SECTIUNEA II
CAIET DE SARCINI

CAIET DE SARCINI

Achiziție de echipamente pentru creșterea securității IT

Cuprins

1. Descrierea stării prezente

Infrastructura de comunicații la nivelul companiei este una complexă administrată centralizat și distribuită în mai multe sedii. Având în vedere natura companiei securitatea și protecția datelor sunt un aspect foarte important. La nivel de acces infrastructura de comunicații date este formată din echipamente de tip switch de la producătorul Cisco.

Echipamentul de tip firewall implementat în cadrul infrastructurii este format dintr-un cluster de servere care rulează soluția Microsoft TMG 2010

2. Prezentare generală a lucrării:

Achiziție de echipamente pentru creșterea securității IT.

Soluția trebuie sa conțină:

a. Un cluster firewall NGFW pentru zona de border
b. Un cluster firewall NGFW pentru zona de SCADA

Soluția va fi oferită sub forma a 2 clustere de firewall (câte două echipamente fizice pentru fiecare cluster) unul pentru zona de border (către internet) și unul pentru separea rețelei de SCADA de rețea Conpet și va cuprinde echipamentele hardware necesare, instalarea și toate licențele software necesare funcționării depline și asigurării tuturor funcționalităților cerute.

3. Cerințe tehnice

a. Cluster firewall pentru zona de border

Cluster-ul de firewall NGFW trebuie să fie de tip hardware (nu mașină virtuală), trebuie să asigure funcționalitățile cluster-ului TMG 2010 aflat în producție pe care-l va și înlocui și în plus să ofere cele mai noi tehnologii în domeniul firewall-urilor la nivel de rețea 7: anti-bot și anti-virus, firewall statefull inspection, să conțină un sistem de detecție și protecție avansat (IDS,IPS), să poată verifica identitatea utilizatorilor, VPN IPSEC, controlul aplicațiilor, filtrare URL și să conțină un sistem de management al

politicilor de securitate dar nu trebuie să se limiteze la acestea. Trebuie să fie de tip Next Generation Firewall si interfata grafica de configurare (GUI).

Trebuie să asigure:

- Threat Protection/Prevention Throughput - performanța Threat Protection/Prevention este măsurată cu serviciile de tip IPS, Filtrare URL, Antivirus, Zero Day protecție, Application Control și Malware protecție activate în același timp, bazate pe un trafic de tip Enterprise Mix : min. 2 Gbps
- Un minim de 200 Tunele IPSEC VPN concurente
- Un număr suficient de mare de sesiuni TCP concurente, mai mare de 5.000.000.

Furnizorul va avea obligația ca în cadrul procesului de punere în funcțiune, să realizeze următoarele:

- Să asigure configurarea și instalarea echipamentelor astfel încât procesul să nu afecteze activitatea companiei.
- Integrarea echipamentelor în cadrul infrastructurii de comunicație existente asigurând comunicația de date la nivelul infrastructurii așa cum se desfășoară ea în prezent și în acord cu capabilitățile oferite de echipamentele ofertate.
- Să implementeze/configureze politicile de securitate existente pe noile echipamente în acord cu cerințele funcționale existente la nivelul infrastructurii de comunicație precum și cu recomandările la zi privind cerințele moderne de securitate.
- Să integreze și să configureze echipamentul la nivel logic în cadrul infrastructurii de autentificare a utilizatorilor interni și externi astfel încât utilizatorii să nu fie afectați de acest proces.
- Să configureze echipamentele astfel încât să asigure funcționarea serviciilor existente, publicate prin intermediul echipamentelor existente și să asigure prin politici de Securitate adecvate cel puțin același nivel de Securitate și Protecție.
- În cazul în care echipamentele ofertate dispun de funcționalități suplimentare față de soluția actuală furnizorul va avea obligația de configurare acestor funcționalități în acord cu cerințele beneficiarului.

