ZAKŁAD ENERGETYKI CIEPLNEJ Sp. z o.o. w Wałczu
78 – 600 Wałcz, ul. Budowlanych 9/4
www.zec-walcz.pl
e-mail: sekretariat@zec-walcz.pl
NIP: 765-14-58-778; REGON 570339470;
KRS nr 0000095113;
tel. 67 258 50 32 ÷35; fax. 67 250 08 62

Wałcz, dnia 28.01.2025 r.

L.Dz./TR /...../2025

Strona internetowa
ZEC Sp. z o.o. w Wałczu

Dotyczy postępowania nr 4/2025: **„Poprawa poziomu cyberbezpieczeństwa i przygotowanie do spełnienia kryteriów dyrektywy NIS 2 w Zakładzie Energetyki Cieplnej Sp. z o. o. w Wałczu„**

Pytanie nr 1: *„Co dokładnie oznacza "ochrona przed cyberzagrożeniami"? Czy chodzi o wykrywanie i informowanie o zagrożeniach, czy także o ich aktywne neutralizowanie?*
Odpowiedź Zamawiającego:
Zamawiającemu zależy na wykrywaniu i informowaniu o zagrożeniach.

Pytanie nr 2: *Czy oczekiwane działania w ramach reagowania na incydenty obejmują jedynie zarządzanie incydentami (Incident Management), czy także szersze zarządzanie infrastrukturą, takie jak np. regularne aktualizowanie systemów (Patch Management)?*
- Jeśli tak, czy Klient przewiduje, że zespół SOC będzie w pełni odpowiedzialny za wdrażanie aktualizacji i konfiguracji systemów, czy tylko za rekomendacje, które mają być realizowane przez
wewnętrzny zespół IT?
-Czy takie podejście oznacza, że dostawca usługi SOC w praktyce przejmie część obowiązków związanych z utrzymaniem infrastruktury IT Klienta?
Odpowiedź Zamawiającego:
Zamawiający oczekuje tylko zarządzanie incydentami.

Pytanie nr 3:*Czy Klient posiada już procesy i harmonogramy związane z zarządzaniem łatami (Patch Management), które mogą być zintegrowane z działaniami SOC, czy też oczekuje ich opracowania i prowadzenia przez dostawcę?*
Odpowiedź Zamawiającego:
Zamawiający nie posiada żadnych opracowań, oczekuje ich opracowania i wprowadzenia.

Pytanie nr 4:*. Czy monitoring ma obejmować tylko stacje robocze, czy także serwery, urządzenia sieciowe, aplikacje oraz chmurę?*
Odpowiedź Zamawiającego:
Tak.

Pytanie nr 5: *„Czy Klient oczekuje monitorowania tylko incydentów krytycznych, czy również mniej istotnych zdarzeń (np. potencjalnie niebezpiecznych aktywności)?*
Odpowiedź Zamawiającego:
Incydentów krytycznych oraz mniej istotnych zdarzeń.

Pytanie nr 6: *Jakie systemy i aplikacje Klient uważa za krytyczne, wymagające natychmiastowego reagowania?*
Odpowiedź Zamawiającego:
Systemy produkcyjne i SCADA, ***Systemy bezpieczeństwa IT,*** *Bazy danych i systemy magazynowe*

Pytanie nr 7: *Czy Klient wymaga monitorowania również ruchu sieciowego, czy wyłącznie działań na urządzeniach końcowych?*
Odpowiedź Zamawiającego:
Również ruchu sieciowego.

Pytanie nr 8: *Jak ma wyglądać reakcja na incydenty? Czy oczekiwane jest:*
a) Zdalne przejęcie kontroli nad systemami i natychmiastowe działania naprawcze?
b) Tylko konsulting i wskazanie działań do podjęcia przez wewnętrzny zespół IT?
c) Wyłącznie powiadamianie o zdarzeniach?
Odpowiedź Zamawiającego:
Tylko konsulting i wskazanie działań do podjęcia przez wewnętrzny zespół IT.

Pytanie nr 9: *Czy Klient posiada wewnętrzny zespół IT, który będzie wspierał działania SOC, czy oczekuje pełnej obsługi ze strony dostawcy?*
Odpowiedź Zamawiającego:
Tak.

Pytanie nr 10: *Czy reakcje naprawcze mają obejmować zmiany w konfiguracjach, restartowanie usług, czy tylko rekomendacje dla Klienta?*
Odpowiedź Zamawiającego:
Zamawiający oczekuje tylko rekomendacji.

Pytanie nr 11: *Czy Klient posiada plan reakcji na incydenty i jasno określone role, czy oczekuje od dostawcy pełnego opracowania procedur?*
Odpowiedź Zamawiającego:
Zamawiający nie posiada planu reakcji, oczekuje wprowadzenia i opracowania procedór.

Pytanie nr 12: *Czy wszystkie urządzenia w infrastrukturze Klienta posiadają najnowsze aktualizacje systemowe i oprogramowania? - Jeśli nie, kto ma odpowiadać za ich wdrażanie?*
Odpowiedź Zamawiającego:
Zamawiający jest w trakcie wymiany urządzeń wraz z ich dostosowaniem do wymogów cyberbezpieczeństwa.

