SECTIUNEA II
CAIET DE SARCINI

CAIET DE SARCINI

Sistem de Securitate retea comunicatii

SPECIFICAȚII TEHNICE

CUPRINS

1. Generalități

1.1 Date Generale

1.1.1 Prezentul Caiet de Sarcini contine principalele cerinte minimale ce trebuie indeplinite de catre ofertant in vederea contractarii serviciilor de proiectare, furnizare, configurare si instalare solutie de securitate a serviciilor Ethernet furnizate prin reteaua de multiplexoare ECI NPT din cadrul Sistemului de Telecomunicatii al CONPET SA.

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

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

1.1.4 Înaintea întocmirii ofertei, Prestatorul va vizita amplasamentul lucrărilor și va prezenta în acest sens un document semnat pe propria răspundere care să confirme faptul că și-a însușit condițiile din teren privind execuția lucrărilor. Lucrările trebuie să se execute în ordinea descrisă în desfășurător (etapizarea lucrărilor).

1.1.5 Oferta trebuie să fie prezentată atât pe hârtie cât și în format electronic « searchable ».

1.2 Denumirea Beneficiarului

Beneficiarul lucrărilor este CONPET SA, cu sediul in Ploiești, Str.Anul 1848 nr.1-3.

1.3 Prezentarea Generala a Sistemului de management multiplexoare ECI Lightsoft

CONPET SA deține și administrează un sistem propriu de comunicații PDH/SDH/Ethernet voce și date, alcătuit din echipamente multiplexoare ECI NPT 1200, 1020 și 1010, întreaga rețea fiind configurată, monitorizată și gestionată cu soluția de management ECI Lightsoft.

1.3.1 Situația actuală: în prezent soluția de management a rețelei de multiplexoare este instalată pe o mașină Oracle, în urmatoarea configurație:

- Hardware - Oracle Sun Server X4-2 având instalat SO Sun Solaris 5.10.
- Software ECI Lightsoft: Element Management System și Network Management System, v.11.2.
- UPS Tripplite 1.5Kva

Soluția este instalată in site-ul Ploiești Garaj, direct conectată la rețeaua de multiplexoare ECI NPT.

2. Prezentarea ofertei

2.1 Toate cerințele prezentului Caiet de Sarcini trebuie să fie îndeplinite de către ofertanți. Ofertele care nu respectă aceste cerințe vor fi excluse din licitație.

2.2 Răspunsurile trebuie să confirme îndeplinirea cerințelor din fiecare poziție și paragraf din Caietul de Sarcini și fiecare afirmație de conformitate trebuie susținută de ofertant cu trimiteri clare la specificațiile de firmă care certifică conformitatea declarată îndicând explicit documentul, manualul, pagina, articolul, paragraful, figura, certificatul, etc. Pot fi înserate și copii de documente relevante în fiecare caz.

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

2.4 Oferta trebuie să fie prezentată în limba română. Documentația tehnică ce insoțește oferta trebuie să fie prezentată în limba română sau engleză.

3. Scopul Serviciilor

3.1 Acest Caiet de Sarcini se refera la proiectarea, furnizarea, configurarea și instalarea unei soluții de securitate a serviciilor Ethernet furnizate prin reteaua de multiplexoare ECI NPT si prin operatori telecom, si va avea în componența sa toate modulele/echipamentele/licențele (permanente neexpirabile)/etc. compatibile cu cele existente in sistemul de management Lightsoft. Prestatorul va actualiza la ultima versiune software disponibila comercial la momentul licitatiei atat echipamentele NPT cat si platforma de management LightSoft. Pentru platforma de management LightSoft se va livra un pachet de software pentru consolidarea securitatii sistemului de operare constand in: actualizari software (patch-uri) pentru

toate defectele si vulnerabilitatile cunoscute al sistemului de operare, reguli de configurare a securitatii, setari avansate pentru autentificarea utilizatorilor, dezactivarea serviciilor pe care sistemul nu le foloseste, intarirea serviciilor esentiale ale sistemului si retelei, detectarea incercarilor de intruziune.

3.2 Solutia de Securitate va avea o arhitectura distribuita, care va împiedica atacurile cibernetice la nivelul punctelor de acces ale infrastructurii operationale, respectiv echipamentele de retea de proces si retea de comunicatii, atat fizice cat si virtuale.
Aceasta va consta in instalarea la nivel de site-uri a unor module HW si SW care sa permita implementarea diverselor functii de Securitate.

