Departament Dezvoltare Mentenanta
Serviciu Telecomunicatii
Nr 36057/24.09.2024

AVIZAT,

Sef Departament Dezvoltare Mentenanta
Ing.Dan Buzatu
Dan Buzatu
Digitally signed by Dan Buzatu
Date: 2024.09.25 13:49:12 +03'00'

CAIET DE SARCINI

CUPRINS

Cap. 1 Informatii generale

1.1 Tip :[X] Obiectiv investiții/[ ] Lucrare/[ ] Serviciu/[ ] Produs

1.2 Denumire: Modernizare sistem de securitate cibernetica retea telecomunicatii

1.3 Beneficiar: CONPET SA

1.4 Scop: prin proiectul actual se urmareste ridicarea nivelului de protectie a datelor IT+OT transmise din punctele de lucru catre Sediul Central.

1.5 Date de identificare

1.5.1 Amplasament (descriere, particularități) – prin proiectul actual se urmareste instalarea in punctele de lucru a unor echipamente hardware si software de protectie cibernetica.

Cap. 2 Descriere

Prezentul Caiet de Sarcini contine principalele cerinte minimale ce trebuie indeplinite de catre Ofertant in vederea contractarii serviciilor de proiectare, furnizare, configurare si instalare a unei solutii de securitate cibernetica pentru datele transmise din punctele de lucru ale Beneficiarului catre Sediul Central al acestuia. Transmiterea datelor din aceste locatii se efectueaza prin reteaua proprie de telecomunicatii a Beneficiarului (fibra optica si radiorelee in microunde) si prin conexiuni terte VPN, puse la dispozitie de Beneficiar.

Cap. 3 Specificatii Tehnice

3.1 Generalitati

3.1.1 Execuția lucrărilor trebuie să fie realizată în conformitate cu prevederile standardelor de calitate și a legislației în vigoare.

3.1.2 Prezentele specificații nu înlocuiesc celelalte acte normative legislative și de execuție care vor trebui să fie cunoscute și respectate pe parcursul desfășurării lucrărilor.

3.1.3 Înaintea întocmirii ofertei, Ofertantul va vizita amplasamentul lucrărilor (minim 3 locatii) și va prezenta în acest sens un document vizat de reprezentantii desemnati ai Beneficiarului, care să confirme faptul că și-a însușit condițiile din teren privind execuția lucrărilor. In lipsa acestui document Oferta va fi declarata neconforma.

3.1.4 Oferta trebuie să fie prezentată atât pe hârtie cât și în format electronic .

3.1.5 Beneficiarul detine si poate pune la dispozitie pentru integrare in acest proiect urmatoarele resurse:

1. Server Maguay eXpert 242-S-2U – 1 buc
2. Windows Server 2022 – 1 buc
3. Router AT-R4050S - 1buc
4. Advantech ECU-4784-E3 – 10 buc
5. Nozomi Guardian Appliance NS1-100 – 1 buc
6. Nozomi Virtual Remote collector – 5 buc
7. Palo Alto Panorama - 1 buc
8. Palo Alto Virtual NGFW – 11 buc

Toate aceste resurse se afla sub contract de garantie si suport pana la data de 15.12.2024. Toate aceste resurse sunt instalate si configurate in locatii din Tabelul 2 de mai jos.

In cazul in care Ofertantul doreste sa le integreze in solutia propusa, oferta va include costurile pentru upgrade software la ultimele versiuni, integrare in solutia propusa (inclusiv in sistemele de management centralizat solicitate la 3.3.16), prelungire garantie (inclusiv continuitate), suport si licente conform cap. 3.8 din prezentul Caiet de Sarcini.

3.2. Prezentarea ofertei

3.2.1 Toate cerințele prezentului Caiet de Sarcini trebuie să fie îndeplinite de către ofertanți. Ofertele care nu respectă oricare dintre aceste cerințe vor fi declarate neconforme.

3.2.2 Oferta trebuie să fie structurată pe formatul și numerotarea prezentului Caiet de Sarcini.

3.2.3 Răspunsurile trebuie să confirme punctual îndeplinirea tuturor cerințelor din fiecare poziție și paragraf din Caietul de Sarcini și fiecare afirmație de conformitate **trebuie** susținută de Ofertant cu trimiteri clare la specificațiile care certifică conformitatea declarată indicând explicit documentul, manualul, pagina, articolul, paragraful, figura, certificatul, etc. Vor

fi incluse copii de documente relevante în fiecare caz. Nu este suficient un raspuns gen « conform », « de acord » etc. In plus va fi mentionata licenta de producator care indeplineste fiecare functionalitate/cerinta in parte.

3.2.4 Oferta va contine obligatoriu preturile detaliate pentru fiecare modul echipament/hardware/software/licenta/server/etc din fiecare locatie. Oferta va contine obligatoriu preturile pentru instalarea tuturor echipamentelor din fiecare locatie. Oferta va fi transmisa si in format editabil Excel.

3.2.5 Oferta va contine fisele tehnice si detalii despre rolul si functionarea fiecarui echipament hardware/software din solutia ofertata.

3.2.6 Oferta va contine detalii clare despre necesitatea si functionalitatea fiecarei licente in parte.

3.2.7. Oferta va fi intocmita conform Tabelului 1 de mai jos :

Denumire	Cantitate	Pret Unitar	Locatia 1	…..	Locatia 59	Pret total
Proiectare						
Echipamente si software, instalare echipamente/configurare software						
Teste de acceptanta						
Instruire personal						
Documentatie "As-built"						

3.2.8 Oferta trebuie sa contina schema bloc logica si fizica a echipamentelor ofertate si a legaturilor de date aferente din locatia 12 din Tabelul 2 de mai jos. Schema bloc logica si fizica trebuie sa detalieze modul de lucru al arhitecturii de management si de date, inclusiv catre locatiile adiacente.

