ROMÂNIA
MINISTERUL APĂRĂRII NAȚIONALE
COMANDAMENTUL APĂRĂRII CIBERNETICE
Nr BA - 377 din 20.02.2026
–București –

NECLASIFICAT
Exemplarul nr.
Dosar nr. ___
Termen de păstrare: 5 ani

APROB
COMANDANTUL COMANDAMENTULUI APĂRĂRII CIBERNETICE
General de brigadă
ing. Răzvan-Marian TUDOSE

AVIZAT:
Șeful Agenției de apărare cibernetică
Col.
ing. Sorin MANOLE

Specificație tehnică pentru
"Soluție de detecție și analiza a traficului de rețea tip 2"

BUCUREȘTI
2026

Pagină albă

CUPRINS

1. SCOP

Prezenta specificație stabilește cerințele tehnice în vederea achiziționării unei soluții pentru protejarea infrastructurii de rețea a organizației prin monitorizarea și analiza continuă a traficului, indentificarea și prevenirea atacurilor cibernetice și asigurarea securității. integrității și continuității operațiunilor IT.

2. CERINȚE

Ofertantul va furniza o soluție de detecție și analiza a traficului de rețea capabilă să monitorizeze în timp real atât a traficului de rețea inbound, cât și outbound, va identifica și bloca automat atacurile cibernetice, inclusiv malware, ransomware și exploituri necunoscute. va permite analiza fișierelor și pachetelor suspecte în medii virtuale (sandboxing) pentru detectarea comportamentelor malițioase necunoscute. va oferi rapoarte și vizualizări detaliate ale evenimentelor de securitate, și va permite integrarea cu alte soluții de securitate. asigurând în același timp scalabilitate și performanță în funcție de dimensiunea rețelei organizației

2.1. Cerințe de performanță și specifice produsului

Nr. cerință	CERINȚA
C1.	Soluția ofertată trebuie să includă componente hardware și software complet licențiate. capabile să funcționeze independent. fără necesitatea unui sistem de operare extern
C2.	Soluția ofertată trebuie să fie un echipament dedicat pentru detecția. inspecția și blocarea traficului de rețea la nivel aplicație și conținut
C3.	Soluția ofertată trebuie să asigure analiza traficului de rețea. detecția amenințărilor avansate. analiza comportamentală și prevenirea atacurilor
C4.	Soluția ofertată trebuie să fie nouă, livrată cu licență completă și suport de actualizări de securitate pe durata garanției
C5.	Soluția ofertată trebuie să asigure detecția și prevenirea atacurilor de rețea și aplicație (IPS/IDS)
C6.	Soluția ofertată trebuie să asigure inspecția traficului pentru protocoalele HTTP. HTTPS. FTP și SMB
C7.	Soluția ofertată trebuie să poată efectua inspecția traficului criptat SSL/TLS. incluzând JA3 fingerprinting, whitelisting și clasificare URL
C8.	Soluția ofertată trebuie să poată detecta etapele atacurilor de tip web. inclusiv exploit inițial. descărcare cod binar, callback și comunicații C2
C9.	Soluția ofertată trebuie să poată detecta răspândirea laterală a atacurilor prin analiza traficului SMB
C10.	Soluția ofertată trebuie să includă un mecanism de analiză dinamică (sandbox) bazat pe virtualizare, capabil să execute fișiere suspecte într-o mașină virtuală izolată
C11.	Sistemul hypervizor trebuie să conțină cel puțin o mașină virtuală de tip sandbox pentru analiză malware. cu sistem de operare preinstalate din următoarea listă: Microsoft Windows (Windows 7, Windows XP, Windows 10, Windows 11), Linux (CentOS) și MacOS, cu diferite versiuni de aplicații și plugin-uri uzuale
C12.	Soluția ofertată trebuie să poată funcționa offline. fără conectivitate la internet, în vederea analizei fișierelor
C13.	Soluția ofertată trebuie să permită actualizarea offline a semnăturilor și componentelor software
C14.	Soluția ofertată trebuie să suporte detecția pe baza regulilor YARA
C15.	Soluția ofertată trebuie să poată genera alerte retroactive (retrospective alerting)