3.3 Aceste functii trebuie sa asigure detectarea comportamentului anormal al retelei operationale, descoperirea atacurilor de tip "0-Day", atacuri evazive, atacuri bazate pe script, segregarea retelei pentru prevenirea miscarilor laterale in cazul unei intruziuni, prevenirea atacului de tip MiM (Man in the Middle), DoS, DDoS, Watering hole.

3.4 Solutia trebuie sa ofere o componenta centralizata pentru identificarea si managementul riscurilor de Securitate, bazata pe colectarea, validarea, corelarea si analiza informatiilor primite de la modulele distribuite, si pe care sa le prezinte intr-un mod unitar si agregat, printr-o interfata grafica (GUI). Pentru toate modulele software ce vor fi furnizate, Prestatorul va livra kit-urile de instalare și licențele aferente.

3.5 Solutia de Securitate trebuie sa fie bazata pe o platformă flexibilă, cu capacitatea de a adăuga aplicații de securitate atunci când este necesar, permițând cresterea perimetrului de securizare în faze.

3.6 Pentru modulele distribuite, configuratia hardware minimala va fi compusa din:
- un processor cu minim 4 nuclee si capabilitati hyperthreading (total 8 vCPUs);
- 16GB RAM;
- 64 GB memorie;
- interfete trafic: 4 x 1GE;
- interfete management: Consola, USB, port GE;
- NFVi: KVM-based hypervisor;

Pentru serverul de management al solutiei, configuratia minimala va fi compusa din:
- un procesor cu minim 12 nuclee
- 128 GB RAM
- 1 TB SSD

3.7 In site-urile in care exista instalat echipament ECI NPT Solutia va fi livrata sub forma unui card instalabil in echipamentul NPT 1020/1200; in site-urile fara echipament ECI NPT sau unde configuratia NPT este completa, Solutia va fi furnizata ca dispozitiv/"box" separat, cu dimensiune maxim 2U instalat in rack 19", cu alimentare redundanta ce va fi inclusa in oferta. Functionalitatile si configurarile software ale celor 2 variante vor fi identice.

3.8 Toate functionalitatile de Securitate vor fi implementate in respectivul modul HW. Nu se accepta mai multe echipamente HW intr-un site care sa livreze in mod separat functiile de Securitate cerute.

3.9 Pentru fiecare din site-urile de mai jos, Solutia va folosi actualele conexiuni "up-link" catre reteaua MPLS.

3.10 Soluția de securitate va fi integrata cu Solutia de management a retelei de multiplexoare Lightsoft, care va permite managementul modulelor HW distribuite.
Ofertantul va include in propunerea comerciala toate accesoriile necesare instalarii modulelor HW.

3.11 Dispunerea echipamentelor va fi efectuata conform tabelului de mai jos. In fiecare site Solutia va furniza cate 4 porturi RJ45 1 Gbps pentru serviciile de mai jos.

Nr.crt	Nume site	ECI NPT	Port SCADA	Port Intranet	Port LD
1	Ticleni	1020	2	UNI	1
2	Barbatesti	1020	2	E-NNI	1
3	Orlesti	1020	2	E-NNI	1
4	Otesti	1020	2	UNI	1
5	Leleasca	1020	0	0	1
6	Poiana Lacului	1200	2	E-NNI	1
7	Arpechim	1020	1	UNI	1
8	Oarja	1020	0	0	1
9	Saru	1020	0	0	1
10	Siliste	1020	2	E-NNI	1

11	Ghercesti	1020	2	E-NNI	1
12	Icoana	1020	2	UNI	1
13	Cartojani	1020	2	E-NNI	1
14	Potlogi	1020	0	UNI	1
15	Videle	1020	2	UNI	1
16	Petrobrazi	1020	2	UNI	1
17	Petrobrazi Depo	1020	2	UNI	
18	Ploiesti CD	1020	**ROOT**		**ROOT**
19	Ploiesti 1848	1200		**ROOT**	
20	Petrotel	1020	2	UNI	1
21	Lucacesti	1020	2	UNI	
22	Ciresu	1020	0	UNI	
23	Calareti	1020	2	E-NNI	1
24	Baraganu	1020	2	E-NNI	1
25	Borcea C4	1020	1	UNI	1
26	Borcea C3	1020	1	UNI	1
27	Cernavoda C2	1020	1	UNI	1
28	Cernavoda C1	1020	1	UNI	1
29	Nisipari	1020	1	UNI	1
30	Constanta	1020	2	E-NNI	1
31	Baicoi	1020	1	E-NNI	
32	Moinesti	1020	0	E-NNI	
33	Moreni	1020	1	E-NNI	1
34	Petromidia	1020	1	UNI	1
35	Biled	nu	2	UNI	
36	Marghita	nu	0	UNI	
37	Pecica	nu	0	UNI	
38	Suplacu de Barcau	nu	0	UNI	
39	Rampa Independenta	nu	0	UNI	
40	Statia Urlati	nu	1	UNI	1
41	Depozit Inotesti	nu	0	UNI	
42	Totea	nu	0	0	1
43	Parc Gara Vest	nu	0	0	1
44	Bucsani	nu	0	0	1
45	Mavrodin	nu	1	0	1
46	Madulari	nu	1	0	1
47	Boldesti	nu	1	UNI	1