3.2.9 Oferta trebuie să fie prezentată în limba română. Documentația tehnică ce însoțește oferta trebuie să fie prezentată în limba română sau engleză.

3.2.10 In scopul indeplinirii cerintelor Directivei (EU) 2022/2555 (Directiva NIS2), solutia ofertata trebuie sa furnizeze urmatoarele functionalitati:

- Inventarierea echipamentelor
- Detectarea amenintarilor
- Segmentarea retelei si monitorizarea traficului
- Evaluarea si Managementul permanent al riscurilor
- Prevenirea, Detectarea si Raspunsul la incidente
- Continuitate a business-ului

Oferta va detalia modalitatea in care produsele incluse (NGFW, SAD si aplicatiile de management aferente) contribuie la indeplinirea acestor functionalitati.

3.3 Scopul Serviciilor

3.3.1 Acest Caiet de Sarcini se refera la contractarea serviciilor de proiectare, furnizare, instalare si configurare a unei Soluții de securitate a datelor (SCADA, Leak Detection, Sistem Cantare, Intranet, Voip, Supraveghere Video, Videoconferinta, UPS, Climatizare, etc) din locatiile distante si va avea în componența sa toate modulele/echipamentele/licențele/serverele/etc. necesare functionarii Solutiei conform specificatiilor de mai jos.

3.3.2 Toate licentele ofertate vor avea o valabilitate de minim 5 ani. La expirarea licentelor, solutia propusa va permite in continuare traficul de date intre locatiile distante si locatia 12 din Tabelul 2 de mai jos.

3.3.3 Termenul de 5 ani se considera incepand de la data semnarii Procesului Verbal de Receptie la Terminarea Lucrarilor prevazut la cap. 3.7.

3.3.4 Solutia de Securitate va avea o arhitectura distribuita, care va împiedica atacurile cibernetice la nivelul locatiilor distante si a punctelor de acces. Aceasta va consta in instalarea in locatii a unor module hardware/software care sa permita implementarea diverselor functii de securitate.

3.3.5 Locatiile ce fac obiectul proiectului sunt cele din Tabelul 2 de mai jos. Toate porturile vor fi RJ45 1 Gb.

	LOCATIE	**NGFW**	**SAD**	**ALIMENTARE**
1	Ticleni	1	1	48 V cc

2	Barbatesti	1	1	48 V cc
3	Orlesti	1	1	48 V cc
4	Leleasca	1	0	48 V cc
5	Otesti	1	1	48 V cc
6	Poiana Lacului	1	1	48 V cc
7	Oarja	1	0	48 V cc
8	Saru	1	0	48 V cc
9	Siliste	1	1	48 V cc
10	Moreni	1	1	48 V cc
11	Baicoi	1	1	48 V cc
12	Ploiesti Garaj	1	0	48 cc+220 ca
13	Ploiesti 1848	1	0	48 cc+220 ca
14	Ploiesti CD	1	1	48 V cc
15	Arpechim	1	1	48 V cc
16	Petrobrazi Depozit	1	0	48 V cc
17	Petrobrazi	1	1	48 V cc
18	Petrotel	1	1	48 V cc
19	Ghercesti	1	1	48 V cc
20	Icoana	1	1	48 V cc
21	Cartojani	1	1	48 V cc
22	Videle	1	1	48 V cc
23	Mavrodin	1	1	48 V cc
24	Calareti	1	1	48 V cc
25	Baraganu	1	1	48 V cc
26	Borcea C3	1	1	48 V cc
27	Borcea C4	1	1	48 V cc
28	Cernavoda C1	1	1	48 V cc
29	Cernavoda C2	1	1	48 V cc
30	Nisipari	1	1	48 V cc
31	Petromidia	1	1	48 V cc
32	Constanta Sud	1	1	48 V cc
33	Martinesti	1	0	48 V cc
34	Moinesti	1	0	48 V cc
35	Lucacesti	1	1	48 V cc
36	Biled	1	1	220 ca
37	Boldesti	1	1	220 V ca
38	Bucsani	1	0	220 V ca
39	Inotesti	1	0	220 V ca
40	Madulari	1	1	220 V ca
41	Parc Gara Vest	1	1	220 V ca
42	Urlati	1	1	220 V ca
43	Totea	1	0	220 V ca
44	R. Moinesti	1	0	220 V ca
45	R. Berca	1	0	220 V ca
46	R. Independenta	1	1	220 V ca
47	Statia Urziceni	1	1	220 V ca
48	R.Suplac	1	0	220 V ca

49	R.Marghita	1	1	220 V ca
50	R. Pecica	1	1	220 V ca
51	R. Salonta	1	0	220 V ca
52	R. Imeci	1	0	220 Vca
53	R. Ciresu	1	1	48 V cc
54	SatChinez	1	1	220 V ca
55	Mislea	1	1	220 V ca
56	Potlogi	1	1	48 V cc
57	Ochiuri	1	1	220 V ca
58	Slobozia PH	1	1	220 V ca
59	Sistem Teste	1	1	48 V cc

Legenda :

NGFW=modul hardware/software Next Generation Firewall

SAD= modul hardware/software SCADA Anomaly Detection hardware/software de colectare a datelor SCADA.

3.3.6 In toate locatiile exista rack-uri de telecomunicatii cu spatiu liber pentru instalare echipamente si cu alimentare energie electrica 220 V ca / 48 V cc. In toate locatiile exista instalate echipamente de telecomunicatii care realizeaza agregarea si transmiterea datelor catre locatia 12 din Tabelul 2. Echipamentele ce vor fi instalate in acest proiect vor trebui sa fie conectate Ethernet Layer 3 « up-link » cu echipamentele de telecomunicatii existente si « down-link » catre echipamentele locale tip switch IT, SCADA, telefoane Voip, etc.

