Executiv CEO Departament T.I.C
Nr. 1285/DTIC/15.04.2020
Nr. 385/DTSC/15.04.2020

1. INTRODUCERE

Pentru această achiziție, Societatea Complexul Energetic Oltenia S.A. îndeplinește rolul de entitate contractantă în cadrul contractului.

Orice activitate descrisă într-un anumit capitol din caietul de sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului contractului.

2. CONTEXT REALIZARE ACHIZIȚIE

2.1. Informații despre entitatea contractantă și despre beneficiar

Entitatea contractantă este Societatea Complexul Energetic Oltenia S.A., cu sediul în str. Alexandru Ioan Cuza, nr. 5, Municipiul Tg.-Jiu, județul Gorj, cod 210140, fax: 0253-227.280, înregistrată la Oficiul Registrului Comerțului de pe lângă Tribunalul Gorj cu nr. J18/311/2012, cod fiscal RO30267310, cont virament RO59 RZBR 0000 0600 1465 2248, deschis la Raiffeisen Bank – Tg.-Jiu, web: www.ceoltenia.ro, e-mail: office@ceoltenia.ro.

Denumire și adresă beneficiar: Societatea Complexul Energetic Oltenia S.A., str. Alexandru Ioan Cuza nr. 5, municipiul Târgu Jiu, județul Gorj, România, Fax: 0253 227 280.

Misiunea Complexului Energetic Oltenia S.A. este: producerea de energie electrică curată și sigură, bazată pe valorificarea cu maximă eficientă a potențialului de lignit din Oltenia, cu rol de a asigura securitatea energetică a României.

Activitățile principale ale Complexului Energetic Oltenia S.A. sunt: producerea energiei electrice și termice pe bază de lignit, extracția și prepararea lignitului.

2.2. Informații despre contextul care a determinat această achiziție

În prezent soluția software de securitate antimalware, nu acoperă numărul de stații locale aflate în cadrul Complexului Energetic Oltenia și există riscul să apară disfuncționalități generate de infectarea stațiilor ce nu au instalate soluții software profesionale de securitate.

2.3. Informații despre beneficiile anticipate de către beneficiar

Prin achiziționarea acestor pachete software de securitate, Societatea Complexul Energetic Oltenia S.A. va elimina din riscurile infectării cu softuri malițioase care ar putea compromite desfășurarea activității în bune condiții.

2.4. Alte inițiative/proiecte/programe asociate cu această achiziție de produse

Nu este cazul.

2.5. Cadrul general al sectorului în care entitatea contractantă își desfășoară activitatea

Societatea Complexul Energetic Oltenia S.A. este un producător de cărbune și energie din sectorul de servicii energetice din România.

Politica Societății Complexul Energetic Oltenia S.A. este: să devină un operator principal în plan regional, prin valorificarea cu maximă eficiență a rezervelor de lignit, în producerea energiei electrice și termice pe bază de lignit.

Instituțiile și sistemele care operează în acest sector: Ministerul Energiei, Departamentul pentru Energie, Autoritatea Națională de Reglementare în Domeniul Energiei, Agenția Națională pentru Resurse Minerale, Dispecerul Energetic Național, Sistemul Energetic Național – Transelectrica s.a.

2.6. Factori interesați și rolul acestora

Societatea Complexul Energetic Oltenia S.A. aduce o creștere substanțială a nivelului de trai în regiunea Oltenia, motiv pentru care factorii politici, sociali, economici (atât la nivel local, cât și la nivel național) contribuie la îndeplinirea obiectivului activității companiei.

3. DESCRIERE PRODUSE SOLICITATE

3.1. Descriere situație actuală la nivelul beneficiarului

În prezent la nivelul companiei există o soluție de securitate antimalware Enterprise, dar care nu acoperă pe deplin nevoile de securitate informatică.

Bunele practici în domeniul securității informatice, recomandă ca o companie de anvergura Complexului Energetic Oltenia să dețină cel puțin două soluții de securitate informatică, pentru a putea răspunde mai eficient la atacuri informatice de tipul: Powershell script-based, Phishing, atacuri fără fișiere, Ransomware, Malware necunoscut.

3.2. Obiectivul general la care contribuie furnizarea produselor

Producerea de energie electrică și termică.

3.3. Obiectivul specific la care contribuie furnizarea produselor

Asigurarea securității infrastructurii I.T. din cadrul companiei.

3.4. Produsele solicitate și operațiunile cu titlu accesoriu necesar a fi realizate

Se va încheia un contract pentru furnizare produse.

