BANCA NAȚIONALĂ A ROMÂNIEI

Direcția Servicii Informatice

Aprob,

Ovidiu Dragomir

Director

CAIET DE SARCINI

privind achiziționarea unui sistem de protecție anti-malware

I. Forma documentului:

Inițială	x
Modificată	
Numărul revizuirii	

Elemente privind operațiunea de revizuire a Caietului de sarcini - modificare, adăugare, suprimare sau altele asemenea - în perioada planificării portofoliului de procese de achiziție publică sau a procesului de achiziție publică:

Nr. rev.	Obiectul modificării	Data realizării modificării	Capitolul revizuit	Motivul	Persoana care realizează modificarea	Semnătura persoanei care realizează modificarea	Persoana care aprobă modificarea	Semnătura persoanei care aprobă	Data aprobării modificării
[Nr revi-zuirii]		*[Introduceți: zz-ll-aaaa]*	*[Capitolul revizuit]*	*[Introdu ceți]*	*[Introduceți numele, compartimen tul, funcția]*		*[Introduceți numele și funcția]*		*[Introduceți: zz-ll-aaaa]*

II. Denumirea contractului

Achizitia unei soluții de protecție anti-malware, precum și a serviciilor conexe de instalare, configurare, testare, punere în productie și suport post instalare.

III. Informații generale

Obiectul contractului:

Obiectivul principal al acestei proceduri îl reprezintă achizitionarea și implementarea unui soluții de securitate informatică ce va permite Băncii Nationale a României să detecteze, să analizeze și să răspundă la atacuri cibernetice în timp real, atacuri ce au ca țintă infrastructura tehnică hardware și software a bancii, utilizată pentru operarea aplicatiilor informatice critice.

Soluția de securitate informatică va permite identificarea de anomalii de rețea, va permite detectarea amenintatilor de tip „Advanced Persistent Threat" (APT) și va include o solutie de emulare a amenințărilor de tip „zero-day". Acest sistem va complementa sistemul de securitate existent, astfel încât specialiștii de securitate BNR să obțină vizibilitate în cazul unor atacuri de tipul Zero-Day threat si va furniza informatii necesare pentru a atenua riscul cauzat de potentiale atacuri.

Tipul de contract: achiziție publică de produse precum și a serviciilor aferente de instalare/ integrare în cadrul infrastructurii informatice a autorității contractante, testare/validare a capabilitătilor solutiei , precum și instruirea personalului de specialitate.

Atribuțiile și responsabilitățile BNR în implementarea contractului, inclusiv preluarea riscurilor ce cad în sfera de control a acesteia:

- Directia Servicii Informatice (DSI) din cadrul BNR va raspunde de managementul contractului și de sarcinile specifice:
    - desemnarea echipei implicate și responsabile cu interacțiunea și suportul asigurat de către Contractant;
    - punerea la dispoziția Contractantului a tuturor informațiilor necesare pentru livrarea solutiei;
    - asigurarea tuturor resurselor care sunt în sarcina sa pentru buna derulare a Contractului.
- Mecanismul de monitorizare a activităților/bunurilor livrate de furnizor:
  Autoritatea Contractantă consideră obligatorie o abordare generală bazată pe o metodologie recunoscuta international de Management de proiect.

IV. Specificații tehnice si functionale:

Cerințe generale soluție de securitate informatică

4.1. Soluția de securitate informatică va fi formată din 2 sisteme:

I. Sistemul pentru analiză și detecție;

II. Sistemul pentru vizibilitate la nivelul rețelei;

4.2. Se vor achizitiona cate 2 soluții similare care vor fi instalate în 2 centre de date ale autorității contractante, diferența fiind volumul de trafic ce urmează a fi inspectat, dupa cum urmează:

a. Soluția de securitate informatică pentru infrastructura de la sediul central al BNR, soluție capabilă să proceseze un volum de trafic de minim 10Gbps;

b. Soluția de securitate informatică pentru infrastructura de la sediul secundar BNR, soluție capabilă sa procese un volul de trafic de minim 4Gbps.

4.3. Suplimentar, pentru interconectarea sistemului de securitate cu infrastructura BNR prin intermediul subsistemului care va asigura vizibilitate la nivelul rețelei, se vor achizitiona:

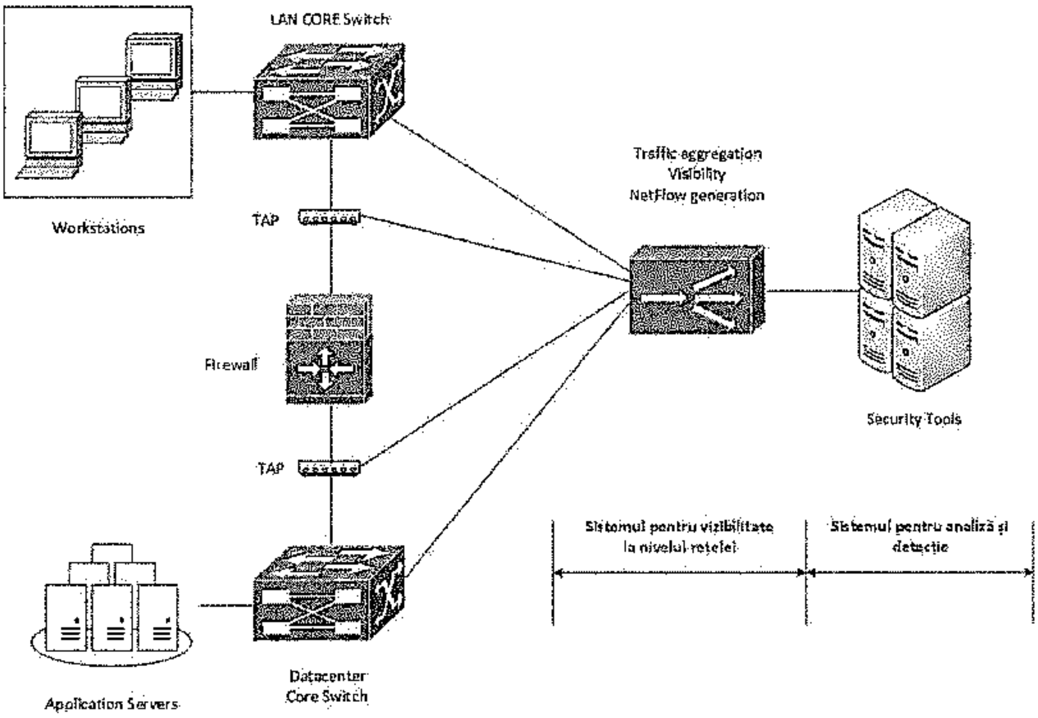
- 24x echipamente de tip „Traffic Access Point" (TAP) optic
- 4x rack-uri 19" pentru TAP

4.4. Solutiile oferate vor include servicii servicii de management de proiect, instalare, configurare la locatiile BNR, instruire personal precum si suport local si de la producator dupa trecerea in productie.

Ficare sistem de analiză și detecție în parte, care va fi instalat la sediul principal, respectiv sediul secundar, trebuie să indeplinească următoarele specificații minime obligatorii

Arhitectură și mod de funcționare soluție de securitate informatică

4.5. La modul general, schema bloc simplificată pentru arhitectura soluției de securitate avută in vedere este:



4.6. Arhitectura solutiei de securitate trebuie să fie flexibilă, să permită instalarea si configurarea acesteia fără a perturba mediul de productie al Bancii Nationale a Romaniei;

4.7. **Sistemul de analiză și detecție** pentru breșele de securitate se va integra în rețea BNR prin intermediul unui **sistem de vizibilitate la nivel infrastructură de rețea,** sistem hardware si software care va asigura o monitorizare și descoperire continuă a resurselor din rețea.

4.8. Pentru conectarea sistemului de analiză si detectie fără a fi impactată infrastructura BNR se urmăreste achizitionarea unui soluții de vizibilitate la infrastructurii de comunicatii, bazat pe un „appliance" de tip „all-in-one" și sisteme de interceptie de tip **„Traffic Access Point (TAP)"** care vor permite conectarea și agregarea traficului din zone / segmente diferite de rețea.

