ZAŁĄCZNIK NR 2

# Oświadczenie potwierdzające opis przedmiotu zamówienia.

**Opis wymagań w zakresie realizacji usługi SOC.**

W ramach świadczonych usług Dostawca usługo zapewni

1) Świadczenie usługi SOC w modelu chmurowym ( SOC as a Service ) bez konieczności instalowania dodatkowych urządzeń w infrastrukturze Zamawiającego.
2) Świadczenie usługi SOC z dostępnością zespołu SOC 24/7/365 oraz możliwością sprawdzenia dostępności zespołu SOC w w/w modelu poprzez dokonanie wizytacji w siedzibie SOC przez Zamawiającego bez konieczności wcześniejszego umówienia takiej wizytacji
3) Przeprowadzenie dla wskazanych przez Zamawiającego osób szkolenia w zakresie architektury i obsługi systemów SOC w modelu chmurowym ( SOC as a Service )

4) Przyjmowanie i rejestracja zgłoszeń związanych z incydentami lub podejrzeniami incydentów cyberbezpieczeństwa. Zgłoszenia mogą być dokonywane przez osoby wskazane przez zamawiającego za pośrednictwem ustalonych kanałów komunikacji (e-mail, telefon, komunikator internetowy, interfejs systemu obsługi zgłoszeń). Przyjmowanie zgłoszeń musi być realizowane przez personel dysponujący wiedzą i doświadczeniem w zakresie analizy incydentów cyberbezpieczeństwa.
5) Możliwość dokonywania zgłoszeń na portalu wykonawcy o zgłoszeniach. Rejestr zgłoszeń, wraz ze wszystkimi szczegółami dotyczącymi zgłoszeń będzie przechowywany przez cały okres trwania umowy.
6) Stały monitoring alertów i zdarzeń, o priorytecie wskazanym przez zamawiającego (ograniczenie dziennej liczby alertów) / o ustalonym priorytecie (jeśli nie ma ograniczania alertów), występujących w ustalonych systemach bezpieczeństwa.
7) Prowadzenie rejestru obejmującego szczegółowe informacje o alertach ze szczególnym uwzględnieniem: czasu wystąpienia alertu, osób zaangażowanych w proces obsługi, przebiegu i wyników analizy, historii podjętych czynności i komunikacji. Informowanie o wynikach analizy zgodnie z ustalonymi ścieżkami eskalacji. Każde wystąpienie alertu musi być oznaczone unikalnym identyfikatorem wykorzystywany w dalszej komunikacji. Rejestr zdarzeń, wraz ze wszystkimi szczegółami dotyczącymi alertów będzie przechowywany przez cały okres trwania umowy. Zamawiający otrzyma dostęp do informacji o każdym zdarzeniu niezwłocznie, na każde żądanie.
8) Ustalenie szczegółów technicznych incydentów bezpieczeństwa, ich wpływu na systemy zamawiającego oraz klasyfikacja incydentów zgodnie z ustalonymi metodami klasyfikacji. Określenie metod powstrzymania incydentów bezpieczeństwa, działań naprawczych oraz działań, które powinny być podjęte w celu uniknięcia podobnych incydentów w przyszłości.
9) Informowanie zamawiającego zgodnie z ustalonymi ścieżkami eskalacji o wystąpieniu incydentu lub podejrzeniu wystąpienia incydentu z uwzględnieniem ustalonej klasyfikacji incydentów.
10) Informowanie zamawiającego na żądanie o postępach prac związanych z analizą incydentów.
11) Niezwłoczne informowanie zamawiającego zgodnie z ustalonymi ścieżkami eskalacji o ustaleniach dotyczących incydentów ważnych oraz krytycznych jeśli ustalenia te wskazują na istotny wpływ na systemy lub aktywność organizacji.
12) Współpraca z osobami wskazanymi przez zamawiającego w ramach obsługi incydentów w zakresie organizacyjnym i technicznym. W szczególności informowanie zamawiającego o rekomendacjach dotyczących działań związanych z powstrzymaniem incydentu, oraz zalecanych środkach naprawczych.