3.4.1. Produse solicitate

Denumire produs: Licențe software de tip Endpoint Detection and Response (EDR)							
Denumire produs	**Cantitate**	**Unitate de măsură**	**Loc de livrare**	**Dată de livrare solicitată**	**Specificații tehnice SAU cerințe funcționale minime**	**Specificații tehnice SAU cerințe funcționale extinse**	**Durată minimă garanție**
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Licențe Software Securitate EDR	600	buc	Societatea Complexul Energetic Oltenia S.A., str. Alexandru Ioan Cuza nr. 5, municipiul Târgu Jiu, județul Gorj, România	In maximum 5 zile de la data înregistra-rii contractului	Conform subcap. **3.4.1.4.**	-	*Minimum 12 luni de la data recepției*

3.4.1.1. Denumire produs

Endpoint Detection and Response (EDR)

3.4.1.2. Cantitate

600 buc

3.4.1.3. Loc de livrare

Societatea Complexul Energetic Oltenia S.A., str. Alexandru Ioan Cuza nr. 5, municipiul Târgu Jiu, județul Gorj, România, Fax: 0253 227 280.

Ofertantul este responsabil pentru livrarea produselor în termenul solicitat și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca niciun motiv de întârziere sau costuri suplimentare.

3.4.1.4. Specificații tehnice / cerințe funcționale minime/extinse

I. CARACTERISTICI GENERALE ALE PRODUSULUI

A. Trebuie să aibă o consolă de management care asigură funcționalități de administrare.

B. Trebuie să asigure protecție antimalware pentru stații fizice/virtuale, laptop-uri și servere

A. Consola de management

A.1. Cerințe generale:

a) Interfața consolei de management trebuie să fie în limba română.
b) Interfața clientului de securitate, care se instalează pe stații și servere, trebuie să fie în limba română.
c) Manualul de instalare a produsului trebuie să fie în limba română.
d) Manualul de administrare a produsului trebuie să fie în limba română.
e) Soluția trebuie să permită activarea/dezactivarea actualizărilor de produs/semnături.
f) Trebuie să permită actualizări automate a consolei de management făcute de către producătorul soluției, fără intervenția utilizatorului.
g) Trebuie să permită ca notificările – prezente în interfața, notificările necitite să fie trimise către una sau mai multe adrese de email, să alerteze administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de produs disponibile.
h) Consola de management trebuie să fie accesibilă de oriunde în lume (soluție de tip Cloud), fără a fi nevoie de setări suplimentare din partea utilizatorului.
i) Consola de management trebuie să fie accesibilă atât de pe stații de lucru cât și de pe dispozitive mobile (smartphone, tabletă).

A.2. Panou de monitorizare și raportare (Dashboard):

a) Rapoartele din panoul de monitorizare trebuie să poată fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul după care o stație este considerată neactualizată).
b) Panoul central trebuie să conțină rapoarte pentru toate modulele suportate.
c) Rapoartele din panoul central de comandă trebuie să permită: adăugarea altor rapoarte, ștergerea lor și rearanjarea.

A.3. Inventarierea rețelei – managementul securității:

a) Soluția trebuie să permită integrarea cu domeniul Active Directory și să poată importa inventarul.
b) Trebuie să permită descoperirea stațiilor stații fizice neintegrate în Active Directory cu ajutorul Network discovery.
c) Soluția trebuie să ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare, adresa IP, politica aplicată, ultima dată când s-a conectat (online și/sau offline) și FQDN.

d) Soluția trebuie să permită crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Administratorul să poată descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac.
e) Soluția trebuie să permită instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale.
f) Soluția trebuie să permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.
g) Soluția trebuie să permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distantă pentru clientul antimalware.
h) Soluția trebuie să ofere posibilitatea de repornire a mașinilor fizice de la distantă.
i) Soluția trebuie să ofere informații detaliate despre fiecare task și să sesizeze dacă task-ul s-a finalizat sau nu cu succes.
j) Soluția trebuie să permită configurarea centralizată a clienților antimalware prin intermediul politicilor.
k) Soluția trebuie să ofere în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.

A.5. Politici:

a) Soluția trebuie să permită configurarea setărilor clientului antimalware prin intermediul unei singure politici care să conțină setări pentru toate module.
b) Politica trebuie să conțină opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user.
c) Soluția trebuie să permită aplicarea politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale.
d) Politica trebuie să poată fi schimbată automat în funcție de:
   a. IP sau clasa de IP al stației.
   b. Gateway-ul alocat.
   c. DNS serverul alocat.
   d. WINS serverul alocat.
   e. Sufix DNS pentru conexiunea dhcp.
   f. Clientul este/nu este în aceeași rețea cu infrastructura de management (stația de lucru poate soluționa implicit numele gazdei).
   g. Tipul rețelei (lan, wireless).

