GTL/DZM/2144/2026

Pyrzowice, 04. 11. 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 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2026.793 ze zm), udziela wyjaśnień.

Pytanie nr 31
Prosimy o podanie liczby urządzeń końcowych objętych usługą, z podziałem na: stacje robocze, laptopy, serwery fizyczne, serwery wirtualne (VM) oraz urządzenia mobilne.
Odpowiedź nr 31
Zgodnie z odpowiedzią na pytanie nr 1 udzieloną pismem GTL/DZM/2122/2026 z dn. 30.10.2026r., 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 32
Prosimy o wskazanie liczby serwerów Windows i Linux objętych monitoringiem, w tym liczby serwerów krytycznych.
Odpowiedź nr 32
Zgodnie z odpowiedzią na pytanie nr 1 udzieloną pismem GTL/DZM/2122/2026 z dn. 30.10.2026r.
Dodatkowo Zamawiajacy wyjaśnia, że serwerów krytycznych jest 10 szt.
Pytanie nr 33
Prosimy o wskazanie liczby lokalizacji (ośrodków przetwarzania danych, serwerowni) objętych usługą oraz sposobu ich polaczenia (łącza WAN, przepustowości).

Odpowiedź nr 33
Zamawiający posiada jedną lokalizację.

Pytanie nr 34
Prosimy o wskazanie liczby domen Active Directory, liczby kontrolerów domeny oraz przybliżonej liczby kont użytkowników i kont uprzywilejowanych.
Odpowiedź nr 34
Zabawiający wyjaśnia, że posiada 2 domeny Active Directory (po 2 kontrolery na domenę), około 300 kont użytkowników, w tym około 30 uprzywilejowanych.

Pytanie nr 35
Prosimy o podanie szacunkowego wolumenu zdarzeń (EPS lub GB/dobę) oraz liczby i typów źródeł logów planowanych do objęcia monitoringiem SIEM.
Odpowiedź nr 35
Zamawiający posiada wdrożony monitoring SIEM. Przybliżona ilość danych to 5GB/dobę.

Pytanie nr 36
Prosimy o wskazanie, czy komponenty SIEM/kolektory logów maja byc zlokalizowane w infrastrukturze Zamawiającego (on-prem), czy dopuszczalna jest infrastruktura Wykonawcy. W przypadku on-prem - czy Zamawiający zapewnia zasoby (VM, storage, siec, licencje OS).
Odpowiedź nr 36
Kolektory logów muszą być zlokalizowane w infrastrukturze Zamawiającego. Zamawiajacy zapewnia zasoby.

Pytanie nr 37
Prosimy o potwierdzenie, czy Zamawiający posiada obecnie system klasy SIEM/SOAR, a jeśli tak, czy przedmiotem zamowienia jest jego przejecie i współzarządzanie, czy dostarczenie nowego.
Odpowiedź nr 37
Zamawiający posiada wdrożony monitoring SIEM oraz udostępni Wykonawcy wgląd do tego systemu.

Pytanie nr 38
Prosimy o wskazanie wymaganego okresu retencji logów (online i archiwalnej) oraz ewentualnych wymagań dotyczących lokalizacji przechowywania danych (na terenie RP / UE).
Odpowiedź nr 38
Zgodnie z odpowiedzią na pytanie nr 3 udzieloną pismem GTL/DZM/2122/2026 z dn. 30.10.2026r.
Zamawiający wymaga retencji logów przez okres 2 lat.

Pytanie nr 39
W odniesieniu do pkt 19 OPZ (Zamawiający posiada system Endpoint Security): prosimy o wskazanie konkretnego produktu EDR/XDR (producent, wersja) oraz liczby stacji i serwerów objętych licencja.

Odpowiedź nr 39
Zgodnie z odpowiedzią na pytanie nr 4 udzieloną pismem GTL/DZM/2122/2026 z dn. 30.10.2026r.

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 40

Prosimy o potwierdzenie zakresu: czy Wykonawca ma przejąć i współzarządzać istniejącą konsola/licencja EDR/XDR Zamawiającego, czy dostarczyć nowe licencje i rozwiązanie. Jeśli przejecie - kto ponosi koszt odnowień licencji w okresie umowy?

Odpowiedź nr 40

Wykonawca ma współzarządzać istniejącą konsolą EDR/XDR. Koszty odnowień licencji są po stronie Zamawiającego.