13) Podejmowanie działań związanych z reakcją na incydenty zgodnie z ustaloną autoryzacją oraz poziomem dostępu za pośrednictwem ustalonych systemów bezpieczeństwa.
14) Dla przeanalizowanego incydentu, żądanie, niezwłoczne dostarczenie raportu uwzględniającego co najmniej:
    - czas wystąpienia alertu / przyjęcia zgłoszenia.
    - Opis analizy z uwzględnieniem prowadzonych działań.
    - Rezultat analizy i klasyfikację incydentu.
    - Rekomendację specjalisty.
    - Osob przeprowadzająca alizę.
15) Raz w miesiącu wykonawca prześle zamawiającemu raport zawierający Informacje zbiorcze na temat ilości przeanalizowanych alertów, Zestawienie typów alertów i incydentów ich priorytetów
16) Posiadanie narzędzi do zabezpieczania danych takich jak: logi, zrzuty pamięci operacyjnej, obrazy dysku, związanych z incydentem na żądanie zamawiającego, w ramach reakcji na incydenty.
17) Rekomendacje zmian w konfiguracji i architekturze systemów bezpieczeństwa zamawiającego w celu podnoszenia poziomu bezpieczeństwa . Informowanie zamawiającego o rekomendacjach po wystąpieniu takich.
18) Możliwość skanowania podatności zasobów zamawiającego z wykorzystaniem automatycznych narzędzi. Informacje o podatnościach będą uwzględniane jako dodatkowy kontekst w procesach obsługi incydentów.
19) Możliwość prowadzenia ciągłego monitoringu i analizy informacji o ruchu sieciowym sieci zamawiającego.
20) Wykonawca będzie prowadził ciągły monitoring i analizę danych na podstawie logów zdarzeń ustalonych aplikacji, systemów bezpieczeństwa oraz urządzeń sieciowych.
21) W przypadku poważnych incydentów dostawca zapewni pomieszczenie umożliwiające spotkanie i wspólną pracę wydzielonego zespołu powołanego w celu reakcji na incydent.

22) Wykonawca musi umożliwić wskazanym Zamawiającemu przeprowadzenie wizyt kontrolnych w pomieszczeniu w którym wykonywane będą prace na rzecz zamawiającego.
23) Zamawiający musi dostarczyć listę członków zespołu zaangażowanego w świadczenie usługi.

**Wymagania 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***

1) Wykonawca musi posiadać, certyfikat systemu zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN-EN ISO/IEC 27001 w zakresie obejmującym co najmniej świadczone usługi;
2) Wykonawca musi zapewnić ciągłość działania potwierdzony certyfikatem ISI 22301 usłudze obsługi incydentu oraz wsparcie operatorowi usługi kluczowej z czasem reakcji adekwatnym do charakteru usługi kluczowej;
3) Wykonawca musi potwierdzić możliwość wykonywania identyfikacji zagrożeń w odniesieniu do systemów informacyjnych Zamawiającego oraz Wykonawca musi zapewnić potwierdzenie osiadania odpowiedniej kardy przeszkolonej do proponowania rozwiązań ograniczających ryzyko wynikające z tych zagrożeń
4) Wykonawca musi potwierdzić możliwość wykonywania wykrywania przełamania lub ominięcia zabezpieczeń systemu informacyjnego Zamawiającego, prowadzenia analizy po włamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego operatora usługi kluczowej,
5) Wykonawca musi potwierdzić możliwość wykonywania zabezpieczania informacji potrzebnych do analizy po włamaniowej, 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;
6) Wykonawca musi dysponować prawem do wyłącznego korzystania z pomieszczenia lub zespołu pomieszczeń – w których będzie realizowana usługa SOC
7) Wykonawca musi dysponować redundantnymi środkami łączności umożliwiającymi prawidłową i bezpieczną wymianę informacji z podmiotami, dla których świadczą usługi SOC,
8) Wykonawca musi posiadać odpowiedni poziom zabezpieczeń fizycznych potwierdzony odpowiednimi dokumentami:
a. drzwi do pomieszczenia lub zespołu pomieszczeń spełniające co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627, wyposażone w zamek spełniający co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 12209,
b. ściany i stropy pomieszczenia lub zespołu pomieszczeń, w których będą świadczone usługi z zakresu SOC, powinny mieć klasę odporności ogniowej co najmniej EI 60, określoną w Polskiej Normie PN-EN 13501, a budynek, w którym będą świadczone usługi z zakresu cyberbezpieczeństwa, powinien mieć klasę odporności pożarowej nie niższą niż klasa B, określoną w przepisach wydanych na podstawie art. 7 ust. 2 pkt 1 ustawy z dnia 7 lipca 1994 r. – Prawo budowlane (Dz. U. z 2019 r. poz. 1186, z późn. zm.2));
c. system sygnalizacji napadu i włamania spełniający co najmniej wymagania systemu stopnia 2 określone w Polskiej Normie PN-EN 50131-1, stale monitorowany przez personel bezpieczeństwa oraz wyposażony w rezerwowe źródło zasilania i obejmujący ochroną wejścia i wyjścia kontrolowanego obszaru oraz sygnalizujący co najmniej: otwarcie drzwi, okien i innych zamknięć chronionego obszaru, poruszanie się w chronionym obszarze, stan systemu, w tym generujący ostrzeżenia i alarmy;
d. system sygnalizacji pożarowej obejmujący urządzenia sygnalizacyjno-alarmowe, służące do samoczynnego wykrywania i przekazywania informacji o pożarze, a także urządzenia odbiorcze alarmów pożarowych i urządzenia odbiorcze sygnałów uszkodzeniowych, przy czym obiekty wyposażone w stałe urządzenia gaśnicze i objęte całodobowym nadzorem co najmniej jednej osoby nie muszą być wyposażone w system sygnalizacji pożarowej.