

Zadanie: Zakup i wdrożenie usługi System Operation Center SOC

Założenia ogólne

1. Przedmiotem zamówienia jest Dostarczenie i uruchomienie usługi monitorowania Security Operations Center dla Urzędu Miasta Dąbrowa Górnicza w ramach projektu „Podniesienie poziomu Cyberbezpieczeństwa w Urzędzie Miejskim w Dąbrowie Górniczej” realizowanego ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC)
2. Termin realizacji oraz miejsce świadczenia Usługi
 - Planowany czas trwania umowy: 14 miesięcy (zamówienie podstawowe).
 - Zamawiający może zlecić świadczenie Usługi przez okres kolejnych 24 miesiące (zamówienie opcjonalne).
 - Usługa musi działać w środowisku serwerowym wykonawcy i łączyć się ze środowiskiem informatycznym Urzędu Miejskiego w Dąbrowie Górniczej za pomocą tunelu VPN typu Side to Side.
3. Parametry usługi
 - 3.1 Usługa będzie świadczona w trybie 24/7 przez 365 dni w roku.
 - 3.2 W ramach usługi Wykonawca będzie monitorował i reagował na zdarzenia na podstawie logów udostępnionych przez Zamawiającego ze wskazanych źródeł
 - 3.3 Usługa musi zawierać mechanizmy zwiększające poziom ochrony środowiska IT m.in. pozwalające na bieżące zarządzanie podatnościami oraz zapewniać zgodność z politykami bezpieczeństwa.
 - 3.4 Usługa musi agregować informacje o zdarzeniach sieciowych z różnorodnych źródeł,
 - 3.5 Zamawiający wskazuje jako źródła dla logów następujące systemy:
 - system klasy EDR/XDR (logi z endpoint - stacji roboczych serwerów)
 - kolektor logów sieciowych lub poszczególne urządzenia sieciowe (routery, switchy, Firewall, IPS/IDS oraz VPN)
 - Domena Active Directory (logi min. administracji użytkownikami)
 - Platforma M365
 - 3.6 Zaproponowane rozwiązanie 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.
 - 3.7 W skład usługi musi wchodzić co najmniej:
 - monitorowanie zdarzeń i incydentów pochodzących z urządzeń sieciowych, serwerów oraz komputerów użytkowników przy wykorzystaniu rozwiązania klasy SIEM i zaimplementowanych reguł analizy i korelacji logów (scenariusze);
 - reagowanie na pojawiające się zdarzenia zgodnie z ustalonymi procedurami i scenariuszami. Scenariusze i procedury muszą być przygotowane w oparciu o framework MITRE ATT&CK;

- udostępnianie rekomendacji mających na celu jak najlepsze zabezpieczenie środowiska IT oraz zminimalizowanie ryzyka skutecznego ataku;
- udostępnianie rekomendacji i raportów związanych z bieżącym monitorowaniem środowiska IT;
- śledzenie zagrożeń i trendów rynkowych w celu implementacji nowych reguł i procedur reakcji;
- zapewnienie kontroli nad zgodnością bezpieczeństwa monitorowanych systemów Urzędu z obowiązującymi w Polsce regulacjami dotyczącymi jednostek samorządowych, w szczególności z Ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne, Rozporządzeniem KRI, Rozporządzeniem RODO, Ustawą o Krajowym Systemie Cyberbezpieczeństwa.

3.8 Usługa musi obejmować poniższe funkcjonalności:

- analiza zdarzeń sieciowych
- analiza zdarzeń urządzeń końcowych
- monitorowanie integralności plików konfiguracyjnych;
- wykrywanie podatności aplikacji środowiska IT wewnętrznego oraz udostępnionego w Internecie;
- monitorowanie konfiguracji i polityk bezpieczeństwa;
- dostęp do pulpitu (dashboard) umożliwiającego bieżący wgląd w bezpieczeństwo środowiska IT.

3.9 Kategoryzacja incydentów przez Wykonawcę:

- 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,
- nie krytyczne – pozostałe,
- false positive – zdarzenia nie będące incydem i nie wymagające podjęcia działań

3.10 Czas reakcji to podjęcie działań przez operatorów SOC Wykonawcy w celu zdiagnozowania zdarzenia. Zamawiający wyznacza czas reakcji na wszystkie incydenty (niezależnie od kategorii, wskazane w punkcie 3.9):

- podjęcie reakcji do 30 minut od momentu wystąpienia zdarzenia/incydentu,
- przekazanie rekomendacji lub działań naprawczych do 150 minut od rozpoczęcia reakcji,
- szczegółowy raport ze zdarzenia/incydentu do 24h po jego wystąpieniu.