4.9. Cele 2 soluții care vor fi instalate la fiecare din centrele de date în parte vor functiona în mod independent.

Sistemul de analiză și detecție

Cerințe generale sistem de analiză și detecție

4.10.**Sistemul de analiză și detecție** va include următoarele subsisteme (hardware si software):

a) **componentă de tip senzor**, care să permită preluarea în timp real a copiei traficului de rețea, normalizarea și analiza acestuia.

b) **componentă de tip sandbox**, care să permită simularea rulării probelor suspicioase într-un mediu virtualizat izolat, în vederea descoperirii comportamentului de atac.
c) **management centralizat**, care să dispună de funcționalități de colectare centralizată a evenimentelor, gestiunea componentelor, portal de schimb de informații cu privire la indicatorii de compromis.

4.11. Sistemul de securitate informatică trebuie să permită monitorizarea traficului de rețea nord-sud și est-vest, pentru a putea construi o vizibilitate completă asupra tuturor aspectelor legate de atacurile direcționate, amenințările avansate și de tip „ransomware".

4.12. Sistemul de securitate informatică trebuie să conțină tehnologii specializate de detecție, inclusiv un mediu de sandbox local, în vederea identificarii atacurilor cu malware avansat si necunoscut, ransomware, exploituri zero-day, comunicații către centre de comandă și control, mișcare laterală în rețea și exfiltrare de date.

4.13. Sistemul de analiză și detecție ofertattrebuie să fie recunoscut de instanțe de validare externe (de ex. NSS Labs) ca fiind recomandată și cu un nivel de eficacitate a securității de peste 95% sau cu o rată de detecție a amenințărilor avansate de 95%.

4.14. Sistemul de analiză și detecție trebuie să ofere următoarele capabilități:
a) trebuie să monitorizeze peste 100 de protocoale și aplicații pentru a detecta aplicatii de tip „malware" și activitatea atacatorului pe întreg ciclul de viață al atacului;
b) va permite o abordare consolidată pentru o gamă largă de protocoale pentru a ajuta la identificarea exploatării și exfiltrarea datelor pe mai multe canale de comunicatii, nu doar a celor uzuale, dupa cum sunt aplicatiile web și e-mail;
c) solutia va include o componenta de emulare complet integrată pentru a ajuta la identificarea vulnerabilitatii și remedierea riscului cauzat de vulnerabilitățile de tip „zero-day". Aceasta va contine un modul de tip sandboxing personalizat, motoare și reguli avansate de detectare, informații despre amenințări și actualizări de securitate care, atunci când sunt combinate, vor permite Bancii Nationale a Romaniei să detecteze, să se adapteze și să răspundă la atacuri țintite și amenințări avansate;
d) Modulul sandboxing va rula mai multe motoare de detectare, reguli de corelație și informații de protecție inteligentă ce vor va permite detecția de malware pentru sisteme de operare Windows, Mac OS, Linux, precum și malware-ul mobil;
e) Modulul sandboxing va permite detecția de malware cunoscut și necunoscut atât pentru platformele Windows 32 cât și pe 64 biți;

4.15. Sistemul de analiză și detecție ofertat va include acces la infrastructura de tip „threat inteligence" a producătorului și la un portal de informații despre amenințări cibernetice, alimentat cu date de la sute de milioane de informatii de pe glob.

4.16.Toate motoarele de scanare, tehnologiile și componentele de detecție locale și de tip „cloud" ale sistemului trebuie să fie proprii ale producătorului și trebuie să fie incluse în soluție fără costuri suplimentare pentru autoritatea contractantă;

Cerințe funcționale pentru sistemul de analiză și detecție

4.17. Sistemul de analiză și detecție va avea capabilitatea de a descoperi atacurile în care se utilizează protocoale standard care rulează pe porturi non-standard.

4.18. Sistemul de analiză și detecție va pemite urmărirea unui atac cibernetic în toate stadiile sale, astfel încât să poată furniza informații despre cel puțin următoarele faze de atac: puncte de intrare, conexiuni C&C, miscare laterală și propagare, identificare resurse și exfiltrare de date.

4.19. Sistemul de analiză și detecție va detecta atacurile cu malware polimorfic, de tip zero-day, pentru care nu există semnături.

4.20. Sistemul de analiză și detecție va dispune de mecanisme de detecție a amenințărilor cunoscute, cât și pe cele potențiale, pentru care nu există semnături.

4.21. Sistemul de analiză și detecție va putea fi configurat pentru a monitoriza tot traficul sau doar anumite zone din rețea, și doar anumite porturi.

4.22. Sistemul de analiză și detecție va include servicii de prefiltrare pentru a optimiza analiza locală inițială, cum ar fi:

i. servicii de reputație web și e-mail
ii. servicii de reputație a aplicațiilor sau fișierelor
iii. liste de prevalență a fișierelor.

4.23. Sistemul de analiză și detecție va dispune de un set de reguli de detecție preconfigurate și gestionate de către producător, grupate pe niveluri de încredere și pe categorii de risc, care să poată fi activate sau dezactivate din interfața de management.

4.24. Sistemul de analiză și detecție va asigura detectarea comportamentelor suspicioase și a mișcărilor laterale, inclusiv prin utilizarea uneltelor de administrare legitime în mod fraudulos (cum ar fi PSExec, WMI), ca parte a unui atac.

4.25. Sistemul de analiză și detecție va dispune de mecanisme eficiente de detectie a conexiunilor comandă și control (C&C) nu doar din punct de vedere reputațional, ci și din perspectiva execuției. Soluția trebuie să poată simula accesul către resursele URL suspicioase pentru a valida că sunt într-adevăr C&C.

4.26. Sistemul de analiză și detecție trebuie să permită definirea zonelor de rețea într-o structură ierarhică multi-nivel, domenii interne, dar și sisteme critice, în funcție de rolurile funcționale ale acestora în infrastructură (de ex: web server, mail server, server Active Directory, etc).

4.27. Sistemul de analiză și detecție trebuie să permită detectarea cel puțin a următoarelor tipuri de atacuri:

i. amenințări zero-day
ii. atacuri cu embedded exploit code
iii. detecția în baza regulilor pentru vulnerabilitățile cunoscute
iv. parsere pentru gestiunea fișierelor deformate
v. detecția și analiza exploiturilor din documente
vi. detecția eficientă a tipului real de fișier analizat (nu doar pe bază de extensie)
vii. detecție a emulării de scripturi.

4.28. Sistemul de analiză și detecție trebuie să dispună de un mecanism de captură a pachetelor de rețea în timp real, parametrizabil în functie de anumite surse sau destinații de trafic și pe baza criteriilor legate de detecție: tipul detecției sau niveluri de risc al acesteia.

4.29. Capturile de trafic parametrizate trebuie să poată fi stocate în echipament pentru o perioadă de cel puțin o lună. Perioada de timp pentru stocarea capturilor de trafic trebuie să fie configurabilă.

Administrare și investigare a sistemului de analiză și detecție

4.30. Sistemul de analiză și detecție trebuie să dispună de ecrane operaționale de investigare a evenimentelor și incidentelor detectate, în care să se regasească informații despre:

i. actorii implicați în eveniment (sursă și destinație);
ii. amenințarea detectată;
iii. nivelul de risc;
iv. denumirea și referința către aceasta în nomenclatorul informațional al producătorului;

v. sume de control ale fișierului analizat sau detalii despre alte tipuri de artefacte investigate;

vi. faza de atac în care se încadrează evenimentul.

4.31. Sistemul de analiză și detecție trebuie să permită operații de filtrare avansată pentru identificarea evenimentelor relevante, folosind cel puțin urmatoarele tipuri de filtre:

i. detalii despre host: IP, hostname, adresa MAC;

ii. trafic de rețea: protocoale folosite, direcție de trafic;

iii. detalii despre detecție: tip de detecție, faza de atac, referințe despre amenințare, detalii C&C, analiza în sandbox, captura de trafic;

iv. detalii despre obiectul sau proba detectate: denumire fișier, indicatori de compromis (IP, domeniu, URL, hash fisier), tipul de detecție a fișierului;

v. nivelul de risc;

vi. perioada identificării evenimentelor.

4.32. Sistemul de analiză și detecție trebuie să permită descarcarea din interfața de management a obiectelor/probelor identificate ca fiind amenințări în cadrul unui eveniment, cât și a capturilor de trafic.

4.33. Sistemul de analiză și detecție trebuie să dispună de ecrane cu informații corelate pe fazele de atac, pentru fiecare dintre resursele implicate în evenimentele detectate.

4.34. Sistemul de analiză și detecție trebuie să includă mecanismele de scanare retroactivă să poată rula în mod programat, periodic, dar și la cerere, în mod manual.

4.35. Mecanismele de scanare retroactivă să poată folosi liste cu resurse C&C actualizate în mod automat de către producător, dar și liste personalizate de resurse C&C, furnizate de către administratorii soluției.