Nota: In tabelul de mai sus,
Port SCADA = Numarul canalelor ethernet SCADA necesar a fi transportate la site-ul Ploiesti CD.
Port Intranet = Tipul portului ethernet IT folosit in locatie: E-NNI= port trunk switch L2 existent, UNI = port acces, PC conectat direct la NPT, sau operator. Datele sunt transportate la site-ul Ploiesti 1848
Port LD = Numarul canalelor Ethernet utilizate pentru Leak Detection necesar a fi transportate la site-ul Ploiesti CD.
La site-ul Ploiesti CD vor fi instalate module pentru preluarea traficului SCADA si LD din locatiile fara echipament ECI NPT.
La site-ul Ploiesti Garage vor fi instalate module pentru preluarea traficului Intranet din locatiile fara echipament ECI NPT.

3.12 Solutia trebuie să colecteze datele în modul pasiv.

3.13 Solutia trebuie să aibă capacitatea de a utiliza mai multe imagini NPT/Lightsoft OS care să permita revenirea la o versiune anterioara in timpul upgrade-urilor software.
Solutia trebuie să aibă memorie locală pentru a păstra diferitele log-uri.

Solutia trebuie să poată realiza capturarea tuturor pachetelor Ethernet ale traficului infectat și sa le trimita catre alte aplicații pentru analiză.

3.14 Solutia trebuie sa fie capabila să înregistreze evenimentele capturate de pe toate echipamentele retelei operationale identificate, pentru o perioadă de 6 luni.
Solutia trebuie sa aiba configuratia serverului care sa permita procesarea tuturor evenimentelor și datele de activitate pentru o perioadă de 6 luni.
Solutia trebuie sa aiba capacitatea de a stoca centralizat logurile și configuratiile tuturor echipamentelor retelei operationale și trebuie să le poata trimite către serverul central de colectare a logurilor, pentru o perioadă de 6 luni.

3.15 In fiecare din site-urile din tabelul mai sus, in functie de tipul porturilor utilizate Solutia va furniza functionalitatile de Securitate asa cum sunt specificate in sectiunile urmatoare :
A) Functia de Segregare a retelei trebuie sa asigure filtrarea traficului de intrare si de iesire din site pe baza unui set de reguli conform politicii de Securitate a CONPET.
Deasemeni, Solutia trebuie sa indeplineasca urmatoarele functionalitati:

- să separe retelelele securizate de retelele nesecurizate;
- să filtreze accesul la Internet/Intranet;
- să folosească canalul de control securizat și criptat;
- să suporte IPSec VPN, NAT, controlul identitatii;
- să furnizeze o analiză a header-elor;
- să sigure protectie impotriva IP spoofing;
- să ofere managementul de stare în cadrul sesiunii complete (full-session state management);
- să furnizeze ACL bazat pe IP / Port / User;
- să asigure controlul aplicațiilor (application control) prin crearea de politici granulare care identifica, blocheaza sau limiteaza utilizarea unei aplicatii;
- sa valideze că o aplicație este autorizată să utilizeze un port de comunicare specific, pe baza indicatorilor găsiți în header-ul pachetului;
- să valideze utilizarea autorizate a protocoalelor SCADA suportate;
- să ofere o granularitate mai fina pentru definirea politicilor de autorizare, bazate pe protocolul SCADA specific, precum și setul de comenzi autorizate din cadrul acelui protocol și chiar și intervalul autorizat al parametrilor de comandă;
- să furnizeze IPS (Intrusion Prevention) împotriva traficului de rețea rău intenționat și nedorit. Modulul IPS trebuie actualizat în mod regulat cu noi mijloace de apărare împotriva amenințărilor emergente. Trebuie să fie posibilă actualizarea IPS online.
- Soluția solicitată trebuie să fie capabilă să inspecteze, să scaneze și să securizeze traficul criptat SSL care trece prin gateway.
- trebuie să fie posibilă actualizarea tuturor platformelor distribuite offline dintr-o locație centralizată.
- trebuie sa fie furnizate log-uri pentrua analiza istoricului de evenimente

Toate site-urile vor fi gestionate de la o singură stație centralizată de management. În cazul în care este necesar hardware sau software suplimentar, ofertantul trebuie să îl includă în oferta tehnica si comerciala.
Ofertantul trebuie sa ofere o descriere a solutiei.

