Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU SZACOWANIA

Spis treści

I. WPROWADZENIE

Przedmiotem szacowania jest realizacja kompleksowej analizy bezpieczeństwa dla Generalnej Dyrekcji Ochrony Środowiska (dalej: „GDOŚ" lub „Zamawiający"), we wskazanych lokalizacjach oraz świadczenie usługi Security Operations Center (dalej: „SOC") dla GDOŚ.

Zamówienie finansowane w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności (dalej: „KPO"), Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd.

II. OPIS PRZEDMIOTU SZACOWANIA

1. Zakres Przedmiotu szacowania

Wykonanie Przedmiotu zamówienia obejmuje:

1.1. analizę bezpieczeństwa – audyt i pentesty, obejmujące analizę kluczowych procesów, audyt compliance, przeprowadzenie testów penetracyjnych infrastruktury sieciowej oraz skanów podatności w 17 lokalizacjach wskazanych przez Zamawiającego;
1.2. integrację systemu monitorowania zdarzeń Wykonawcy (dalej: „SIEM") z kluczowymi źródłami danych Zamawiającego oraz przygotowanie do uruchomienia usługi Security Operations Center (dalej: „**SOC**");
1.3. świadczenia usługi SOC, polegającej na aktywnym monitorowaniu, detekcji i reakcji na incydenty bezpieczeństwa w GDOŚ przez okres 12 miesięcy (24 h / 365 dni).

2. Wykonanie Przedmiotu szacowania

2.1. Wykonanie Przedmiotu zamówienia obejmuje poniższe etapy:

2.1.1. **Etap 1** – analiza procesów, audyt compliance i testy penetracyjne w 17 lokalizacjach:

Lp.	Miasto	Lokalizacja
1.	Warszawa	Generalna Dyrekcja Ochrony Środowiska (Zamawiający) Al. Jerozolimskie 136 02-305 Warszawa
2.	Białystok	Regionalna Dyrekcja Ochrony Środowiska w Białymstoku ul. Dojlidy Fabryczne 23 15-554 Białystok
3.	Bydgoszcz	Regionalna Dyrekcja Ochrony Środowiska w Bydgoszczy ul. Dworcowa 81 85-009 Bydgoszcz
4.	Gdańsk	Regionalna Dyrekcja Ochrony Środowiska w Gdańsku ul. Chmielna 54/57 80-748 Gdańsk

5.	**Gorzów**	Regionalna Dyrekcja Ochrony Środowiska w Gorzowie Wielkopolskim ul. Jagiellończyka 13 66-400 Gorzów Wielkopolski
6.	**Katowice**	Regionalna Dyrekcja Ochrony Środowiska w Katowicach Plac Grunwaldzki 8-10 40-127 Katowice
7.	**Kielce**	Regionalna Dyrekcja Ochrony Środowiska w Kielcach ul. Szymanowskiego 6 25-361 Kielce
8.	**Kraków**	Regionalna Dyrekcja Ochrony Środowiska w Krakowie ul. Mogilska 25 31-542 Kraków
9.	**Lublin**	Regionalna Dyrekcja Ochrony Środowiska w Lublinie ul. Bazylianówka 46 20-144 Lublin
10.	**Łódź**	Regionalna Dyrekcja Ochrony Środowiska w Łodzi ul. Traugutta 25 90-113 Łódź
11.	**Olsztyn**	Regionalna Dyrekcja Ochrony Środowiska w Olsztynie ul. Dworcowa 60 10-437 Olsztyn
12.	**Opole**	Regionalna Dyrekcja Ochrony Środowiska w Opolu ul. Firmowa 1 45-594 Opole
13.	**Poznań**	Regionalna Dyrekcja Ochrony Środowiska w Poznaniu ul. Kościuszki 57, 61-891 Poznań
14.	**Rzeszów**	Regionalna Dyrekcja Ochrony Środowiska w Rzeszowie Al. Józefa Piłsudskiego 38 35-001 Rzeszów
15.	**Szczecin**	Regionalna Dyrekcja Ochrony Środowiska w Szczecinie ul. Juliusza Słowackiego 2 71-434 Szczecin
16.	**Warszawa**	Regionalna Dyrekcja Ochrony Środowiska w Warszawie ul. Henryka Sienkiewicza 3 00-015 Warszawa
17.	**Wrocław**	Regionalna Dyrekcja Ochrony Środowiska we Wrocławiu ul. Jana Długosza 68 51-162 Wrocław