4.36. Sistemul de analiză și detecție trebuie să permită accesul la informații extinse despre amenințările detectate și prevalența acestora (cum ar fi de pildă: tipul și comportamentul obiectului malware detectat, informații din CVE, exploituri folosite, hash-uri de fișiere, etc), indiferent că sunt livrate local sau dintr-un serviciu informațional al producătorului de tip „Threat Intelligence". Accesul la serviciul informațional trebuie să fie furnizat ca parte a soluției, fără costuri suplimentare.

4.37. Sistemul de analiză și detecție să dispună de următoarele funcționalități în ceea ce privește gestiunea indicatorilor de compromis:

a) Să permită adăugarea și stergerea manuală de indicatori de compromis care să fie ulterior folosiți ca elemente de analiză, și care să conțină cel puțin următoarele tipuri de obiecte: sume de control sau hash pentru fișiere, adrese IP, URL și domenii.
b) Să permită adăugarea de indicatori de compromis prin import în interfața web a unor liste de tip STIX în format XML, care să conțină cel puțin următoarele tipuri de obiecte: liste cu sume de control/hash-uri de fișiere, liste de adrese IP, liste de URL și liste de domenii.
c) Să permită adăugarea, importul și ștergerea de excepții pentru obiectele suspicioase, care să poată rescrie indicatorii de compromis rezultați în urma detecției și analizei, dar și a celor importați în mod manual în interfața de management centralizat a soluției.
d) Să permită utilizarea unor liste particularizate de obiecte permise și de obiecte blocate.
e) Prin intermediul consolei de management centralizat, soluția să permită importul listelor de indicatori de compromis și de atac în cel puțin următoarele moduri: import manual de reguli YARA, import de fisiere STIX, liste personalizate de IOC, import de IOC din resurse de tip feed, precum și prin importul IOC detectați de către senzorii soluției și sincronizați in componenta de management centralizat.

4.38. Prin intermediul consolei de management centralizat, sistemul de analiză și detecție trebuie să permită partajarea informațiilor cu privire la IOC printr-un server TAXII propriu, inclus în soluție, servicii web sau prin integrare nativă cu alte soluții.

Componenta de sandbox a sistemului de analiză și detecție

4.39. Componenta de „sandboxing" a sistemului de analiză și detecție trebuie să permită particularizarea rapidă și eficientă a sistemelor din mediul virtual din sandbox, folosind unelte și proceduri flexibile și ușor de utilizat pentru administratori, astfel încât să acopere cerințele și particularitățile interne ale sistemelor organizației, inclusiv prin utilizarea de copii de tip șablon standard al stațiilor de lucru interne.

4.40. Componenta de „sandboxing" a sistemului de analiză și detecție trebuie să poată rula cel puțin 2 tipuri de sisteme virtuale pentru simulare și cel puțin cate 8 instanțe ale acestora, în total minim 16 instanțe.

4.41. Imaginile virtuale ale sistemelor din sandbox trebuie să acopere cel puțin următoarele aspecte de configurație: sistem de operare, suita MS Office și aplicații de sistem: Adobe Reader, Adobe Flash, JavaScript, .NET Framework, etc.

4.42. Sistemele virtuale din mediul intern de sandbox al soluției trebuie să poată avea configurații regionalizate, cum ar fi de pildă: sistem de operare și aplicații cu interfețe în limba română.

4.43. Sistemul de analiză și detecție va suporta următoarele sisteme de operare configurabile ca imagini virtuale în mediul de sandbox intern: Windows 7 32bit/64bit, Windows 8/8.1 32bit/64bit, Windows 10 32bit/64bit, Windows Server 2003, 2008, 2012/R2, 2016, 2019

4.44. Componenta de sandbox trebuie să permită conectarea la o rețea dedicată cu acces la internet pentru sistemele din mediul virtual din sandbox, separată de rețeaua interfeței de management.

4.45. Sistemul de analiză și detecție trebuie să asigure posibilitatea configurării centralizate a unui proxy de acces la internet pentru toate sistemele virtuale din soluția de sandbox.

4.46. Sistemul de analiză și detecție trebuie să dispună de urmatoarele tehnologii de analiză în mediul virtual de sandbox:

i. analiza statica
ii. analiza euristica
iii. analiza comportamentala
iv. reputatie web
v. reputatie a fisierelor
vi. detectia conexiunilor de iesire suspicioase ale anumitor obiecte catre destinatii C&C
vii. modificari ale fisierelor de sistem sau cheilor de registri
viii. comportamente anormale

4.47. Componenta de sandbox trebuie să dispună de tehnici și controale avansate de anti-evasion, la mai multe niveluri: informații despre sistem, memorie, regiștri, sistem de fisiere, dispozitive și mecanisme pentru interfața grafică.

4.48. Componenta de sandbox trebuie să conțină suport de analiză pentru cel puțin următoarele tipuri de fișiere:

i. Office (doc, docx, rtf, xls, xlsx, ppt, pptx)
ii. executabile (bat, cell, class, cmd, exe, ps1, vbs, vbe)
iii. resurse și scripturi (chm, htm, iqy, mov, slk, swf, svg, xml, wsf)

4.49. Componenta de sandbox trebuie să dispună de metode de detecție pentru ransomware, cel puțin pentru următoarele tipuri de mecanisme: script emulation, zero-day exploit, password-protected malware attack.

4.50. Componenta de sandbox trebuie să conțina mecanisme de analiză a arhivelor, inclusiv arhive multi-nivel. În cadrul arhivelor criptate sau protejate cu parole, trebuie să existe posibilitatea utilizării unei liste cu parole pentru decriptare.

4.51. Rezultatele analizei în sandbox trebuie să fie disponibile în format PDF sau HTML și să cuprindă cel puțin următoarele detalii: imaginile virtuale în care s-a făcut analiza, comportamentul în mediul de sandbox, activitate pe sistem, tipul detecției, informații despre caracteristicile amenințării identificate, nivelul de risc al amenințării, obiecte analizate, inclusiv acțiuni de creare fișiere, modificări regiștri și configurații de sistem, precum și detalii legate de conexiunile de rețea.

4.52. Sistemul de analiză și detecție trebuie să poată a folosi minim 3000 de reguli YARA pentru analiză și detecția de malware în sandbox.

4.53. Sistemul de analiză și detecție ofertat trebuie să pemită managementul centralizat al tuturor alertelor, jurnalelor și rapoartelor pentru toate componentele de detecție și analiză.

Capabilități de alertare și raportare a sistemului de analiză și detecție

4.54. Sistemul de analiză și detecție trebuie să suporte mecanisme de afișare a alertelor, rapoartelor și logurilor administrative de sistem, care să implementeze cel puțin următoarele opțiuni:

i. Un sistem de alerte și notificări, care, în baza unor reguli predefinite, să poată trimite e-mailuri către liste de contacte configurabile în soluție. Conținutul mesajelor transmise să fie configurabil astfel încât să includă și variabile dinamice, cum ar fi: ora și data, surse și destinații de rețea implicate, lista de componente, detalii despre detecții, amenințări, comportamente, detalii despre analiza în sandbox, etc. Aceste notificari să poată fi activate și dezactivate din interfața web, iar frecvența trimiterii lor trebuie să poată fi configurata de către administrator.

ii. Rapoarte la cerere sau programate, în format PDF, care să se poată trimite prin e-mail către liste de contacte sau să se poată descarca direct din interfața web a soluției.

iii. Șabloane predefinite de rapoarte executive.

iv. Loguri de sistem disponibile în interfața web, în care să se poată opera căutari și filtrari, cel puțin în funcție de tipul evenimentului, dată/timp sau perioadă, utilizator cu drepturi administrative în interfața web de management.

v. Logurile de sistem să poată fi exportate cel puțin în format CSV, integral sau particularizat în urma aplicării filtrelor în interfața de management.

vi. Cel puțin următoarele tipuri de evenimente generate de către soluție să poată fi trimise către sisteme externe de syslog sau SIEM: evenimente de sistem și legate de actualizări de sistem, evenimente legate de detecții: conținut rău-intenționat, comportamente suspicioase, exploituri, grayware, resurse URL rău-intenționate, detecții în urma analizei în sandbox, incidente corelate, scanare retroactivă.

vii. Logurile trimise către sisteme externe de syslog sau SIEM să fie structurate cel puțin în următoarele formate standard: Common Event Format (CEF) și Log Event Extended Format (LEEF).

viii. Posibilitatea de extragere a logurilor de debug ale sistemului, în funcție de componentele funcționale și de nivelurile de debug.