B) Functia de Criptare trebuie sa asigure securizarea arhitecturii de comunicatii la nivel L2 si L3 OSI intre site-uri si serverul central.
Soluția solicitată trebuie să fie poata gestiona cheile de criptare.
Nivelul de criptare trebuie să fie cel puțin la fel de puternic ca nivelul de criptare furnizat de AES256.
Canalul de comandă trebuie sa fie securizat și criptat.
Soluția solicitată trebuie să permită gestionarea cheilor terților.
In ceea ce priveste topologia, Solutia trebuie sa poata cripta orice serviciu in topologie P2P, P2MP, MP2MP.
Ofertantul trebuie sa ofere o descriere a solutiei.
Activarea functiilor **A)** si **B)** pe un port nu trebuie sa duca la scaderea semnificativa a vitezei de transfer a datelor (throughput minim 50%)

C) Functia de detectare a Anomaliilor SCADA trebuie sa detecteze comportamentul si activitatile anormale pentru reteaua operationala SCADA.
Aceasta functie este necesar sa fie complet pasiva si neintruziva, care doar sa analizeze traficul si sa genereze alerte in situatiile in care au fost identificate operatiuni anormale asupra retelei SCADA. Alertele trebuie sa fie trimise in timp real catre platforma centralizata de management si evaluare a riscurilor.
Aceasta trebuie sa inspecteze pachetele de date (DPI – Deep Packet Inspection) pentru a 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 CONPET. Solutia trebuie sa suporte mai multe profile de trafic pentru aceeasi retea.
Deasemeni soluția solicitată trebuie să ruleze pe baza unor reguli care alocă potrivirea profilului de pachete cu semnăturile (IDS) si să poată efectua analiza acestora. Ofertantul trebuie să descrie procesul de analiză.

Solutia trebuie sa fie complet automata, sa nu necesite configurarea unor reguli asemănătoare firewall-ului, nici definirea protocoalelor de monitorizare și a alertelor pe care să le genereze.
Soluția trebuie să specifice direcția canalelor de comunicații (sursă și destinație). Canalul de comanda trebuie securizat si criptat. Solutia trebuie să prezinte statistici ale pachetelor trimise și recepționate de către dispozitive in reteaua operationala.
Solutia trebuie să ofere vizibilitate și să urmărească comunicarea pentru dispozitivele instalate în spatele PLC-urilor (nested devices), cum ar fi dispozitive I/O distante, PLC-uri conectate în serie, IIOT și altele.
Soluția trebuie să genereze automat o hartă a tuturor dispozitivelor monitorizate.
Protocoalele SCADA suportate trebuie sa fie minim IEC-104, Modbus, DNP-3, S7, OPC, Profinet.
Solutia trebuie să reasambleze și să decompileze codul de program utilizat de principalii furnizori de sisteme de automatizare și să urmareasca modificările din secțiunile de cod.
Solutia trebuie să afișeze / detecteze diferențele de coduri la nivel de linie de cod care a fost modificat in programul aplicației.
Solutia trebuie să aibă capacitatea de a vizualiza baza de date cu dispozitivele detectate in reteaua operationala, cu atributele acestora, astfel încât acestea să fie recunoscute automat în timpul analizei. Dispozitivele detectate sa fie atat echipamentele SCADA cat si echipamentele de comunicatii nivel 2 si nivel 3 conectate la reteaua operationala Atributele dispozitivelor pe care sistemul trebuie sa le afiseze sunt: numele, tipul, sistemul de operare, adresa IP, adresa MAC, producătorul și ora la care dispozitivul a fost văzut pentru prima oară în retea și când dispozitivul a fost văzut ultima oară în retea.
Solutia trebuie sa permita 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.
Solutia trebuie să poată defini propriile descrieri (marcare) pentru dispozitivele din rețea pentru o căutare și identificare mai bună. Sistemul trebuie să permită căutarea de tip text a obiectelor din rețea și ulterior sa afiseze activitatea respectivelor dispozitive in istoricul listelor de activitati.
Solutia trebuie sa defineasca intarzierile introduse de functionalitatile activate pe fiecare canal in parte.