C16.	Soluția ofertată trebuie să asigure clasificarea alertelor bazată pe fazele ciclului de viață ale infecției
C17.	Soluția trebuie să indice severitatea incidentului analizat
C18.	Soluția trebuie să detecteze cel puțin următoarele faze ale atacurilor de tip Web: exploit-ul inițial. descărcare de cod binar malware. funcții de tip call-back sau conexiuni către centre de comanda si control (C2)
C19.	Soluția ofertată trebuie să detecteze atacurile de tip Web Shell
C20.	Soluția ofertată trebuie să permită whitelistarea claselor de adrese IP
C21.	Soluția trebuie să poată utiliza anteturile XFF pentru a identifica mașina client care generează alertele atunci când este implementată în spatele unui server proxy
C22.	Soluția ofertată trebuie să permită autentificarea utilizatorilor prin servicii de tip RADIUS. TACACS+ și LDAP
C23.	Soluția ofertată trebuie să ofere administrare securizată. atât din linie de comandă (CLI). cât și prin interfață web HTTPS
C24.	Soluția ofertată trebuie să permită definirea rolurilor și privilegiilor de acces pentru utilizatori (administrator. operator. auditor etc.)
C25.	Soluția ofertată trebuie să poată exporta rapoarte și alerte în format PDF
C26.	Soluția ofertată trebuie să asigure notificarea alertelor prin protocoalele SNMP. Syslog și SMTP.
C27.	Soluția ofertată trebuie să afișeze în interfața web starea de funcționare și integritatea sistemului (health status).
C28.	Soluția trebuie să asigure analiza cel puțin a următoarelor tipuri de fișiere: msi. exe. dll. pdf. doc. jar. docx. xls. xlsx. gif. jpeg. png. tiff. eml. html. url. ppt. pptx. rtf. zip
C29.	Soluția ofertată trebuie să asigure aplicarea de reguli predefinite pentru identificarea acțiunilor malware și să ofere posibilitatea actualizării acestora prin intermediul informațiilor de tip "threat intelligence".
C30.	Soluția trebuie să asigure evidențierea URL-urilor suspecte din cadrul unei alerte și descărcarea capturilor de trafic asociate.
C31.	Soluția trebuie să poată funcționa ca ICAP server pentru a asigura primirea datelor prin protocolul ICAP pentru analiză.
C32.	Soluția trebuie să aibă capabilități de clasificare a detecției malware (ex.: Backdoor. Trojan. Exploit etc.)
C33.	La finalul analizei unui fișier malware extras din traficul monitorizat. soluția trebuie să prezinte un raport complet care să conțină informații precum: • Tipul fișierului analizat; • Numele fișierului analizat: • Copie a fișierului malware: • Sumele de control (de exemplu în format MD5. SHA1/256/512) ale fișierelor: • Clasificarea în funcție de familia de malware: • Tipul de exploit folosit; • URL-uri; • Date de identificare ale sistemului compromis (IP. MAC); • Modificări aduse la nivelul sistemului de operare: • Aplicațiile targetate: • Modificări asupra sistemului de fișiere: • Modificări aduse asupra bazei de date Windows Registry: • Librării DLL încărcate: • Funcțiile Windows API apelate. în ordine cronologică: • Informații despre procesele create/modificate/oprite: • Detalii despre comportamentul la nivel de rețea format grafic (Conexiuni de rețea create și protocoalele de transport folosite. porturi utilizate. interogări și răspunsuri