2.1.2. **Etap 2** – integracja SIEM Wykonawcy z źródłami danych Zamawiającego (EDR, FW, AD) oraz przygotowanie do uruchomienia usługi Security Operations Center (dalej: „**SOC**”);

Etap 3 – świadczenie usługi SOC dla Zamawiającego. W ramach wdrożenia i opracowania usługi SOC.

3. Minimalne wymagania dla Etapu 1

3.1. Wykonanie audytu i testów penetracyjnych infrastruktury sieciowej, w szczególności:

3.1.1. weryfikacja topologii, sieci oraz kluczowych punktów styku z internetem,
3.1.2. skanowanie zewnętrznych adresów IP w celu wykrycia podatności a po wykryciu bezinwazyjna metoda wykorzystania podatności,
3.1.3. rekonesans sieci – które stacje widoczne są w sieci, jakie usługi na nich działają oraz jakie systemy operacyjne a także skanowanie w poszukiwaniu wszystkich podłączonych urządzeń,
3.1.4. wykrycie, czy jest dostęp z jednej podsieci do innej,
3.1.5. wykrycie podatności na hostach, skanowanie zostanie powtórzone dla wybranych przez Zamawiającego hostów (Wykonawca nie może ograniczać się do ilości),
3.1.6. skanowanie istotnych hostów jak serwery poprzez weryfikacje podatności, luk systemowych, weryfikacja złożoności haseł (próby włamania słownikowe, bruteforce, itd.),
3.1.7. weryfikacja dostępu użytkowników do odpowiednich usług,
3.1.8. weryfikacja luk bezpieczeństwa w systemach operacyjnych oraz oprogramowaniu firm trzecich,
3.1.9. sprawdzanie domyślnych haseł dla wszystkich hostów i serwerów,
3.1.10. sprawdzanie możliwości wylistowania użytkowników i zdobycia ich poświadczeń,
3.1.11. weryfikacja uzyskania dostępów do zasobów współdzielonych,
3.1.12. weryfikacja urządzeń sieciowych pod kątem podatności, prób nieuprawnionego logowania siłowego oraz skuteczności separacji w zakresie podsieci VLAN,
3.1.13. weryfikacja bezpieczeństwa monitoringu wizyjnego,
3.1.14. testy sieci bezprzewodowej pod kątem dostępu i zabezpieczeń z możliwością przechwycenia haseł a w przypadku przechwycenia weryfikacja pod kątem złamania hasła,

3.2. Po zakończeniu audytu i testów penetracyjnych w każdej z 17 lokalizacji, Wykonawca przekaże Zamawiającemu szczegółowy raport końcowy (dalej: „raport"). **Ze względu na poufność zawartych informacji, wszelka dokumentacja musi zostać przekazana w formie zabezpieczonej (np. w formie zaszyfrowanych plików lub kontenerów danych), do których hasła zostaną przekazane kanałem alternatywnym (np. za pośrednictwem wiadomości SMS na wskazany numer telefonu osoby upoważnionej po stronie Zamawiającego).**