A.6. Rapoarte:

a) Soluția trebuie să conțină rapoarte care prezintă statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
b) Rapoartele programate trebuie să poată fi trimise către un număr nelimitat de adrese de email (nu este nevoie sa aibă un cont în consola de management).
c) Soluția trebuie să permită vizualizarea rapoartelor curente programate de administrator.
d) Soluția trebuie să permită exportarea rapoartelor în format .pdf și detaliile ca format .csv.
e) Soluția trebuie să includă un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. Astfel, soluția va trebui să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.
f) Interogarea legată de starea terminalului trebuie să includă informații precum:
   a. tip mașină.
   b. infrastructura rețelei căreia îi aparține terminalul.

c. datele agentului de securitate.
d. starea modulelor de protecție.
e. rolurile terminalelor.

g) Interogarea legată de evenimente terminal trebuie să includă informații precum:
a. calculatorul țintă pe care a avut loc evenimentul.
b. tipul starea și configurația agentului de securitate instalat.
c. starea modulelor și rolurilor de protecție instalate pe agentul de securitate.
d. denumirea și alocarea politicii.
e. utilizatorul autentificat în timpul evenimentului.
f. evenimente (site-uri blocate, aplicații blocate, detecțiile etc).

h) Interogarea legată de evenimente Exchange să includă informații precum:
a. Direcția traficului e-mail.
b. Evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate).
c. Măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau carantinarea fișierului, ștergerea sau respingerea e-mail-ului).

A.7. Carantina:

a) Soluția trebuie să permită restaurarea fișierelor carantinate în locația originală sau într-o cale configurabilă.
b) Carantina trebuie să fie locală, pe fiecare stație administrată și va trebui să poată fi administrată, fie local, fie din consola de management.

A.8. Utilizatori:

a) Administrarea trebuie să se poată să se facă pe baza de roluri.
b) Trebuie să permită roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat.
I. Administrator companie: administrează arhitectura consolei de management;
II. Administrator rețea: administrează serviciile de securitate;
III. Reporter: monitorizează și generează rapoarte.
c) Utilizatorii trebuie să poată fi importați din Microsoft Active Directory sau creați în consola de management.
d) Trebuie să permită configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări.
e) Trebuie să permită deconectarea automată a oricărui tip de utilizator după un anumit timp pentru o protecție sporită a datelor afișate în consola de administrare. Acest interval să poată fi personalizat de administratorul soluției.

A.9. Log-uri:

a) Trebuie să permită înregistrarea acțiunilor utilizatorilor.
b) Trebuie să ofere informații detaliate pentru fiecare acțiune a unui utilizator.
c) Trebuie să permită filtrarea acțiunilor utilizator după numele utilizatorului, acțiune.

A.10. Actualizare:

a) Trebuie să permită definirea de locații de actualizare multiple.
b) Trebuie să permită activarea/dezactivarea actualizărilor de produs și semnături.
c) Trebuie ca orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus.
d) Soluția trebuie să permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare va trebui să includă 2 tipuri de actualizări de produs:
I. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei;
II. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc).

e) Soluția va trebui să permită stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management.

B. PROTECȚIE STAȚII și SERVERE FIZICE/VIRTUALE

B.1. Caracteristici generale minimale și eliminatorii:

a) Pentru reducerea la minim a consumului de resurse, soluția antimalware va trebui să permită instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției antimalware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall).
b) Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includă un vaccin anti-ransomware. Acest vaccin va asigura protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare.
c) Vaccinul anti-ransomware trebuie să primească actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.
d) Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includă protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de învățare automată (machine learning).
e) Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includă un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil să identifice și remedieze în mod automatizat sau manual un număr mare de riscuri existente la nivel de rețea sau sistem de operare ce pot afecta funcționalitatea și nivelul de securizare al endpoint-ului.
f) Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includă un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" pentru a putea detecta atacuri avansate și activități suspecte în faza pre-execuție. Acest modul avansat de securitate va trebui să protejeze împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare menționat, vor trebui să li se poată stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv.
g) Modulul avansat de securitate trebuie să aibă posibilitatea de a raporta, bloca accesul, dezinfecta, șterge sau muta în carantină pentru fiecare din categoriile descrise. Astfel, administratorul va trebui să poată decide dacă dorește întâi monitorizare sau dorește și blocarea amenințărilor. Aceste acțiuni menționate, vor trebui să poată fi stabilite independent, pentru fișiere sau pentru traficul din rețea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenințările care ar fi fost detectate dacă nivelul de protecție era stabilit mai agresiv).
h) Pentru a oferi un nivel adițional de protecție a stațiilor și serverelor, soluția trebuie să includă un sandbox în cloud-ul public al producătorului acesteia.

- Modulul de Sandbox va trebui să poată trimiterea automată a fișierelor în Sandbox-ul din cloud-ul producătorului unde vor trebui să poată fi „detonate" pentru o analiză în profunzime.
- Modulul de Sandbox va trebui să includă doua variante de analiză: doar monitorizare sau blocare. În modul monitorizare utilizatorul va trebui să poată accesa fișierul dorit, pe când în modul blocare, utilizatorului va trebui să i se blocheze rularea fișierului până când Sandbox-ul din cloud-ul producătorului va da verdictul.
  - Modulul de Sandbox va trebui să includă două tipuri de acțiuni remediere: implicită și de siguranță. Pentru acțiunea implicită va trebui să se poată stabili: doar raportare,

dezinfecție, ștergere și carantinarea. Pentru acțiunea de siguranță va trebui să se poată stabili: ștergere sau carantinare.