Pytanie nr 41

Prosimy o potwierdzenie, czy w zakresie XDR dopuszczalna jest wyłącznie obsługa (współzarządzanie) posiadanego systemu, czy również jego migracja/wymiana w trakcie trwania umowy.

Odpowiedź nr 41

Zamawiający Wymaga współzarządzania systemem EDR/XDR.

Pytanie nr 42

Prosimy o wskazanie liczby i typów serwerów Windows objętych usługą Patch Management, ze wskazaniem serwerów krytycznych oraz dostępnych okien serwisowych.

Odpowiedź nr 42

Usługą Patch Management objętych jest 60 serwerów Windows, w tym 10 krytycznych. Okna serwisowe Zamawiający będzie ustalał na bieżąco w trakcie pocesu aktualizacji.

Pytanie nr 43

Prosimy o potwierdzenie zakresu odpowiedzialności Wykonawcy: czy obejmuje on faktyczne wdrażanie poprawek wraz z restartem serwerów produkcyjnych, oraz kto ponosi odpowiedzialność za dostępność usług po instalacji poprawki.

Odpowiedź nr 43

Wykonawca będzie odpowiedzialny za wdrażanie poprawek i restarty serwerów produkcyjnych we wskazanych przez Zamawiającego oknach serwisowych. Wykonawca ponosi odpowiedzialność za dostępność usług po instalacji poprawek.

Pytanie nr 44

Prosimy o potwierdzenie, czy wymóg dla poprawek krytycznych/0-day (np. do 12 godzin) dotyczy rozpoczęcia procesu wdrażania, czy jego zakończenia (pełnego wdrożenia z restartem).

Odpowiedź nr 44

Zgodnie z odpowiedzią na pytanie nr 22 udzieloną pismem GTL/DZM/2122/2026 z dn. 30.10.2026r.,
Zamawiający wskaże grupę pilotażową serwerów, po braku negatywnego wpływu na działanie systemów zaczyna 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 45
Prosimy o wskazanie, czy Zamawiający posiada narzędzie do dystrybucji poprawek (np. WSUS, SCCM/MECM, Intune) oraz czy Wykonawca ma z niego korzystać, czy dostarczyć własne.
Odpowiedź nr 45
Zamawiający posiada narzędzia do dystrybucji poprawek, Wykonawca może z niego korzystać.

Pytanie nr 46
Czy Zamawiający dopuszcza realizacje wymagań Threat Hunting (sekcja 8) w oparciu o rozwiązanie zawierające komponenty open-source (np. klasy Zeek/Suricata) utrzymywane jako usługa zarządzana, czy wymaga nazwanego produktu komercyjnego z licencja producenta.
Odpowiedź nr 46
Zamawiający dopuszcza rozwiązania/komponenty open source. Wykonawca może realizować usługę Threat Hunting w oparciu o dostępne rozwiązania aby spełnić wymagania Zamawiającego.

Pytanie nr 47
Czy wymagania sekcji 8 (29 punktów) maja być spełnione jednym narzędziem, czy dopuszczalny jest zestaw zintegrowanych narzędzi realizujących łącznie cały zakres detekcji.
Odpowiedź nr 47
Wykonawca może realizować usługę Threat Hunting w oparciu o dostępne rozwiązania aby spełnić wymagania Zamawiającego.

Pytanie nr 48
Prosimy o potwierdzenie, czy detekcje ataków warstwy 2 (ARP, Spanning Tree, VLAN hopping, MAC flooding, LLMNR/NBT-NS/mDNS, WPAD, mitm6) maja obejmować cala siec LAN, czy wskazane segmenty krytyczne. Zakres ten determinuje liczbę sond pasywnych i koszt.
Odpowiedź nr 48
Monitorowaniem objęte będzie 6 podsieci o masce 24 bity.

Pytanie nr 49
Prosimy o potwierdzenie, czy monitoring sekcji 8 ma być wyłącznie pasywny (analiza ruchu z port mirroring/TAP, bez agentów), zgodnie z pkt 2 OPZ, oraz czy Zamawiający zapewnia konfiguracje SPAN/TAP, czy ma ja dostarczyć Wykonawca.
Odpowiedź nr 49
Wykonawca musi dostarczyć kompleksowe rozwiązanie bez agentów. Konfigurację SPAN/TAP musi dostarczyć Wykonawca.