	DNS, pachete http); • Adrese IP contactate;
C34.	Soluția ofertata trebuie să asigure o analiză a traficului de rețea de minim 1Gbps
C35.	Soluția ofertată trebuie să suporte minimum 450.000 conexiuni concurente
C36.	Soluția ofertată trebuie să suporte minimum 9.000 conexiuni noi pe secundă
C37.	Soluția ofertată trebuie să fie echipat cu: - minimum 4 interfețe de monitorizare 1G/10G RJ45 cu bypass - minimum 4 interfețe 10G SFP+ - minimum 4 interfețe 1G/10G SFP+
C38.	Senzorii soluției vor fi echipați cu cel puțin 2 conectori SFP+ 10GbE
C39.	Soluția ofertată trebuie să suporte moduri de operare in-line, fail-open, fail-close (hardware bypass) sau TAP/SPAN
C40.	Soluția ofertată trebuie să suporte funcționarea în mod High Availability (HA)
C41.	Soluția ofertată trebuie să dispună de minimum 1 interfață de management 1G
C42.	Soluția ofertată trebuie să includă un port de management hardware (IPMI) de tip 100/1000BASE-T.
C43.	Soluția ofertată trebuie să fie echipat cu minimum 3 porturi USB de tip A
C44.	Soluția ofertată trebuie să fie echipat cu minimum port VGA
C45.	Soluția ofertată trebuie să includă un port serial configurat la 115.200 bps, 8 biți, 1 stop bit, fără paritate
C46.	Soluția ofertată trebuie să includă minimum 2 HDD de 4 TB fiecare, 3.5 inch, configurate în RAID 1, hot-swappable (FRU) pentru redundanță completă
C47.	Soluția ofertată trebuie să fie echipat cu surse de alimentare redundante (1+1) de minimum 850 W, compatibile cu 200–240 VAC
C48.	Soluția ofertată trebuie să fie compatibil cu montare în rack 19" maxim 2U, livrat împreună cu toate accesoriile necesare pentru instalare
C49.	Soluția ofertată trebuie să funcționeze la temperaturi de operare cuprinse între 10°C și 35°C
C50.	Soluția ofertată trebuie să funcționeze la umidități relative între 8% și 90%, fără condens
C51.	Soluția ofertată trebuie să respecte cerințele de conformitate de mediu RoHS REACH
C52.	Soluția ofertată trebuie să fie conform standardelor de siguranță EN 62368 sau echivalent
C53.	Soluția ofertată trebuie să fie conform standardelor europene de compatibilitate electromagnetică EN 55032, EN 55035 și EN 61000-3-2 sau standarde echivalente

2.2. Cerințe de licențiere

C54.	Licențierea pentru produsul ofertat va fi de tipul cod de activare, cu subscripție pe minim 36 luni, de la data recepției produsului
C55.	Soluția ofertată trebuie să ofere administrare securizată, atât din linie de comandă (CLI), cât și prin interfață web HTTPS
C56.	Soluția va fi asociată de servicii de suport și mentenanță pe o perioadă de minim 3 ani
C57.	Soluția și serviciile de suport asociate vor permite ca în cazul defectelor mediilor de stocare permanentă HDD, SD CARD, SSD, acestea se vor înlocui fără returnarea pieselor defecte