3.3. Raport będzie zgodny z poniższymi wymaganiami:

3.3.1. raport będzie zgodny z uznanymi standardami branżowymi (np. CVSS, OSSTMM, OWASP),
3.3.2. raport będzie zawierał szczegółowy wykaz wszystkich elementów infrastruktury IT poddanych audytowi i testom penetracyjnym;
3.3.3. raport będzie posiadał wyszczególnienie i klasyfikacje wszystkich zidentyfikowanych podatności, z podziałem na kategorie ryzyka: wysokie, średnie i niskie, stosując ogólnie przyjęte metody oceny ryzyka, np. system CVSS (Common Vulnerability Scoring System) lub równoważny;

3.3.4. raport będzie zawierał przedstawienie szczegółowych zaleceń, rekomendacji naprawczych oraz odniesienie do dobrych praktyk dla każdej wykrytej podatności – każde zalecenie powinno wskazywać priorytet oraz sugerowany sposób wdrożenia poprawek;

3.3.5. raport będzie zawierał podsumowanie prezentujące ogólny poziom bezpieczeństwa środowiska IT Zamawiającego oraz podmiotów we wskazanych lokalizacjach – obejmujące liczbę, typy oraz poziom ryzyka wykrytych podatności, wraz z oceną punktową poziomu bezpieczeństwa (np. wg skali CVSS lub innej zatwierdzonej przez Zamawiającego) .

3.4. Wykonawca jest zobowiązany do zorganizowania i przeprowadzenia, w terminie nie później niż 5 dni roboczych od dnia przekazania Zamawiającemu raportu, zdalnego spotkania warsztatowego (online) służącego szczegółowemu omówieniu wyników przeprowadzonych prac.

3.5. W warsztacie muszą brać udział audytorzy bezpośrednio zaangażowani w realizację danego audytu oraz przedstawiciele Zamawiającego odpowiedzialni za bezpieczeństwo teleinformatyczne.

3.6. Celem warsztatu jest szczegółowe wyjaśnienie wykrytych podatności, sposobów klasyfikacji ich ryzyka, omówienie rekomendacji naprawczych oraz odpowiedzi na pytania i wątpliwości Zamawiającego dotyczące raportu.

4. Minimalne wymagania dla Etapu 2

4.1. Wykonawca dokona konfiguracji i integracji platformy klasy SIEM z źródłami danych Zamawiającego (EDR, FW, AD). Prace obejmują realizację dedykowanych parserów, reguł korelacyjnych oraz wyznaczenie scenariuszy detekcji i reakcji. Wykonawca odpowiada za utrzymanie środowiska SIEM przez cały okres świadczenia usługi SOC, w tym za bieżącą aktualizację systemu oraz eliminację zdarzeń typu false positive.

4.2. Etap 2 musi być realizowany równolegle z Etapem 1.

4.3. System klasy SIEM Wykonawcy musi posiadać następujące funkcje:

4.3.1. środowisko SIEM i konsola centralna, skonfigurowane i zarządzane w pełni przez Wykonawcę na jego serwerach. Zamawiający nie udostępnia swoich zasobów i nie mogą być one wymagane do działania systemu SIEM Wykonawcy;

4.3.2. możliwość implementacji agenta monitorującego zasoby pod kątem optymalizacji, agent służy do komunikacji ze środowiskiem SIEM i gromadzenia logów w formie buforu, na wypadek zerwania połączenia pomiędzy Zamawiającym a Wykonawcą;

4.3.3. musi umożliwić dodawanie kolejnych źródeł logów bez dokupywania lub dodawania kolejnych licencji. Koszty licencji muszą być stałe, wliczone w cenę usługi SOC i nie mogą zależeć od ilości danych;

4.3.4. musi umożliwiać integrację z rozwiązaniami firm trzecich i nie może być zależne od ich typu licencji;

4.3.5. musi posiadać możliwość tworzenia reguł bezpieczeństwa w oparciu o machine learning, badając trendy w oparciu o wiele indeksów;

4.3.6. powinno zapewniać instalację i konfigurację agenta do monitorowania endpointów pod kątem malware. Agent powinien działać na środowisku Windows i Linux;

4.3.7. musi mieć możliwość reindeksowania (kopiowania danych z jednego indeksu do drugiego) bez konieczności zatrzymania procesu przesyłania logów;

4.3.8. musi zapewnić możliwość budowania własnych pluginów w oparciu o JavaScript służący do weryfikacji lokalizacji adresu IP ale także nowych zupełnie indywidualnych (z poza już dostępnych do wyboru) form wizualizacji zdarzeń w dashboard.

