**Dotyczy postępowania: Dostawa usługi Security Operations Center (SOC) dla potrzeb „MCZ” S.A.**

**Opis Przedmiotu Zamówienia**

**Wykonawca: ……………………………………………**

**(nazwa, adres, NIP)**

\* - odpowiedź NIE w przypadku parametrów wymaganych może spowodować podstawę do odrzucenia oferty

| **L.p.** | **Wymagane parametry** | **Parametr wymagany** | **Parametr oceniany** | **Potwierdzenie spełnienia parametru wymaganego / opis oferowanego rozwiązania\*** |
| --- | --- | --- | --- | --- |
|  | **Przedmiot zamówienia** |  |  |  |
|  | Świadczenie usługi SOC (Security Operations Center), polegającej na monitorowaniu, analizowaniu i reagowaniu na incydenty związane z cyberbezpieczeństwem w modelu usługowym (dostawca usługi zapewnia po swojej stronie wymaganą infrastrukturę, oprogramowanie i niezbędne zasoby) wraz z wdrożeniem, uruchomieniem i utrzymaniem systemu klasy SIEM (Security Information and Event Management), zgodnie z poniższymi wymaganiami: | | | |
|  | **Wymagania formalne dotyczące wykonywanej usługi:** |  |  |  |
|  | Posiadanie przez Wykonawcę certyfikatu na zgodność działań z normą ISO 27001, ISO 22301 wdrożone w obszarze kompetencyjnym usługi SOC **lub równoważne[[1]](#footnote-1)**  **Posiadane certyfikaty należy dołączyć do oferty** | Tak, podać | Bez oceny |  |
|  | Wykonywanie usługi SOC, stanowiącej przedmiot postepowania zgodnie z wymaganiami Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa w zakresie wsparcia Operatorów Usług Kluczowych, rozporządzeniem Ministra Cyfryzacji z dnia 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo; | Tak, podać | Bez oceny |  |
|  | Podejmowanie działań i procesów operacyjnych zgodnie z wymogami norm PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301 | Tak, podać | Bez oceny |  |
|  | ***Wymagania formalne dotyczące wykonywanej usługi wynikające z 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:*** | | | |
|  | Wykonawca musi posiadać, utrzymywać i aktualizować system zarządzania bezpieczeństwem informacji spełniającym wymagania Polskiej Normy PN-EN ISO/IEC 27001, 22301 lub równoważne w zakresie obejmującym co najmniej świadczone usługi; | Tak, podać | Bez oceny |  |
|  | Wykonawca musi zapewnić ciągłość działania usługi obsługi incydentu oraz wsparcia operatora usługi kluczowej z czasem reakcji adekwatnym do charakteru usługi kluczowej; | Tak, podać | Bez oceny |  |
|  | Wykonawca musi przez cały okres obowiązywania umowy z Zamawiającym dysponować personelem posiadający umiejętności, o których mowa w par. 1 ust. 1 pkt 4 rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, przy czym Zamawiający uzna za spełnienie tego obszaru jeśli Wykonawca dysponuje minimum:   1. SOC Team Leader – min 1 osoba 2. Analitycy SOC – min 6 osób 3. Zespół audytowy oraz pentesterski – min 5 osób 4. Inżynierowie Systemowi odpowiedzialni za produkty EDR/XDR, NGFW/UTM, DLP – min 5 osób 5. Zespół Incident Response – min 3 osoby 6. Project Manager – min 2 osoby   **Należy wymienić zespół osób oraz dołączyć do oferty ww. certyfikaty/dokumenty/uprawnienia.** | Tak, podać | Bez oceny |  |
|  | Wykonawca musi posiadać możliwość wykonywania identyfikacji zagrożeń w odniesieniu do systemów informacyjnych Zamawiającego w oparciu o logi udostępnione przez Zamawiającego z systemów:  EDR  NGFW/UTM  DLP  Active Directory | Tak, podać | Bez oceny |  |
|  | Wykonawca musi posiadać możliwość wykonywania wykrywania przełamania lub ominięcia zabezpieczeń systemu informacyjnego Zamawiającego, prowadzenia analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego operatora usługi kluczowej; | Tak, podać | Bez oceny |  |