- Modulul de Sandbox va trebui să includă și posibilitatea de trimitere manuală a fișierelor în Sandbox-ul din cloud-ul producătorului. Astfel, dacă administratorul va suspecta un fișier ca fiind malițios, să îl poată trimite manual în Sandbox pentru a fi „detonat" și a afla verdictul. Administratorul să aibă posibilitatea de a trimite mai multe fișiere deodată, cu posibilitate de a specifica dacă vor fi „detonate" individual sau toate în același timp.
- Modulul de Sandbox va trebui să poată suporta „detonarea" următoarelor tipuri de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.
- Fișierele menționate anterior, vor trebui să poată fi detectate corect chiar dacă sunt incluse în arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

i) Trebuie să conțină un modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response") capabil sa identifice amenințări avansate sau atacuri în curs de desfășurare. Acest modul va trebui să cuprindă colectare de date și evenimente despre hardware și software aferent fiecărei stații de lucru și să poată aduce informații detaliate referitoare la incidentele detectate, o hartă detaliată a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate - – HyperDetect. din punct de vedere funcțional modulul EDR ce va trebui să cuprindă 2 componente distincte: senzorul ce colectează și procesează datele respectiv partea de analiză de securitate care va avea ca obiect interpretarea acestora.

- Modulul EDR va trebui să aibă capacitatea de a evalua activitatea tipică a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și va trebui să poată raporta orice deviație de la acest comportament sub forma unui incident.
- Modulul EDR va trebui să permită filtrarea incidentelor din interfața grafică în funcție intervalul de timp, pe baza unui scor de încredere („confidence score"), indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cât și după IP, nume fișier, nume stație.
- Modulul va trebui să permită vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat după cum modelul: tabul „rezumat" care să poată genera o hartă de principiu a incidentului, tabul „timeline" care să detalieze incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, respectiv butonul „acționează" care să poată genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantină – la nivel de nod, investigații – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod).
- Modulul va trebui să poată bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferenta incidentului sau importate folosind un fișier CSV.
- Modulul va trebui să poată excepta fișiere non-malițioase de la acțiunea de investigare sau să poată genera/adauga un set de fișiere malițioase într-o lista neagră pentru a putea preveni mișcarea laterală a fișierelor/proceselor malițioase.
- Modulul va trebui să permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru a permite o investigare rapidă a gazdei, colecta date despre atac respectiv remedia în timp real breșe de securitate pentru a putea fi eliminate astfel posibile incertitudini privitoare la comportamentul potențial malițios al unor

fișiere/procese, în scopul reducerii timpului de remediere (downtime) în cazul în care un atac a avut succes și stația țintă trebuie reconfigurată/reinstalată, să poată permite executarea unor comenzi în linia de comandă care să se execute cu privilegii de kernel și care să permită eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare.

B.2. Cerințe de sistem:

a) Soluția trebuie să ofere compatibilitate cu:

- Sisteme de operare pentru stații de lucru: **Windows 10, Windows 8/8.1, Windows 7**, Windows Vista (SP1), Windows XP (SP3), **Mac OS X Mojave (10.14.x), Mac OS X High Sierra (10.13.x), Mac OS X Sierra (10.12.x), Mac OS X El Capitan (10.11.x), Mac OS X Yosemite (10.10.5), Mac OS X Mavericks (10.9.5);**
- Sisteme de operare embedded: **Windows 10 IoT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7,** Windows Embedded POSReady 2009, Windows Embedded Standard 2009, Windows XP Embedded with Service Pack 2, Windows XP Tablet PC Edition;
- Sisteme de operare pentru servere: **Windows Server 2019, Windows Server 2016 (inc Core), Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011,** Windows Small Business Server (SBS) 2008, **Windows Server 2008 R2**, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server;
- Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 6 sau mai recent, Ubuntu 14.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 SP4 sau mai recent, OpenSUSE LEAP 42.x sau mai recent, Fedora 25 sau mai recent, Debian 8.0 sau mai recent, Oracle Linux 6.3 sau mai recent, Amazon Linux AMI 2016.09 sau mai recent.

B.3. Administrare și instalare remote:

a) Înainte de instalare, administratorul trebuie să aibă posibilitatea să particularizeze pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.

b) Instalarea trebuie să se poată face în mai multe moduri:
   a. prin descărcarea directă a pachetului pe stația pe care se va face instalarea;
   b. prin instalarea la distanță, direct din consola de management;
   c. trimiterea pe email (oricâte adrese) a pachetului de instalare pentru Windows, Linux, Mac.

c) Instalarea clienților la distantă în alte locații decât cele în care este instalată consola de management trebuie să se poată face prin intermediul unui alt client antivirus existent în locațiile respective pentru a minimiza traficul în WAN.

d) În consolă trebuie să fie disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc.

e) Din consolă trebuie să se poată trimite o singură politică pentru configurarea integrală a clientului de pe stații/servere.

f) Consola trebuie să includă o secțiune, „Audit", unde să poată fi menționate toate acțiunile întreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc.

g) Trebuie să aibă posibilitatea creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cât și pentru cele pe 64 de biți.

h) Trebuie să aibă posibilitatea creări unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange.

i) Trebuie să aibă posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
j) Administratorul trebuie să aibă posibilitatea de a crea grupuri sau chiar subgrupuri, unde să poată muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu.
k) Trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu.

