Grodzisk Mazowiecki,30.05.2025

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 II

Pytanie nr 3

W związku z dość obszernym zakresem zadań związanych z zapewnieniem Zamawiającemu usług związanych z cyberbezpieczeństwem OT i IT, oraz dobraniem przez Oferenta adekwatnych i proporcjonalnych rozwiązań, zgodnie z zasadą należytej staranności, prosimy o wydłużenie terminu złożenia ofert do dnia 6.06.2025 r.

Odpowiedź na pytanie nr 3

Zamawiający przedłuża termin złożenia oferty z dnia 02.06.2025 godz:10:00 na dzień 05.06.2025 godz. 10:00.

Pytanie nr 4

Zakres infrastruktury OT
• Ile urządzeń OT znajduje się w infrastrukturze? (np. PLC, HMI, sensory, radiolinie)
• Jaki jest producent systemu SCADA?
• Jakie są typy i modele urządzeń OT?
• Czy urządzenia OT działają w odizolowanych segmentach sieci, czy są połączone z siecią **IT?**

Odpowiedź na pytanie nr 4

- znajdują się 123 urządzenia

- SCADA IFIX , TelWin SCADA

-urządzenia producentów: Siemens, Saia burgess, Schneider electric, Moxa, Dynacon, Moeller, HW group, ICP DAS.

- urządzenia działają w odizolowanych segmentach sieci.

Pytanie nr 5

Topologia i wielkość sieci OT
• Ile lokalizacji (np. zakładów, oddziałów) obejmuje infrastruktura OT?
• Jak wygląda segmentacja sieci OT – są oddzielne VLANy, sieć produkcyjna?
• Ile ringów zawiera sieć OT (tzw. Infrastruktura wyspowa)?
• Czy dostęp do sieci OT odbywa się zdalnie (VPN, terminale)?

Odpowiedź na pytanie nr 5

- 2 lokalizacje

- Sieć jest podzielona w sposób fizyczny i logiczny.

- W 1 lokalizacji znajduje się 1 ring

- Nie odbywa się dostęp zdalnie (VPN, Terminale)

Pytanie nr 6

Monitoring i integracja
• Czy urządzenia OT generują logi? Jeśli tak, to w jakim formacie i przez jakie protokoły (Syslog, OPC, SNMP)?

Odpowiedź na pytanie nr 6

-Tak Syslog , SNMP itp

Pytanie nr 7

Wymagania w zakresie SLA
• Czy Zamawiający oczekują takiego samego czasu reakcji i poziomu SLA dla incydentów OT jak dla IT?

Odpowiedź na pytanie nr 7

TAK

Pytanie nr 8

Zarządzanie incydentami OT
• Czy Zamawiajacy oczekuje w postępowaniu by Oferent przywrócił środowisko OT do poprawnego działania po zmaterializowaniu incydentu bezpieczeństwa w środowisku OT?
• Po czyjej stronie (Zamawiający/Realizujący) będą podejmowane działania minimalizujące skutki incydentu w środowisku OT?
• Czy Zamawiający posiada wewnętrzne procedury obsługi incydentów OT, z którymi Oferent powinien się zapoznać?

Odpowiedź na pytanie nr 8

- TAK

- TAK

-Zamawiający nie posiada wewnętrznych procedur obsługi incydentów OT.

Pytanie nr 9

Dostępność dokumentacji
• Czy posiadają Państwo dokumentację urządzeń OT i topologii sieci? I czy po podpisaniu umowy możemy do niej uzyskać wgląd?

Odpowiedź na pytanie nr 9

Posiadamy ww. dokumentację. Po podpisaniu umowy i zgodzie Zarządu, Zamawiający udostępni dokumentacje do wglądu.

Pytanie nr 10

Zamawiający odpowiedział, że SIEM działa obecnie tylko z częścią infrastruktury – obejmujący 9 stacji roboczych, 7 serwerów aplikacyjnych, 1 firewall oraz aplikacje stacji zlewnych i system SCADA. W opisie przedmiotu zamówienia, wymienionych systemów jest więcej. W jaki sposób zamawiający chce realizować monitoring tych systemów? Kto będzie odpowiedzialny za ewentualne skonfigurowanie pozostałych źródeł w SIEM?

Odpowiedź na pytanie nr 10

Wykonawca jest odpowiedzialny za konfigurację ewentualnych źródeł w SIEM.

Pytanie nr 11

Jakim systemem SIEM dysponuje zamawiający?

Odpowiedź na pytanie nr 11

Dynacon

Pytanie nr 12

Zwracamy się z uprzejmą prośbą o wydłużenie terminu na złożenie oferty.

Odpowiedź na pytanie nr 12

Odpowiedzi udzielono w odpowiedzi nr 3.

Pytanie nr 13

SIEM - Proszę o potwierdzenie, że usługa SOC ma opierać się o usługowo udostępnione zasoby na platformie SIEM Wykonawcy

Odpowiedź na pytanie nr 13

Zależy od analizy przeprowadzonej przez Wykonawcę.

Pytanie nr 14

SIEM - proszę o informacje jakie źródła z infrastruktury Klienta z wymienionych w SWZ zasilają obecnie SIEM Zamawiającego

Odpowiedź na pytanie nr 14

Aktywne urządzenia sieciowe.

Pytanie nr 15

OT - automatyka przemysłowa dla poprawnego monitorowania wymaga wykorzystania pasywnych sond do analizy ruchu w tej sieci. Czy Zamawiający posiada wdrożone rozwiązanie do monitorowania OT? Jeśli nie, czy Wykonawcy mają zakładać implementację takiego rozwiązania w ramach oferty na SOC na czas realizacji usługi SOC?

Odpowiedź na pytanie nr 15

Wykonawca ma zakładać implementację takiego rozwiązania.

Pytanie nr 16

Ile logów i EPS w ciągu doby na ten moment przetwarza SIEM Zamawiającego?

Odpowiedź na pytanie nr 16

około 250 MB na dobę logów 4-5 EPS

Pytanie nr 17

Z jakiego rozwiązania SIEM korzysta Zamawiający?

Odpowiedź na pytanie nr 17

Dynacon