|  | Wykonawca musi posiadać możliwość wykonywania zabezpieczania informacji potrzebnych do analizy powłamaniowej, pozwalających na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej, w tym informacji dotyczących: rodzajów usług kluczowych, na które incydent miał wpływ, liczby użytkowników usługi kluczowej, na których incydent miał wpływ, momentu wystąpienia i wykrycia incydentu oraz czas jego trwania, zasięgu geograficznego obszaru, którego dotyczy incydent poważny, wpływu incydentu na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych, przyczyny zaistnienia incydentu i sposobu jego przebiegu oraz skutków jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe na potrzeby postępowań prowadzonych przez organy ścigania; | Tak, podać | Bez oceny |  |
|  | Wykonawca musi dysponować prawem do wyłącznego korzystania z pomieszczenia lub zespołu pomieszczeń, w których będzie realizowana usługa SOC, a pomieszczenia te muszą posiadać odpowiedni poziom zabezpieczeń fizycznych zgodny z w/w rozporządzeniem (**należy załączyć do oferty certyfikaty, potwierdzenie spełnienia ww. warunku**). | Tak, podać | Bez oceny |  |
|  | Wykonawca musi dysponować redundantnymi środkami łączności umożliwiającymi prawidłową i bezpieczną wymianę informacji z podmiotami, dla których świadczą usługi SOC oraz właściwym CSiRT. | Tak, podać | Bez oceny |  |
|  | Wykonawca dostosuje system do wymogów prawnych stawianych przez NIS2. | Tak, podać | Bez oceny |  |
| **III.** | **Zakres usługi:** |  |  |  |
|  | Monitorowanie bezpieczeństwa wraz z identyfikacją niebezpiecznych zdarzeń w ramach SOC w trybie ciągłym: 24/7/365 zbierając logi z 4 systemów: EDR, NGFW, DLP oraz Active Directory w zakresie scenariuszy:   1. Monitorowania stacji roboczych oraz serwerów, urządzeń sieciowych w tym urządzeń brzegowych, systemów/aplikacji serwerowych, w tym systemów informacji medycznej, kontrolerów domeny, 2. Powiadamiania o zagrożeniach ze stacji roboczych oraz serwerów, w szczególności generowane z narzędzi ochrony, 3. Powiadamiania o dezaktywacji narzędzi bezpieczeństwa na danym hoście, 4. Powiadamiania z modułów ochrony / bezpieczeństwa urządzeń brzegowych oraz wewnętrznych urządzeń sieciowych, 5. Zdarzeń dotyczących nieudanych, wielokrotnych prób logowania dla wszystkich monitorowanych aktywów 6. Kluczowych zdarzeń (np. utworzenie konta, zmiana hasła, usunięcie konta, zmiana grupy) związanych z kontami uprzywilejowanymi dla wszystkich monitorowanych aktywów, 7. Zdarzeń sieciowych oraz systemowych (np. enumeracja, skanowanie portów i adresacji) mogących świadczyć o rekonesansie infrastruktury, 8. Zdarzeń związanych z modyfikacją mechanizmów harmonogramu w systemach operacyjnych, 9. Zdarzeń związanych z modyfikacją audytu zdarzeń / dzienników systemowych, 10. Zdarzeń dotyczących integralności plików, w szczególności zasobów sieciowych mogących świadczyć o zainfekowaniu oprogramowaniem złośliwym 11. Zdarzeń związanych z logowaniem zdalnym. | Tak, podać | Bez oceny |  |
|  | Uruchomienie środowiska SIEM (Security Information and Event Management)  **(należy podać: nazwę, typ oprogramowania, producent, kraj)** | Tak, podać | Bez oceny |  |
|  | Comiesieczne raporty wraz z dostępem do Portalu Klienta oraz realizacja cyklicznych tj. comiesięcznych spotkań podsumowujących | Tak, podać | Bez oceny |  |
|  | Uruchomienie usługi Drugiej Linii Wsparcia, minimum w zakresie:   1. Analizy zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowania raportów i zaleceń poincydentalnych 2. Realizacji Scenariuszy Reakcji zgodnie z wymaganiami. 3. Przygotowania miesięcznych raportów z realizacji prac. 4. Oczekiwanej dostępności usługi Drugiej Linii Wsparcia - 8 godzin dziennie, 5 dni w tygodniu | Tak, podać | Bez oceny |  |
|  | Środowisko, na którym realizowana jest usługa SOC oraz SIEM będzie uruchomione na dedykowanym środowisku wysokiej dostępności HA będących w infrastrukturze Wykonawcy, której Wykonawca jest właścicielem. Zamawiający nie wyraża zgody na przesyłanie danych do zewnętrznych Data Center w tym do chmur obliczeniowych będących poza kontrolą Wykonawcy. | Tak, podać | Bez oceny |  |
