

Opis przedmiotu zamówienia – Usługa Security Operations Center (SOC)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest świadczenie usługi Security Operations Center (SOC) dla Zakładu Gospodarki Wodno-Ściekowej w Słońsku, obejmującej monitoring bezpieczeństwa systemów teleinformatycznych, analizę zdarzeń bezpieczeństwa, obsługę incydentów oraz wsparcie administratora systemów informatycznych.

Umowa zostanie zawarta na okres od dnia podpisania do **31 grudnia 2026 r.**, z możliwością jej przedłużenia na kolejny okres na warunkach określonych w umowie, zgodnie z obowiązującymi przepisami prawa zamówień publicznych.

2. Czas świadczenia usługi

Usługa świadczona będzie:

- od poniedziałku do piątku,
- z wyłączeniem dni ustawowo wolnych od pracy,
- w godzinach **07:00–15:00**.

W powyższych godzinach Wykonawca zapewni bieżący monitoring środowiska, analizę incydentów, wsparcie oraz powiadamianie Zamawiającego.

Poza wskazanymi godzinami świadczenie usługi nie jest wymagane.

3. Zakres monitorowanej infrastruktury

Usługa obejmować będzie monitorowanie infrastruktury Zamawiającego obejmującej w szczególności:

- stacje robocze użytkowników,
- serwery fizyczne i wirtualne,
- klaster wysokiej dostępności (HA),
- macierz dyskową,
- zapory sieciowe UTM pracujące w klastrze HA,
- zaporę UTM zainstalowaną w Stacji Uzdatniania Wody,
- przełączniki zarządalne,
- system SIEM (Wazuh lub rozwiązanie równoważne),
- system monitoringu infrastruktury (Zabbix lub rozwiązanie równoważne),
- system EDR/XDR,

- system kopii zapasowych obejmujący repozytorium lokalne oraz repozytorium off-site,
- urządzenia UPS,
- inne urządzenia i systemy wskazane przez Zamawiającego w okresie obowiązywania umowy.

Zmiana liczby urządzeń wynikająca z rozbudowy infrastruktury Zamawiającego nie stanowi zmiany przedmiotu zamówienia, o ile nie powoduje istotnego zwiększenia zakresu świadczonej usługi.

4. Zakres świadczonej usługi

Wykonawca zobowiązany będzie do:

1. monitorowania zdarzeń bezpieczeństwa,
2. analizy i korelacji logów,
3. identyfikacji incydentów bezpieczeństwa,
4. klasyfikacji incydentów według poziomu zagrożenia,
5. niezwłocznego powiadamiania Zamawiającego o incydentach wymagających podjęcia działań,
6. przekazywania rekomendacji dotyczących ograniczenia skutków incydentów,
7. wsparcia administratora podczas analizy oraz usuwania skutków incydentów,
8. monitorowania dostępności urządzeń bezpieczeństwa,
9. monitorowania poprawności działania systemów EDR/XDR,
10. przygotowywania raportów z realizacji usługi.

Usługa nie obejmuje administrowania infrastrukturą Zamawiającego ani wykonywania zmian konfiguracyjnych bez odrębnego zlecenia.

5. Powiadamianie o incydentach

Powiadomienie powinno zawierać co najmniej:

- datę i godzinę wykrycia,
- opis zdarzenia,
- ocenę poziomu zagrożenia,
- określenie potencjalnego wpływu na działalność ZGWŚ,
- rekomendowane działania.

6. Raportowanie

Wykonawca sporządzi miesięczny raport obejmujący:

- liczbę wykrytych zdarzeń,
- liczbę incydentów,

- klasyfikację incydentów,
- wykryte podatności i zagrożenia,
- rekomendacje dotyczące poprawy poziomu bezpieczeństwa,
- podsumowanie wykonanych działań.

7. Minimalne wymagania SLA

- rozpoczęcie analizy incydentu krytycznego – do 1 godziny,
- rozpoczęcie analizy incydentu wysokiego – do 2 godzin,
- rozpoczęcie analizy incydentu średniego – do końca dnia roboczego,
- rozpoczęcie analizy incydentu niskiego – do 2 dni roboczych.

Czasy SLA obowiązują wyłącznie w godzinach świadczenia usługi, tj. od 07:00 do 15:00 w dni robocze.

8. Wymagania wobec Wykonawcy

Wykonawca powinien:

- posiadać doświadczenie w świadczeniu usług SOC,
- dysponować personelem posiadającym wiedzę z zakresu cyberbezpieczeństwa,
- zapewnić poufność informacji uzyskanych podczas realizacji umowy,
- prowadzić dokumentację obsługiwanych incydentów,
- współpracować z administratorem systemów Zamawiającego.

9. Cel usługi

Celem świadczenia usługi jest zapewnienie bieżącego nadzoru nad bezpieczeństwem infrastruktury teleinformatycznej Zakładu Gospodarki Wodno-Ściekowej w Słonsku, wsparcie w wykrywaniu i analizie incydentów bezpieczeństwa oraz zwiększenie odporności organizacji na zagrożenia cybernetyczne przy zachowaniu proporcjonalności zakresu usługi do wielkości i charakteru działalności Zamawiającego.