Consola de management pentru sistemul de analiză și detecție

4.55. Sistemul de analiză și detecție ofertat trebuie să suporte managementul centralizat al componentelor care asigură inspecția și analiza traficului, prin intermediul componentei de management centralizat.

4.56. Sistemul de analiză și detecție trebuie să conțină următoarele funcționalități de ordin administrativ în cadrul interfeței de management a componentelor de detecție și analiză:

i. O consolă unică de management a echipamentului, inclusă, din care să se poată configura toate aspectele administrative ale soluției.

ii. In cazul interfetei de tip web, obligatoriu consola de administrare va utiliza HTTPS cu certificate private emise de către BNR.

iii. Consola de management trebuie să includă ecrane de tip tablou de bord (dashboard), cu module configurabile pentru cel puțin următoarele tipuri de informații:

a. sumarul amenințărilor pe categorii de detecții și perioade de timp, harta cu locațiile geografice ale surselor de atac pe categorii de detecții și perioade de timp.

b. top comportamente detectate.

c. top sisteme infectate cu malware, grayware, exploituri sau aplicații perturbatoare.

d. top resurse URL sau conținut rău-intenționate detectate.

e. liste de urmărire pentru sisteme, configurabile în funcție de detecții, dar și parametri de status al sistemului.

iv. Se va asigura posibilitatea de backup și restaurare a configurației sistemului, prin export sau import din interfața de management;

v. Se va asigura posibilitatea de optimizare a spațiului pe disc prin ștergerea logurilor, rapoartelor, și capturilor de trafic în funcție de tipul sau de vechimea acestora, direct din interfața de administrare;

vi. Actualizările de sistem trebuie să poată fi ușor de gestionat din interfața de management, prin import.

vii. Actualizările motoarelor interne de scanare trebuie să se poată realiza în mod automat sau la cerere;

viii. Consola de management trebuie să implementeze un mecanism de drepturi de acces bazat pe roluri operaționale, cu posibilitatea utilizării unor servere de autentificare externe (LDAP, Active Directory).

4.57. Sistemul de analiză și detecție trebuie să dispuna de o interfața API prin intermediul căreia să se poată extinde capabilitățile soluției către orice tip de aplicație sau sistem care poate interoga rezultatele analizei soluției, și să acopere cel puțin următoarele tipuri de acțiuni: interogarea listelor de indicatori de compromis, a listelor predefinite de obiecte permise și blocate, extragerea unor evenimente de sistem.

4.58. Sistemul de analiză și detecție trebuie să poată fi integrată cu soluții ale producătorului sau cu soluții ale altor producători, astfel încât informațiile legate de amenințările detectate să poată fi folosite pentru a construi reguli active de protecție în celelalte soluții configurate inline sau în mod activ în infrastructură. În sensul acestei integrări, soluția să poată include în evenimentele transmise și informații legate de instrucțiuni de blocare/reset, pe care soluțiile integrate să le poată înțelege și procesa.

4.59. Componenta de management centralizat trebuie să poată rula ca sistem virtual la nivelul unei platforme de virtualizare.

4.60. Managementul componentelor care asigură inspecția, analiza si normalizarea informațiilor cu privire la traficul de rețea din cadrul soluției propuse să fie realizat prin intermediul unei interfețe web de administrare, fără a fi necesară instalarea unei componente software auxiliare (aplicație de tip fat-client).

Caracteristici hardware pentru sistemul de analiză și detecție

4.61. Componenta de detecție și analiză a soluției să fie livrată într-o configurație de echipamente hardware all-in-one de tip servere rack-abile, cu dimensiunea de maxim 2x RU rackspace, și care să includă toate funcționalitățile descrise anterior.

4.62. Configurația hardware al soluției de detecție a breșelor de securitate să asigure inspectarea și procesarea unui volum de trafic de 10 Gbps la sediul principal al autorității contractante, respectiv 4 Gbps de trafic de rețea în centrul secundar de date.

4.63. Componentele de detecție să fie echipate cu interfete de rețea după cum urmează:

i. interfață de 1 Gbps pentru management (separată de interfețele de procesare a traficului)
ii. cel puțin 4 interfețe de 1Gbps (RJ45) pentru traficul de date, din care una din interfețe să poate fi alocată pentru accesul la internet al sandboxului intern
iii. cel puțin 4 interfețe de 10 Gbps (fibră optică multi-mode) pentru traficul de date

4.64. Soluția ofertată să includă toate elementele auxiliare accesorii pentru echipamentele hardware: cabluri de alimentare pentru alimentare din PDU, conectori SFP pentru interfetele optice sau electrice după caz, șine pentru montarea în rack 19", etc.

4.65. Echipamentele hardware din componenta de detecție trebuie să asigure redundanță la nivelul surselor de tensiune și a discurilor de stocare.

4.66. Componenta de management centralizat și portal de partajare de informații cu privire la indicatorii de compromis trebuie să poată fi instalată în următoarele sisteme de virtualizare:
i. VMware vSphere ESXi 6.7 sau ulterior,
ii. Microsoft Hyper-V pe Windows Server 2019 sau ulterior

4.67. Componenta de management centralizat trebuie dimensionată astfel încât să asigure o retenție minimă a logurilor de detecție pentru 180 de zile.

Sistemul pentru vizibilitate la nivelul rețelei

Cerințe generale ale sistemului pentru vizibilitate la nivelul rețelei

4.68. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte o capacitate de transfer internă (în backplane) de cel putin 640Gbps;

4.69. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte gruparea optională a cel putin 10 echipamente într-un sistem de tip cluster, sistem logic cu capacități de configurare unitară la nivelul clusterului.

4.70. Sistemul pentru vizibilitate la nivelul rețelei trebuie să funcționeze la viteza maximă de transfer a interfetei de unde se preia traficul de rețea, fără pierderi de pachete.

4.71. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte cel putin 64 de porturi de 10Gbps în 1x RU rackspace;

4.72. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte cel puțin 4 porturi native 40Gbps în 1x RU rackspace;

4.73. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte agregarea porturilor, maparea portului de intrare la portul de iesire printr-o interfață grafică simplă, fără a necesita codarea într-o interfață cu linii de comandă.

4.74. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte configurarea tuturor optiunilor de filtrare într-o interfață grafică.

4.75. Sistemul pentru vizibilitate la nivelul rețelei trebuie sa permită schimbarea tipului interfetei de retea din 1Gbps in 10Gbps și invers doar prin alocarea licentei corespunzatoare.

4.76. Sistemul pentru vizibilitate la nivelul rețelei trebuie să fie flexibila din punctul de vedere al porturilor de rețea si sa suporte atât porturi de 1G cat si de 10G. Același port trebuie să fi compatibil cu 1Gbps sau 10Gbps in funcție de tipul de transmițător al portului, SFP sau respectiv SFP+.

4.77. Sistemul pentru vizibilitate la nivelul rețelei trebuie sa suporte pachete de mărime foarte mare (jumbo frames) de peste 9100B

4.78. Echipamentele hardware sa suporte surse complet redundante de curent continuu sau alternativ.

4.79. Echipamentele hardware sa suporte surse de curent alternativ capabile sa lucreze la 100-240 VAC.

4.80. Echipamentele hardware sa suporte surse de curent continuu capabile sa lucreze la tensiuni de la 40 pana la -60 V

4.81. Echipamentele hardware trebuie să suporte schimbarea surselor de curent si a ventilatoarelor fără a fi necesara repornirea echipamentului.

4.82. Echipamentele hardware trebuie sa permită montarea in rack-uri standard de 19 inch.

4.83. Echipamentele hardware trebuie sa aibă răcire cu flux de aer front-to-back.

4.84. Sistemul pentru vizibilitate la nivelul rețelei trebuie sa fie compatibilă cu următoarele tipuri de transceivere:

- 1000Base-T
- 1000Base-SX
- 1000Base-LX
- 10GBASE-SR
- 10GBASE-LR
- 10GBASE-T-XCVR
- 40GBASE-SR4
- 40GBASE-LR4
- 40 Gig BiDi, Multimode SR RX-only
- 40 Gig BiDi, Multimode SR (Tx and Rx)

4.85. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte porturi flexibile de intrare (sursa de trafic) sau ieșire (destinație de trafic).

4.86. Toate porturile trebuie să poată fi configurate de către utilizator ca porturi de intrare sau iesire.

4.87. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită ca fiecare port sa fie utilizat simultan pentru intrare si iesire.

4.88. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită definirea de porturi de rețea logice de tip buclă software.