|  | Obsługa w systemie SIEM nieograniczonej ilości EPSów, bez ograniczeń dla przepustowość łączy, ilość assetów i retencje dobową logów. Ponad to SIEM musi realizować:   1. możliwość implementacji agentów do zbierania logów i komunikacji 2. integracja z rozwiązaniami firm trzecich niezależnie od typu licencjonowania 3. Reguły operate o machine learning (analiza trendów, wiele indeksów) 4. Możliwość instalacji i konfiguracji agenta anty-malware na środowisku Windows oraz Linux 5. Reindeksacja bez zatrzymywania procesu zbierania logów 6. Możliwość tworzenia pluginów m.in. do geolokalizacji IP oraz niestandardowe wizualizacje dashboardów | Tak, podać | Bez oceny |  |
|  | Ilość źródeł logów: min 650, w tym serwery Windows, serwery Linux (różne dystrybucje) oraz urządzenia sieciowe, EDR, system klasy DLP, dane z kontrolerów domeny | Tak, podać | Bez oceny |  |
|  | Kolektor logów musi znajdować się w infrastrukturze Zamawiającego. | Tak, podać | Bez oceny |  |
|  | Zestawienie, zabezpieczenie i obsługa połączenia w relacji Zamawiający do SOC poprzez uruchomienie łącza szyfrowanej transmisji danych w technologii VPN IP SEC | Tak, podać | Bez oceny |  |
|  | Realizowanie zadań - w szczególności:   1. reagowanie na podejrzenia i obsługa zidentyfikowanych incydentów w oparciu o wdrożony system klasy EDR zgodnie z wyznaczonymi scenariuszami reakcji min. odseparowanie hosta od sieci i/lub zakończenie działania procesu odpowiedzialnego za incydent 2. analiza incydentów i ich klasyfikowanie, 3. zarządzanie incydentami, 4. raportowanie incydentów, w tym przekazywania minimum raz w miesiącu raportów zbiorczych wykrytych incydentów / zdarzeń lub informacji o ich braku, 5. przygotowywanie dziennych raportów wykrytych zdarzeń bezpieczeństwa. 6. opracowanie i obsługa scenariuszy monitorowania i reagowania, 7. wsparcie Zamawiającego w raportowaniu incydentów poważnych w rozumieniu ustawy o Krajowym Systemie Bezpieczeństwa do CSIRT NASK do 24h, 8. tworzenie rekomendacji bezpieczeństwa na podstawie incydentów bezpieczeństwa – dotyczących działań związanych z powstrzymaniem incydentu oraz zalecanych środkach naprawczych. 9. Przeprowadzenie analizy bezpieczeństwa infrastruktury Zamawiającego w zakresie:  * przeprowadzanie testów bezpieczeństwa, obejmujących skanowanie podatności testowanego środowiska, przeprowadzone zgodnie z założeniem, że zespół testujący, przystępując do realizacji testów ma wiedzę o przedmiocie testów na poziomie analogicznym jak inni jej użytkownicy. Raport z testów musi wyszczególniać zakres przeprowadzonych testów oraz wszystkie wyniki ze szczególnym uwzględnieniem potencjalnych skutków wpływu zmaterializowania się zagrożenia, wskazanie środków które wpłyną na poprawę stanu zabezpieczenia systemu oraz szczegóły techniczne wykrytych podatności wraz z określeniem poziomu ich istotności (należy przedstawić harmonogram min. 1 raz w roku). * wykonywanie analizy procesów kluczowych i krytycznych dla Zamawiającego w oparciu o przyjęte standardy z Załącznika A normy ISO 27001 * przekazanie raportu z wykonanych prac wraz ze spotkaniem warsztatowym celem omówienia całości | Tak, podać | Bez oceny |  |
|  | **SLA** |  |  |  |
|  | Czas notyfikacji (powiadomienia o zdarzeniu) – do ……..godz. od wystąpienia incydentu. (**min. 1 godz. – max. 2 godz.** - należy podać oferowany czas), | Tak, podać | Oceniany |  |
|  | Czas reakcji na incydent krytyczny - do …….. godz. (**min. 1 godz. – max. 4 godz.** - należy podać oferowany czas) | Tak, podać | Oceniany |  |
|  | Czas reakcji na incydent niekrytyczny - do …….. godz. (**min. 1 godz. – max. 8 godz.** - należy podać oferowany czas) | Tak, podać | Oceniany |  |
|  | Klasyfikacja (poziomy) incydentów uzgadniane będą w ramach wdrożenia i opracowywania scenariuszy monitorowania i reagowania, | Tak, podać | Bez oceny |  |
|  | Kanały komunikacji obejmujące notyfikację: e-mail i kontakt telefoniczny (należy podać) | Tak, podać | Bez oceny |  |
