sieciowego, wykrywania ataków sieciowych lub polowania na zagrożenia (Threat Hunting), uzyskany po zdaniu egzaminu? Jeżeli nie, czy Zamawiający wskaże, które zadania Analityka bezpieczeństwa sieci opisane w OPZ wymagają kompetencji ofensywnych potwierdzanych przez OSWP i OSCP oraz jakie kompetencje potwierdza staż dłuższy niż 5 lat?

Odpowiedź nr 17

Zgodnie z odpowiedzią na pytanie nr 13.

Pytanie nr 18

Zgodnie z art. 16 pkt 3 i art. 112 ust. 1 ustawy Pzp warunki udziału określa się w sposób proporcjonalny do przedmiotu zamówienia. Rozdział XIII pkt 1.4.2 lit. G SWZ wymaga dwóch osób posiadających status biegłego sądowego z zakresu informatyki, co najmniej 2 kadencji, z podaniem numeru wpisu na listę biegłych sądowych. Status ten nie jest warunkiem wykonywania czynności opisanych w pkt 13 Załącznika nr 2 do SWZ (zabezpieczenie materiału dowodowego, analiza powłamaniowa, wsparcie przy współpracy z organami ścigania, zachowanie łańcucha dowodowego). W postępowaniu karnym biegłego powołuje postanowieniem organ procesowy (art. 194 kpk), biegłym może być każda osoba mająca odpowiednie wiadomości (art. 195 kpk), a osoba powołana w sprawie w charakterze świadka nie może być biegłym (art. 196 § 1 kpk). Osoby wykonawcy zabezpieczające materiał na rzecz Zamawiającego jako pokrzywdzonego nie będą więc biegłymi w jego sprawie, a wartość dowodowa materiału zależy od zachowania łańcucha dowodowego (pkt 13 ppkt 12). Zamawiający sam dopuszcza zdobycie doświadczenia w analizach powłamaniowych, śledczych i zabezpieczaniu materiału cyfrowego u jednego podmiotu (Rozdział XIII pkt 1.4.2, Uwaga nr 3), a wymóg certyfikatu w zespole zabezpieczającym materiał dowodowy zapewnia już § 3 ust. 14 wzoru umowy. Czy Zamawiający potwierdza, że warunek z lit. G spełnia także osoba posiadająca co najmniej 5 lat doświadczenia w informatyce śledczej, w tym w analizach powłamaniowych i zabezpieczaniu materiału dowodowego z zachowaniem łańcucha dowodowego? Jeżeli nie, czy Zamawiający wskaże, które czynności opisane w OPZ wymagają statusu biegłego sądowego?

Odpowiedź nr 18

Zgodnie z odpowiedzią na pytanie nr 13.