3.16 Solutia trebuie să colecteze informații, să analizeze activitatea comportamentală și activitatea rețelei și să aibă capabilitatea să le folosească pentru a investiga riscurile de securitate pe următoarele valori din rețea:
• Conexiuni de rețea - în cadrul rețelei OT
• Conexiuni de rețea - generale
• Transferuri de date
• Transferuri externe de date
• Transferuri interne de date
• Dispozitive de rețea conectate
• Dispozitive de rețea externe conectate
• Dispozitive interne de rețea conectate
• Conexiuni active
• Detectarea mișcării caracteristice pentru malware
• Detectarea sistemului de operare
• Conexiuni externe active
• Conexiuni interne active
• Evenimente neobișnuite legate de activitatea dispozitivelor
• Broadcasts
• Cereri DNS
• Transfer de date (dispozitiv client)
• Transfer de date (dispozitiv server)
• Transfer de date extern (dispozitiv client)
• Transfer de date extern (dispozitiv server)
• Multicast extern
• Solicitări DNS nereușite
• Transfer intern de date (dispozitiv client)
• Transfer intern de date (dispozitiv server)
• Multicasts
• Noi conexiuni de rețea nereușite din afara rețelei OT
• Noi conexiuni de rețea nereușite în interiorul rețelei OT
• Noi comunicări interne
• Conectari reusite POP3
• Interogări SMB reusite pentru cataloage
• Interogări unice DNS nereușite
• Scanari de adrese în rețea
• Minare Bitcoins
• Modificări de trafic la nivel de servere DNS
• Informații privind abandonarea pachetelor
• Cereri DNS DynDNS
• Cereri DynDNS http
• Cereri DynDNS SSL DNS
• Pierderea excesivă a conexiunilor

- Interogări DNS catre servere externe
- Factor de transfer extern de date (rata de descărcare pentru datele descărcate)
- Factor de transfer intern de date (rata descărcare / descărcate)
- Pachete externe trimise și primite de dispozitiv
- Servere externe PROXY
- Fast Travel Warning - conectari rapide din diferite locații pentru același utilizator
- Transfer fișiere EXE
- Transfer fisiere RAR
- Atacuri asupra server FTP
- Atacuri de tip Heartbleed
- Atacul reusite de tip Heartbleed
- Conectare la un computer fără interogarea serverului DNS pentru numele acestuia
- Formate de fișier invalide
- Timp internal call
- Servere PROXY interne
- Nume invalide de host-uri
- Certificate SSL invalide
- Utilizarea permisiunilor noi pentru un dispozitiv
- Utilizarea de noi aplicații / protocoale pe dispozitiv
- Dispozitive noi
- Comunicarea cu rețeaua TOR
- Scanarea pe porturi
- Modificări în serverele PROXY
- Repornirea dispozitivelor
- Servere conectate la porturi non-standard
- Blocări SMTP
- Încercarea de a ghici parolele prin SSH
- Încărcarea excesivă a sistemelor
- Utilizarea permisiunilor atipice
- Domenii observate
- Observarea adreselor IP
- Acces dispozitive pe baza de MAC, user/pass

Solutia trebuie sa permita analiza vectorilor de atac dintre oricare doua elemente ale retelei operationale.

Functiile de Securitate enumerate mai sus trebuie sa fie disponibile intr-un singur modul HW in fiecare site; Toate licentele necesare vor avea caracter permanent, fara a fi necesara innoirea periodica a acestora

3.17 Toate functiile de Securitate descrise mai sus vor furniza in timp real toate informatiile despre toate incidente de securitate din intreaga retea catre o platforma centralizata. Aceasta platforma centralizata va realiza consolidarea log-urilor evenimentelor primite de la elementele distribuite; agregarea evenimentelor se va face pe baza unor criterii predefinite: tipul atacului, sursa (ce element realizeaza atacul), destinatie (ce element este atacat), intervalul de timp in care a avut loc evenimentul.
Deasemeni platforma centralizata va corela informatiile din surse multiple, inclusiv din surse externe, pentru a detecta amenintarile reale de Securitate si va elimina alertele fals-pozitive, jucand astfel si un rol de preventie. Platforma va realiza analiza si prioritizarea riscurilor pentru amenintarile detectate, prin indentificarea, asignarea si inchiderea alertelor.
Platforma centralizata de detectare a amenintarilor va avea o interfata grafica (GUI) web-based care va afisa starea de Securitate a intregii retele.