Pytanie nr 50
Prosimy o wskazanie, czy Zamawiający posiada licencje Microsoft 365 (E5 / E5 Security lub Defender for Identity), które mogłyby zostać wykorzystane w warstwie detekcji tożsamości (AD).
Odpowiedź nr 50
Zamawiający nie posiada licencji Microsoft 365 E5 / E5 Security lub Defender for Identity.

Pytanie nr 51
Prosimy o wskazanie liczby segmentów sieci (IT i OT) oraz liczby punktów styku, w których możliwe jest zestawienie port mirroring (SPAN) lub TAP na potrzeby monitoringu pasywnego.
Odpowiedź nr 51
Monitorowaniem objęte będzie 6 podsieci o masce 24 bity.

Pytanie nr 52
Prosimy o wskazanie przepustowości kluczowych łączy (core, dystrybucja, DMZ, styki OT), które maja być objęte monitoringiem, w celu dobrania wydajności sond.
Odpowiedź nr 52
Wszystkie punkty styku mogą zostać skonfigurowane na przełącznikach core o przepustowości portów 10G.

Pytanie nr 53
Prosimy o potwierdzenie, czy Zamawiający udostępni (na etapie realizacji, z zachowaniem poufności) schemat logiczny sieci i listę systemów, niezbędne do zaprojektowania architektury monitorin.
Odpowiedź nr 53
Zamawiający udostępni na etapie realizacji dokumentację sieci Wykonawcy, z którym zostanie zawarta umowa.

Pytanie nr 54
W odniesieniu do systemów OT i specjalistycznych (SCADA bagażowni, TETRA, siec prześwietlarek rentgenowskich, INFLOT, kontrola dostępu, CCTV): prosimy o wskazanie protokołów komunikacyjnych oraz potwierdzenie, czy dopuszczalne jest wpięcie pasywnej sondy sieciowej (SPAN/TAP) do monitoringu tych segmentów bez ingerencji w prace systemów.
Odpowiedź nr 54
Zamawiający dopuszcza wpięcie pasywnych sond sieciowych do systemów OT.

Pytanie nr 55
Prosimy o wskazanie ewentualnych ograniczeń monitoringu OT wynikających z gwarancji lub umów serwisowych dostawców OEM (czy wpięcie sondy nie narusza warunków serwisu).
Odpowiedź nr 55
Zamawiający wyjaśnia, że wpięcie sond nie narusza warunków serwisu.

Pytanie nr 56
Prosimy o potwierdzenie, czy w zakresie OT oczekiwana jest wyłącznie detekcja anomalii sieciowych, czy również analiza stanu procesowego (deep packet inspection protokołów przemysłowych).
Odpowiedź nr 56
W zakresie OT Zamawiający wymaga wyłącznie detekcji anomalii sieciowych.

Pytanie nr 57
W odniesieniu do zarzadzania podatnościami: prosimy o wskazanie, czy Zamawiający posiada skaner podatności (np. Qualys, Nessus/Tenable), oraz liczby zasobów (IP/hostow) objętych skanowaniem.

Odpowiedź nr 57
Zamawiający nie posiada skanera podatności.

Pytanie nr 58
W odniesieniu do ASM (sekcja 9) oraz Threat Intelligence: prosimy o wskazanie zakresu (liczba domen, zakresów IP, marek do monitorowania ekspozycji zewnętrznej) oraz czy dopuszczalne jest wykorzystanie rozwiązań/platform podmiotów trzecich.
Odpowiedź nr 58
Zgodnie z odpowiedzią na pytanie nr 9 udzieloną pismem GTL/DZM/2122/2026 z dn. 30.10.2026r.
Usługą Attack Surface Management, objętych jest w szczególności:

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

W przypadku wykorzystania rozwiązań/platform podmiotów trzecich Wykonawca zobowiązany jest do korzystania jedynie rozwiązań zgłoszonych podwykonawców.

Pytanie nr 59
W odniesieniu do pkt 24 OPZ (audyt na prośbę Zamawiającego, nie częściej niż co 3 miesiące): prosimy o wskazanie maksymalnej liczby audytów w skali roku przyjmowanej do wyceny oraz zakładanego zakresu pojedynczego audytu.
Odpowiedź nr 59
Zamawiajacy wyjaśnia, że pytanie dotyczy treści załacznika nr 2.1 SWZ – Szczegółowy Opis Przedmiotu Zamówienia, pkt 24, zgodnie z którym: *„Wykonawca na prośbę Zamawiającego (nielimitowana ilość razy, ale nie częściej niż co 3msc) przeprowadzi kolejny Audyt i wyda zalecenia"*
Mając na uwadze powyższe maksymalna liczna audytów w ciągu roku nie przekroczy 4 audytów.