Pytanie nr 19

Zgodnie z art. 99 ust. 1 i 4 ustawy Pzp przedmiot zamówienia opisuje się w sposób jednoznaczny i nie można go opisywać „w sposób, który mógłby utrudniać uczciwą konkurencję". Załącznik nr 2 pkt 8 ppkt 2-20 oraz Załącznik nr 2.1 pkt 43, 56-70 i 72 opisują jedną konstrukcję rozwiązania do Threat Huntingu, dostarczanego „na własny koszt" (pkt 8), które „nie powinno wymagać instalacji agenta, rekonfiguracji sieci, przekierowywania ruchu sieciowego czy nadawania jakichkolwiek uprawnień" (pkt 43), z mechanizmami takimi jak „DHCP Option 55" (pkt 8 ppkt 20 lit. a, pkt 59) i „minimum piętnastu niezależnych źródeł danych protokołowych" (pkt 63). Takie rozwiązanie odbiera co do zasady wyłącznie ruch rozgłoszeniowy i grupowy w swoim segmencie oraz ruch kierowany do niego samego, a Zamawiający wymaga analizy lateral movement i komunikacji pomiędzy stacjami (pkt 8 ppkt 24 i 26), ataków password spray (pkt 8 ppkt 21, pkt 49), połączeń pomiędzy stacjami (pkt 53) i wersji przeglądarek na podstawie ruchu (pkt 55). § 5 ust. 2 wzoru umowy zobowiązuje Zamawiającego do zapewnienia Wykonawcy dostępu do systemów, urządzeń i logów. Czy Zamawiający usunie pkt 8 ppkt 2-20 Załącznika nr 2 oraz pkt 43, 56-70 i 72 Załącznika nr 2.1, wstępowi pkt 8 nada brzmienie „W ramach Threat Huntingu Wykonawca zapewni:", a pkt 42 Załącznika nr 2.1 brzmienie: „Wykonawca prowadzi Threat Hunting oparty na hipotezach i technikach MITRE ATT&CK, z wykorzystaniem własnych narzędzi oraz telemetrii systemów EDR/XDR, logów systemów i urządzeń sieciowych udostępnianych zgodnie z § 5 ust. 2 umowy"? Jeżeli Zamawiający nie usunie któregokolwiek z tych punktów, czy wskaże co najmniej dwa dostępne na rynku rozwiązania różnych producentów spełniające je łącznie oraz sposób, w jaki rozwiązanie spełniające pkt 43 realizuje analizy z pkt 8 ppkt 24 i 26 oraz pkt 49, 53 i 55?

Odpowiedź nr 19

Zamawiający nie wyraża zgody.

Zamawiający wyjaśnia, że Wykonawca może realizować usługę Threat Hunting w oparciu o dostępne rozwiązania aby spełnić wymagania Zamawiającego.

Pytanie nr 20

Zgodnie z art. 99 ust. 1 ustawy Pzp przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty. Wynagrodzenie za usługę jest miesięcznym wynagrodzeniem ryczałtowym (Rozdział XXVI pkt 1 SWZ, § 7 ust. 3 wzoru umowy), a § 11 ust. 2 pkt 4 i 6 wzoru umowy odnoszą zmianę wynagrodzenia do zakresu i „wartości przyjętych do kalkulacji oferty". Załącznik nr 2 do SWZ w pkt 3 wymienia 12 obszarów bez danych ilościowych. Prosimy o podanie: liczby stacji roboczych, serwerów (w tym serwerów Windows Server objętych pkt 11 OPZ) i urządzeń mobilnych objętych systemem endpoint security oraz producenta tego systemu; listy typów źródeł logów i szacowanego wolumenu zdarzeń (EPS lub GB na dobę); liczby publicznych adresów IP i domen objętych pkt 9 i 10 OPZ. Czy Zamawiający potwierdza, że podane wartości będą wartościami przyjętymi do kalkulacji oferty w rozumieniu § 11 ust. 2 pkt 4 i 6 wzoru umowy?

Odpowiedź nr 20

Patrz odpowiedź na pytanie nr 1.

Pytanie nr 21

Zgodnie z art. 99 ust. 1 ustawy Pzp przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, uwzględniając okoliczności mogące mieć wpływ na sporządzenie oferty. Załącznik nr 2.1 do SWZ przewiduje, że Zamawiający „może korzystać nielimitowaną ilość godzin z konsultacji" (pkt 26) oraz że Wykonawca przeprowadzi symulacje kampanii phishingowych „na prośbę Zamawiającego" (pkt 20), przy wynagrodzeniu ryczałtowym. Nieokreślony wolumen świadczeń uniemożliwia porównywalną wycenę ofert. Czy Zamawiający nada pkt 26 brzmienie: „Zamawiający może korzystać z konsultacji w wymiarze do 8 godzin w miesiącu; niewykorzystane godziny przechodzą na kolejne miesiące danego roku umowy", a w pkt 20 doda słowa: „nie więcej niż 2 razy w roku umowy"? Jeżeli nie, czy Zamawiający wskaże, jaki wymiar konsultacji i jaką liczbę kampanii phishingowych wykonawcy mają przyjąć do kalkulacji ceny ryczałtowej?