3.18 Un alt rol pe care trebuie sa il aiba aceasta platforma este cel de management al echipamentelor/ modulelor distribuite cat si a functiior de securitate, care va consta in:
- controlul si configurarea echipamentelor distribuite;
- activarea si configurarea functiilor de Securitate pe fiecare echipament distribuit ;
- configurarea secventei functiilor de Securitate (service chaining);
- operarea si mentenanta echipamentelor distribuite.
Prestatorul va descrie modul in care sunt implementate cerintele de mai sus.

3.19 Platforma va permite conectarea simultana a mai multor utilizatori, cel putin 5, printr-o conexiune securizata HTTPS/SSL. Autentificarea utilizatorilor trebuie sa se faca pe baza de nume utilizator si parola. Deasemeni este necesar ca alertele si notificarile de Securitate sa fie trimise prin SMS sau email.

3.20 Solutia va fi configurata pentru a se sincroniza cu celelalte aplicatii folosind serverul NTP din Lightsoft.

3.21 Soluția va fi configurată pentru a efectua backup-uri în mod automat, cel puțin de 2 ori pe zi, fără a fi nevoie de intervenția umană.

3.22 Pentru accesul remote la softul de management al solutiei Prestatorul va furniza o aplicație licențiată pentru acces remote. Soluția va permite operarea solutiei remote în mod securizat de pe laptop (sau local prin conectarea laptop-ului in acelasi LAN) și va include toate modulele/echipamentele/software-urile necesare in acest sens. Pentru acces securizat din internet la noul server, Prestatorul va furniza și configura un router Fortinet 60E. Conpet va asigura conectivitatea la Internet a acestuia. Pentru funcționarea noului server timp de 8 ore în caz de cădere a alimentării cu energie electrică, Prestatorul va livra și instala UPS. Echipamentele propuse vor fi montate în rack 19" furnizat și instalat de Prestator.

3.23 Se va stabili de comun acord cu Beneficiarul site-ul în care va fi instalat serverul pe care va rula solutia. Prestatorul va furniza toate modulele necesare (patchcorduri, atenuatoare optice, SFP, convertoare FO, module NPT, etc.) atât pentru interconectarea cu serverul Lightsoft existent instalat în site-ul Ploiești Garaj cât și cu rețeaua ECI NPT sau reteaua operatorului telecom.

3.24 Prestatorul va defini conexiuni redundante Ethernet către site-urile Ploiesti 1848 si Ploiesti CD astfel încât în cazul unor indisponibilități de site/link intre site-ul sursa si Ploiesti 1848/Ploiesti CD să poată fi furnizate în continuare serviciile Ethernet cu toate functionalitatile de Securitate incluse. În acest sens Beneficiarul va pune la dispoziție conexiuni "dark fiber" suficiente. Prestatorul va furniza eventualele module hardware/software necesare realizarii acestei redundante.

3.25 Prestatorul 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, integrarea, și acceptanța echipamentelor și aplicațiilor asociate așa cum sunt specificate în acest Caiet de Sarcini.

3.26 Prestatorul trebuie să furnizeze toate materialele, echipamentele, sculele, ingineria, calificarea și forța de muncă necesare pentru a îndeplini în totalitate și în timp util cerințele din acest Caiet de Sarcini.

4. Livrări

4.1 Toate echipamentele furnizate, inclusiv materialele pentru instalații trebuie să fie noi, neutilizate, de cea mai înaltă calitate, nedeteriorate, de fabricație recentă, sau de un tip fabricat în prezent.

4.2 Orice element/modul/licență/funcționalitate/accesoriu (de exemplu: aplicatie, cartele, cablu alimentare, etc.) care lipsește din ofertă și care se va dovedi necesar pentru îndeplinirea cerințelor prezentului Caiet de Sarcini, trebuie să fie inclus ulterior fără nici un cost suplimentar pentru Beneficiar.

5. Servicii

5.1 Servicii de design trafic și management

Trebuie sa fie furnizate documentatii de proiectare de detaliu ale solutiei, diagrame bloc ale solutiei pe fiecare site, connectivitatea intre site-urile sursa si cele destinatie. Informatia trebuie furnizata in format electronic editabil.

Prestatorul trebuie să furnizeze manualele complete, detaliate, incluzând proceduri "step by step" de instalare, operare, configurare, programare, administrare și troubleshooting pentru echipamentele/software-urile livrate. Manualele vor fi livrate in format electronic.

5.2 Servicii de instalare

Toate lucrările de instalare (Hardware & Software) trebuie să fie efectuate în conformitate cu legile românesti, standardele naționale și internaționale și cu specificațiile de producător. Instalarile trebuie sa fie efectuate de personal certificat de Producatorul Solutiei.

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

Prestatorul este responsabil pentru depozitarea tuturor materialelor achiziționate de către Client până la semnarea procesului verbal de recepție.