	Cerințe minime solicitate
Specificații hardware	- Montabil în rack - 1 x interfețe dedicate pentru management GE RJ-45 - 8 x interfețe GE RJ45 sau 8 x interfețe GE SFP - 1 x USB

	- 1 x port consola RJ-45 - Sursă redundantă internă sau atașabilă - 1 modul de stocare intern instalat minim 100 GB de tip SSD
Funcționalități	- Să permită formarea de zone/separa rețelele de Internet – DMZ1- DMZ2 – LAN local - Să ofere acces securizat către site-uri web atât din DMZ cat și din LAN local - Să ofere acces la site-uri securizate cu autentificare (ex. OWA) - Să permită utilizatorilor să facă VPN IPSEC cu autentificare prin Cisco ISE și Active directory pentru minim 200 de utilizatori - Să permită NAT - Să poată autentifica userii automat din lan local bazat pe user-ul de domeniu la cererile de internet. - Să poată face URL filtering bazat pe grupuri de acces ale userilor și ale site-urilor care pot fi accesate - Să poată face categorizarea site-urilorn de internet - Configurații High availability Active-Active, Active-Passive - Sursă alimentare redundantă pentru fiecare echipament livrat **Să ofere minim următoarele servici de rețea:** - Rutare/Rețea: - Suport WAN multiplu - Client/Server/Relay DHCP - Policy-based routing - Rutare dinamică IPv4/IPv6- RIP, OSPF ,BGP, IS-IS - Suport multi-zone - Rutare între zone - VLAN Tagging(802.1q) - Link aggregation (802.3ad) - Rutare între VLAN-uri - Multi-link aggregation(802.3ad) - Suport IPv6 (Firewall, AntiVirus, Web-Filtering, IPS, DNS, Transparent Mode, SIP, rutare dinamică, Admin access, Management) **Traffic shaping :** - Policy-based - Suport DiffServ

	- Banda Garantată/Maximă/Prioritară - Shaping per- IP, per-Policy, per application **High Availability:** - Activ/Activ, Activ/Pasiv - Statefull Failover - Link status monitor - Link failover - Server Load balancing **Identificarea device-urilor:** - Colectarea informațiilor device-urilor conectate la rețea precum adresa MAC, adresa IP, sistem de operare, hostname, username.
Firewall de tip Stateful Inspection	- Trebuie să utilizeze mecanisme de filtrare a conexiunilor bazate pe informațiile legate de starea acestora. - Soluția trebuie să suporte și să controleze accesul la servicii și protocoale de comunicație predefinite. - Firewall-ul trebuie să suporte metode de autentificare a utilizatorilor de tip user, client și sesiune. - Soluția trebuie să ofere suport pentru gateway high availability (cluster HA). - Rutare dinamică-RIP, OSPF, BGP, Multicast, Policy-based NAT - NAT, PAT, Transparent - Domenii Virtuale (NAT/Transparent) - VLAN Tagging (802.1q) - Profile granulare de protecție per-policy - Suport proxy explicit - Suport pentru autentificarea userilor la nivel de politici firewall : • bază locală de date • Windows AD • External RADIUS/LDAP/TACACS+ • XAUTH over RADIUS (IPSEC) • RSA Secure ID • 2-factor authentication cu tokenuri hardware/software dedicate