Odpowiedź nr 21 /zmiana/

Zamawiający wyraża zgodę. Zamawiający zmienia zapisy załącznika nr 2.1 do SWZ- Szczegółowy OPZ, jak niżej:

Pkt 20 otrzymuje brzmienie:

Wykonawca posiada umiejętności przeprowadzenia symulacji kampanii Phishingowych przeciwko organizacji i będzie je przeprowadzał na prośbę Zamawiającego ***nie więcej niż 2 razy w roku umowy.***

Pkt 26 otrzymuje brzmienie:

Zamawiający może korzystać z konsultacji w zakresie bezpieczeństwa, czy wdrażanych procedur bezpieczeństwa w organizacji ***w wymiarze do 8 godzin w miesiącu. Niewykorzystane godziny przechodzą na kolejne miesiące danego roku umowy.***

Pytanie nr 22

Zgodnie z art. 99 ust. 1 ustawy Pzp przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, a zgodnie z art. 433 pkt 3 ustawy Pzp umowa nie może przewidywać odpowiedzialności wykonawcy za

okoliczności, za które wyłączną odpowiedzialność ponosi zamawiający. Załącznik nr 2 pkt 11 i Załącznik nr 2.1 pkt 74-80 przewidują instalację poprawek na serwerach Windows Server Zamawiającego, w tym wdrożenie „na środowisku testowym lub pilotażowym" (pkt 76) oraz rozpoczęcie wdrażania poprawek typu 0-day „nie później niż 12h po ich opublikowaniu" (pkt 78), a okna serwisowe są ustalane z Zamawiającym (pkt 75). Czy Zamawiający potwierdza, że: a) wymaganie pkt 76 spełnia wdrożenie poprawek w pierwszej kolejności na wskazanej przez Zamawiającego grupie pilotażowej serwerów; b) rozpoczęcie wdrażania w rozumieniu pkt 78 oznacza rozpoczęcie oceny wpływu poprawki, a wdrożenie na grupie pilotażowej następuje w najbliższym uzgodnionym oknie serwisowym; c) czas oczekiwania na okno serwisowe wyznaczone przez Zamawiającego nie stanowi zwłoki Wykonawcy? Jeżeli nie, czy Zamawiający wskaże, od jakiego zdarzenia biegnie termin z pkt 78?

Odpowiedź nr 22

Zamawiający wyjaśnia, że wskaże grupę pilotażową serwerów, na których wykonawca dokona aktualizacji. Po braku negatywnego wpływu na działanie systemów zaczynie biec termin 12h, który ma jedynie odniesienie do wskazanych przez Zamawiającego okien serwisowych. Czas oczekiwania na okno serwisowe nie wlicza się do czasu wskazanego 12h.

Pytanie nr 23

Zgodnie z art. 99 ust. 1 ustawy Pzp przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący. Formularz oferty (pkt 5 poz. 2) i Rozdział XXVI SWZ przewidują wynagrodzenie za „badanie incydentów (usługa III linii SOC) rozliczane za każdy pojedynczy incydent", przy szacunkowej liczbie 4 incydentów; § 7 ust. 2 i 4 wzoru umowy obejmują wynagrodzeniem miesięcznym I i II linię, a III linię rozliczają „za każde zdarzenie", natomiast § 11 ust. 3 pkt 4 przewiduje, że przy zwiększeniu liczby incydentów strony określą zmianę wynagrodzenia „w drodze aneksu". Zakres III linii (Załącznik nr 2 pkt 6 lit. c i pkt 13) nie określa nakładu pracy na jedno badanie. Czy Zamawiający potwierdza, że: a) „badanie incydentu" oznacza każde zdarzenie, w którym Wykonawca wykonuje czynności III linii dotyczące jednego incydentu, także po eskalacji zgodnie z pkt 15 OPZ; b) czynności z pkt 13 OPZ są rozliczane jako badanie incydentu; c) każde badanie, także ponad szacunkowe 4, jest rozliczane według ceny jednostkowej z oferty na podstawie § 7 ust. 4, bez aneksu; d) jedno badanie obejmuje do 80 osobogodzin pracy, a czynności ponad ten nakład rozlicza się jako kolejne badanie? Jeżeli nie, czy Zamawiający wskaże zakres czynności objętych ceną jednostkową jednego badania?