3.3.7 Modulele NGFW+SAD de mai sus pot fi ofertate in varianta hardware sau virtualizate software (pe mediu Linux) pe un device hardware. In ambele variante, hardware-ul ofertat pentru fiecare locatie (cu exceptia locatiei 12) trebuie sa respecte urmatoarele cerinte:

- temperatura de functionare -20 +60 ℃ (IEC 60068-2-1, IEC 60068-2-2)
- racire pasiva (fara ventilatoare)
- putere consumata maxima totala 60 W (cumulat NGFW+SAD)
- 10 porturi LAN/WAN RJ45 1Gb (cumulat NGFW+SAD)
- certificate IEC 61850-3 si IEEE 1613
- sa includa toate accesoriile de montaj in rack 19”
- led-uri de stare
- protectie IP30
- protectie la : polaritate inversa, supra si sub-voltaj, curenti de suprasarcina si scurtcircuit, supraincalzire, etc.
- monitorizare local si remote parametri tehnici
- management local si remote prin interfata grafica si linie de comanda.

3.3.8 Modulul NGFW pentru locatia 12 (modulul concentrator pentru toate celelalte locatii) trebuie sa fie ofertat in configuratie HA – practic doua module identice conectate intre ele. Fiecare din cele 2 module va avea cel putin 12 porturi 1Gb RJ45. In situatia in care vor fi ofertate module virtuale, acestea trebuie livrate pe 2 echipamente hardware diferite. Oferta va descrie in detaliu functionarea HA.

3.3.9 Modulul NGFW din locatia 12 va avea o capacitate Threat Protection de minim 3 Gbps.

3.3.10 Toate echipamentele NGFW+SAD vor fi configurate astfel incat la revenirea tensiunii de alimentare dupa o intrerupere accidentala, acestea sa reporneasca automat, fara a fi necesara interventia personalului Beneficiarului.

3.3.11 Solutia in totalitatea sa va functiona « on premise », pe servere ce vor fi livrate de Ofertant. Nu se admite indeplinirea cerintelor prin servicii tip “cloud” extern. Se accepta conexiune catre serverele producatorilor doar pentru update protectie antimalware.Pentru ambele module NFGW si SAD update-urile software/firmware vor fi efectuate offline.

3.3.12 Traficul de date din locatii trebuie sa fie transportat catre/de la locatia 12. In plus, traficul OT trebuie sa poata fi transportat si intre 30% din locatiile din tabel.

3.3.13 Serverele pentru managementul operational si functional al celor 2 tipuri de module de mai sus vor fi instalate in locatia 12 si vor respecta cerinta de functionare in gama de temperatura 0-40 ℃. Serverele vor avea incluse surse de alimentare interna duale redundante.

3.3.14 Echipamentele trebuie sa poata fi manageriate (administrate) in mod securizat local si remote prin interfata grafica si linie de comanda (https, ssh, SNMPv3). Traficul https trebuie sa fie criptat TLS 1.3 . Traficul ssh trebuie sa fie criptat SSH-2. Traficul de management trebuie sa fie separat de traficul de date.

3.3.15 Pentru toate software-urile ce vor fi furnizate, Ofertantul va livra kit-urile de instalare și licențele aferente.

3.3.16 Solutia va furniza functionalitatile de securitate asa cum sunt specificate in sectiunile urmatoare :

A) Functionalitati Modul NGFW:

-filtrarea traficului de intrare si de iesire din locatie pe baza unui set de reguli definit de Beneficiar si trebuie configurat astfel incat sa indeplineasca urmatoarele functionalitati:

- Next Gen Firewall
- Intrusion Prevention System
- Intrusion Detection System
- Application Control
- sa definineasca zone diferite de securitate
- să foloseasca canalul de control securizat și criptat pentru conectare cu managementul centralizat
- sa foloseasca inspectia pachetelor de date (DPI)
- să foloseasca IPSec VPN cu criptare AES256-SHA256
- să asigure protectie impotriva IP spoofing
- sa poata restricționa aplicațiile care folosesc porturi non-standard
- să suporte decriptarea următoarelor protocoale: SSL, SSH
- sa asigure protectie impotriva atacurilor de tip “0-Day”, ransomware, MitM (Man in the Middle), DoS, atacuri evazive, miscari laterale
- să furnizeze ACL bazat pe IP / Port
- să valideze utilizarea autorizata a protocoalelor SCADA suportate
- sa fie furnizate log-uri pentru analiza istoricului de evenimente - aceste log-uri sa poata fi sterse si manual pentru a evita umplerea spatiului de stocare
- sa utilizeze NTP centralizat
- managementul local se va realiza prin conexiune securizata criptata TLS 1.3, SSH-2 sau SNMPv3.

Managementul centralizat al tuturor modulelor NGFW din Tabelul 2 trebuie sa fie configurat astfel incat:
-va permite configurarea in mod centralizat a modulelor din locatii
-va permite implementarea centralizata a politicilor de trafic
-va permite managementul configuratiilor echipamentelor (backup/restore)
-va fi instalat pe un server corespunzator dimensionat sau appliance separat daca acesta este disponibil, ce va fi instalat in locatia 12. Daca se foloseste server cu sistem de operare de sine statator, acesta va fi de tip Linux si va avea instalate solutii de protectie impotriva amenintarilor malware
- va permite configurarea restrictionarii automate a traficul modulului care alerteaza o amenintare
- va include interfata grafica pentru monitorizarea tuturor modulelor instalate
- va evidentia in timp real starea conexiunilor modulelor
- va include functia de remote firmware upgrade
- va permite modificari de configuratii simultan pe multiple echipamente
- va permite conectarea simultana a mai multor utilizatori, minim 5 printr-o conexiune securizata HTTPS
- va avea o capacitate licentiata de management pentru minimum 70 de module NGFW
- va fi capabil sa realizeze in mod automat raportarea, colectarea si managementul log-urilor colectate
- va fi capabil sa realizeze in mod automat corelarea evenimentelor/amenintarilor colectate in vedere detectarii gradului de risc al echipamentelor din retea, a anomaliilor de retea (IP-uri cu activitate suspecta, command-and-control, exploituri cunoscute de vulnerabilitati, etc)
- va avea configuratia serverului/serverelor care sa permita procesarea tuturor evenimentelor și datele de activitate pentru o perioadă de 30 zile
- va include functia de stergere automata loguri la atingerea a 85% din capacitatea de stocare proiectata.