B.4. Caracteristici și funcționalități principale ale modulului antimalware:

a) Soluția trebuie să permită administratorului să stabilească acțiunea luată de produsul antimalware la detectarea unei amenințări noi. Astfel administratorul va trebui să poată alege între următoarele acțiuni:
   I. Acțiune implicită pentru fișiere infectate:
      - interzice accesul;
      - dezinfectează;
      - ștergere;
      - mută fișierele în carantină;
      - nici o acțiune.
   II. Acțiune alternativă pentru fișierele infectate:
      - interzice accesul;
      - dezinfectează;
      - ștergere;
      - mută fișierele în carantină.
   III. Acțiune implicită pentru fișierele suspecte:
      - interzice accesul;
      - ștergere;
      - mută fișierele în carantină;
      - nici o acțiune.
   IV. Acțiune alternativă pentru fișierele suspecte:
      - interzice accesul;
      - ștergere;
      - mută fișierele în carantină.
b) Scanarea automată în timp real trebuie să poată fi setată să nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor trebuind să poată fi definită de către administratorul soluției.
c) Trebuie să permită definirea până la 16 nivele de profunzime pentru scanarea în arhive.
d) Trebuie să permită scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos în scopul protejării sistemului de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă.
e) Trebuie să permită scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). De asemenea, va trebui să se poată anula scanarea în cazul în care sunt detectate unități care au informații stocate mai mult de « x » MB.
f) Trebuie să aibă posibilitatea scanării automate a emailurilor la nivelul stației de lucru pentru POP3/SMTP.
g) Trebuie să permită configurarea căilor ce urmează a fi scanate la cerere.
h) Clienții antimalware pentru workstation trbuie să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese.
i) Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware.

j) Trebuie să aibă posibilitatea de a configura ca scanările programate să se execute cu prioritate redusă.
k) Produsul antimalware trebuie să poată fi configurat să folosească scanarea în cloud, și parțial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea să se poată face cu o mașină de scanare instalată în rețea.
l) Administratorul trebuie să aibă posibilitatea de a personaliza și motoarele de scanare și să poată alege între mai multe tehnologii de scanare:
   - Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală va trebui să aibă toate semnăturile și motoarele stocate local.
   - Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare va trebui să asigure un consum mai bun de resurse, fără să implice scanarea locală.
   - Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu va trebui să se stocheaze local nici o semnătură, iar scanarea să poată fi transferată către serverul de securitate.
   - Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback pe Scanare locală (motoare full).
   - Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback pe Scanare hibrid (cloud public cu motoare light).
m) Pentru o protecție sporită, soluția antimalware trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazată pe monitorizarea proceselor.
n) Pentru o protecție sporita, soluția antimalware trebuie să aibă posibilitatea de a scana paginile HTTP.
o) Pentru o mai bună gestionare a antimalware instalat pe stații, produsul trebuie includă opțiunea de setare a unei parole pentru protecția la dezinstalare.
p) Pentru siguranța utilizatorului, clientul trebuie să includă un modul de antiphishing.
q) Soluția trebuie să ofere protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată.

B.5. Anti-Exploit-Avansat trebuie să permită:

a) Posibilitatea de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive.
b) Depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare.
c) Protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem" cum ar fi browserele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare.

B.6. Firewall:

a) Trebuie să aibă posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
b) Modulul trebuie să poată fi instalat/dezinstalat în funcție de preferința administratorului.
c) Trebuie să aibă posibilitatea de a defini rețele de încredere pentru mașina destinație.

B.7. Carantina:

a) Produsul antimalware trebuie să permită trimiterea automată a fișierelor din carantină către laboratoarele antimalware ale producătorului.
b) Trimiterea conținutului carantinei trebuie să poată fi expediat în mod automat, la un interval definit de administrator.

c) Produsul antimalware să trebuie permită ștergerea automată a fișierelor carantinate mai vechi de o anumită perioadă, pentru a nu încărca inutil spațiul de stocare.
d) Trebuie să existe posibilitatea de a restaura un fișier din carantină în locația lui originală.
e) Modulul de carantină trebuie să permită rescanarea obiectelor după fiecare actualizare de semnături.