Odpowiedź nr 23

Zamawiający wymaga oszacowania wartości obsługi 4 incydentów przy założeniu, że każdy incydent będzie Wykonawca w stanie obsłużyć w 1 roboczodzień.

Pytanie nr 24

Zgodnie z art. 99 ust. 1 ustawy Pzp przedmiot zamówienia opisuje się w sposób jednoznaczny, zgodnie z art. 433 pkt 3 ustawy Pzp umowa nie może przewidywać odpowiedzialności wykonawcy za okoliczności, za które wyłączną odpowiedzialność ponosi zamawiający, a zgodnie z art. 16 pkt 3 postępowanie prowadzi się w sposób proporcjonalny. § 16 ust. 3 pkt 4 i 5 wzoru umowy przewidują kary za „przekroczenie czasów reakcji" oraz „czasów obsługi, kwalifikacji lub eskalacji incydentów" w wysokości 0,05% i 0,1% łącznego wynagrodzenia brutto za każdy przypadek, a § 4 ust. 2 odsyła do czasów „określonych w procedurach obsługi incydentów obowiązujących u Zamawiającego", których dokumentacja nie zawiera. Załącznik nr 2 pkt 15 określa czas reakcji SOC i kierunek eskalacji, bez czasów obsługi i kwalifikacji oraz bez początku i końca biegu czasu reakcji. Czy Zamawiający: a) doda w pkt 15 definicje: „Czas reakcji SOC: czas od zarejestrowania alertu

w narzędziach SOC obsługiwanych przez Wykonawcę albo od przyjęcia zgłoszenia Zamawiającego do podjęcia analizy przez analityka Wykonawcy" oraz „Eskalacja natychmiast: powiadomienie niezwłocznie po zakwalifikowaniu incydentu jako krytycznego"; b) potwierdzi, że czasami w rozumieniu § 4 ust. 2 i § 16 ust. 3 pkt 4 i 5 są wyłącznie czasy określone w pkt 15 OPZ; c) potwierdzi, że do tych czasów nie wlicza się okresów oczekiwania na działania lub informacje Zamawiającego i podmiotów trzecich; d) zmieni podstawę kar z § 16 ust. 3 pkt 4, 5 i 9 na wynagrodzenie miesięczne brutto? Jeżeli nie, czy Zamawiający udostępni procedury, o których mowa w § 4 ust. 2, i wskaże początek i koniec biegu czasu reakcji?

Odpowiedź nr 24

Czas reakcji zaczyna biec od momentu pojawienia się zdarzenia w systemach monitoringu Wykonawcy i/lub od momentu zgłoszenia przez Zmawiającego zgodnie z procedurą, która zostanie przygotowana w porozumieniu z Wykonawcą w trakcie wdrażania usługi.