2.3. Cerințe privind garanția produsului

C58.	Garanția produsului trebuie să fie de minim 36 de luni de la data finalizării recepției produsului
C59.	Soluția ofertată va beneficia de garanție hardware este de minim 36 de luni, acordată de ofertant. Garanția va acoperi orice defect de fabricație sau de funcționare apărut în condiții normale de utilizare
C60.	Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day) care să garanteze diagnosticarea echipamentului sau modului defect, înlocuirea acestuia în maxim o zi lucrătoare de la momentul deciziei, fără alte costuri
C61.	Ofertantul va detalia în propunerea tehnică modul în care va asigura acest serviciu (personal tehnic, puncte de intervenție, suport logistic, etc.)
C62.	În cazul în care, pe durata garanției, discurile SSD/Flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite de ofertant cu altele noi, funcționale. Costurile aferente acestor activități vor fi incluse în oferta financiară Discurile de stocare defecte (SSD/Flash) rămân în posesia beneficiarului și nu vor fi returnate ofertantului sau producătorului, din considerente de securitate a informației
C63.	Suportul software va fi de minim 36 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar
C64.	Suportul software aferent produselor livrate va fi asigurat de ofertant, pe întreaga perioadă de suport solicitată. Aceasta va avea responsabilitatea de a furniza, prin resurse proprii sau prin rețeaua autorizată de suport a producătorului, acces 24/7 la suportul tehnic necesar, inclusiv posibilitatea raportării incidentelor critice, acces la patch-uri, precum și actualizări de firmware și software
C65.	În cazul în care suportul este asigurat prin implicarea producătorului, ofertantul va prezenta documente justificative (ex. scrisoare de suport, certificat de partener autorizat sau acord de suport) care să confirme că poate activa serviciile de suport necesare. Responsabilitatea față de autoritatea contractantă pentru întreaga prestație revine ofertantului
C66.	Toate produsele livrate trebuie să fie noi, în linia curentă de fabricație a producătorului. Nu se acceptă echipamente recondiționate, uzate moral sau scoase din fabricație
C67.	Nu se acceptă condiționarea acordării garanției produsului de acordarea accesului ofertantului la produsul instalat în rețele private ale beneficiarului

2.4. Cerințe privind livrarea, ambalarea, etichetarea, transportul și asigurarea pe durata transportului

C68.	Termenul de livrare trebuie să fie de maxim 60 de zile de la data semnării contractului subsecvent de furnizare de către ambele părți
C69.	Livrarea produsului ofertat trebuie să se realizeze la sediul beneficiarului din str. Drumul Taberei 7-9, Sector 6, București
C70.	Odată cu livrarea produselor, ofertantul trebuie să transmită documentația de însoțire, care va cuprinde: - avizul de însoțire a mărfii; - inventarul cantitativ-valoric, în limba română, care trebuie să coincidă cu prețul unitar al produsului ofertat cu TVA; - certificatul de garanție al produsului; - certificatul/documentul de licențiere pentru componenta software a produsului;

	- documentația de exploatare, cunoaștere și întreținere, în format electronic sau prin specificarea link-ului din internet unde se regăsește.
C71.	Ofertantul este responsabil pentru livrarea în termenul agreat al produselor și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu trebuie să invoce nici un motiv de întârziere sau costuri suplimentare

2.5. Cerințe privind instalarea, punerea în funcțiune, testarea

C72.	Instalarea, punerea în funcțiune și testarea produsului se va realiza de către personalul de specialitate al beneficiarului

2.6. Cerințe privind instruirea

C73.	Ofertantul trebuie să ofere instruire pentru minim 5 reprezentanți ai beneficiarului, pe o durată de minim 40 de ore (5 zile) , pentru buna înțelegere a funcționării produsului ofertat.
C74.	Instruirea se va executa în termen de maxim 60 de zile de la semnarea contractului subsecvent de ambele părți și trebuie să permită personalului beneficiarului să opereze și să administreze soluția livrată.
C75.	Instruirea trebuie să se facă în București, într-o locație pusă la dispoziție de ofertant, cu acordul beneficiarului, care să ofere toate facilitățile necesare instruirii profesionale a personalului pentru administrarea și utilizarea produsului ofertat.
C76.	Ofertantul trebuie să asigure instructorul, sala de instruire, materialele didactice, infrastructura IT&C, (sisteme informatice, rețeaua și domeniul virtual al cursului, instrumente software), precum și suportul instruirii și multiplicarea acestuia.
C77.	Instructorul desemnat trebuie să dețină certificări tehnice valide aferente soluției ofertate, emise de producător sau de un centru autorizat de instruire al producătorului.
C78.	Instruirea trebuie să se facă în limba română sau engleză.
C79.	Instruirea trebuie să exemplifice modul practic prin care se verifică toate funcționalitățile solicitate prin caietul de sarcini.
C80.	Instruirea trebuie să fie de tip "hands-on" (implicarea participanților în mod direct în activitățile practice, crearea și testarea de exemple bazate pe noțiunile teoretice prezentate și accesul la resursele materiale corespunzătoare în timpul desfășurării cursului), cu activități practice în care cursanții utilizează, administrează și testează produsul ofertat, aplicând noțiunile specific privind integrarea software, configurarea, administrarea și exploatarea produsului ofertat.
C81.	Cheltuielile de instruire a personalului care care va utiliza produsul trebuie să fie incluse în prețul ofertei.