B.8. Protecția datelor:

a) Produsul trebuie să permită blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

B.9. Controlul conținutului:

a) Consola trebuie să aibă integrat un modul dedicat controlului accesului la Internet cu următoarele particularități:
   I. Va trebui să permită blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini;
   II. Va trebui să permită blocarea accesului la Internet pe intervale orare;
   III. Va trebui să permită blocarea paginilor de internet care conțin anumite cuvinte cheie;
   IV. Va trebui să permită controlul accesului numai la anumite pagini de internet specificate de administrator;
   V. Va trebui să permită blocarea accesului la anumite aplicații definite de administrator;
   VI. Va trebui să permită restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

B.10. Controlul dispozitivelor:

a) Modulul trebuie să poată fi instalat/dezinstalat în funcție de preferința administratorului.
b) Modulul trebuie să permită controlul următoarelor tipuri de dispozitive:
   - Bluetooth Devices;
   - CDROM Devices;
   - Floppy Disk Drives;
   - Security Policies 153;
   - IEEE 1284.4;
   - IEEE 1394;
   - Imaging Devices;
   - Modems;
   - Tape Drives;
   - Windows Portable;
   - COM/LPT Ports;
   - SCSI Raid;
   - Printers;
   - Network Adapters;
   - Wireless Network Adapters;
   - Internal and External Storage.
c) Modulul trebuie să permită configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.
d) Modulul trebuie să permită configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

B.11. Power User:

a) Modulul trebuie să poată fi instalat/dezinstalat în funcție de preferința administratorului.

b) Modulul trebuie să permită posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii să aibă posibilitatea de a accesa și modifica setările clientului antimalware dintr-o consola disponibilă local pe mașina client.
c) Administratorul va trebui să poată suprascrie din consolă setările aplicate de utilizatorii Power User.

B.12. Actualizare:

a) Trebuie să aibă posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare).
b) Trebuie să permită un sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
c) Trebuie să permită actualizarea pentru locațiile remote prin intermediul unui client antimalware care va trebui să aibă și rol de server de actualizare.

Specificațiile tehnice care indică o anumită origine, sursă, producție, un procedeu special, o marcă de fabrică sau de comerț, un brevet de invenție, o licență de fabricație sunt menționate doar cu scopul de a identifica cu ușurință tipul de produs din punct de vedere conceptual si funcțional. Aceste specificații vor fi considerate ca având mențiunea de **„sau echivalent"**, iar ofertantul are obligația de a demonstra echivalenta produselor ofertate cu cele solicitate în prezentul caiet de sarcini.

3.4.2. Disponibilitate

Nu este cazul.

3.5. Extensibilitate/Modernizare

3.5.1. Garanții

Termenul de garanție va fi de minimum 12 luni de la data recepției, pe perioada cât se asigură suportul tehnic din partea producătorului.

Termenul de intervenție pentru constatarea neconcordanțelor/neconformităților apărute în termenul de garanție este de **2** zile de la notificare.

Termenul de remediere pentru produsul la care au apărut neconformități în perioada de garanție, este de maximum **7** zile de la constatare.

Produsul care în perioada de garanție îl înlocuiește pe cel necorespunzător, beneficiază de o nouă perioadă de garanție care începe de la data înlocuirii produsului.

3.5.2. Livrare, ambalare, etichetare, marcare, depozitare, transport si asigurare pe durata transportului

3.5.2.1. Cerințe privind livrarea

La livrare, produsele vor fi însoțite de următoarele documente de calitate:
- certificat garanție;
- certificat de calitate.

Termenul de livrare este: maximum **5** de zile de la data înregistrării contractului.

Un produs este considerat livrat când toate activitățile în cadrul contractului au fost realizate, produsul funcționează la parametrii agreați și este acceptat de beneficiar.

Fiecare produs va fi însoțit de toate părțile componente necesare punerii și menținerii în funcțiune.

3.5.2.2. Cerințe privind ambalarea

Nu este cazul.

3.5.2.3. Cerințe privind etichetarea și marcarea

Nu este cazul.

3.5.2.4. Cerințe privind depozitarea

Nu este cazul.

3.5.2.5. Cerințe privind transportul și asigurarea pe durata transportului

Transportul si toate costurile asociate sunt în sarcina exclusiva a ofertantului. Produsele vor fi asigurate împotriva pierderii sau deteriorării intervenite pe parcursul transportului si cauzate de orice factor extern.

3.5.3. Operațiuni cu titlu accesoriu

3.5.3.1. Instalare, punere în funcțiune, inspecții, teste

Nu este cazul.

3.5.3.2. Cerințe privind instruirea personalului

Nu este cazul.

3.5.3.3. Mentenanță preventivă în perioada de garanție

Nu este cazul.

3.5.3.4. Mentenanță corectivă în perioada post-garanție

Nu este cazul.

3.5.3.5. Suport tehnic

Acces la portalul de service on-line al producătorului, 24x7x365 zile Live Phone/Web/Chat Suport precum și asistență de la distanță.

Soluția trebuie să includă suport tehnic care să permită actualizări la zi pentru program, baze de viruși, atacatori, inclusiv trecerea la versiunile superioare care sunt publicate de producător în termenul contractual.

Condițiile minimale pentru suportul tehnic sunt:

- 12 ore pe zi de luni până vineri între orele 8:00 – 20:00;
- Timp de răspuns în funcție de severitatea incidentului
  - Critical (Severity 1) – 4 ore;
  - Major (Severity 2) – 8 ore;
  - Minor (Severity 3) – 12 ore.
- Metoda de acces/rezolvare a problemelor: interfață pagina web, email, telefon, remote acces.