Pytanie nr 25

Zgodnie z art. 99 ust. 1 ustawy Pzp opis przedmiotu zamówienia uwzględnia wszystkie okoliczności mogące mieć wpływ na sporządzenie oferty. Załącznik nr 2 pkt 4 przewiduje Etap I (uruchomienie usługi SOC), obejmujący 12 czynności, m.in. integrację narzędzi, przygotowanie reguł korelacyjnych, audyt konfiguracji endpoint security i test gotowości usługi. Termin realizacji wynosi „cztery lata od dnia protokolarnego przejęcia świadczenia" (§ 2 ust. 1 wzoru umowy), a wynagrodzenie jest płatne miesięcznie przez 48 miesięcy. Czy Zamawiający potwierdza, że Etap I jest realizowany w okresie 48 miesięcy liczonym od dnia protokolarnego przejęcia świadczenia i jest objęty wynagrodzeniem miesięcznym od tego dnia? Jeżeli nie, czy Zamawiający wskaże, w jakim okresie jest realizowany Etap I i w której pozycji formularza oferty wykonawcy mają ująć jego koszt?

Odpowiedź nr 25

Szczegółowe zasady rozliczeń zostały określone w §7 wzoru umowy.

Pytanie nr 26

Zgodnie z art. 16 pkt 2 ustawy Pzp zamawiający prowadzi postępowanie w sposób przejrzysty. § 13 część II ust. 3 wzoru umowy stanowi, że suma gwarancyjna ubezpieczenia odpowiedzialności cywilnej zawodowej „nie może być niższa niż 5 000 000 PLN (słownie: dziesięć milionów złotych)". Zapis cyfrowy i słowny są rozbieżne. Czy Zamawiający potwierdza, że wymagana suma gwarancyjna wynosi 5 000 000 PLN, i poprawi zapis słowny na „pięć milionów złotych"?

Odpowiedź nr 26 /zmiana/

Zamawiający poprawia omyłkę pisarką, w związku z czym §13 cześć II ust 3 wzoru umowy otrzymuje brzmienie:

„Suma gwarancyjna ubezpieczenia, o którym mowa w pkt 1, nie może być niższa niż 5 000 000 PLN (słownie: ***pięć*** *milionów złotych) na jedno i wszystkie zdarzenia w okresie ubezpieczenia"*

Pytanie nr 27

Zgodnie z art. 439 ust. 1 ustawy Pzp umowa na usługi zawarta na okres dłuższy niż 6 miesięcy zawiera postanowienia dotyczące zasad wprowadzania zmian wysokości wynagrodzenia w przypadku zmiany ceny materiałów lub kosztów związanych z realizacją zamówienia. § 12 ust. 4 wzoru umowy wiąże zmianę wynagrodzenia z różnicą między wskaźnikiem inflacji z roku poprzedzającego złożenie wniosku a wskaźnikiem z roku poprzedzającego otwarcie ofert (W3 = W2 - W1), dopuszcza wniosek „w terminie do 30 dni po upływie

12 miesięcy, licząc od dnia otwarcia ofert" (pkt 1) i ogranicza łączną zmianę do 5% wynagrodzenia netto (pkt 6). Przy utrzymującym się stałym poziomie inflacji wzór daje zmianę równą zero, choć koszty realizacji usługi w okresie 48 miesięcy rosną co roku o ten wskaźnik; ryzyko to wykonawcy muszą uwzględnić w cenie oferty. Czy Zamawiający zmieni § 12 ust. 4 tak, aby zmiana wynagrodzenia odpowiadała skumulowanej zmianie wskaźnika cen towarów i usług konsumpcyjnych ogłaszanego przez Prezesa GUS, liczonej od miesiąca otwarcia ofert, z łącznym limitem zmiany 10% wynagrodzenia netto, a wniosek mógł być złożony w każdym czasie po upływie 12 miesięcy od otwarcia ofert, nie częściej niż raz na 12 miesięcy? Jeżeli nie, czy Zamawiający wskaże, w jaki sposób przy stałym poziomie inflacji wynagrodzenie uwzględni zmianę kosztów, o której mowa w art. 439 ust. 1?

Odpowiedź nr 27

Zamawiający informuje, że zasady waloryzacji wynagrodzenia zostały określone w § 12 wzoru umowy. Postanowienia tego paragrafu zostały opracowane zgodnie z wymaganiami ustawy Prawo zamówień publicznych dotyczącymi obowiązkowego wprowadzania klauzul waloryzacyjnych do umów zawieranych na okres dłuższy niż 6 miesięcy.