Ofertantul va descrie modul in care sunt implementate cerintele de mai sus si licentele incluse pentru indeplinirea acestora.

B) Functionalitati modul SAD – Scada Anomaly Detection

- colectarea si monitorizarea continua a datelor printr-un senzor local utilizand tehnica « port mirroring »
-transmiterea datelor catre serverul de analiza (Scada Anomaly Detection) se va face in timp real, fara utilizarea unui buffer local
- colectarea datelor de la maxim 5 active OT, maxim 5 Mbps pentru fiecare locatie
- va include optiunea de scanare activa.

Managementul centralizat al tuturor modulelor SAD din Tabelul 2 trebuie sa fie configurat astfel incat:
- va furniza pentru fiecare element al retelei OT cel putin urmatoarele informatii, fara a fi necesare modificari asupra configuratiei acestora si indiferent de protocolul de comunicatie folosit de acestea:
  - producatorul
  - adresa IPv4, adresa MAC
  - tipul elementului: server, endpoint, switch, RTU, PLC, etc, inclusiv sub-modulele componente
  - modelul hardware, versiunea firmware si sistemul de operare

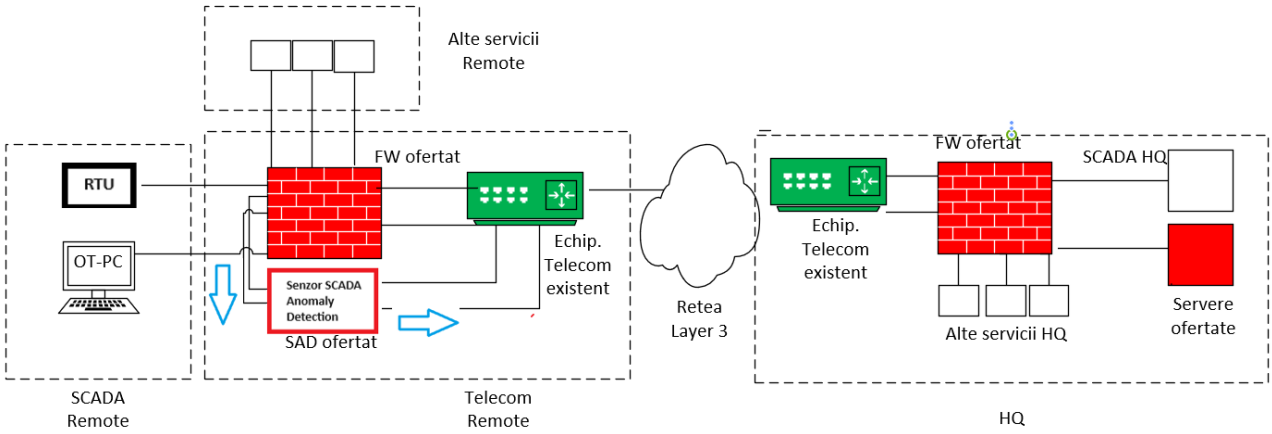
- vulnerabilitatile CVE pe baza informatiilor colectate mai sus
- data primei si ultimei aparitii in retea
- rolul elementului
- protocoalele de comunicatie utilizate
- senzorul local utilizat in detectare
- traficul de date efectuat
- gradul de Infectie, Accesibilitate, Vulnerabilitate, Criticitate