Prestatorul trebuie să colecteze de la depozitul său și trebuie să transporte pe site echipamentul necesar și materialele pentru instalatii.

La finalizarea lucrărilor, întreaga zonă de lucru trebuie să fie lăsată curată și liberă de gunoi, praf, resturi și materiale în exces.Toate materialele utilizabile rămase în urma instalărilor vor fi predate Beneficiarului.

Prestatorul trebuie să documenteze instalarea cu imagini.

5.3 Teste de acceptanță operațională

5.3.1 Ofertantul va include in oferta procedura de verificare pentru acceptanță conformă cu specificațiile producătorului solutiei de Securitate cibernetica. Procedura va fi validata de Beneficiar cu 30 de zile înainte de efectuarea testelor de acceptanță operațională. Procedura de acceptanță va include cel puțin următoarele teste:
- Test de functionare corecta a functiei firewall;
- Test de verificare a blocarii protocoalelor SCADA neutilizate;
- Test de verificare a functionarii protectiei DoS, DDoS, MiM;
- Test de verificare a criptarii L2 si L3;
- Test de detectare a anomaliilor in reteaua SCADA;
- Test de verificare a intarzierilor si functionalitatilor pe canalele SCADA;
- Test de penetrare PenTesting;
- Test de masurare a vitezei de transfer a datelor cu functionalitatile activate (throughput);
- Test de verificare a bunei functionări a soluției de Securitate cibernetica, a rețelei de comunicatii cat si a platformei de management asociate.

5.3.2 Acceptanța trebuie să asigure că Solutia livrata:
• Este instalata corect;
• Este configurata corect;
• A trecut toate testele pentru parametrii necesari;
• Operează conform planului, rulează alarme și este error-free;
• Are înregistrate toate datele relevante ale commissioning-ului pentru utilizări viitoare ca referință;

5.4 Training

5.4.1 Trainingul se va desfașura la producatorul solutiei furnizate, pe o durata de minim 10 zile pentru un numar minim de 4 persoane, inainte de inceperea instalarii solutiei. Trainingul va fi efectuat de personal certificat de Producator si va aprofunda situația reală a configurației solutiei ce va fi instalata în cadrul Sistemului de Telecomunicații al Beneficiarului, si nu va contine detalii despre functii/configuratii/solutii ce nu fac obiectul contractului.Trainingul va cuprinde testare finala si certificarea personalului Beneficiarului.
Modulele de training vor consta in:
- Modul 1: Noile functionalitati introduse de ultimele versiuni SW pentru echipamenele NPT si platforma de management LightSoft, in comparatie cu versiunea operationala actuala (2 zile);
- Modul 2: Introducere notiuni fundamentale de Securitate cibernetica pentru Infrastructuri Critice (1 zi);
- Modul 3: Introducere arhitectura si functionalitati ale solutiei de Securitate cibernetica propusa (2 zile);
- Modul 4: Operare si Mentenanta a solutiei de Securitate cibernetica propusa (5 zile).

Trainingul va detalia pas cu pas activitățile ce se execută, în ceea ce priveste instalarea, configurarea, integrarea, utilizarea și mentenanța soluției furnizate.
Prestatorul va furniza o procedură scrisă detaliată a operațiilor necesar a fi efectuate de Beneficiar pentru utilizarea cu succes a soluției, luând în considerare toate situațiile posibile ce pot apare în operarea soluției. Prestatorul va furniza deasemenea manualul conținând toate comenzile CLI necesare în configurarea, operarea și mentenanța soluției.
Toate cheltuielile de deplasare si cazare vor fi suportate de Prestator.

5.4.2 De asemenea pe toată perioada lucrărilor de instalare, configurare și acceptanța în site prestatorul va explica in detaliu personalului Beneficiarului toate activitatile ce se executa.

5.5 Managementul Proiectului

5.5.1 Prestatorul va fi responsabil de planificarea, urmărirea și coordonarea proiectului incluzând, dacă este cazul, și planificarea și urmărirea lucrărilor subPrestatorilor. Prestatorul va solicita aprobarea Beneficiarului pentru înlocuirea oricărui subPrestator.

5.5.2 Prestatorul va trebuie sa aiba personal certificat de producator pentru derularea activitatilor de planificare, implementare si mentenanta a sistemului de comunicatii existent cat si a Solutiei de Securitate propusa.