W § 12 wzoru umowy wskazano przesłanki waloryzacji, sposób ustalania zmiany wynagrodzenia, częstotliwość dokonywania waloryzacji oraz limity zmian wynagrodzenia. Określono również zasady wykazywania wpływu zmiany cen materiałów lub kosztów na koszty realizacji zamówienia oraz obowiązki stron związane z przeprowadzeniem procesu waloryzacji.

Przyjęte postanowienia w pełni realizują wymagania określone w ustawie Prawo zamówień publicznych, zapewniając zachowanie równowagi ekonomicznej stron umowy przy jednoczesnym zabezpieczeniu interesów Zamawiającego i Wykonawcy. W związku z powyższym Zamawiający nie przewiduje zmian w zakresie postanowień dotyczących waloryzacji wynagrodzenia.

Pytanie nr 28

Zgodnie z art. 99 ust. 1 ustawy Pzp przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący. Załącznik nr 2 do SWZ w pkt 5 stanowi, że usługa będzie świadczona „zgodnie z obowiązującymi wymaganiami. 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 (Dz.U. z 2019r. poz. 2479)". Rozporządzenie wydano na podstawie art. 14 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa. Art. 14 tej ustawy w brzmieniu nadanym art. 1 pkt 22 ustawy z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. z 2026 r. poz. 252) nie zawiera upoważnienia do wydania rozporządzenia, art. 4 pkt 16 ustawy (podmioty świadczące usługi z zakresu cyberbezpieczeństwa) został uchylony, a art. 32 ustawy zmieniającej utrzymuje w mocy wyłącznie przepisy wykonawcze wydane na podstawie art. 11 ust. 4 i art. 66 ust. 9. Czy Zamawiający potwierdza, że odesłanie do rozporządzenia z dnia 4 grudnia 2019 r. w pkt 5 Załącznika nr 2 do SWZ nie stanowi wymagania wobec Wykonawcy, i usunie z pkt 5 zdanie odsyłające do tego rozporządzenia? Jeżeli nie, czy Zamawiający wskaże przepis, na podstawie którego rozporządzenie obowiązuje?

Odpowiedź nr 28 /zmiana/

Zamawiający wyjaśnia, że usługa ma być realizowana na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2026.20 t.j. ze zm.).

Mając na uwadze powyższe zmienia się zapis załącznika nr 2 do SWZ – Opis Przedmiotu Zamówienia, jak niżej:

Z pkt 5 Zamawiający wykreśla treść:
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 (Dz.U. z 2019 r. poz. 2479).

Pkt 5 zdanie pierwsze otrzymuje brzmienie:

Usługa w zakresie cyberbezpieczeństwa będzie świadczona na Infrastrukturze Zamawiającego, z wykorzystaniem zarówno narzędzi Wykonawcy, jak i narzędzi Zamawiającego obsługiwanych przez jego zespół, zgodnie z obowiązującymi wymaganiami ***na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2026.20 t.j. ze zm.).***