Sistem de detecție și prevenție a intruziunilor (IPS):	- Trebuie să folosească mecanisme de detecție a atacurilor bazate pe: semnături, anomalii de protocol, controlul aplicațiilor și comportamentul acestora. - IPS și modulul Firewall de tip Stateful Inspection trebuie să fie integrate pe aceeași platformă. - Trebuie să aibă opțiunea de a defini profile IPS pentru client sau pentru server, sau o combinație de amândouă. - Trebuie să ofere cel puțin doua profile/politici IPS predefinite. - Trebuie să ofere un mecanism automat pentru activarea și administrarea noilor semnături provenite din update-uri. - Trebuie să suporte adăugarea de excepții bazate pe sursa și destinația traficului sau serviciu, indiferent de combinația acestora. - Trebuie să poată detecta și preveni următoarele amenințări: folosirea necorespunzătoare a protocoalelor, comunicația folosită în scopuri distructive, atacuri asupra canalelor VPN și atacurile generice care nu au semnături. - Trebuie să poată detecta și bloca atacurile la nivel rețea și aplicații, protejând cel puțin următoarele servicii: e-mail, DNS, FTP, serviciile Windows (Microsoft Networking), SNMP. - IPS trebuie să includă posibilitatea de a detecta sau bloca traficul peer to peer, folosind tehnici evazioniste. - Administratorul trebuie să poată defini excluziuni de rețea și host de la inspecția IPS-ului. - Soluția trebuie să ofere protecție împotriva DNS Cache Poisoning și să blocheze utilizatorii în a accesa adrese de domeniu blocate. - IPS și/sau Application Control trebuie să detecteze și să blocheze aplicațiile de tip control remote, inclusiv cele care sunt capabile să tuneleze traficul specific prin intermediul protocolului HTTP. - Soluția trebuie să permită administratorului să poată bloca ușor traficul inbound și/sau outbound în funcție de zone geografice, țări, fără să fie nevoie să definească grupuri de IP-uri corespunzătoare zonei geografice vizate.
Autentificare Utilizatori:	- Bază de date locală - Integrare Active Directory - Trebuie să suporte utilizarea de grupuri LDAP - Integrare LDAP/RADIUS/Tacacs+ - IP/MAC address binding - Suport 2-factor authentication

Anti-Virus	- Soluția trebuie să utilizeze un motor de detectare pe mai multe niveluri, care include reputația IP-urilor, URL-urilor și adreselor de DNS și să detecteze modele de comunicare specific aplicațiilor de tip bot. - Soluția trebuie să folosească un mecanism de corelare și raportare a evenimentelor de securitate. - Soluția anti-virus trebuie să fie în măsură să prevină accesul la site-uri infectate sau suspectate drept malițioase. - Soluția anti-virus trebuie să fie capabilă de a inspecta trafic HTTP/HTTPS, POP/POP3S, SMTP/SMTPS, IMAP/IMAPS, IM . - Soluția Anti-Virus trebuie să aibă actualizări pentru semnături în timp real. - Soluția Anti-Virus trebuie să ofere suport Antispyware și Worm Prevention. - Politicile de scanare anti-virus trebuie să fie gestionate cu posibilitate de configurare și aplicare selectivă.
VPN	- PPTP, IPSec, SSL - Suport criptare DES, 3DES, AES - Autentificare SHA-I I MD5 - PPTP, L2TP, VPN Client pass through - Suport VPN "Hub and Spoke" - Autentificare IKE cu Certificate (x.509 v1 si v2) - IPSec NAT Traversal - Producătorul trebuie să aibă în portofoliu client de VPN propriu, atât pentru PC-uri cât și pentru device-uri mobile - Trebuie să suporte autorități de certificare internă (proprietară) și externe (publice).
Controlul Aplicațiilor	- Soluția să permită Identificarea și controlul la nivel de aplicație (control Layer 7 indiferent de port/protocol) - Diff Serv per aplicație - Suport inspecție trafic SSL - Soluția de control a aplicațiilor trebuie să poată fi actualizată permanent - Traffic shaping (per aplicație)
Web filtering	- Blocarea accesului utilizatorilor la site-uri de tip malițios sau cu conținut nepotrivit folosind o bază de date globală cu certificare recunoscută - Soluția trebuie să permită opțiunea de a modifica mesajul/notificarea de blocare a accesului. - Soluția trebuie să poate crea reguli de filtrare cu multiple categorii.