Pytanie nr 60
Prosimy o wskazanie obecnie używanych narzędzi bezpieczeństwa i zarzadzania (SIEM, SOAR, NDR, EDR/XDR, skanery podatności, systemy ticketowe, ASM) wraz z producentem, wersja i zakresem dostępnych integracji API - w celu zaprojektowania integracji z usługa SOC.
Odpowiedź nr 60
Zamawiajacy posiada narzędzia bezpieczeństwa i zarządzania (SIEM i EDR). Szczegółowe informacje Zamawiający udostępni Wykonawcy, z którym zostanie zawarta umowa.

Pytanie nr 61
Dot. Rozdz. XIII pkt 1.4.2. lit. G SWZ.
Wnosimy o zmianę SWZ poprzez wykreślenie wymagania dysponowania przez Wykonawcę co najmniej dwoma osobami posiadającymi status biegłego sądowego z zakresu informatyki (specjalizacja: cyberbezpieczeństwo, analizy powłamaniowe, zabezpieczanie materiału dowodowego), w tym wymagania posiadania tego statusu przez co najmniej dwie kadencje, oraz o odpowiednie dostosowanie pozostałych dokumentów zamówienia, w szczególności § 3 ust. 8 wzoru umowy i wymagań dotyczących wykazu osób.

Zakwestionowany warunek wykracza poza minimalny poziom zdolności niezbędny do należytego wykonania zamówienia i ogranicza konkurencję w stopniu nieuzasadnionym zakresem powierzanych czynności. Wymaga zatem zmiany w świetle art. 16 pkt 1 i 3 w związku z art. 112 ust. 1 oraz art. 116 ust. 1 ustawy Prawo zamówień publicznych. Uprawnienie Zamawiającego do określenia wymagań dotyczących personelu nie oznacza bowiem dowolności ich kształtowania - wymagania te powinny odpowiadać rzeczywistym potrzebom realizacyjnym i pozostawać proporcjonalne do przedmiotu zamówienia.

Niezależnie od wymogu dotyczącego biegłych sądowych, Zamawiający wymaga już bowiem od Wykonawcy dysponowania personelem posiadającym specjalistyczne kompetencje z zakresu cyberbezpieczeństwa, analiz śledczych, reagowania na incydenty oraz zabezpieczania materiału dowodowego. Co istotne, zgodnie z § 3 ust. 12–14 wzoru umowy Wykonawca ma utworzyć co najmniej czteroosobowy zespół reagowania na incydenty (IRT), zdolny do podjęcia działań we wskazanym miejscu w terminie nie dłuższym niż 24 godziny od zgłoszenia incydentu, z zachowaniem integralności i ciągłości materiału dowodowego. Co najmniej jedna osoba w tym zespole musi posiadać aktualny certyfikat potwierdzający kompetencje w zakresie informatyki śledczej, analizy śledczej urządzeń cyfrowych lub reagowania na incydenty bezpieczeństwa. Ochronie interesów Zamawiającego służą zatem już konkretne wymagania dotyczące składu, gotowości operacyjnej i kompetencji zespołu.

Z kolei pkt 13 OPZ obejmuje m.in. zabezpieczanie materiału dowodowego, obrazów dysków, pamięci operacyjnej i logów, analizy powłamaniowe, przygotowanie raportu technicznego, wsparcie przy współpracy z organami ścigania oraz zachowanie łańcucha dowodowego. Są to zadania wymagające wiedzy i doświadczenia w zakresie informatyki śledczej oraz stosowania odpowiednich procedur technicznych i dokumentacyjnych. Samo ich ujęcie w przedmiocie zamówienia nie uzasadnia jednak zastrzeżenia ich wykonywania wyłącznie dla osób wpisanych na listę biegłych sądowych.