-va descoperi in mod automat elementele retelei OT
- va putea identifica cel putin urmatoarele tipuri de device-uri : switch, router, printer, computer, PLC, HMI, controller, firewall, RTU, server, gateway, OT, IoT, sensor, IED
- va permite definirea de asset-uri custom
- va colecta informatiile in mod pasiv, fara a fi necesara efectuarea de catre Beneficiar a unor configurari/modificari ale functiilor si protocoalelor echipamentelor monitorizate
-va fi compatibil cu echipamentele OT de la principalii producatori: ABB, Siemens, Emerson, Yokogava, Honeywell, Eaton, etc
- va contine baza de date cu dispozitivele detectate in reteaua OT, cu atributele acestora, astfel încât acestea să fie recunoscute automat în timpul analizei
- va permite un mecanism de căutare dupa atributele dispozitivelor, cum ar fi numele dispozitivului, adresa MAC, numele de utilizator al rețelei, adresa IP, tag-uri, adresele IP externe, comenzi SCADA
- va genera automat o hartă a tuturor dispozitivelor monitorizate, pe fiecare layer al modelulului Purdue
- va suporta protocoale de retea pentru identificarea asset-urilor
-va include interfata grafica in care sa fie reprezentate toate device-urile retelei, topologia si sesiunile de date active dintre ele
- va preciza direcția canalelor de comunicații (sursă și destinație)
- va genera statistici ale pachetelor trimise și recepționate de către dispozitive in reteaua OT
- va evidentia in timp real starea conexiunilor
-va identifica asset-urile ce comunica catre exteriorul retelei si le va putea grupa separat
- va identifica tentativele de comunicatie (ghost asset)
-va avea compatibilitate completa cu principalele protocoale SCADA: DNP3, Modbus TCP, Modbus RTU, IEC60870-5-104, IEC60870-5-101, S7,etc
-va permite update-ul senzorilor remote atat pentru patch-uri de securitate cat si versiuni noi de software
- va include posibilitatea de modificare a configuratiei sau analiza activitate din linia de comanda CLI a senzorilor
- va include functia restore a configuratiei modulelor si serverului
- va include interfata grafica pentru monitorizarea tuturor modulelor instalate
- va colecta informatiile indiferent de volumul de date pe care echipamentele monitorizate il genereaza
- va putea fi manageriat prin interfata grafica protocol HTTPS si linie de comanda SSH
- va permite conectarea simultana a mai multor utilizatori, minim 5 printr-o conexiune securizata HTTPS
- va avea o capacitate licentiata de management pentru minimum 50 de module SAD
- va utiliza un server NTP configurabil
- se va integra nativ tehnologic cu Next Gen Firewall-ul de la punctul A). Vor fi prezentate documente care sa ateste aceasta integrare. Se va detalia si configura de catre Ofertant integrarea celor 2 module
- va fi instalat pe un server corespunzator dimensionat sau appliance separat daca acesta este disponibil, ce va fi instalat in locatia 12. Daca se foloseste server cu sistem de operare de sine statator, acesta va fi de tip Linux si va avea instalate solutii de protectie impotriva amenintarilor malware
- va fi capabil să înregistreze evenimentele capturate de pe toate echipamentele retelei OT identificate, pentru o perioadă de 30 zile
- va avea configuratia serverului/serverelor care sa permita procesarea tuturor evenimentelor și datele de activitate pentru o perioadă de 30 zile
- va avea capacitatea de a stoca centralizat logurile și configuratiile tuturor echipamentelor retelei OT pentru o perioadă de 30 zile
-va permite updatarea protectiei antimalware prin incarcare de fisier offline
- va rula in 2 moduri distincte : Learning/Training si Protecting/Operational. Trecerea intre cele 2 moduri sa poata fi efectuata manual/automat
- va inspecta pachetele de date (DPI – Deep Packet Inspection) pentru a arata protocolul de date utilizat si va realiza un profil de trafic SCADA in mod automat; perioada pentru “invatarea” profilului de trafic trebuie sa fie de maxim 30 de zile, cu posibilitatea reinitializarii perioadei de invatare in orice moment in functie de modificarea retelei SCADA si a deciziei Beneficiarului.
- va utiliza regulile Yara, Snort, CVE, MITRE ATT&CK
- va colecta informații, va analiza activitatea comportamentală a rețelei OT și va avea capabilitatea să le folosească pentru a investiga riscurile de securitate
-va detecta si clasifica diferite tipuri de atacuri
-va utiliza algoritmi ML (machine learning) pentru analiza si identificarea diferitelor modele de comportament anormal
-va calcula un scor de risc al intregii retele OT monitorizate
-va genera automat fisiere PCAP pentru analize ulterioare ale evenimentelor/alertelor
-va permite incarcarea in interfata grafica de fisiere PCAP pentru analiza
-va putea utiliza zone distincte in cadrul retelei, definite conform IEC 62443
-va putea calcula un scor de risc pentru fiecare zona IEC 62443
-va detecta diferite tipuri de atacuri, printre care brute force, port scanning, ARP poisoning, SYN flood

-va identifica si analiza riscurile cunoscute pentru calcularea scenariilor in care poate apare un atac
-va analiza traficul si va genera alerte in situatiile in care au fost identificate operatiuni anormale asupra retelei OT
-va trimite alarme prin e-mail catre adrese alese de Beneficiar.Tipul alarmelor trebuie sa fie configurabil si flexibil
-va genera rapoarte configurabile, la cerere sau programate, asupra riscurilor si masurilor de reducere ale acestora
-va permite evaluarea riscurilor conform IEC62443 evidentiind asset-urile si riscurile associate
-va permite gruparea asset-urilor conform zonelor IEC62443 si va determina vectorii de atac probabili
-va permite un plan de reducere a riscurilor conform IEC62443.

Ofertantul va descrie modul in care sunt implementate cerintele de mai sus.

3.3.17 Schema bloc de conectare a modulelor NGFW si SAD dintr-o locatie va fi:



Oferta va include (in plus fata de cablurile si conectica aferente functionarii solutiei) si furnizarea si instalarea a 2 cabluri FTP CAT5E intre echip. Scada Remote si Telecom Remote din fiecare locatie. Lungimea maxima 25 m.

3.3.18 Soluția va fi configurată pentru a efectua backup-uri în mod automat, cel puțin odata pe zi, fără a fi nevoie de intervenția umană. Log-urile vor fi stocate pe serverul aplicatiei, pentru o perioada de minim 30 de zile.

3.3.19 Ofertantul va include o solutie de backup software in ansamblu pentru a putea fi realizate activitati de backup si restore ale tuturor modulelor software livrate si configurate, pentru utilizarea acestora in caz de necesitate (business continuity).Ofertantul va include mediul hardware pentru stocarea backup-urilor.

3.3.20 Ofertantul va livra, instala si configura un server de email pentru a trimite alarmele generate de modulele NGFW+SAD si aplicatiile de management ale acestora prin e-mail catre adrese alese de Beneficiar.Tipul alarmelor trebuie sa fie configurabil si flexibil.

3.3.21 Pentru toate aplicatiile, softurile, echipamentele, etc. furnizate in acest proiect, Beneficiarul va avea acces total la conturile de administrare, configurare, mentenanta si troubleshooting (admin, root, expert, etc).

3.3.22 Pentru acces remote la Managementul centralizat al solutiei, Ofertantul va furniza, configura si instala in locatia 12 un firewall fizic altul decat modulul NGFW prevazut la pct. 3.3.8 utilizat pentru traficul datelor din locatii, de la acelasi producator ca modulele NGFW ofertate, cu cel putin 2 porturi WAN si 6 porturi LAN avand licenta UTM activata pe intreaga perioada de garantie. Beneficiarul va asigura conectivitatea la Internet a acestuia. Accesul va fi realizat printr-o aplicație dedicata, de la acelasi producator al firewall-ului mentionat, cu licență neexpirabila. Aceasta va permite operarea solutiei remote în mod securizat și va include toate modulele/echipamentele/software-urile necesare in acest sens. Pentru operarea solutiei in mod remote Ofertantul va include in oferta 2 buc laptop cu urmatoarele caracteristici minime: display 15” 1920x1080, CPU Intel i5, 32 Gb RAM, 1 Tb SSD, RJ45+wifi 802.11AX, docking station USB-C, HDMI, capacitate baterie min 70 Wh, Windows 11 si antivirus+firewall, greutate max. 1.8 kg, kit mouse+tastatura, rucsac.