3.5.4. Mediul în care este operat produsul

Nu este cazul.

3.5.5. Constrângeri privind locația unde se va efectua instalarea

Nu este cazul.

3.6. Atribuțiile și responsabilitățile părților

Obligațiile principale ale furnizorului:

1.- Furnizorul se obligă să livreze produsele, conform termenului de livrare din contract.

2.- Furnizorul se obligă să livreze produsele la standardele și/sau performanțele prezentate în propunerea tehnică si a caietului de sarcini;

3.- Furnizorul se obligă să despăgubească Entitatea contractanta împotriva oricăror:

i) reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalațiile sau utilajele folosite pentru sau în legătură cu produsele achiziționate;

ii) daune-interese, costuri, taxe și cheltuieli de orice natură, aferente, cu excepția situației în care o astfel de încălcare rezultă din respectarea caietului de sarcini întocmit de către achizitor.

Obligațiile principale ale entității contractante si beneficiarului:

1.- Entitatea contractantă se obligă să achiziționeze, produsele solicitate prin prezentul Caiet de Sarcini.

2.- Beneficiarul se obligă să recepționeze produsele în termenul convenit de la livrarea acestora.

3.- Entitatea contractanta se obligă să plătească prețul produselor către furnizor în termenul menționat în contract.

4. DOCUMENTAȚII CE TREBUIE FURNIZATE BENEFICIARULUI

Furnizorul va prezenta odată cu livrarea produselor:

- fișele tehnice ale produselor traduse in limba română.

5. RECEPȚII

Recepția va fi efectuată în maximum 10 zile din momentul transmiterii datelor de conectare pe platformă și livrării Certificatului de Licențiere emis de către producătorul soluției pentru Societatea Complexul Energetic Oltenia S.A din care sa rezulte in clar cele 600 de licențe deținute.

Pentru produsele cu defecțiuni ascunse sau care prezintă neconformități la recepție, reclamarea de către beneficiar va fi făcută în termen de **2** zile de la data constatării neconformităților. Delegatul furnizorului se va prezenta pentru constatarea deficiențelor în termen de **2** zile de la primirea comunicării.

Furnizorul are următoarele obligații:

- Să stabilească, la depistarea unei neconformități de către beneficiar în cadrul activității de recepție, în termen de **48** de ore, soluția pentru remediere și termenul pentru aplicarea acesteia.
- Să suporte costurile generate de încercările efectuate după eliminarea neconformităților.

6. MODALITĂȚI ȘI CONDIȚII DE PLATĂ

Plata produselor livrate se face în lei în baza facturii emise de furnizor și acceptate de către beneficiar, prin virament bancar sau compensare.

Plățile se fac în termen de 60 de zile calendaristice de la data recepției, conform prevederilor Legii nr. 72/2013.

Factura emisă de furnizor va conține datele de identificare complete și legal stabilite, inclusiv contul și banca pentru fiecare parte.

Facturarea contravalorii produselor se va face către **SOCIETATEA COMPLEXUL ENERGETIC OLTENIA S.A.**, societate administrata în sistem dualist, cu sediul în municipiul Târgu Jiu, Strada Alexandru Ioan Cuza, nr. 5, Județul Gorj, având C.U.I./C.I.F. RO 30267310, înregistrata în Registrul Comerțului de pe lângă Tribunalul Gorj sub nr. J18/311/31.05.2012, cont virament RO59 RZBR 0000 0600 1465 2248 deschis la Raiffeisen Bank, Sucursala Târgu Jiu.

Pe factură, sub rubrica "cumpărător", se va menționa beneficiarul.

Entitatea contractantă nu se angajează sub nici o forma la plăti în avans.

7. CADRUL LEGAL CARE GUVERNEAZĂ RELAȚIA DINTRE BENEFICIAR ȘI FURNIZOR (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Cadrul legal este reprezentat de: Legea nr. 99/2016 privind achizițiile sectoriale, Hotărârea Guvernului nr. 394/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului sectorial/acordului-cadru din Legea nr. 99/2016 privind achizițiile sectoriale, Legea nr. 101/2016 privind remediile și căile de atac în materie de atribuire a contractelor de achiziție publică, a contractelor sectoriale și a contractelor de concesiune de lucrări și concesiune de servicii, precum și pentru organizarea și funcționarea Consiliului Național de Soluționare a Contestațiilor.

Se vor avea în vedere respectarea următoarele normative, standarde (sau echivalente):

- SR EN ISO 17050 - 1 /2010 - Evaluarea conformității. Declarația de conformitate dată de furnizor. Partea 1. Cerințe generale;

- SR EN ISO 17050 - 2/2005 - Evaluarea conformității. Declarația de conformitate dată de furnizor. Partea 2. Documentație suport;
- Legea nr. 240/2004, cu modificările aduse prin Legea nr. 76/2012, privind răspunderea producătorilor pentru pagubele generate de produsul cu defecte;
- Ordonanța Guvernului nr. 20/2010, cu modificările aduse prin următoarele acte: Ordonanța Guvernului nr. 8/2012; Legea nr. 50/2015, privind stabilirea unor măsuri pentru aplicarea unitară a legislației Uniunii Europene care armonizează condițiile de comercializare a produselor;
- Legea nr. 449/2003, cu modificările si completările ulterioare, privind vânzarea produselor și garanțiile asociate acestora;
- OUG nr. 195/2005 privind protecția mediului, cu completările și modificările ulterioare;
- Legea nr. 319/2006 a securității și sănătății în muncă, cu completările și modificările ulterioare;
- Legea nr. 307/2006 privind apărarea împotriva incendiilor, cu completările și modificările ulterioare.