5.5.3 Prestatorul trebuie să desemneze un Project Manager al cărui CV trebuie să fie anexat documentației de calificare și care trebuie să evidențieze studiile relevante și experiența persoanei desemnate de ofertant în managementul unor proiecte similare ca obiect și amploare. Prestatorul trebuie să prezinte compunerea echipei de management și executare a proiectului atât general pe calificări/roluri, cât și nominal. Componența echipei prezentată în ofertă va putea fi schimbată numai cu aprobarea Beneficiarului.

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

6. Receptia la terminarea lucrarilor

6.1 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, după terminarea ultimului test de acceptanță operațională.

6.2 Prestatorul are obligația de a livra cu 30 de zile inainte de finalizarea lucrarilor documentatia tehnica a Solutiei, respectiv „As built". Prestatorul va comunica Beneficiarului data finalizării lucrarilor transmițându-i acestuia, pentru confirmare, o înștiințare scrisă.

6.3. Beneficiarul va organiza recepția în maximum 5 zile de la notificarea finalizării serviciilor și va comunica Prestatorului data stabilită.

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

7. Garanție

7.1 Prestatorul trebuie să furnizeze Beneficiarului garanție comerciala de 3 ani de la data semnării procesului verbal de recepție pentru toate echipamentele furnizate, modulele hard/soft, licențele și lucrările efectuate .

7.2 Acestă garanție trebuie să includă repararea sau înlocuirea oricărui echipament, sistem, subsistem, hardware și/sau software care s-a defectat în condiții normale de uzură și de utilizare, atat pentru Solutia de Securitate cibernetica cat si pentru echipamentele de comunicatii NPT si sistemul de management LightSoft. Această activitate va include montarea/demontarea și transportul aferent.

7.3 In plus fată de astfel de defectări, garanția trebuie să includă, pentru aceeași perioadă, suport tehnic pentru asistență în operare și configurare în timpul normal de lucru, atât din partea echipei de suport oficiale a producătorului ECI (Gold Maintenance Service Package, 24x7, cu timp de raspuns de maxim 30 minute), cât și din partea echipelor oficiale de suport în cazul produselor non-ECI furnizate în cadrul acestui proiect.Vor fi furnizate datele de contact relevante.

7.4 Prestatorul trebuie să organizeze și să furnizeze intervenție pe site/remote în maxim 8 ore (business hours) atunci când este semnalată de către Beneficiar nefuncționarea sau funcționarea defectuoasă a echipamentelor

7.5 Prestatorul trebuie să presteze servicii Swap de reparare prin schimbare pe site, cu un timp de swap de maxim 10 zile.

7.6 Prestatorul trebuie să anexeze la oferta tehnică documentul „Propunere pentru asigurarea intervenției în amplasamente, în perioada de garanție", în care trebuie să descrie în detaliu modalitățile prin care va asigura îndeplinirea timpilor de remediere asumați.

7.7 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.

7.8 Pe perioada garantiei Prestatorul trebuie să furnizeze gratuit update-uri/patch-uri pentru software-urile livrate, inclusiv pentru semnaturile malware.

8. Etapizarea lucrărilor

8.1 Proiectare integrala detaliata a solutiei- 3 luni de la semnarea contractului.
8.2 Livrare echipamente/software – maxim 3 luni de la semnarea contractului.
8.3 Implementare echipamente/software – maxim 6 luni de la livrarea echipamentelor.
8.4 Teste acceptanță operațională și predare documentație As built – 3 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.
8.5 La solicitarea Prestatorului, Beneficiarul poate aproba decalarea termenelor etapelor intermediare, fără a se modifica termenul final al Contractului.
8.6. Termenul de execuție a tuturor serviciilor contractate este de 12 luni de la semnarea contractului.

9. Standarde si Certificari

9.1 Prestatorul trebuie sa detina urmatoarele certificari:

- ISO IEC 27001 Information Security Management System;
- ISO IEC 17025-2005 General Requirements for the Competence of Testing and Calibration Laboratories

9.2 Solutia trebuie sa fie conforma cu urmatoarele standarde:

- IETF RFC 2560: Certificate Revocation OSCP
- IETF RFC 5280: Certificate Revocation CRL
- IETF RFC 2409: The Internet Key Exchange
- IETF RFC 2408: Internet Security Association and Key Management Protocol
- IETF RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP
- IEEE 1686: IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
- TR 103 303 Protection measures for ICT in the context of CI
- TR 103 309 Secure by Default adoption – Platform Security Technology
- TR 103 305 Security Assurance by Default; Critical Security Controls for Effective Cyber Defence
- NERC CIP v5 Regulations

Sef Serviciu Telecomunicatii
Ing. Catalin Ruse

Intocmit
Coordonator activitate
Ing. Iulian Bucur