2.7. Cerințe privind recepția produsului

C82.	Recepția produselor constă în recepția cantitativă și calitativă a produsului.
C83.	Recepția cantitativă și calitativă se va realiza la sediul beneficiarului din str. Drumul Taberei 7-9, Sector 6, București, în prezența reprezentanților beneficiarului și furnizorului.
C84.	Recepția se va realiza în termen de maxim 10 (zece) zile calendaristice de la data livrării produsului.

C85.	În cadrul activității de recepție se vor parcurge următoarele etape: • verificarea livrării cantitative a produsului; • verificarea livrării documentelor prevăzute la pct. 4 din caietul de sarcini; • verificarea funcționării produsului în acord cu prevederile cerințelor tehnice prevăzute în anexa nr. 1 la caietul de sarcini
C86.	La finalul activității de recepție se va întocmi un proces verbal de recepție a activului fix, prin care se va finaliza activitatea de recepție.
C87.	Dacă în cadrul recepției se constată că unele produse nu corespund din punct de vedere cantitativ sau calitativ, beneficiarul are dreptul de a respinge produsele, iar furnizorul are obligația de a remedia neconformitățile constatate în decurs de 5 zile de la constatarea lor.
C88.	Activitățile de recepție se consideră a fi finalizate la momentul semnării de către beneficiar a procesului verbal de recepție a activului fix (dacă din acest document nu rezultă obiecțiuni).

2.8. Alte cerințe

C89.	Echipamentele livrate vor fi noi și nefolosite. Nu se acceptă echipamente remanufacturate și/sau care au în componență elemente care au fost folosite anterior.
C90.	Specificațiile tehnice și de calitate ale produsului oferit trebuie, obligatoriu, susținute de documentații originale: prospecte, foi de catalog sau documentații în format electronic.
C91.	Produsul va fi livrat împreună cu toate accesoriile necesare punerii în funcțiune chiar dacă acestea nu au fost solicitate în mod expres.
C92.	Toate cerințele enumerate sunt considerate ca având mențiunea «sau echivalent» și vor fi considerate specificații minimale din punct de vedere al performanței, indiferent de marcă sau producător.
C93.	Produsele și accesoriile ofertate trebuie să fie noi și să nu fie declarate EoL (End of Life), EoS (End of Sale) sau End of Support de către producător.
C94.	Ofertantul trebuie să precizeze detaliat în oferta tehnică modul de îndeplinire concretă a cerințelor tehnice software pentru toate componentele, indicând pagina și paragraful din documentația oficială detaliată a produsului emis de producătorul acestuia, unde se găsesc informațiile legate de îndeplinirea cerinței respective. Nu sunt luate în considerare ofertele care prezintă simpla confirmare a îndeplinirii cerinței, sau numai copierea acesteia, fără a fi detaliată modalitatea de îndeplinire.

Toate cerințele definite în cadrul prezentei specificații tehnice sunt obligatorii. Nerespectarea lor va conduce la respingerea ofertei.

ÎNTOCMIT:
Sef birou soluții de monitorizare
Lt.
ing. Adrian Trocan