4.4. Wykonawca w celu realizacji zamówienia i zbierania logów musi dostarczyć rozwiązanie klasy SIEM w formie usługi. Wszelkie licencje będą po stronie Wykonawcy.

4.5. Wykonawca wykona prace przygotowawcze do uruchomieni usługi SOC, w tym:

4.5.1. zapewni pełną infrastrukturę do obsługi systemu klasy SIEM, wraz z wdrożeniem wszystkich niezbędnych parserów, przygotowanie reguł korelacji oraz obsługę incydentów a także udostępnienie niezbędnych dashboardów (tablic wizualizujących dane) Zamawiającemu;

4.5.2. przeprowadzi analizę przedwdrożeniową, obejmującą:

- audyt kluczowych procesów bezpieczeństwa IT (w oparciu o normę PN-ISO/IEC 27001 oraz dobre praktyki rynkowe),
- testy penetracyjne infrastruktury sieciowej, realizowane zgodnie z uznaną metodyką, np. OSSTMM lub równoważną.

4.6. Zamawiający dopuszcza realizację prac, o których mowa w pkt 4.5.2. w formie zdalnej, o ile specyfika danej czynności na to pozwala i nie wpłynie to negatywnie na jakość oraz rzetelność przeprowadzanych analiz. W przypadku realizacji prac w trybie zdalnym, Wykonawca jest zobowiązany do zachowania najwyższych standardów bezpieczeństwa oraz korzystania wyłącznie z bezpiecznych i szyfrowanych kanałów komunikacji uzgodnionych z Zamawiającym.

4.7. Zamawiający wskazuje jako źródła dla logów następujące systemy:

4.7.1. ESET Inspect – zakres logów: system klasy EDR/XDR;

4.7.2. Stormshield – zakres logów: Firewall, IPS/IDS oraz VPN;

4.7.3. Domena Active Directory – zakres logów min.: dodania, usunięcie i modyfikacja.

4.8. Wykonawca zapewni możliwość rozbudowy i dodawania kolejnych źródeł logów w trakcie trwania usługi bez dodatkowych kosztów po stronie Zamawiającego – maksymalnie 3 dodatkowe źródła w ciągu trwania usługi. SOC nie może być zależna od ilości pracowników, sprzętu czy wielkości infrastruktury Zamawiającego. W trakcie trwania usługi SOC Zamawiający dopuszcza możliwość rozbudowy swojej infrastruktury i użytkowników, co nie spowoduje zwiększenia kosztów po jego stronie.

4.9. Logi zebrane ze wskazanych przez Zamawiającego źródeł będą, począwszy od dnia uruchomienia Etapu 3 Umowy, przechowywane przez Wykonawcę w formie zaszyfrowanej, przez okres 3 miesięcy w sposób ciągły, co oznacza, że każdego dnia przechowywany jest zakres danych obejmujący ostatnie 3 miesiące, a okres przechowywania ulega przesunięciu o każdy kolejny dzień. Ponadto, raz w miesiącu w trakcie trwania SOC, Wykonawca zobowiązany jest do przekazywania Zamawiającemu kompletu zebranych logów w bezpiecznej, zaszyfrowanej formie w celu ich archiwizacji w zasobach Zamawiającego. Sposób bezpiecznego przekazania danych (np. szyfrowany nośnik danych lub dedykowany, bezpieczny kanał transmisyjny) zostanie każdorazowo uzgodniony z Zamawiającym, przy czym hasła do zaszyfrowanych danych muszą być przekazywane kanałem alternatywnym.