Pytanie nr 29
Zgodnie z art. 95 ust. 1 ustawy Pzp zamawiający może wymagać zatrudnienia na podstawie stosunku pracy wyłącznie do czynności wykonywanych w sposób określony w art. 22 § 1 Kodeksu pracy, czyli pod kierownictwem oraz w miejscu i czasie wyznaczonym przez pracodawcę, a art. 16 pkt 1 i 3 ustawy Pzp wymaga zapewnienia uczciwej konkurencji i proporcjonalności. W wyroku z dnia 5 lutego 2024 r. (KIO 154/24) Izba wskazała, że art. 95 „nie statuuje bezwzględnego obowiązku zatrudnienia wszystkich pracowników wykonawców na podstawie umowy o pracę", wymaga analizy na etapie przygotowania postępowania i nie może prowadzić do niezasadnego ograniczenia konkurencji, w tym wobec wykonawców świadczących usługi osobiście lub przez podwykonawców prowadzących jednoosobową działalność gospodarczą. Rozdział III pkt 6 SWZ i § 8 ust. 1 i 9 wzoru umowy obejmują wymogiem role zespołu SOC (Kierownik Usługi SOC, Liderzy Operacyjni SOC, Analitycy SOC Linia 1, 2 i 3), także u Podwykonawców, bez wskazania czynności. Zamawiający określa czasy reakcji usługi (Załącznik nr 2 pkt 15), a nie miejsce i czas pracy poszczególnych osób; działania w lokalizacji Zamawiającego są przewidziane tylko w związku z incydentem lub „w przypadku konieczności" (§ 3 ust. 13 i § 5 ust. 5 wzoru umowy), a wynagrodzenie to ryczałt miesięczny i cena za każdy incydent III linii (§ 7 ust. 2 i 4). Czy Zamawiający usunie w całości wymóg zatrudnienia na podstawie umowy o pracę, to jest Rozdział III pkt 6 SWZ oraz § 8 i § 16 ust. 3 pkt 2 wzoru umowy? Jeżeli nie, czy Zamawiający udostępni analizę, o której mowa w art. 95 ust. 1, wskazującą dla każdej roli z Rozdziału III pkt 6 SWZ konkretne czynności oraz kto i w jaki sposób wyznacza miejsce i czas ich wykonywania, oraz wyjaśni, dlaczego wymóg nie ogranicza konkurencji?
Odpowiedź nr 29
Zgodnie z art. 95 ust 1 ustawy Pzp, Zamawiający określił w dokumentach postepowania wymagania związane z realizacją zamówienia w zakresie zatrudnienia przez Wykonawcę lub podwykonawcę na podstawie stosunku pracy osób wykonujących wskazane przez zamawiającego czynności w zakresie realizacji zamówienia.
Zgodnie z art. 95 ust 2 Pzp w dokumentach zamówienia zostały określone:
1) rodzaj czynności związanych z realizacją zamówienia, których dotyczą wymagania zatrudnienia na podstawie stosunku pracy przez wykonawcę lub podwykonawcę osób wykonujących czynności w trakcie realizacji zamówienia;
2) sposób weryfikacji zatrudnienia tych osób;

3) uprawnienia zamawiającego w zakresie kontroli spełniania przez wykonawcę wymagań związanych z zatrudnianiem tych osób oraz sankcji z tytułu niespełnienia tych wymagań.
Mając na uwadze powyższe Zamawiający nie wyraża zgody na wykreślenie zapisów z dokumentów zamówienia.

Pytanie nr 30
Zamawiający wymaga wykazania wykonania co najmniej trzech usług SOC o wartości nie mniejszej niż 1 000 000 zł brutto każda w okresie ostatnich 3 lat. Prosimy o wyjaśnienie, w jaki sposób określono poziom tego warunku oraz czy Zamawiający rozważy jego modyfikację poprzez: obniżenie wymaganej wartości referencji, dopuszczenie większej liczby usług o niższej wartości, wydłużenie okresu referencyjnego do 5 lat. W ocenie wykonawcy obecne brzmienie warunku może prowadzić do nieuzasadnionego ograniczenia konkurencji i ograniczenia dostępu do postępowania podmiotom posiadającym doświadczenie w świadczeniu usług SOC o porównywalnym zakresie funkcjonalnym, lecz realizowanych w ramach umów o niższej wartości.
Odpowiedź nr 30
Zgodnie z odpowiedzią na pytanie nr 13.

Załączniki:
- zmieniony załącznik nr 2.1 do SWZ - Szczegółowy OPZ ZMIANA.

WICEPREZES ZARZĄDU
Norbert Henzel

PROKURENT
Paweł Wojda