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

3.12 Wykonawca jest zobowiązany do przesyłania cyklicznych raportów oraz raportowania wykonania usługi poprzez:

- dostęp do systemu ticketowego gdzie Zamawiający może przeglądać zdarzenia/incydentu,
- dostęp do dedykowanego dashboardu. Dashboard powinien zawierać przyjęte przez system Zamawiającego logi zakwalifikowane do kategorii zgodnie z punktem 3.9 specyfikacji,
- szczegółowy raport ze zdarzenia/incydentu do 24h od jego wystąpienia,
- raz w tygodniu raport zbiorczy ze wszystkich zdarzeń z poprzedniego tygodnia wykonany do końca pierwszego dnia roboczego kolejnego/nowego tygodnia,
- raz w miesiącu raport zbiorczy z całego miesiąca przygotowany do 5 dnia każdego nowego miesiąca,

- raz w miesiącu spotkanie (forma zdalna/online) omawiająca przesłany raport miesięczny – spotkanie w II tygodniu roboczym nowego miesiąca,
 - raporty 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.
- 3.13 Wykonawca będzie w zakresie zidentyfikowanego incydentu krytycznego współpracował z Zamawiającym celem rozpoznania, zebrania danych i przeciwdziałania.
- 3.14 Zamawiający wymaga aby Wykonawca w ramach dostarczonej usługi SOC przeznaczył pulę zgłoszeń wynoszącą 10 zgłoszeń w okresie umowy na zgłoszenie incydentu krytycznego do odpowiedniego CSIRT oraz nadzorował i koordynował proces wymiany informacji.
- 3.15 Wykonawca będzie realizował usługę w oparciu o źródła logów. Usługa nie może być zależna od ilości pracowników, sprzętu czy wielkości infrastruktury Zamawiającego. W trakcie trwania usługi Zamawiający dopuszcza możliwość rozbudowy swojej infrastruktury i personelu co nie może mieć wpływu na koszt świadczonej przez Wykonawcę usługi.
- 3.16 Logi zebrane ze wskazanych przez Zamawiającego źródeł będą składowane przez Wykonawcę przez okres 3 miesięcy w formie zaszyfrowanej. Miejsce składowanie logów musi zostać wskazane w ofercie.
- 3.17 Wykonawca w ramach wdrożenia i opracowania usługi SOC dla Zamawiającego wykona analizę przedwdrożeniową.

Warunki udziału w postępowaniu

Wykonanie co najmniej dwóch zamówień o wartości minimum 150 000 zł brutto każde w zakresie świadczenia usługi monitorowania cyberbezpieczeństwa infrastruktury IT klienta przekraczającej 300 stanowisk komputerowych.

Wykonawca spełni warunek jeżeli wykaże w wykazie wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, usług w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, że wykonał należycie co najmniej dwa zamówienia o wartości minimum 150 000 zł brutto każde w zakresie świadczenia usługi monitorowania cyberbezpieczeństwa, oraz wykaże, że infrastruktury IT ww. klientów przekracza 300 stanowisk komputerowych

Wykonawca musi dysponować następującym zespołem do realizacji usług. Security Operation Center:

- analitycy pierwszej linii wsparcia – min 5 osób,
- analitycy wewnętrzni/ inżynierowie systemów – min 5 osób,
- SOC manager – min 1 osoba,

Wykonawca musi spełniać wymagania posiadania minimum (po jednym dla każdego) aktualnych certyfikatów. Zamawiający dopuszcza użycie certyfikatów równoważnych dla niżej wskazanych przy 100% pokryciu założeń programowych (teoria i praktyka):

- CEH (certified ethical hacker)
- CISSP (certified information systems security professional)
- CISM (CIS information security manager)
- OSCP (offensive security certified professional)

- Certyfikat z zakresu wskazywania podatności systemu informatycznego na ataki

Wykonawca chcący ubiegać się o świadczenie usługi Security Operation Center musi posiadać ważny i aktualny certyfikat ISO 27001 (lub równoważny) obejmujący swoim zakresem świadczoną przez niego usługę Security Operation Center.

Kary

Wykonawca za odstąpienie od umowy, niewykonanie lub nienależyte wykonanie zapisów umowy przewiduje zastosowanie kar powszechnie stosowanych dla zamówień tego typu.

Jeżeli w okresie trwania umowy nastąpi niewykryty cyberatak, który wywoła negatywne skutki w systemach informatycznych zamawiającego, który nastąpił poprzez kanał monitorowany w związku z realizacją niniejszej umowy, wykonawca poniesie koszty związane z naprawieniem powstałych szkód do wysokości wartości umowy.

Jeżeli zamawiający wskaże wykonawcy niewykryty cyberatak w kanałach monitorowanych poprzez wykonawcę, który nie wywołał negatywnych skutków, Wykonawca zapłaci Zamawiającemu karę w wysokości 20% płatności przewidzianej w danym okresie rozliczeniowym za każdy niewykryty cyberatak.