Administrare și monitorizare a sistemului pentru vizibilitate la nivelul rețelei

4.89. Sistemul pentru vizibilitate la nivelul rețelei trebuie sa aibă o interfață grafică de tip web (WEB GUI) intuitivă pentru administrare.

4.90. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte configurarea integral utilizând interfață grafică.

4.91. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte configurarea drepturilor de acces pe baza de rol si grupuri de utilizatori. Aceste grupuri de utilizatori trebuie sa fie folosite pentru a configura accesul în interfața de administrare și pentru alocarea privilegiilor la nivelul porturilor de rețea și filtre.

4.92. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte „Authentication, Authorization & Accounting (AAA)" folosind:

- TACACS+
- RADIUS

4.93. Sistemul pentru vizibilitate la nivelul rețelei trebuie să pună la dispozitie interfete de tip RESTFULL Web based API pentru automatizari si raspuns adaptiv.

4.94. Sistemul pentru vizibilitate la nivelul rețelei trebuie să pună la dispoziție un instrument offline de simulare a interfetei grafice, care să poată fi utilizat pentru a pregăti pachetul de configurarea si importul in productie a acestuia.

4.95. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită trimiterea de evenimente folosind:

- Syslog
- SNMP Traps

4.96. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită configurarea la nivelul fiecarui port de notificari prin SNMP traps atunci când anumite condiții sunt indeplinite.

4.97. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită vizualizarea statisticilor și a graficelor de trafic în interfața GUI la nivelul fiecarui port sau filtru, respectiv agregat pentru toate filtrele sau porturile.

4.98. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită exportarea în format .CSV a statisticilor pentru fiecare port pentru raportare

4.99. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită exportul sau importul elementelor specifice de configurare.

4.100. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită configurarea transmiterii semnalului optic pentru fiecare port.

4.101. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită vizualizarea informatiilor despre transceivere și puterea semnalului optic prin intermediul interfetei grafice.

4.102. Sistemul pentru vizibilitate la nivelul rețelei trebuie să furnizeze fără licență sau hardware suplimentar un dashboard prin intermediul căruia să se poată urmări performanța sau statisticile globale ale traficului procesat.

Procesarea traficului în cadrul sistemului pentru vizibilitate la nivelul rețelei

4.103. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită configurarea tuturor filtrelor necesare procesării traficului utilizând doar interfața grafică.

4.104. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte următoarele profiluri de agregare și replicare:

- port la port
- port la mai multe porturi
- mai multe porturi la un port
- mai multe porturi la mai multe porturi

4.105. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permita filtrarea în 3 etape: la portul de intrare, filtrul de mijloc și portul de iesire;

4.106. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită balansarea dinamică a încărcării și configurarea a până la 64 de porturi de 10G pe grup de balansare;

4.107. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită simultan filtrarea IPv4 și IPv6;

4.108. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită configurarea și alocarea manuală a memorie folosită pentru filtrare pe porturile L2 / L3, IPv4 / IPv6, portul de intrare, filtrul de nivel mediu și portul de ieșire.

4.109. Sistemul pentru vizibilitate la nivelul rețelei trebuie să susțină cel puțin 4000 de reguli de filtrare și suplimentar 8000 de surse IPv4 și 8000 de reguli IPv4 de destinație.

4.110. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită filtrarea dupa etichete VLAN (802.1Q sau 802.1 Q-in-Q) la nivelul portul de intrare, filtrul dinamic și portul de iesire.

4.111. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită adăugarea sau eliminarea etichetelor VLAN din pachete.

4.112. Sistemul pentru vizibilitate la nivelul rețelei trebuie să accepte funcții avansate de procesare a pachetelor fără a fi nevoie de adaugarea unui hardware nou.

4.113. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte urmatoarele tehnici de procesare avansată a pachetelor:

- Eliminarea pachetelor duplicate
- Reducerea dimensiunii pachetelor prin configurarea numarului de octeti care sa ramana in fiecare pachet.
- Stergerea etichetelor MPLS. Trebuie sa fie capabil sa stearga pana la 8 etichete
- Stergerea etichetelor VNTag
- Stergerea antetelor GRE GRE/ERSPAN Termination
- Stergerea antetelor VxLAN (Virtual Extensible LAN)
- Adaugarea de amprente de timp (timestamping) pe pachete
- Mascarea datelor din pachete
- Configurarea de tunele GRE.

4.114. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită pentru motorul de procesare avansată a pachetelor enumerate mai sus o performanta care să poată gestiona cel puțin 170 milioane pachete pe secundă pentru a evita pierderea pachetelor.

4.115. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită alocarea flexibilă a resurselor de procesare avansata a pachetelor; de ex. alocarea pentru porturile de intrare, de ieșire și la nivelul filtrelor.

4.116. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită simultan activarea diferitelor funcții avansate de procesare a pachetelor pe același port sau filtru.

4.117. Sistemul pentru vizibilitate la nivelul rețelei trebuie să poată susține viteza de transfer atunci când mai multe funcții avansate de procesare a pachetelor sunt active pe același port cu cele mai mici dimensiuni ale cadrelor Ethernet.

4.118. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte afișarea statisticilor de trafic prelucrate de funcțiile avansate de procesare a pachetelor.

4.119. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte inspecția traficului la nivelul aplicatie la o viteză de până la 30 Gbps.

4.120. Sistemul pentru vizibilitate la nivelul rețelei trebuie să poată suporta, prin adaugarea de licente suplimentare, o performanță de procesare avansată a pachetelor de cel puțin 160Gbps.

4.121. Sistemul pentru vizibilitate la nivelul rețelei va permite filtrarea traficului pe baza „geolocation".

4.122. Sistemul pentru vizibilitate la nivelul rețelei va permite identificarea categoriilor de aplicații

4.123. Sistemul pentru vizibilitate la nivelul rețelei va include cel puțin 300 de semnături de aplicatii

4.124. Sistemul pentru vizibilitate la nivelul rețelei va asigura identificarea dinamică a aplicațiilor pe echipamentul de vizibilitate fără a fi necesară adugarea de echipament hardware suplimentar.

4.125. Sistemul pentru vizibilitate la nivelul rețelei va permite identificarea sistemelor de operare

4.126. Sistemul pentru vizibilitate la nivelul rețelei va include un dashboard pentru a urmări statisticile globale ale traficului procesat.

4.127. Sistemul pentru vizibilitate la nivelul rețelei va permite învățarea dinamică a aplicațiilor necunoscute și ulterior utilizarea acestor in statistici sau filtre similar celor predefinite

4.128. Sistemul pentru vizibilitate la nivelul rețelei va suporta definirea de plaje de IP-uri si gruparea acestora în locații geografice

4.129. Sistemul pentru vizibilitate la nivelul rețelei va suporta activarea simultana a tuturor functiilor inteligente ale aplicației.

4.130. Sistemul pentru vizibilitate la nivelul rețelei va suporta generarea de NetFlow v9 si v10

4.131. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte generarea de NetFlow pe baza traficului procesat cu o performanță de până la 100,000 sesiuni pe secunda.

4.132. Sistemul pentru vizibilitate la nivelul rețelei trebuie să combine fluxurile bidirectionale astfel încât numărul inregistrărilor netflow generate sa fie injumătățit (o intregistrare netflow conține ambele direcții ale traficului).

4.133. Sistemul pentru vizibilitate la nivelul rețelei va suporta până la 10 colectori (destinații) NetFlow

4.134. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte eșantionarea NetFlow cu o rata de 1:1000

4.135. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte urmatoarele extensii IPFIX:

i. Client/Server IP COUNTRY CODE
ii. Client/Server IP COUNTRY NAME
iii. Client/Server IP CITY NAME
iv. Client/Server IP REGION CODE
v. Client/Server Latitude/Longitude
vi. Client/Server AS Nname
vii. HTTP Hostname
viii. HTTP URI
ix. HTTP User agent
x. Application ID
xi. Application Name
xii. DNS TXT
xiii. dnsQueryName
xiv. dnsResponseName
xv. dnsQueryClass
xvi. Latency
xvii. OS Device ID
xviii. OS Devie Name
xix. Browser ID
xx. Browser name

4.136. Sistemul pentru vizibilitate la nivelul rețelei trebuie să permită mascarea datelor din pachete prin intermediul expresiilor Regex (regular expressions).

4.137. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte filtre Regex multiple pentru aplicatii diferite.

