Grodzisk Mazowiecki,04.06.2025

Wykonawcy biorący udział w postępowaniu

DOT.: postępowania o udzielenie zamówienia w trybie rozeznania rynku pn.: Świadczenie usługi Security Operations Center (SOC), ID: 1117436.

WYJAŚNIENIE TREŚCI ZAPYTANIA IV

Pytanie nr 20

Czy Zamawiający oczekuje poza ofertą na usługę Security Operations Center (SOC) również oferty na usługę wsparcia technicznego, serwisu i fizycznej naprawy infrastruktury AKPiA i środowiska OT, w zakresie przywrócenia jej do poprawnego działania po incydencie bezpieczeństwa , w tym również fizycznej naprawy/wymiany urządzeń AKPiA.

Zgodnie z udostępnionym przez Zamawiającego OPZ usługa SOC została określona jako usługa polegająca na ciągłym: monitorowaniu systemów 24/7, analiza ruchu sieciowego, reagowanie na incydenty, raportowaniu, wparciu po włamaniowym , proaktywnym wsparciu bezpieczeństwa.

Jeśli tak, w ocenie Wykonawcy powoduje to znaczące rozszerzenie zakresu usług jakie mają być świadczone obok usługi SOC co w ocenie Wykonawcy wymaga znaczącego doprecyzowania wymagań w tym zakresie w udostępnianym przez Zamawiającego OPZ

Odpowiedź na pytanie nr 20

Zamawiający oczekuje, że usługa SOC *"polegająca na ciągłym: monitorowaniu systemów 24/7, analiza ruchu sieciowego, reagowanie na incydenty, raportowaniu, wparciu po włamaniowym , proaktywnym wsparciu bezpieczeństwa."*, zapewni poziom bezpieczeństwa infrastruktury OT w stopniu wykluczającym powstanie incydentów bezpieczeństwa skutkujących niepoprawnym działaniem lub fizycznym uszkodzeniem urządzeń AKPiA.

Pytanie nr 21

Pytanie dotyczące odp. na pytanie nr 18 : co Zamawiający rozumie przez "zapewnia przywrócenie środowiska do poprawnego działania."

Odpowiedź na pytanie nr 21

Zamawiający rozumie, że wykonawca jest odpowiedzialny w całości za świadczone przez siebie usługi SOC i będzie uczestniczył w przywróceniu poprawnego działania środowiska.

Pytanie nr 22

Pytanie dotyczące odp. na pytanie nr 19 - co zamawiający rozumie przez: " Wykonawca usługi odpowiada za przywrócenie infrastruktury do stanu sprzed ataku."

Odpowiedź na pytanie nr 22

W przypadku, gdy wykonawca usługi SOC przewiduje możliwość wystąpienia incydentów mogących skutkować zakłóceniem lub uszkodzeniem infrastruktury zamawiającego, należy uwzględnienić w zakresie świadczonych usług również działania umożliwiające przywrócenie tej infrastruktury do stanu sprzed incydentu. Zamawiający zakłada, iż Wykonawca będzie pełnić pełny cykl obsługi incydentu – od wykrycia po odtworzenie i wyciągnięcie wniosków.