

Szczegółowy Opis Przedmiotu Zamówienia

NAZWA POSTĘPOWANIA: Audyt Sieci i Systemów OT/ICS (automatyka przemysłowa) w LPEC S.A.

1. Wymagania dla wykonawcy:

- 1) Potwierdzenie posiadania wiedzy i doświadczenia udokumentowane wykonaniem w okresie ostatnich 5 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, minimum trzech audytów sieci i systemów OT/ICS o wartości nie mniejszej niż: 40 000 zł każdy.
- 2) Zespół uczestniczący w audycie legitymujący się certyfikatami co najmniej:
 - GICSP– Global Industrial Cyber Security Professional GIAC
 - CEH – Certified Ethical Hacker
 - GRID – GIAC Response and Industrial Defence
 - ISA/IEC 62443 Cybersecurity Fundamentals Specialist
 - (C)PTE – Certified Penetration Testing Engineer
 - (C)NFE – Certified Network Forensice Examiner
 - CompTIA Network+
- 3) Wykonawca posiada ważną certyfikację - zgodność z systemami jakości i bezpieczeństwa informacji - ISO/IEC 27001, ISO 9001, wystawioną przez jednostkę akredytowaną w PCA (Polskie Centrum Akredytacji).

2. Zakres prac

- 1) Przeprowadzenie badania Sieci i Systemów OT/ICS w LPEC
 - a) Inwentaryzacja automatyczna - dane dostępne przy realizacji metodą pasywną z analizą ruchu sieciowego w wariantcie White-Box. Inwentaryzacja musi się odbyć z wykorzystaniem IDS klasy Enterprise dla sieci i systemów infrastruktury krytycznej (np. SCADA, DCS, BMS itd.) np. iSID Radiflow lub równoważnym.
 - b) ocena poziomu bezpieczeństwa sieci i systemów OT/ICS - obserwacje/rekomendacje wynikające z dobrych praktyk i standardu ISA/IEC 62443).
 - c) Rekomendacje dla sieci OT/ICS – (analiza, obserwacje i rekomendacje w odniesieniu do standardu ISA/IEC 62443)
- 2) Opracowanie i przekazanie raportu dla sieci i systemów infrastruktury krytycznej (np. SCADA, DCS, BMS itd.). Raport zawierać będzie następujące informacje:
 - inwentaryzacja sieci i pokazanie kontekstu komunikacyjnego,
 - prezentacja urządzeń i połączeń logicznych pomiędzy nimi na mapie,
 - statystyki – informacje o połączeniach,
 - alarmy zgodnie z zestawem bazy reguł automatycznych lub dodanych przez analityka,
 - wykryte potencjalne wektory ataków oraz przygotowane podstawowe rekomendacje,
 - rekomendacje dotyczące poprawy bezpieczeństwa sieci i systemów OT/ICS,
 - lista adresów IP biorących udział w komunikacji dwukierunkowej, lista urządzeń będących tylko źródłem komunikacji, lista urządzeń będących tylko celem komunikacji
 - statystyki komunikacji TCP – lista par adresów IP z podaniem kierunku komunikacji (które urządzenie inicjowało połączenia),
 - lista wykrytych podsieci,
 - kierunki komunikacji pomiędzy podsieciami,
 - statystyki dot. ilości linków pomiędzy podsieciami,
 - statystyki dot. ilości danych przesłanych w podsieciach,
 - listy urządzeń przypisanych do zidentyfikowanych producentów,
 - listy urządzeń pogrupowane wg. typu,
 - statystyki dot. zidentyfikowanych protokołów sieciowych TCP i UDP,
 - lista linków logicznych pomiędzy urządzeniami,
 - lista urządzeń z podaniem: nazwy, adresu IP, adresu MAC, producenta, systemu operacyjnego, czy urządzenie znajduje się za routerem, poziomu ryzyka związanego z urządzeniem,
 - statystyki dot. ilości sesji,
 - lista alertów,
 - lista nieaktywnych urządzeń.

- **ocena poziomu bezpieczeństwa sieci i systemów OT/ICS** - obserwacje/rekomendacje wynikające z dobrych praktyk i standardu ISA/IEC 62443,
- **rekomendacje dla sieci i systemów OT/ICS** – analiza, obserwacje i rekomendację będą się odbywać w odniesieniu do standardu ISA/IEC 62443, który określa referencyjną architekturę dla sieci i systemów OT/ICS.

Raport ma zostać przygotowany i przekazany w formie dokumentu oraz elektronicznie, a jego wynik omówiony w ramach dedykowanego spotkania w ramach wideokonferencji.

3. Termin realizacji przedmiotu zamówienia:

Przewidywane zakończenie prac – do 20.12.2024 r.