	- Soluția trebuie să ofere la nivelul politicilor de filtrare granularitate pe utilizator și grupuri. - Soluția trebuie să permită mecanisme de tip "black/white list" pentru a da opțiunea administratorului de a permite sau nu accesul la URL-uri specifice indiferent de categoria în care se regăsește acel URL, - Soluția trebuie să permită excepții de la regulile de filtrare definite prin intermediul unui grup pentru un anume utilizator membru al acelui grup. - Posibilitatea de customizare a categoriilor globale prin suprascriere - Soluția de filtrare WEB trebuie să poată fi actualizată permanent.
Sistem management	- Consola, SSH, HTTPS , GUI. - Soluția trebuie să includă o Autoritate de Certificare internă, care poate genera certificate utilizatori și care permite autentificarea pe VPN. - Soluția trebuie să includă posibilitatea de a folosi autorități de certificare externe - Trebuie să permită monitorizarea accesului la regulile de securitate, pe măsură ce acestea au fost aplicate pentru traficul specific, pe baza unui contor. - Soluția trebuie să includă opțiunea de a segmenta baza de reguli cu ajutorul etichetelor sau a titlurilor de secțiune, cu scopul de a organiza mai bine politica de securitate. - Log Viewer ar trebui să aibă capacitatea de a exclude cu ușurință adrese IP vizualizate în log-urile IPS, atunci când sunt depistate ca fals pozitiv. - Log Viewer ar trebui să aibă capacitatea să creeze filtru folosind obiectele predefinite (clienți, rețele, grupuri, utilizatori, s.a).
Licențiere	- Licențe pentru activarea actualizărilor serviciilor Prevenirea Intruziunilor, Filtrare Web , Antivirus, Antispam, Controlul Aplicațiilor, Anti-Botnet de la producătorul sistemului de operare instalat pe echipament pentru întreaga perioadă de garanție. - Trebuie să asigure licențierea pentru minim 540 de utilizatori. - Semnăturile asociate serviciilor Prevenirea Intruziunilor, Filtrare Web , Antivirus, Antispam, Controlul Aplicațiilor, Anti-Botnet să rămână la ultimul nivel de actualizare la finalul garanției de 3 ani.

b. Cluster firewall pentru zona de SCADA

Cluster-ul de NG firewall trebuie să fie de tip hardware (nu mașină virtuală), trebuie să asigure funcționalitățile: statefull inspection, să poată verifica identitatea utilizatorilor, VPN IPSEC și să conțină un sistem de management al politicilor de securitate. Trebuie să fie de tip Next Generation Firewall și interfață grafică de configurare (GUI).

Trebuie să asigure:

- Threat Protection/Prevention Throughput - performanța Threat Protection/Prevention este măsurată cu serviciile de tip IPS, Antivirus, Zero Day protecție, Malware protecție activate în același timp, bazate pe un trafic de tip Enterprise Mix : min. 200 Mbps
- IPSEC VPN Throughput minim 200 Mbps
- Un minim de 25 Tunele IPSEC VPN concurente
- Un număr suficient de mare de sesiuni TCP concurente

Furnizorul va avea obligația ca în cadrul procesului de punere în funcțiune, să realizeze următoarele:

- Să asigure configurarea și instalarea echipamentelor astfel încât procesul să nu afecteze activitatea companiei.
- Integrarea echipamentelor în cadrul infrastructurii de comunicație existente asigurând comunicația de date la nivelul infrastructurii așa cum se desfășoară ea în prezent și în acord cu capabilitățile oferite de echipamentele ofertate.
- Să implementeze/configureze politicile de securitate existente pe noile echipamente în acord cu cerințele funcționale existente la nivelul infrastructurii de comunicație precum și cu recomandările la zi privind cerințele moderne de securitate.
- Să integreze și să configureze echipamentul la nivel logic în cadrul infrastructurii de autentificare a utilizatorilor interni și externi astfel încât utilizatorii să nu fie afectați de acest proces.
- Să configureze echipamentele astfel încât să asigure funcționarea serviciilor existente, publicate prin intermediul echipamentelor existente și să asigure prin politici de Securitate adecvate cel puțin același nivel de Securitate și Protecție.
- În cazul în care echipamentele ofertate dispun de funcționalități suplimentare față de soluția actuală furnizorul va avea obligația de configurare a acestor funcționalități în acord cu cerințele beneficiarului.