4.138. Sistemul pentru vizibilitate la nivelul rețelei trebuie să fie capabilă să creeze fișiere PCAP din traficul procesat.

4.139. Sistemul pentru vizibilitate la nivelul rețelei trebuie să suporte decriptarea pasivă a traficului SSL, prin furnizarea cheii private, și transmiterea traficului decriptat către porturile de ieșire asociate.

4.140. Sistemul pentru vizibilitate la nivelul rețelei trebuie să includă un modul software de profilare a traficului capabil să identifice specificul traficului procesat doar folosind informatiile din Netflow.

4.141. Modulul de profilare de rețea permite generarea de configurații de testare de rețea pe baza specifiului traficului analizat fără adăugarea de hardware suplimentar

4.142. Modulul de profilare trebuie să stocheze până la 7 zile metdatele de trafic de rețea primite de la solutia de vizibilitate de rețea

4.143. Modulul de profilare a traficului trebuie să exporte configurații de testare de rețea rezumând traficul specific unei zile.

4.144. Sistemul pentru vizibilitate la nivelul rețelei trebuie să includă licențele necesare pentru utilizarea serviciilor netflow, decriptarea SSL și profilare a traficului.

Cerințe specifice pentru sistemul de vizibilitate la nivelul rețelei la sediul central

4.145. Interfețe de retea licențiate:

- 32x porturi de 10Gbps
- 12x porturi de 1Gbps

4.146. Transceivere incluse:

- 32x transceivere SFP+, Fibra Optică, ShortRange (850nm), 10Gbps
- 6x transceivere SFP, Fibra Optică, ShortRange (850nm), 1Gbps
- 6x transceivere SFP, 1000BaseT

4.147. Licente incluse:

- Licenta pentru activarea procesarii avansate a pachetelor cu o performanță de 40 Gbps.
- Licenta pentru activarea decriptarii pasive a traficului SSL
- Licență penru inspecția traficului la nivelul aplicatie la o viteză de până la 10 Gbps

Cerințe specifice pentru sistemul de vizibilitate la nivelul rețelei la sediul secundar

4.148. Interfețe de retea licențiate:

- 16x porturi de 10Gbps
- 8x porturi de 1Gbps

4.149. Transceivere incluse:

- 16x transceivere SFP+, Fibra Optică, ShortRange (850nm), 10Gbps
- 4x transceivere SFP, Fibra Optică, ShortRange (850nm), 1Gbps
- 4x transceivere SFP, 1000BaseT

Cerinte specifice pentru echipamentele pasive de captura de tip TAP optic

4.150. Echipamentele TAP optice trebuie să includă:

- Interfațe de tip LC pentru fibra optică cu viteze de transfer de la 1Gbps pana la 100Gbps
- Factorul de multiplicarea al luminii trebuie sa fie 30/70

4.151. Echipamentele TAP trebuie să poată fi montate într-un „cage" compact 1x RU , care la rândul lui să poată fi instalat într-un rack standard de 19", „cage" care va suporta până la 24x de echipamente TAP.

4.152. Centralizator cantități TAP:

- 24x echipamente de tip Tap optic cu specificatiile de mai sus
- 4x dispozitive de prindere in rack de 19"

V. Aspecte calitative, cantitative și organizatorice privind obiectul contractului, inclusiv operațiuni cu titlu accesoriu, necesar a fi realizate, după caz:

Termenul de începere efectivă a derulării contractului	*la data semnării de către părți*
Loc livrare	Bucuresti – Sediul Central
Termenul de livrare/ graficul de livrare	Maxim 2 luni de la data semnarii contractului. Instalare punere in functiune , 1 lună de la data livrării
Persoana de contact la punctul de livrare	Va fi desemnata la momentul semnarii contractului
Activități pregătitoare	
Cerințe privind instalarea și punerea în funcțiune și testarea	Livrarea, instalarea și testarea solutiei se va face în maxim 3

	luni de la data semnării contractului. Contractantul trebuie să prezinte un plan de testare / validare a capabilităților soluției precum și scenariile de testare folosite.
Cerințe privind necesitatea instruirii personalului cu privire la modul de utilizare a echipamentelor *(dacă este cazul– se vor preciza inclusiv informații privind numărul de persoane ce urmează să fie instruite și durata minimă instruirii)*	Contractantul va realiza instruirea a 2 persoane în vederea instalării, configurării și administrării soluției ofertate. Instruirea se va realiza prin transfer de „know-how", durata de minim 6 zile lucrătoare;
Documentații ce trebuie furnizate în legătură cu produsul	Cf. cerintentei 7.4. din caietul de sarcini: • contractantul va pune la dispoziția Bancii Nationale a Romaniei documentația aferentă instruirii; • Contractantul va pune la dispoziția Bancii Nationale a Romaniei documentația privind instalarea și configurarea soluției;
Durata minimă garanție	Cf. cerintei 7.6. din caietul de sarcini: 24 de luni de la data punerii în funcțiune în mediu productiv
Modalitatea de intervenție în perioada de garanție *(termen de intervenție, reparație/înlocuire, termen de reparație aceptat, asigurare de echipament de schimb etc.)*	Cf. cerintei 7.8 din caietul de sarcini
Suport tehnic (help desk, etc.)	Cf. cerintei 7.6 din caietul de sarcini
Alte condiții	
Personalul cheie *(dacă este cazul)* *(Alegerea tipului și a numărului de personal cheie este justificată prin corelarea cu activitățile pe care aceștia le vor efectua în cadrul*	Cf. cerintei 7.14 din caietul de sarcini

contractului, cu dimensiunea/ cantitatea/ categoria de echipamente complexe din cadrul contractului. Personalul cheie este solicitat in situația in care se identifică și activități (servicii, lucrări) conexe obiectului contractului (lucrări de instalare, servicii de montaj, etc.), care necesită personal specializat, cu expertiză în domeniu, ce deține calificările și certificările necesare pentru a fi abilitat să realizeze activitățile conexe. Cerințele impuse privind calificările educaționale și/sau profesionale trebuie să fie relevante pentru activitățile în care membrii personalului vor fi implicați în cadrul contractului, iar documentele-suport necesare demonstrării îndeplinirii cerințelor vor fi specificate și trebuie să fie relevante și nerestrictive.)	

VI. Recepția și plata:

VI.1. Grafic de livrare

Nr. crt.	Denumire	Termen
1	Livrare, instalare, punere în funcțiune	3 luni de la data semnării contractului

VI.2. Recepția *(se alege varianta corespunzătoare)*

Recepția cantitativă și calitativă a produselor se va efectua pe baza de proces verbal semnat de Contractant si Banca Națională a României.

Procesul verbal de recepție calitativă va include unul din următoarele rezultate:

- Acceptat (derularea acceptantei fara identificarea vreunui defect)

- Acceptat cu observații minore (identificarea numai a unor defecte minore care pot fi remediate într-un termen bine specificat)

- Acceptat cu rezerve (presupune remedierea defectelor observate in termenul precizat)

- Refuzat (neacceptarea produselor intrucat acestea nu functioneaza la parametrii agreati)

VI.3. Plata

Factura va fi emisă dupa semnarea de către BNR a procesului verbal de receptie. Procesul verbal de receptie va insoți factura și reprezinta elementul necesar realizarii platii, impreuna cu celelalte documente justificative prevazute mai jos:

1. certificatul de calitate si garantie;

2. declaratia de conformitate;

3. avizul de expeditie a produsului;

VII. Alte cerințe/ informații

Cerințe privind implementarea sistemului

7.1. Soluția ofertată trebuie sa includa servicii de instalare, configurare si suport, precum si de servicii de management de proiect de calitate care să garanteze atingerea cu succes a obiectivelor proiectului.

7.2. Furnizorul va presta toate serviciile necesare pentru implementarea soluției în conformitate cu recomandările producătorului. Toate costurile asociate trebuie să fie cuprinse în oferta financiară.

7.3. Instalarea echipamentelor în rack-urile din spatiile tehnice ale autorității contractante se va efectua de către personal tehnic specializat al contractantului și se vor asigura toate cablurile necesare interconectarii cu infrastructura existentă - cabluri fibra optică, cabluri UTP, cabluri de alimentare electrice, cabluri impământare – kit-uri de instalare pentru rack 19", precum și suruburile și piulitele de rack necesare. Asigurarea rack-urilor, a spatiului necesar în rack-uri, a alimentarii din surse neintreruptibile de tensiune prin intermediul „power distribution units (PDU)" revine în sarcina autorității contractante.