3.3.23 Ofertantul trebuie să furnizeze toate bunurile și serviciile descrise aici ca un proiect “la cheie” și trebuie să își asume responsabilitatea completă pentru proiectarea, livrarea, instalarea, testarea, configurarea și acceptanța echipamentelor și aplicațiilor asociate așa cum sunt specificate în acest Caiet de Sarcini.

3.3.24 Ofertantul trebuie să furnizeze toate materialele, echipamentele, sculele, ingineria, calificarea şi forţa de muncă necesare pentru a îndeplini în totalitate și în timp util cerinţele din acest Caiet de Sarcini.

3.3.25 Ofertantul va livra kit-urile de instalare si licentele pentru toate software-urile furnizate.

3.3.26 Pe parcursul evaluarii ofertelor, la solicitarea Beneficiarului, Ofertantul va pune la dispozitia acestuia acces la conturi demo/laborator pentru verificarea functionalitatilor de la pct. 3.3.16.

3.4 Livrări

3.4.1 Toate echipamentele furnizate, inclusiv materialele pentru instalare trebuie să fie noi, neutilizate, de cea mai înaltă calitate, nedeteriorate, de fabricaţie recentă, sau de un tip fabricat în prezent. Pentru toate acestea Ofertantul va prezenta documente ale producatorilor din care sa reiasa ca echipamentele hardware/software livrate nu sunt declarate « End of Life » la data depunerii ofertei.

3.4.2 Orice element/modul/licență/funcționalitate/accesoriu (de exemplu: aplicatie, surse de energie, cablu alimentare, etc.) care lipsește din ofertă și care ulterior semnarii contractului se va dovedi necesar pentru îndeplinirea cerințelor prezentului Caiet de Sarcini, va fi furnizat fără nici un cost suplimentar pentru Beneficiar.

3.5 Servicii de proiectare, instalare, testare

3.5.1 Servicii de proiectare trafic și management

3.5.1.1 Ofertantul trebuie sa furnizeze documentatii de proiectare fizica si logica de detaliu ale solutiei pe fiecare locatie, diagrame bloc pe fiecare locatie, connectivitatea logica si fizica a canalelor de date si management. Informatia trebuie furnizata in format electronic editabil Microsoft Visio si Microsoft Word.

3.5.1.2 Ofertantul trebuie să furnizeze access la manualele de producator complete, detaliate, incluzând proceduri “step by step” de instalare, operare, configurare, programare, administrare și troubleshooting pentru echipamentele/software-urile livrate.

3.5.2 Servicii de instalare

3.5.2.1 Toate lucrările de instalare (Hardware & Software) trebuie să fie efectuate în conformitate cu legile românesti, standardele naţionale şi internaţionale şi cu specificaţiile de producător.

3.5.2.2 Instalarea trebuie să fie în conformitate cu cele mai bune practici industriale actuale.

3.5.2.3 La incheierea lucrarilor de instalare dintr-o locatie se va semna un Proces Verbal de Instalare Echipamente.

3.5.2.4 Ofertantul este responsabil pentru materialele achiziționate de către Beneficiar până la semnare Proces Verbal de Instalare Echipamente.

3.5.2.5 Ofertantul trebuie să colecteze de la depozitul său şi trebuie să transporte pe locatie echipamentul necesar şi materialele pentru instalatii.

3.5.2.6 La finalizarea lucrărilor, întreaga zonă de lucru trebuie să fie lăsată curată și liberă de gunoi, praf, resturi şi materiale în exces.

3.5.2.7 Ofertantul trebuie să documenteze instalarea cu imagini, pentru fiecare locatie in parte. Din imagine trebuie sa poata fi identificate etichetele cablurilor si porturile conectate.

3.5.2.8 Toate lucrarile de instalari si configurari se vor desfasura sub directa supraveghere a Beneficiarului.

3.5.3 Teste de acceptanţă

3.5.3.1 Ofertantul va include in oferta procedura de verificare pentru acceptanță, care va include teste pentru toate functionalitatile solicitate prin Caietul de Sarcini. Procedura va detalia modalitatea de testare pentru fiecare functionalitate. Procedura poate fi revizuita pe parcursul implementarii proiectului si validata de Beneficiar cu 30 de zile înainte de efectuarea testelor de acceptanță.

3.5.3.2 Acceptanța trebuie să asigure că Solutia livrata:
• Este instalata corect conform documentatie producator
• Este configurata corect conform documentatie producator, informatiilor de proiectare si necesitatii Beneficiarului
• Toate functionalitatile cerute prin prezentul Caiet de Sarcini sunt personalizate pentru prezentul proiect
• Operează fara erori.