Execuția și/sau livrarea produselor se va face într-un sistem de management al calității certificat conform ISO 9001:2015, de un organism acreditat, sau echivalent.

8. MANAGEMENTUL/GESTIONAREA CONTRACTULUI ȘI ACTIVITĂȚII DE RAPORTARE ÎN CADRUL CONTRACTULUI

Părțile contractante au obligația de a numi și de a-și comunica reciproc, în cel mai scurt timp de la semnarea contractului, numele persoanelor specializate/responsabililor de contract, pentru a facilita buna derulare si rezolvare, în timp util, a tuturor problemelor impuse in derularea contractului.

Problemele apărute în perioada de derulare a contractului se vor rezolva cu reprezentanții derulatorului, iar orice modificare a prevederilor contractuale va fi soluționată prin act adițional perfectat între semnatarii prezentului contract.

8.1. Riscuri

Nu este cazul.

9. CERINȚE PRIVIND PREZENTAREA PROPUNERII TEHNICE ȘI FINANCIARE

9.1. Cerințe privind prezentarea propunerii tehnice

Propunerea tehnică va fi întocmită în limba română.

Propunerea tehnică va fi întocmită urmărind structura de conținut și cerințele din prezentul caiet de sarcini, astfel încât aceasta să respecte în totalitate cerințele prevăzute în acesta. Cerințele și specificațiile tehnice din caietul de sarcini vor fi tratate ca fiind cerințe minimale.

Propunerea tehnică va conține codul și producătorul produselor ofertate, termenul de garanție și termenul de livrare.

Se va prezenta fișa tehnică (tradusă în limba română) pentru fiecare produs ofertat.

Toate documentele justificative vor fi certificate de ofertant prin semnare.

Ofertantul trebuie să facă dovada că furnizarea produselor se realizează într-un sistem de management al calității, certificat de către un organism acreditat, pentru domeniul de activitate din sfera produselor ofertate, în conformitate cu standardul SR EN ISO 9001 ediția 2015, sau echivalent.

În cazul în care ofertantul care depune ofertă nu a avut acces la un certificat de calitate astfel cum este solicitat mai sus sau nu are posibilitatea de a-l obține în termenele stabilite, din motive care nu îi sunt imputabile, acesta va prezenta orice alte probe sau dovezi care să confirme asigurarea unui nivel corespunzător al calității, echivalent cu cel solicitat.

Ofertantul va completa tabelul de mai jos și-l va depune odată cu propunerea tehnică.

Nr. crt.	Specificații	Cerință		
		solicitată prin caietul de sarcini	**ofertată**	**poziția/locul unde se regăsește în ofertă (fișe/cataloage/desene etc.)**
0	1	2	3	4
1	Denumire	Licențe software de tip Endpoint Detection and Response (EDR)		
2	Unitate de măsură	buc		
3	Cantitate	600		
4	Specificații tehnice/cerințe funcționale minime	Conform subcap. 3.4.1.4.		
5	Durată minimă garanție	Minimum 12 luni de la data recepției		
6	Loc de livrare	Societatea Complexul Energetic Oltenia S.A., str. Alexandru Ioan Cuza nr. 5, municipiul Târgu Jiu, județul Gorj, România		
7	Termen/dată de livrare	Maximum 5 zile de la data înregistrării contractului.		
8	Cerințe privind transportul și asigurarea	Conform subcap.3.5.2.5.		
9	Suport tehnic	Conform subcap.3.5.3.5.		
10	Documentații si documente furnizate odată cu produsele	Conform subcap.3.5.2.1. și cap. 4.		

9.2. Cerințe privind prezentarea propunerii financiare

Propunerea financiara va fi întocmită în limba română.

Moneda de referința este „leul".

Se va completa propunerea financiară, precizându-se prețul unitar lei/u.m. (cu două zecimale) și valoarea totală în lei fără TVA. În prețul unitar vor fi incluse toate cheltuielile aferente.

10. DISPOZIȚII FINALE

Ofertantul va respecta regulile privind confidențialitatea datelor prin completarea și semnarea declarației de confidențialitate.

11. ANEXE

Nu este cazul.

	Funcția	**Prenume, nume**	**Semnătura**	**Data semnării**
Verificat/ Aprobat	**Șef Departament T.I.C.**	Vlad VANCA		15.04.2020
Elaborat	**Inginer Serv. A.S.C.**	Laurențiu Narcis PÎRVU		15.04.2020