7.4. Contractantul va asigura servicii de instalare, configurare și suport tehnic și mentenanță pentru echipamentele hardware și modulele software de securitate furnizate în cadrul acestui proiect, constând în următoarele:

A. Servicii de instalare, configurare și integrare în arhitectura existenta echipamentelor hardware și modulele software de securitate furnizate astfel:
   I. Instalare si configurare de bază pentru echipamentele noi;
   II. Instalare patch-uri;
   III. Configurare adrese IP, routing, NTP, DNS, utilizatori si grupuri (AAA);
   IV. Configurare fluxuri de retea si decriptare trafic ssl;
   V. Configurare filtre dinamice;
   VI. Parametrizarea si rafinarea configuratiilor de detectie a breselor de securitate informatica prin adaptarea la specificului retelei clientului

B. Servicii de suport tehnic și mentenanță pentru 24 luni, astfel:
   I. Actualizare software echipamente;
   II. Access expertilor Bancii Nationale a Romaniei la portalul producatorului;
   III. Access la upgrade-uri si patch-uri;
   IV. Instalare hotfix/patch-uri/jumbo hotfix-uri;
   V. Suport pentru identificarea și diagnosticarea problemelor de funcționalitate a soluției;
   VI. Suport pentru deschiderea cazurilor de suport către producătorul soluției;
   VII. Suport pentru configurare de noi funcționalități sau modificarea configurației pentru funcționalitățile implementate;
   VIII. Documentarea incidentelor si serviciilor livrate;

C. Instruire, documentație

I. Contractantul va realiza instruirea a 2 persoane în vederea instalării, configurării și administrării soluției ofertate. Instruirea se va realiza prin transfer de „know-how”;

II. Contractantul va pune la dispoziția Bancii Nationale a Romaniei documentația aferentă instruirii;

III. Contractantul va pune la dispoziția Bancii Nationale a Romaniei documentația privind instalarea și configurarea soluției;

Cerințe privind garanția, mentenanța, suportul și serviciile de instruire

7.5. Livrarea, instalarea și testarea solutiei se va face în maxim 3 luni de la data semnării contractului.

Perioada de garanție, mentenanță și suport pentru soluția ofertată, incluzand suportul oferit de producator, va fi de **24 de luni de la data punerii în funcțiune în mediu productiv**.
Toate costurile asociate trebuie să fie incluse în oferta financiară.

7.6. Serviciile de garanție corespunzătoare soluției ofertate vor trebui să răspundă cel puțin următoarelor cerințe:

a. Se vor asigura și transfera către beneficiar toate drepturile care decurg din atributele de garanție așa cum sunt acestea definite de către producător pentru toate componentele soluției, pe o perioada de 24 luni;
b. Ofertantul va asigura mentenanța tuturor produselor hardware incluse în ofertă pentru o perioadă de 24 luni de la începerea procedurilor de instalare;
c. În cazul defectării echipamentelor hardware ofertantul va garanta reparația acestora în maxim următoarea zi lucrătoare (sau, pentru defecțiuni care nu pot fi rezolvate atât de repede, înlocuirea temporară a echipamentului defect până la soluționarea problemei);
d. Ofertantul va asigura acces direct la informații și servicii de suport electronice pe site-ul web al producătorului (acces la motoare web de căutare a documentelor tehnice de suport, căutări de informații in bazele de cunoştințe ale producătorului, acces la ultimele actualizări pentru software, etc.);
e. Ofertantul trebuie sa dispună de un call-center pentru preluarea apelurilor de suport tehnic care să funcționeze in regim 24x7x365. Pentru plasarea apelurilor de suport tehnic în cazul apariției unei defecțiuni trebuie să existe următoarele opțiuni: email, portal web, telefon;

7.7. Serviciile de garanție pentru soluția ofertată vor include și servicii de rezolvare disfuncționalități sau rezolvare defecte ale soluției implementate precum și acces la baza de date cu informații/cunoștințe creată și menținută de producător, în vederea recepționării informațiilor despre reputația unor adrese IP, necesară pentru protecția aplicațiilor web.

7.8. În scopul realizării de Servicii de suport contractantul se angajează:

a. Să numească un *Manager de prestări servicii* (MPS) care va fi singurul punct de contact pentru o solicitare de servicii. Managerul de prestări servicii va administra și monitoriza *Solicitările de Servicii* (SR – „service request”) și va discuta în mod regulat cu reprezentantul desemnat de către BNR (Punct de Contact);
b. Să ofere un diagnostic pentru problema semnalată în *Solicitarea de Servicii* (inclusiv, daca este necesar, trierea și remedierea solicitărilor) pentru a determina cauza acesteia;
c. Să monitorizeze continuu *SR*-urile neonorate, până la soluționarea acestora;

d. Înregistrarea SR-urilor și procesarea nivelului de gravitate.

Fiecare *Solicitare de Servicii* trebuie să dețină un nivel de gravitate (după cum este definit în tabelul de mai jos), care să reflecte impactul asupra disponibilității sistemului. *Punctul de Contact* va aloca nivelul de gravitate inițial în colaborare cu *Managerul de prestări servicii* pentru a facilita luarea unei decizii. Un Nivel de Gravitate poate fi modificat în timpul procesării cererii, în urma acordului dintre *MPS* și *POC*.

Nivel de gravitate	**Descriere**	**Timp de răspuns**	**Timp de remediere**
Nivel 1 – CRITIC	Impact critic asupra disponibilității sistemului. Problema determină întreruperea totală a activității. Lucrul nu poate continua și situația reprezintă o urgență. O problemă cu nivel de gravitate 1 prezintă una sau mai multe din următoarele caracteristici: • Sistemul se blochează pe perioade nedefinite, determinând întârzieri inacceptabile sau nedefinite pentru resurse și răspunsuri. • Sistemul se oprește cu erori și se oprește în mod repetat după încercările de a-l reporni.	Maxim 4 ore de la semnalarea problemei.	Maxim 8 ore lucrătoare de la semnalarea problemei.
Nivel 2 – IMPORTANT	Impact important asupra activității. Problema determină pierderi importante pentru activitate. Nu este disponibilă nicio soluție; totuși operațiile pot continua în mod limitat.	Maxim 8 ore de la semnalarea problemei	Maxim 2 zile lucrătoare de la semnalarea problemei.
Nivel 3 – MEDIU	Un anumit impact asupra activității. Problema determină pierderi minime pentru activitate. Impactul se manifestă sub forma unui neajuns, care ar putea necesita o soluționare pentru repunerea în funcțiune.	Maxim 1 zi lucrătoare de la semnalarea problemei.	Maxim 3 zile lucrătoare de la semnalarea problemei.
Nivel 4- MINOR	Impact minim asupra activității. Problema nu afectează activitatea. Rezultatul este o eroare minoră, un comportament incorect sau o eroare în documentare, care nu împiedică funcționarea sistemului.	Maxim 3 zile lucrătoare de la semnalarea problemei.	Contractantul va genera un timp estimat de remediere insa acesta nu trebuie sa depașească 10 zile lucrătoare de la semnalarea problemei.

În cazul unei probleme de gravitate 1 sau 2 pentru care nu poate fi oferită o rezolvare într-un timp acceptabil, se va furniza o soluție alternativă pentru rezolvarea incidentului („workaround"). O soluție alternativă este un alt mod de a rezolva problema, sau un mod de a continua operarea în timp ce soluția efectivă este realizată.

Pentru fiecare intervenție, ofertantul va redacta Rapoarte de evaluare, în care vor fi descrise serviciile prestate, soluțiile tehnice sau funcționale și vor fi menționate intervalul de timp și durata serviciilor.

Cerințe privind testarea și acceptanța sistemului

7.9. Contractantul trebuie să prezinte un plan de testare / validare a capabilităților soluției precum și scenariile de testare folosite.

7.10. Criteriile de acceptanță vor fi stabilite în acord cu Autoritatea contractantă, astfel încât să asigure conformitatea execuției testelor cu scenariile de testare și cu solutia livrata.

7.11. Procedura de acceptanță finală trebuie să sumarizeze în cadrul raportului de acceptanță toate activitățile efectuate, rezultatele și problemele identificate.

7.12. Acceptanța sistemului se va realiza prin semnarea raportului final de acceptanță de către Comisia de Acceptanță desemnată de Autoritatea contractantă.