	Cerințe minime solicitate
Specificații hardware	- Montabil în rack - 1 x interfețe dedicate pentru management GE RJ-45 - 4 x interfețe GE RJ45 sau 4 x interfețe GE SFP - 1 x USB - 1 x port consolă RJ-45
Funcționalități	- Să poată separa rețelele de LAN - DMZ – LAN SCADA - Să permită utilizatorilor să facă VPN cu autentificare locala pe firewall - Să permită NAT-are de porturi. - Configurații High availability Active-Active, Active-Passive
Firewall de tip Stateful Inspection	- Trebuie să utilizeze mecanisme de filtrare a conexiunilor bazate pe informațiile legate de starea acestora. - Soluția trebuie să suporte și să controleze accesul la servicii și protocoale de comunicație predefinite. - Firewall-ul trebuie să suporte metode de autentificare a utilizatorilor de tip user, client și sesiune. - Soluția trebuie să ofere suport pentru gateway high availability (cluster HA). - Rutare dinamică-RIP, OSPF, BGP, Multicast, Policy-based NAT - NAT, PAT, Transparent - Domenii Virtuale (NAT/Transparent) - VLAN Tagging (802.1q) - Profile granulare de protecție per-policy - Suport proxy explicit - Suport pentru autentificarea userilor la nivel de politici firewall : • bază locală de date • Windows AD • External RADIUS/LDAP/TACACS+ • XAUTH over RADIUS (IPSEC) • RSA Secure ID
Sistem de detecție și prevenție a intruziunilor (IPS):	- Trebuie să folosească mecanisme de detecție a atacurilor bazate pe: semnături, anomalii de protocol, controlul aplicațiilor și comportamentul acestora. - IPS și modulul Firewall de tip Stateful Inspection trebuie să fie integrate pe aceeași platformă. - Trebuie să aibă opțiunea de a defini profile IPS pentru client sau pentru server, sau o combinație de amândouă.

	- Trebuie să ofere cel puțin doua profile/politici IPS predefinite. - Trebuie să ofere un mecanism automat pentru activarea și administrarea noilor semnături provenite din update-uri. - Trebuie să suporte adăugarea de excepții bazate pe sursa și destinația traficului sau serviciu, indiferent de combinația acestora. - Trebuie să poată detecta și preveni următoarele amenințări: folosirea necorespunzătoare a protocoalelor, comunicația folosită în scopuri distructive, atacuri asupra canalelor VPN și atacurile generice care nu au semnături. - Trebuie să poată detecta și bloca atacurile la nivel rețea și aplicații, protejând cel puțin următoarele servicii: e-mail, DNS, FTP, serviciile Windows (Microsoft Networking), SNMP. - IPS trebuie să includă posibilitatea de a detecta sau bloca traficul peer to peer, folosind tehnici evazioniste. - Administratorul trebuie să poată defini excluziuni de rețea și host de la inspecția IPS-ului. - Soluția trebuie să ofere protecție împotriva DNS Cache Poisoning și să blocheze utilizatorii în a accesa adrese de domeniu blocate. - IPS trebuie să detecteze și să blocheze aplicațiile de tip control remote, inclusiv cele care sunt capabile să tuneleze traficul specific prin intermediul protocolului HTTP.
Utilizatori	- Bază de date locală - Integrare Active Directory - Trebuie să suporte utilizarea de grupuri LDAP - Integrare LDAP/RADIUS/Tacacs+ - IP/MAC address binding
Anti-Virus	- Soluția trebuie să utilizeze un motor de detectare pe mai multe niveluri, care include reputația IP-urilor, URL-urilor și adreselor de DNS și să detecteze modele de comunicare specific aplicațiilor de tip bot. - Soluția trebuie să folosească un mecanism de corelare și raportare a evenimentelor de securitate. - Soluția anti-virus trebuie să fie în măsură să prevină accesul la site-uri infectate sau suspectate drept malițioase. - Soluția anti-virus trebuie să fie capabilă de a inspecta trafic HTTP/HTTPS, POP/POP3S, SMTP/SMTPS, IMAP/IMAPS, IM . - Soluția Anti-Virus trebuie să aibă actualizări pentru semnături în timp real.