4.10. Wykonawca zapewni składowanie logów w dwóch fizycznie oddzielonych lokalizacjach. W każdej lokalizacji Wykonawca musi dysponować redundantnym zasilaniem i bazować w oparciu o dwóch niezależnych dostawców usług internetowych. W docelowej lokalizacji (głównej), Wykonawca zapewni również wsparcie agregatem prądotwórczym.

4.11. Zamawiający nie dopuszcza, aby logi były składowane, przetrzymywane, korelowane lub analizowane w oparciu o systemy chmurowe. Wszystkie przesłane logi muszą być zbierane i zabezpieczone w infrastrukturze będącej własnością Wykonawcy. Wykonawca do celu przesyłania logów zestawi odpowiednie połączenia IPsec z Zamawiającym.

4.12. Wykonawca przeprowadzi instruktaż (online) dla maksymalnie 7 pracowników Zamawiającego w zakresie obsługi panelu SIEM, procedur SOC oraz interpretacji raportów.

5. Minimalne wymagania dla Etapu 3

5.1. Świadczenie kompleksowej usługi SOC w trybie ciągłym wraz z aktywną reakcją na incydenty bezpieczeństwa. SOC będzie świadczony od dnia zakończenia i odbioru Etapu 2.

5.2. Wymagania formalne i operacyjne:

5.2.1. Usługa SOC realizowana będzie w trybie 24/7/365 przez zespół analityków Wykonawcy, zapewniając ciągłość monitorowania infrastruktury Zamawiającego.

5.2.2. Wykonawca zobowiązany jest do bieżącego monitorowania i analizy zdarzeń na podstawie logów oraz sygnałów przekazywanych z systemów wskazanych przez Zamawiającego, w szczególności:

- Systemu klasy EDR/XDR (ESET Inspect),
- Rozwiązań brzegowych (Stormshield),
- Usługi katalogowej (Active Directory).

5.3. Czynności Wykonawcy w ramach SOC:

5.3.1. monitorowanie oraz analizowanie zdarzeń/incydentów,

5.3.2. obsługa incydentów zgodnie z przyjętymi procedurami reakcji,

5.3.3. analiza incydentów zgodnie z przyjętymi scenariuszami,

5.3.4. scenariusze wymagające reagowania zgodnie z wytycznymi Zamawiającego,

5.3.5. weryfikacja zgłoszeń od Zamawiającego.

5.4. Zamawiający wymaga reakcji zespołu SOC, w oparciu o udostępnione przez Zamawiającego systemy, o których mowa w ppkt 5.2.2 powyżej, zgodnie z wyznaczonymi scenariuszami, tj. izolacja hosta, ubicie procesu. Zamawiający nie dopuszcza instalacji innych narzędzi, umożliwiających realizację w/w zadań.

5.5. Zamawiający wskazuje, jako konieczność, obsługę minimum 10 różnych scenariuszy po stronie Wykonawcy, zgodnie z wyznaczoną na etapie implementacji SOC ścieżką podłączenia źródeł logów. Scenariusz jest rozumiany poprzez zdefiniowanie warunków wywołania alarmu/incydentu na bazie logów ze źródeł podłączonych do SIEM. Przykład: wykrycie utworzenia użytkownika w AD oraz usunięcie go w krótkim czasie (np. 5 minut) od momentu utworzenia.

