**OPIS PRZEDMIOTU ZAMÓWIENIA**świadczenie usługi **Security Operations Center (SOC)**

Przedmiotem zamówienia jest świadczenie usługi SOC (Security Operations Center) w modelu całodobowego monitoringu i reagowania na incydenty bezpieczeństwa w infrastrukturze IT oraz OT naszej firmy.

**Zakres wymaganych usług:**

1. **Monitoring systemów IT i OT** – całodobowy (24/7/365) nadzór nad systemami informatycznymi oraz komponentami infrastruktury OT (Operational Technology), w tym sterownikami, sieciami przemysłowymi, urządzeniami IoT oraz systemami SCADA.
2. **Analiza ruchu sieciowego** – ciągłe badanie i analiza ruchu sieciowego w celu wykrycia anomalii, ataków, nieautoryzowanego dostępu oraz prób eskalacji uprawnień.
3. **Reagowanie na incydenty** – natychmiastowa reakcja w przypadku wykrycia potencjalnie niebezpiecznego zdarzenia:

* powiadomienie e-mailowe na dedykowany adres,
* kontakt telefoniczny z osobami wskazanymi w umowie,
* rozpoczęcie procedury analizy i klasyfikacji incydentu zgodnie z ustalonym SLA.

1. **Raportowanie**:

* cotygodniowy raport operacyjny zawierający szczegółowe dane dotyczące przeanalizowanych zdarzeń, poziomu zagrożenia oraz rekomendacje działań korygujących,
* comiesięczne spotkania warsztatowe (1 godzina) mające na celu omówienie kluczowych zdarzeń, analizę trendów oraz optymalizację zakresu monitoringu i współpracy.

1. **Pomoc po incydencie bezpieczeństwa / ataku**:

* **wsparcie powłamaniowe** (post-incident response): analiza incydentu, ustalenie przyczyn, analiza wektorów ataku, źródeł zagrożenia oraz skutków naruszenia bezpieczeństwa,
* przygotowanie szczegółowego raportu poreakcyjnego wraz z zaleceniami zmian organizacyjnych i technicznych (hardening, polityki, aktualizacje, procedury) mających na celu zapobieżenie podobnym incydentom w przyszłości.

1. **Proaktywne wsparcie bezpieczeństwa** – przekazywanie bieżących zaleceń konfiguracyjnych, polityk bezpieczeństwa i rekomendacji wynikających z analizy zagrożeń i aktualnych podatności.

Obszary objęte monitoringiem:

* Systemy klasy XDR oraz skanery podatności,
* System backupowy (monitoring integralności i poprawności działania),
* Infrastruktura sieciowa (firewalle, przełączniki, punkty dostępowe),
* System NAC (Network Access Control),
* System PAM (Privileged Access Management),
* Domena Active Directory,
* Centralny system logowania (SIEM lub równoważny),
* **Infrastruktura OT** – urządzenia przemysłowe, systemy automatyki, komponenty sieci przemysłowych.

Zdarzenia są monitorowane z priorytetem dla zdarzeń krytycznych.

**Do oferty należy dołączyć:**

* Szczegółowy opis oferowanego modelu świadczenia usługi SOC (technologie, metody działania, dostępność zespołu).
* Zakres oferowanego monitoringu IT i OT oraz narzędzia wykorzystywane do analizy i reagowania.
* Czas reakcji na incydenty oraz opis procedury eskalacji.
* Zakres usług powłamaniowych – podejście, czas reakcji, zasoby.
* Harmonogram i forma raportowania, przykład raportu tygodniowego.
* Cena usługi – miesięczny koszt netto/brutto oraz informacje o ewentualnych kosztach wdrożenia.
* Czas trwania umowy 12 miesięcy
* Referencje lub case studies z podobnych wdrożeń min
* **Warunek udziału w postępowaniu**: Wykonawca spełni warunek jeżeli wykaże, że w okresie ostatnich 3 (trzech) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, należycie wykonał min 3 usługi polegające na wdrożeniu SOC (Security Operations Center)