	- Soluția Anti-Virus trebuie să ofere suport Antispyware și Worm Prevention. - Politicile de scanare anti-virus trebuie să fie gestionate cu posibilitate de configurare și aplicare selectivă.
VPN	- PPTP, IPSEC, SSL - Suport criptare DES, 3DES, AES - Autentificare SHA-I I MD5 - PPTP, L2TP, VPN Client pass through - Suport VPN "Hub and Spoke" - Autentificare IKE cu Certificate (x.509 v1 si v2) - IPSEC NAT Traversal - Producătorul trebuie să aibă în portofoliu client de VPN propriu, atât pentru PC-uri cât și pentru device-uri mobile - Trebuie să suporte autorități de certificare internă (proprietară) și externe (publice).
Sistem de management al politicilor de securitate	- Consola, SSH, HTTPS , GUI. - Soluția trebuie să includă o Autoritate de Certificare internă, care poate genera certificate utilizatori și care permite autentificarea pe VPN. - Soluția trebuie să includă posibilitatea de a folosi autorități de certificare externe - Trebuie să permită monitorizarea accesului la regulile de securitate, pe măsură ce acestea au fost aplicate pentru traficul specific, pe baza unui contor. - Soluția trebuie să includă opțiunea de a segmenta baza de reguli cu ajutorul etichetelor sau a titlurilor de secțiune, cu scopul de a organiza mai bine politica de securitate. - Log Viewer ar trebui să aibă capacitatea de a exclude cu ușurință adrese IP vizualizate în log-urile IPS, atunci când sunt depistate ca fals pozitiv. - Log Viewer ar trebui să aibă capacitatea să creeze filtru folosind obiectele predefinite (clienți, rețele, grupuri, utilizatori, s.a).
Licențiere	- Licențe pentru activarea actualizărilor serviciilor Prevenirea Intruziunilor, , Antivirus, Antispam, Anti-Botnet de la producătorul sistemului de operare instalat pe echipament pentru întreaga perioadă de garanție. - Semnăturile asociate serviciilor Prevenirea Intruziunilor, Antivirus, Anti-Botnet să rămână la ultimul nivel de actualizare la finalul garanției de 3 ani

4. Servicii

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, configurarea, testarea, integrarea, și acceptanța aplicațiilor așa cum sunt specificate în acest Caiet de Sarcini dar nu va trebui să se limiteze la acestea.

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

Prestatorul trebuie să se alinieze cu arhitectura propusă de beneficiar în totalitate dar nu trebuie să se limiteze la aceasta. Arhitectura dorită poate fi pusă la dispoziția prestatorului doar după semnarea unui contract de confidențialitate.

5. Livrare

Livrarea echipamentelor, licențelor, instalarea și configurarea soluției se va face la Sediul Dispecerat Central din Ploiești str. Anul 1848 nr.1-3 pentru cluster-ul firewall de border și Sediul 2 Conpet din Ploiești, Str. Rezervoarelor, nr. 7 pentru cluster-ul firewall de SCADA.

Orice element/modul/licență/funcționalitate 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.