Nie kwestionujemy, że ustanowienie biegłym sądowym wiąże się z oceną posiadania wiadomości specjalnych oraz rękojmi należytego wykonywania obowiązków. **Status ten nie stanowi jednak odrębnego uprawnienia zawodowego, zastrzegającego wykonywanie objętych zamówieniem analiz technicznych i zabezpieczanie śladów cyfrowych wyłącznie dla osób wpisanych na listę biegłych**. **Sam wpis nie przesądza również o posiadaniu kompetencji wyższych lub bardziej adekwatnych do przedmiotu zamówienia niż kompetencje specjalisty, który nie ubiegał się o taki wpis, lecz posiada udokumentowane doświadczenie i odpowiednie kwalifikacje w zakresie informatyki śledczej i reagowania na incydenty (DFIR).**

Należy również odróżnić wykonywanie ekspertyz technicznych na podstawie umowy od pełnienia funkcji biegłego w konkretnym postępowaniu. Sam fakt sporządzenia ekspertyzy przez osobę wpisaną na listę biegłych sądowych nie nadaje jej automatycznie charakteru opinii biegłego powołanego przez właściwy organ procesowy. Ponadto art. 195 Kodeksu postępowania karnego dopuszcza pełnienie czynności biegłego również przez osobę niewpisaną na listę biegłych sądowych, o której wiadomo, że ma odpowiednią wiedzę w danej dziedzinie. Wpis na listę nie jest zatem bezwzględnym warunkiem nawet procesowego wykorzystania wiadomości specjalnych danej osoby.

Osoby wskazane przez Wykonawcę do realizacji zamówienia będą wykonywały czynności w ramach stosunku prawnego łączącego je z Wykonawcą, na potrzeby realizacji umowy z Zamawiającym. Nie uzyskają z tego tytułu statusu biegłego powołanego w konkretnym postępowaniu. Sporządzane przez nie raporty i ekspertyzy techniczne oraz zabezpieczone materiały mogą służyć współpracy z organami ścigania, jednak ich ocena i sposób wykorzystania w postępowaniu zależą od organu procesowego, a nie wyłącznie od posiadania przez autora wpisu na listę biegłych sądowych. Funkcję eksperta technicznego mogą wykonywać również osoby

nieposiadające statusu biegłego sądowego, lecz posiadające odpowiednie kompetencje i doświadczenie w zakresie informatyki śledczej.
W konsekwencji nie jest uzasadnione uzależnianie dostępu do zamówienia od dysponowania dwiema osobami posiadającymi status biegłego sądowego, jeżeli wymagany poziom jakości usług zapewnia dysponowanie pozostałymi osobami składającymi się na zespół Wykonawcy. Wykonawca nie wnosi o obniżenie standardów zabezpieczania materiału dowodowego ani rezygnację z wymaganych kompetencji, lecz o umożliwienie ich wykazania także przez specjalistów nieposiadających statusu biegłego.
W związku z powyższym wnosimy o wykreślenie zakwestionowanego wymagania, **a ewentualnie** w razie nieuwzględnienia wniosku głównego o dopuszczenie, zamiast wymaganych biegłych sądowych, osób posiadających udokumentowane doświadczenie w prowadzeniu analiz śledczych oraz certyfikaty potwierdzające kompetencje adekwatne do powierzanych czynności z zakresu Digital Forensics, Mobile Forensics lub Incident Response, bez wymogu wpisu na listę biegłych sądowych. Wnosimy również o odpowiednie dostosowanie pozostałych dokumentów zamówienia do przyjętej zmiany.
W przypadku nieuwzględnienia powyższych wniosków prosimy o wskazanie konkretnych czynności objętych zamówieniem oraz okoliczności faktycznych lub podstaw prawnych, które w ocenie Zamawiającego uzasadniają łącznie: wymaganie wpisu na listę biegłych sądowych, wymaganie co najmniej dwóch kadencji oraz konieczność dysponowania co najmniej dwiema takimi osobami. Prosimy również o wyjaśnienie, dlaczego realizacji tych czynności na wymaganym poziomie jakości nie zapewni personel posiadający adekwatne, udokumentowane kompetencje i doświadczenie, lecz niespełniający wskazanych wymagań dotyczących statusu biegłego.

Odpowiedź nr 61

Zamawiający nie wyraża zgody na proponowane zmiany.
Zgodnie z odpowiedzią na pytanie nr 13 udzieloną pismem GTL/DZM/2122/2026 z dn. 30.10.2026r., 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.

PROKURENT
Paweł Wojda

WICEPREZES ZARZĄDU
Norbert Henzel