Cerințe de prezentare a soluției tehnice

7.13. Propunerea tehnică va conține obligatoriu:

a. Descrierea tehnică generală a soluției ofertate;
b. Prezentarea componentelor pentru soluția ofertată;
c. Prezentarea modului de îndeplinire a cerințelor tehnice solicitate în caietul de sarcini
d. Prezentarea sub formă tabelară a explicațiilor, valorilor și documentelor pentru toate caracteristicile solicitate în caietul de sarcini (matrice de complianță). Se vor indica referințe publice care să ateste respectarea cerințelor din caietul de sarcini;
e. Plan de testare
f. Alte informații considerate relevante de către ofertant pentru evaluarea corespunzătoare a propunerii tehnice.

Cerințe privind capacitatea profesională a ofertantului

7.14. Contractantul va desemna 3 specialiști care vor fi alocați pe toata durata derulării proiectului. Echipa contractantului trebuie să includă cel puțin următorii specialiști:

1. Manager de proiect – 1 specialist

Cerințe:

a. Certificare în domeniul managementului de proiect
b. Experiență specifică: Asigurarea managementului de proiect pentru minim 3 contracte similare, în ultimii 3 ani

2. Experți tehnici de securitate informatica – 2 experti cheie

a. Experiență specifică: Participarea ca expert tehnic cel putin pentru un proiect similar, in ultimii 3 ani

7.15. Ofertantul va prezenta în ofertă informații referitoare la studiile, pregătirea profesională și calificările persoanelor responsabile cu îndeplinirea contractului.

7.16. Se va prezenta lista personalului propus de ofertant pentru îndeplinirea contractului. Referitor la experiența și cursurile/certificările solicitate, facem precizarea că acestea au rolul de a demonstra capacitatea/ pregătirea profesională/ calificarea persoanelor responsabile pentru îndeplinirea cu succes a obiectivelor din caietul de sarcini.

Notă:

a. Se vor prezenta diplome, certificate, atestate sau alte documente echivalente.
b. Toate diplomele sau certificările vor fi emise de instituții abilitate conform legislației în vigoare.
c. Certificările și atestatele profesionale depuse trebuie să fie valabile la data limită de depunere a ofertelor.
d. Pentru fiecare specialist se vor prezenta:

    i. curriculum vitae (CV) format EUROPASS
    ii. copii, cu mențiunea „conform cu originalul", ale diplomelor de studii și certificatelor profesionale obținute și mentionate în CV, relevante pentru contractul în cauză
    iii. documentele suport din care să reiasă experiența specifică: recomandări de la beneficiarii contractelor în care experții au îndeplinit rolul solicitat sau extrase din contracte cu menționarea rolului respectiv și a perioadelor aferente sau orice alte documente suport (care pot fi eliberate si de către ofertantul respectivelor servicii), în copie cu mențiunea „conform cu originalul".
    iv. Pe perioada de derulare a contractului, în cazurile foarte bine justificate, experții prevăzuți de către ofertant pot fi înlocuiți doar cu acordul beneficiarului, cu alte persoane care să îndeplinească cerințele minime de calificare pentru experți.
    v. Referitor la experienta specifică solicitată pentru expertul tehnic, cerinta se considera indeplinită dacă se prezintă documente suport pentru 3 contracte în care s-au utilizat tehnologiile menționate

Justificare necesității asigurării experților tehnici:
Luând în considerare faptul că asigurarea serviciilor de instalare, configurare și suport tehnic pentru echipamentele de securitate IT din infrastructura BNR reprezintă un obiectiv strategic, se impune stabilirea unor cerințe minime de calificare referitoare la capacitatea profesională.
Astfel, au fost stabilite cerințele de calificare în conformitate cu legislația în vigoare privind achizițiile publice, cu scopul de a reduce la minim riscul de neîndeplinire a contractului, din cauza lipsei capacității profesionale a ofertantului.
Referitor la experiența și cursurile/certificările solicitate, facem precizarea că acestea au rolul de a demonstra capacitatea/ pregătirea profesională/ calificarea persoanelor responsabile pentru îndeplinirea cu succes a obiectivelor din caietul de sarcini.

1. Manager de proiect

Managerul de proiect trebuie să asigure coordonarea echipei de proiect implicată în derularea serviciilor de instalare și suport tehnic care fac obiectul Caietului de sarcini, astfel încât să asigure îndeplinirea cu succes a obiectivelor proiectului.
Managerul de proiect are, în principal, următoarele responsabilități:

a. Să se asigure că rezultatele proiectului sunt la standardele de calitate necesare și sunt livrate conform termenelor stabilite;
b. Să asigure o bună raportare, conform condițiilor contractuale;
c. Să furnizeze tuturor părților implicate în proiect toate informațiile solicitate referitoare la proiect
d. Să asigure coordonarea echipei de proiect.

Având în vedere complexitatea serviciilor solicitate prin caietul de sarcini și importanța strategică, considerăm necesar că expertul propus de către ofertant pentru rolul de manager de proiect să aibă abilități demonstrate prin certificarea solicitată și prin cei minim 10 ani de experiență specifică în managementul proiectelor IT&C, în scopul implementării cu succes a serviciilor ce urmează a fi prestate.

2. Experții tehnici de securitate informatica

Pe întreaga perioadă a proiectului , contractantul va asigura 2 experți cheie (expert principal si inlocuitorul acestora) au responsabilitatea de a asigura o funcționare optimă și fiabilă a sistemelor hardware și software care se vor instala și administra pe intreaga durata a contractului.
Responsabilitățile principale sunt următoarele:

a. Evaluare initială – cu scopul principal de a intelege situatia curentă.
b. Crearea unei arhitecturi care sa adreseze cerintele mentionate in caietul de sarcini.
c. Instalarea tuturor componentelor mentionate in oferta tehnica.
d. Suport pentru activare licentelor - include gestionarea licențelor, migrarea licențelor sau transformarea (dacă este cazul).
e. Deschiderea de cazuri la producator si escaladara acestora pentru o rezolvare cat mai rapida.
f. Alte servicii operationale. Experții tehnici de securitate informatica vor verifica periodic și va monitoriza sistemul informatic pentru a asigura respectarea nivelelor minime de performanță stabilite în caietul de sarcini.

Alte cerințe legate de personalul direct implicat în prestarea serviciilor

7.17. Urmatoarele cerințe trebuiesc avute în vedere in vederea oferării:

a. Obligația Contractantului de a asigura personalul adecvat (din punct de vedere al calificării educaționale și profesionale) pentru efectuarea eficientă a tuturor activităților enumerate în Caietul de Sarcini și pentru realizarea obiectivelor Contractului din punct de vedere al termenelor și nivelului calitativ solicitat.
b. Obligația Contractantului să se asigure și să urmărească cu strictețe ca oricare dintre experții principali propuși să cunoască foarte bine și să înțeleagă cerințele, scopul și obiectivele Contractului, specificul activităților pe care urmează să le desfășoare în cadrul Contractului precum și a responsabilităților atribuite.

Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului

7.18. În scopul bunei desfăsurări a contractului, cele 2 părți vor asigura toate demersurile necesare astfel încât obiectivele acestuia sa fie atinse. În acest sens vor fi asigurate următoarele activități:

a. De coordonare:
   i. Organizarea întâlnirii de demarare a activităților în Contract, pentru obținerea asigurării că Autoritatea Contractantă și Contractantul au aceeași perspectivă asupra activităților și rezultatelor din Contract;
   ii. Organizarea întâlnirilor de lucru, de monitorizare a progresului activităților și de analiză a rezultatelor intermediare, corespunzătoare fiecărei etape din Contract
   iii. Coordonarea resurselor și activităților de către fiecare parte contractantă separat și împreună;
   iv. Distribuirea informațiilor privind rezultatele/documentele intermediare și finale factorilor interesați relevanți identificați în Caietul de Sarcini și în Propunerea Tehnică;

b. De monitorizare:

i. Măsurarea progresului activităților din Contract prin raportare la Contract;

ii. Pentru măsurarea progresului se utilizează planul de lucru inclus de Ofertant în Propunerea Tehnică pe baza cerințelor din Caietul de Sarcini;

c. De control:

i. Controlul implică identificarea acțiunilor corective pentru abordarea abaterilor de la Contract constatate de comun acord în cadrul întâlnirilor dintre Contractant și Autoritatea Contractantă.

Monitorizarea realizării activităților și a rezultatelor pe perioada derulării Contractului

7.19. Monitorizarea activitătii Contractantului se va face in baza unor evaluari periodice a serviciilor prestate pe tot parcursul contractului.
Urmatorii indicatori vor fi urmariti:

i. Încadrarea în timpul alocat contractului

ii. Progresul înregistrat în timpul contractului

iii. Respectarea cerințelor calitative cu privire la serviciile prestate.