3.5.3.3 Lista minima a testelor ce vor fi efectuate:

A) Teste pentru verificarea corectitudinii implementarii pentru fiecare din modulele NGF+ SAD:
1. Verificari hardware pentru toate echipamentele livrate si instalate
2. Verificari software pentru toate aplicatiile livrate si instalate
3. Verificari configurari conform proiect tehnic

4. Verificari licente conform proiect
5. Verificari documentatie “As-built”
6. Verificare functii de backup si restore a tuturor modulelor si in ansamblu
7. Verificari SLA-uri
8. Verificare offline update
9. Verificare configurari loguri evenimente
10. Verificare management centralizat conform proiect tehnic
11. Verificare migrare servicii in afara solutiei, in caz de defect
12. Verificare stocare log-uri 30 zile

B) Teste pentru verificarea functionalitatii modulului NGFW:

13. Verificare separare retele securizate de retele nesecurizate
14. Verificare filtrare access Internet si Intranet
15. Verificare criptare canal de control
16. Verificare conexiuni IPSec VPN
17. Verificare IP spoofing
18. Verificare ACL IP/port/MAC/user
19. Verificare controlul aplicatiilor si filtrare url
20. Verificarea utilizarii porturilor corecte de catre aplicatii
21. Verificarea utilizarii protocoalelor validate
22. Verificare IPS/IDS
23. Verificare validare comunicatie securizata L3
24. Verificare detectare evenimente ne-uzuale
25. Verificare functionare DPI
26. Verificare monitorizare conexiuni
27. Verificare detectare conectari nereusite la retea
28. Verificare detectare noi comunicatii interne
29. Verificare detectare scanare adrese si porturi
30. Verificare detectare traffic “duplicate IP”
31. Verificare detectare transfer fiziere .exe si .rar
32. Verificare detectare format fisiere invalide
33. Verificare detectare conectari porturi ne-standard
34. Verificare prevenire atacuri MitM
35. Verificare prevenire atacuri Denial of Service
36. Verificare prevenire mutari laterale
37. Verificare descoperire atacuri evasive
38. Verificare descoperire atacuri bazate pe script-uri
39. Verificare prevenire atacuri brute force.
40. Verificare analizei log-urilor colectate
41. Verificarea corelarii evenimentelor/amenintarilor detectate

C) Teste pentru verificarea functionalitatii modulului SAD:

42. Verificare analiza header-e trafic SCADA
43. Verificare criptare canal de control
44. Verificare detectare evenimente ne-uzuale.
45. Verificare detectare directie comunicatie si statistici
46. Verificare detectare echipamente externe
47. Verificare generare harta asset-uri
48. Verificare utilizare protocoale validate
49. Verificare detectare asset-uri si atributele acestora
50. Verificare functionare cautare asset-uri
51. Verificare suport protocoale conform proiect tehnic
52. Verificare detectare trafic “duplicate IP”
53. Verificare detectare conectari nereusite la retea
54. Verificare detectare noi comunicatii interne
55. Verificare analiza vectori de atac

D) Teste pentru verificarea functionalitatii solutiei in ansamblu (pentru toate modulele):

56. Verificare detectare restart device-uri
57. Verificare monitorizare incarcare sisteme
58. Verificare configurare NTP
59. Verificare generare notificari access useri
60. Verificare realizare back-up-uri automate
61. Verificare generare rapoarte

3.5.4 Managementul Proiectului

3.5.4.1 Ofertantul va fi responsabil de planificarea, urmărirea şi coordonarea proiectului incluzând, dacă este cazul, şi planificarea și urmărirea lucrărilor subcontractorilor. Ofertantul va solicita aprobarea Beneficiarului pentru înlocuirea oricărui subcontractor.

3.5.4.2 Ofertantul va trebui sa prezinte in echipa dedicata pentru acest proiect personal certificat pentru derularea activitatilor de implementare, administrare si mentenanta a echipamentelor hardware si software livrate.

3.5.4.3 Ofertantul trebuie să desemneze un Project Manager al cărui CV trebuie să fie anexat documentaţiei de calificare şi care trebuie să evidenţieze studiile relevante şi experienţa persoanei desemnate în managementul unor proiecte similare ca obiect şi amploare. Componența echipei prezentată în ofertă va putea fi schimbată numai cu aprobarea Beneficiarului.

3.5.4.4 Minute ale întalnirilor Ofertant-Beneficiar trebuie să fie întocmite de către Ofertant şi vor fi disponibile ca bază pentru deciziile luate la reuniunile periodice de progres.

3.6 Training

3.6.1 Trainingul trebuie sa se desfasoare inaintea activitatilor de instalare (se va desfasura on-line, cu personal/instructor certificat de producator pentru aceasta activitate) si va fi efectuat pentru fiecare din modulele NGFW si SAD.

3.6.2 Trainingul va detalia pas cu pas activitatile ce se executa, in ceea ce priveste instalarea, configurarea, integrarea, utilizarea, mentenanta si troubleshooting-ul echipamentelor si a aplicatiilor de management ale acestora.

3.6.3 Training-ul va fi furnizat pentru un numar de maxim 4 persoane pentru modulul NGFW si 6 persoane pentru modulul SAD. Oferta va contine cursurile standard ale producatorului pentru echipamentele furnizate. Training-ul va fi cel dedicat pentru ingineri/experti/administratori pentru implementare/configurare/administrare/mentenanta/management/ troubleshooting (inclusiv cursuri pregatitoare daca este cazul) pentru echipamentele si software-urile furnizate. Oferta va include costurile pentru certificari si examinari in vederea administrarii solutiei.

3.7 Receptia la terminarea lucrarilor

3.7.1 Termenul de finalizare a serviciilor din Caietul de Sarcini se consideră împlinit la data semnării fără obiecțiuni de către Comisia de recepție a Procesului Verbal de Recepție la Terminarea Lucrarilor, după terminarea ultimului test de acceptanță prevazut la 3.5.3.

3.7.2 Ofertantul va comunica Beneficiarului data finalizării lucrarilor transmițându-i acestuia, pentru confirmare, o înștiințare scrisă. Ofertantul are obligația de a livra cu 30 de zile inainte de finalizarea lucrarilor documentatia tehnica a Solutiei, respectiv „As built". Documentatia „As built" va include proceduri scrise detaliate ale operațiilor necesar a fi efectuate de Beneficiar pentru utilizarea cu succes a soluției. Documentatia "As built" va contine deasemenea arhitectura detaliata a tuturor componentelor solutiei livrate si a conexiunilor interne, pentru fiecare locatie. Ofertantul va furniza deasemenea manualul conținând toate comenzile CLI necesare în configurarea, operarea, mentenanța si administrarea soluției.Ofertantul va furniza o procedura prin care traficul din locatiile distante sa treaca prin bypass in caz de defect al echipamentului din locatii distante.