6. Instruire

Training-ul va detalia pas cu pas activitățile ce se execută, în ceea ce privește instalarea, configurarea, integrarea, utilizarea și mentenanța soluției furnizate.

Training-ul va fi făcut de un trainer ceritificat de producătorul echipamentelor ofertate și va conține manual de instruire.

Numărul de persoane care vor fi instruite este de 4.

Prestatorul va furniza o procedură scrisă detaliată a operațiilor necesare 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 un manual care va conține și va detalia toate operațiunile necesare în configurarea, operarea și mentenanța soluției.

7. Managementul Proiectului

Prestatorul va fi responsabil de planificarea, urmărirea şi coordonarea proiectului

Prestatorul trebuie să desemneze un Project Manager al cărui CV trebuie să fie anexat documentației de calificare și care trebuie să evidenţieze studiile relevante și experiența persoanei desemnate de ofertant în managementul unor proiecte similare ca obiect și amploare.

Prestatorul trebuie să prezinte compunerea echipei de executare a proiectului atât general pe calificări/roluri, cât și nominal. Aceasta echipa trebuie să aibe în componență personal calificat care să instaleze și să configureze aplicația la nivel de security expert (ex. CCNP security, CCSE, NSE4 sau echivalent).

Componența echipei prezentată în ofertă va putea fi schimbată numai cu aprobarea Beneficiarului.

8. Acceptanță

Prestatorul va prezenta Beneficiarului o procedură de verificare pentru acceptanță conformă cu specificațiile softwareului. Procedura va fi înaintată Beneficiarului cu 14 zile înainte de efectuarea testelor de acceptanță. Beneficiarul va analiza propunerea de procedură și dacă va fi cazul, va solicita modificarea/completarea acesteia sau o va accepta. În cazul în care Beneficiarul va solicita modificarea/completarea testelor de acceptanță, se vor repeta pașii de mai sus până la acceptarea de către Beneficiar.

Testele de acceptanță trebuie să asigure Beneficiarul că Soluția implementată este instalată corect, este configurată corect, operează conform cerințelor.

Procedura de acceptanță va include cel puțin următoarele teste:

- Colectarea de evenimente de la toate echipamentele prezentate.
- Trimiterea evenimentelor colectate într-un mod optimizat și filtrate care să reflecte investigarea doar a alertelor relevante conform bunelor practici.
- Trimitere de alerte pe e-mail în cazul apariției unui incident de securitate (se vor simula incidente de securitate)
- Exportul datelor în vederea păstrării lor pe o perioadă mai lungă.
- Identificare de evenimente repetitive.
- Alte teste ce pot stabili buna funcționare și configurare a soluției.

După finalizarea cu succes a testelor de acceptanță efectuate împreună cu beneficiarul și aprobate de către acesta (beneficiar), prestatorul va notifica în scris Beneficiarul că a finalizat implementarea și se poate organiza punerea în funcțiune a sistemului.

9. Durata lucrărilor

Termenul de execuție pentru lucrarea contractată este de 3 luni de la semnarea contractului.

În acest termen trebuie incluse toate etapele contractului:

- Livrare echipamente și licențe necesare
- Instalare și configurare
- Predare documentației

- Instruire utilizatori
- Teste de acceptanță
- Punere în funcțiune

Prestatorul are obligația de a comunica Beneficiarului data finalizării serviciilor transmițându-i acestuia, pentru confirmare, o înștiințare scrisă, după terminarea cu succes a ultimului test de acceptanță.

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

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.

10. Garanție

Prestatorul trebuie să furnizeze Beneficiarului garanție comercială de 3 ani de la data semnării procesului verbal de recepție pentru toate licențele și lucrările.

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 producătorilor echipamentelor și softwareului (inclusiv update-uri la ultimele versiuni), cât și din partea echipelor de suport ale Prestatorului.

Șef Birou Infrastructură IT
Costin Florescu

Șef Serviciu IT
Cătălin Mereanu