5.6. Kategoryzacja incydentów przez Wykonawcę:

5.6.1. krytyczne – działania powodujące lub mogące powodować dotkliwe zakłócenia operacyjne lub straty finansowe, mogą też wpłynąć na inne osoby fizyczne lub prawne powodując szkody materialne lub niematerialne,

5.6.2. nie krytyczne – pozostałe,

5.6.3. false positive – zdarzenia nie będące incydentem i nie wymagające podjęcia działań

5.7. Czas reakcji to podjęcie działań przez operatorów SOC Wykonawcy w celu zdiagnozowania zdarzenia. Zamawiający wyznacza czas reakcji na wszystkie incydenty (niezależnie od kategorii, wskazanych w punkcie 5.6.):

5.7.1. podjęcie reakcji do 60 minut od momentu wystąpienia zdarzenia/incydentu,

5.7.2. przekazanie rekomendacji lub działań naprawczych do 180 minut od rozpoczęcia reakcji,
5.7.3. szczegółowy raport ze zdarzenia/incydentu do 24h po jego wystąpieniu.

5.8. Obsługa zdarzeń/incydentów będzie realizowana przez zespół SOC Wykonawcy w oparciu o najlepsze praktyki i wiedzę.

5.9. Wykonawca jest zobowiązany do przesyłania cyklicznych raportów oraz raportowania wykonania usługi SOC poprzez:
5.9.1. dostęp do systemu ticketowego – systemu, gdzie Zamawiający może zgłaszać i przeglądać zdarzenia/incydenty,
5.9.2. dostęp do dedykowanych dashboardów – min. dwóch, które Zamawiający może wykorzystać do obserwacji – dashboardy zostaną dostarczone przez Wykonawcę w formie nieedytowalnej przez Zamawiającego. Wskazane dashboardy będą zawierać przyjęte przez SIEM Wykonawcy logi zakwalifikowane do kategorii zgodnie z punktem 5.6 specyfikacji,
5.9.3. przygotowanie dedykowanego raportu ze zdarzenia/incydentu do 24h od jego wystąpienia (jeśli taki wystąpi),
5.9.4. przygotowanie raz w miesiącu cyklicznego zbiorczego raportu obejmującego cały poprzedni miesiąc kalendarzowy i przekazanie go Zamawiającemu do 5. dnia miesiąca następującego po miesiącu, którego raport dotyczy, a w razie potrzeby – w terminie wyznaczonym przez Zamawiającego, nie częściej niż raz w miesiącu – zorganizuje spotkanie online w celu omówienia przesłanego raportu.

5.10. Raporty, o których mowa w ppkt 5.9.3. i 5.9.4. muszą być dostarczane w formie zaszyfrowanej za pośrednictwem poczty e-mail wraz z przesłaniem hasła w wiadomości SMS do otwarcia zaszyfrowanego załącznika – Zamawiający wymaga, aby hasło było zmieniane co 3 miesiące i wysyłane w wiadomości SMS na wskazany przez Zamawiającego numer telefonu.

5.11. Wykonawca będzie w zakresie zidentyfikowanego incydentu krytycznego współpracował z Zamawiającym celem rozpoznania, zebrania danych i przeciwdziałania.

5.12. Wykonawca będzie na bieżąco przekazywał rekomendacje odnośnie dopracowania procesów bezpieczeństwa i działania infrastruktury IT Zamawiającego.

6. Minimalne wymagania dotyczące personelu Wykonawcy

6.1. Wykonawca jest zobowiązany do wyznaczenia stałego zespołu dedykowanego do realizacji zamówienia, zapewniającego nieprzerwaną obsługę oraz realizację wszystkich procesów bezpieczeństwa w trybie 24/7/365.

6.2. Minimalny skład zespołu wynosi:
6.2.1. Analitycy SOC – min. 6 osób;
6.2.2. SOC Manager – min. 1 osoba;
6.2.3. Audytorzy – min. 2 osoby;
6.2.4. Konsultanci – min. 2 osoby;
6.2.5. Project Manager – min. 1 osoba;
6.2.6. Pentesterzy – min. 2 osoby.