3.7.3. Beneficiarul va organiza recepția în maximum 5 zile de la notificarea finalizării lucrarilor și va comunica Ofertantului data stabilită.

3.7.4 Comisia de recepție trebuie să verifice execuția tuturor lucrărilor conform prevederilor contractuale și documentației anexate la contract, după care întocmeste "Procesul Verbal de Recepție la Terminarea Lucrarilor" și recomandă admiterea cu sau fără obiecțiuni a recepției, amânarea sau respingerea ei, conform modului de îndeplinire a condițiilor contractuale.

3.8. Garanţie

3.8.1 Ofertantul trebuie să furnizeze Beneficiarului garanție comerciala de 5 ani de la data semnării Procesului Verbal de Recepție la Terminarea Lucrarilor pentru toate echipamentele furnizate, modulele hard/soft, licențele și lucrările efectuate.
3.8.2 Acestă garanție trebuie să includă repararea sau înlocuirea oricărui echipament, subsistem, hardware și/sau software care s-a defectat în condiții normale de uzură și de utilizare. Această activitate va include montarea/demontarea și transportul aferent.

3.8.3 In perioada de garantie Beneficiarul va avea la dispozitie posibilitatea de deschidere de tichete de asistenta direct la serviciile de suport ale producatorilor/distribuitorilor echipamentelor ofertate, 24/7. Ofertantul va trebui sa respecte urmatorii timpi, in functie de nivelul de prioritate al incidentului:

Nivel prioritate	**Timp de raspuns**	**Timp solutie provizorie**	**Timp solutie definitiva**
Urgent	1 ora	4 ore	24 ore

Critic	4 ore	24 ore	48 ore
Major	8 ore	24 ore	48 ore
Minor	24 ore	48 ore	72 ore

definite astfel:

a) Urgent - mai multe servicii/echipamente din reteaua Beneficiarului sunt indisponibile
b) Critic – un serviciu/echipament din reteaua Beneficiarului este indisponibil
c) Major – unul sau mai multe servicii/echipamente prezinta erori in functionare
d) Minor – nu este afectata functionalitatea serviciilor/echipamentelor

3.8.4 Oferta va include detalii despre serviciile de suport ale producatorilor/distribuitorilor si va evidentia tipul de suport inclus. Ofertantul va deschide la producatori conturi pe numele Beneficiarului si va acorda acestuia acces total la aceste conturi.

3.8.5 In perioada de garantie Ofertantul va oferi suport gratuit in operarea si mentenanta solutiei.

3.8.6 Ofertantul trebuie să organizeze şi să furnizeze intervenţie pe site/remote în maxim 8 ore (business hours) atunci când este semnalată de către Beneficiar nefuncționarea sau funcționarea defectuoasă a echipamentelor. Ofertantul trebuie să presteze servicii swap de reparare prin schimbare pe site, cu un timp de swap de maxim 2 zile.Oferta va contine specificatiile producatorilor pentru serviciul “Next Business Day Replacement”.

3.8.7 Ofertantul trebuie să anexeze la oferta tehnică documentul „Propunere pentru asigurarea intervenţiei în amplasamente, în perioada de garanţie”, în care trebuie să descrie în detaliu modalităţile prin care va asigura îndeplinirea timpilor de remediere asumaţi.

3.8.8 Acolo unde o functionare defectuoasă a fost corectată, înlăturată sau înlocuită în garanție, perioada de garanție corespunzătoare acestei lucrări va fi extinsă cu perioada de nefuncționare după ce această corecție de înlăturare și înlocuire a fost îndeplinită cu succes.

3.8.9 Pe perioada garantiei Ofertantul trebuie să furnizeze atat upgrade-uri cat si update-uri/patch-uri pentru toate software-urile livrate si pentru protectia antimalware. Ofertantul va oferi suport gratuit pentru instalarea si configurarea acestora.

3.9 Etapizarea lucrărilor

3.9.1 Proiectare integrala detaliata a solutiei- in termen de 2 luni de la semnarea contractului.

3.9.2 Livrare echipamente/software – in termen de 4 luni de la semnarea contractului.

3.9.3 Instalare echipamente si integrare software – in termen de 8 luni de la livrarea echipamentelor.

3.9.4 Teste de acceptanță și predare documentație As built – 4 luni de la terminarea lucrărilor de instalare. In cazul respingerii unora dintre testele de acceptanta, problemele semnalate trebuie remediate in termen de maxim 5 zile. Dupa aceasta testele de acceptanta vor fi reluate in integralitatea lor. Procedura se repeta pana la finalizarea cu succes a tuturor testelor. Beneficiarul nu accepta prelungirea termenului de executie a contractului datorita eventualelor repetari ale testelor de acceptanta.

3.9.5 La solicitarea Ofertantului, Beneficiarul poate aproba decalarea termenelor etapelor intermediare, fără a se modifica termenul final al Contractului.

3.9.6. Termenul de execuție a tuturor serviciilor contractate este de 16 luni de la semnarea contractului.

Şef Serviciu Telecomunicatii

Ing. Laurentiu Dumitru

Laurentiu-Alexandru Dumitru
Digitally signed by Laurentiu-Alexandru Dumitru
Date: 2024.09.25 08:13:54 +03'00'

Intocmit,

Coord. activ.specif.

Ing. Catalin Ruse

Gabriel-Catalin Ruse
Digitally signed by Gabriel-Catalin Ruse
Date: 2024.09.24 14:01:44 +03'00'

Coord. activ.specif

Ing. Iulian Bucur

Iulian Bucur
Digitally signed by Iulian Bucur
Date: 2024.09.24 13:42:31 +03'00'