|  | Składowanie logów i dostęp w ramach zasobów dostawcy usługi, zlokalizowane w Polsce, w trybie wysokiej dostępności HA. Okres przechowania – minimum 2 miesiące, | Tak, podać | Bez oceny |  |
|  | Przedstawienie analizy przedwdrożeniowej i harmonogramu realizacji, | Tak, podać | Bez oceny |  |
|  | Wdrożenie, uruchomienie i przekazanie systemu do eksploatacji, uruchomienie usługi | Tak, podać | Bez oceny |  |
|  | Zapewnienie wsparcia grupy projektowej i dedykowanego kierownika projektu **(należy wskazać oraz załączyć uprawnienia/certyfikaty)** | Tak, podać | Bez oceny |  |
|  | Wykonawca przeznaczy pulę 30 godzin rocznie na następujące zagadnienia:  Konsultacje pentesterskie  Konsultacje z zespołem audytorów pod kątem ISO 27001 oraz ISO 22301  Konsultacje inżynierskie w zakresie wdrożonych Systemów  Wsparcie w konfiguracji, tuningu reguł oraz aktualizacji i prac serwisowych dla systemów EDR, DLP oraz NGFW w okresie trwania usługi | Tak, podać | Bez oceny |  |
|  | Zespół Wykonawcy musi posiadać wszystkie aktualne certyfikaty z poniższej listy lub inne równoważne, zgodne co do zakresu z programem certyfikacji:   * CompTIA Network+ * CompTIA Security+ * EC - Fudamentals of Networking Concepts, Protocols, and Security * EC - Planning and Implementing a Security Incident Response * EC - Practical Cyber Threat Intelligence * EC - Project Management for Cybersecurity Professionals * CEH (certified ethical hacker) * OSCP (offensive security certified professional) * eWPT (web application penetration tester) * eWPTX (web application penetration tester eXtreme) * ISO 9001:2015 (Audytor Wiodący) * ISO 27001:2022 (Audytor Wiodący) * CISA (Certified Information Systems Auditor)   **Należy załączyć do oferty.** | Tak, podać | Bez oceny |  |
|  | W ramach analizy przedwdrożeniowej dostawca usługi przeprowadzi analizę źródeł logów oraz określi sposób ich parsowania w SIEM, przeprowadzi analizę potrzebnych i dostępnych informacji do utworzenia reguł bezpieczeństwa dla systemu SIEM, określi wykonalności scenariuszy na podstawie dostępnych danych oraz analizę potencjalnych dodatkowych scenariuszy, wstępnie określi sposób reagowania na poszczególne podejrzenia incydentów. | Tak, podać | Bez oceny |  |
|  | W ramach podłączenia źródeł logów dostawca usługi uruchomi przesyłanie logów do SIEM, przygotuje sposób podłączania źródeł i przekaże go do Zamawiającego w celu realizacji pozostałych zasobów z tego samego typu. | Tak, podać | Bez oceny |  |
|  | Dostawca usługi przeprowadzi wstępne strojenie i implementację reguł bezpieczeństwa, a rezultatem tych prac będzie działające parsowanie logów oraz zaimplementowane uzgodnione reguły. Dostawca usługi przeprowadzi strojenie systemu SIEM w celu zmniejszenia ilości fałszywych alarmów. | Tak, podać | Bez oceny |  |
| **IV.** | **Termin realizacji i warunki:** |  |  |  |
|  | Czynności niezbędne do uruchomienia usługi Wykonawca wykona do dnia 05.03.2026r. od daty zawarcia umowy. | Tak, podać | Bez oceny |  |
|  | Usługa będzie wykonywana w terminie od 05.03.2026r. do 30.06.2029r. | Tak, podać | Bez oceny |  |

**Treść oświadczenia Wykonawcy:**

Oświadczamy, że przedstawione powyżej dane są prawdziwe oraz zobowiązujemy się do realizacji usługi zgodnie z wyspecyfikowanymi parametrami.

...........................................................................................

Podpis Wykonawcy lub osoby uprawnionej do reprezentowania Wykonawcy

należy opatrzyć kwalifikowanym podpisem elektronicznym

1. Przez certyfikat równoważny Zamawiający rozumie certyfikat, który jest analogiczny co do zakresu z przykładowymi certyfikatami wskazanymi z nazwy dla danej roli, co jest rozumiane jako:

   a) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat,

   b) analogiczny stopień poziomu kompetencji,

   c) analogiczny poziom doświadczenia zawodowego wymaganego do otrzymania danego certyfikatu. [↑](#footnote-ref-1)