6.3. Osoby wyznaczone do realizacji zamówienia muszą posiadać aktualne certyfikaty potwierdzające wiedzę teoretyczną i praktyczną (lub udokumentowane certyfikaty równoważne[1]) na poziomie eksperckim, zgodnie z poniższym:

6.3.1. w zakresie testów penetracyjnych (Etap 1): minimum 2 osoby posiadające certyfikat CEH Master lub CEH Practical (Certified Ethical Hacker Practical) oraz certyfikat eWPT (Web Application Penetration Tester);

6.3.2. w zakresie reagowania na incydenty i SOC (Etap 3): minimum 1 osoba posiadająca certyfikat GIAC Forensic Analyst (GCFA) lub równoważny, potwierdzający zaawansowane umiejętności w obszarze informatyki śledczej i analizy powłamaniowej;

6.3.3. pozostałe wymagane certyfikacje w zespole:

- Infrastruktura: CompTIA Network+, CompTIA Security+;
- Bezpieczeństwo operacyjne: EC-Council Fundamentals of Networking Concepts, Protocols and Security; EC-Council Planning and Implementing a Security Incident Response; EC-Council Practical Cyber Threat Intelligence;
- Zarządzanie: EC-Council Project Management for Cybersecurity Professionals;
- Audyt i Zgodność: Audytor Wiodący ISO 9001, Audytor Wiodący ISO 27001:2022, CISA (Certified Information Systems Auditor).

[1] *Jako certyfikat równoważny Zamawiający rozumie przedstawienie przez Wykonawcę certyfikatu, analogicznego co do zakresu wskazanego certyfikatu, co jest rozumiane jako:*

- *analogiczna dziedzina merytoryczna wynikająca z wiedzy, którą obejmuje certyfikat,*
- *analogiczny stopień poziomu kompetencji,*
- *analogiczny poziom doświadczenia zawodowego wymagany dla otrzymania danego certyfikatu,*
- *potwierdzenie certyfikatu egzaminem, jeśli uzyskanie certyfikatu wymaga zdania egzaminu,*
- *został wydany przez uprawniony podmiot, który nie jest powiązany kapitałowo lub osobowo z Wykonawcą.*

6.3.4. Jeśli Wykonawca, w ramach realizacji Umowy, będzie dysponował Analitykiem ds. obsługi systemu ESET i/lub Analitykiem ds. obsługi systemu Stormshield (**skład oraz ilość członków Zespołu Wykonawcy punktowany w ramach kryteriów oceny ofert**), wówczas Zamawiający wymaga, aby Wykonawca zapewnił minimum po 2 godziny miesięcznego wsparcia (łącznie 4 godziny) inżyniera / inzynierów w obsłudze systemów ESET (Protect i Inspect) oraz Stormshield.

7. Wymagania organizacyjne wobec Wykonawcy

7.1. Wykonawca musi udokumentować posiadanie wdrożonych i certyfikowanych systemów zarządzania, które będą utrzymywane przez cały okres realizacji zamówienia:

7.1.1. ISO/IEC 27001 – w zakresie obejmującym świadczenie usług Security Operations Center (SOC);

7.1.2. ISO 22301 – w zakresie zarządzania ciągłością działania dla usług bezpieczeństwa IT.

7.2. Wykonawca musi posiadać infrastrukturę techniczną (lokalizację SOC) na terenie Polski, zapewniającą fizyczne i logiczne bezpieczeństwo przetwarzanych danych Zamawiającego (brak dopuszczenia przetwarzania logów w chmurze publicznej poza infrastrukturą Wykonawcy).

7.3. Przedmiot zamówienia musi być zgodny z zasadą „niewyrządzania znaczącej szkody” (Do No Significant Harm – DNSH). Oznacza to, że Wykonawca musi zapewnić, że jego realizacja nie będzie miała znaczącego negatywnego wpływu na cele środowiskowe, takie jak ochrona klimatu, gospodarka o obiegu zamkniętym, zapobieganie zanieczyszczeniom oraz ochrona bioróżnorodności oraz, że wszystkie wdrażane rozwiązania zostały zaprojektowane w sposób minimalizujący negatywny wpływ na środowisko naturalne.