Pytanie nr 13: *Czy Klient dysponuje istniejącymi rozwiązaniami bezpieczeństwa (np. firewalle, EDR, SIEM), które mają zostać zintegrowane z usługą SOC?*
Odpowiedź Zamawiającego:
Firewalle-tak, EDR, SIEM-nie

Pytanie nr 14: *Jak Klient wyobraża sobie reakcję na incydenty bezpieczeństwa w kontekście zapewnienia ciągłości działania usług? Czy oczekiwane działania naprawcze, takie jak np. resetowanie usług,*
mogą wpłynąć na dostępność systemów dla pracowników lub klientów, czy też powinny być planowane w sposób minimalizujący zakłócenia?
Odpowiedź Zamawiającego:
powinny być planowane w sposób minimalizujący zakłócenia

Pytanie nr 15: *Czy reakcje na incydenty mają być uzgadniane i koordynowane z wewnętrznym zespołem IT?*
Odpowiedź Zamawiającego:
Tak.

Pytanie nr 16: *Czy zespół IT Klienta pracuje w modelu 24/7/365 lub będzie dostępny w takim trybie, aby wspierać działania zespołu SOC w razie potrzeby?*
Odpowiedź Zamawiającego:
Nie.

Pytanie nr 17: Kto ma przeprowadzić instalację agentów na komputerach – administratorzy klienta zgodnie z naszą instrukcją, czy wykonawca ma się zdalnie łączyć i przeprowadzić instalację?
Odpowiedź Zamawiającego:
Informatyk Zamawiającego

Pytanie nr 18: Czy wykonawca będzie miał pełne uprawnienia do instalacji agentów (dostęp do kont administratora)?
Odpowiedź Zamawiającego:
Jeżeli wystąpi taka potrzeba.

Pytanie nr 19: Czy Zamawiający zapewni fizyczny i zdalny dostęp do wszystkich urządzeń objętych monitoringiem (50 stacji roboczych i 8 serwerów)?
Odpowiedź Zamawiającego:
Tak.

Pytanie nr 20: Co dokładnie Zamawiający rozumie przez „zapewnienie ochrony przed cyberzagrożeniami"? Czy chodzi o detekcję i powiadamianie, czy również aktywne blokowanie zagrożeń?
Odpowiedź Zamawiającego:
Dotyczy detekcji i powiadomień.

Pytanie nr 21: Czy reakcja na incydenty ma ograniczać się do informowania wskazanych osób po stronie klienta, czy wykonawca ma podejmować działania na infrastrukturze klienta?
Odpowiedź Zamawiającego:
Zamawiający wyznaczy osobę do przekazywania informacji.

Pytanie nr 24: Czy Zamawiający posiada XDR lub inne rozwiązanie umożliwiające integrację poprzez API?
Odpowiedź Zamawiającego:
Nie

Pytanie nr 25: Czy wykonawca będzie miał dostęp do systemów zabezpieczeń, takich jak firewall czy EDR/XDR?
Odpowiedź Zamawiającego:
Tak, po wdrożeniu przez wykonawcę

Pytanie nr 26: Co Zamawiający rozumie przez „stałe aktualizowanie i współdzielenie wiedzy o incydentach oraz nowych zagrożeniach"?
Odpowiedź Zamawiającego:
Szkolenia, przekazywania informacji o nowych rodzajach zagrożeń.

Pytanie nr 27: Czy codzienny raport Threat Intelligence będzie dla Zamawiającego wystarczający?
Odpowiedź Zamawiającego:
W zależności od występowania zagrożeń.

Pytanie nr 28: W jakiej formie mają być dostarczane raporty Zamawiającemu (PDF, dashboard online, inne)?
Odpowiedź Zamawiającego:
PDF.

Pytanie nr 29: Co według Zamawiającego konkretnie oznacza „przywracanie usług" w kontekście podjęcia działań naprawczych?
Odpowiedź Zamawiającego:
Wydanie rekomendacji.

Pytanie nr 30: Czy wykonawca ma być odpowiedzialny wyłącznie za aspekty cyberbezpieczeństwa, czy również za działania techniczne (np. restart serwera, odtwarzanie systemu z backupu)?
Odpowiedź Zamawiającego:
Za aspekty bezpieczeństwa.

Pytanie nr 31: Czy są jakieś elementy infrastruktury, które wykraczają poza zakres działań wykonawcy (np. wymiana sprzętu)?
Odpowiedź Zamawiającego:
Nie.

Pytanie nr 32: Jakie są dokładne wymagania Zamawiającego wobec serwera monitorującego? Czy wykonawca ma go dostarczyć i skonfigurować, czy wykorzystać istniejącą infrastrukturę klienta?
Odpowiedź Zamawiającego:
Z wykorzystaniem istniejącej infrastruktury Zamawiającego.

Pytanie nr 33: Jakie konkretne funkcje ma spełniać serwer monitorujący – przechwytywanie logów, analiza ruchu sieciowego, integracja z systemami SIEM?
Odpowiedź Zamawiającego:
Zgodnie z regulacjami i wymogami audytu.

Pytanie nr 34: Czy serwer monitorujący będzie miał dostęp do całej infrastruktury klienta, czy będą jakieś ograniczenia?
Odpowiedź Zamawiającego:
Zgodnie z potrzebami.

SPECJALISTA
ds.
Monika Wojtalik