DECIZIE
de atribuire a contractului de achiziții publice ☑

Nr. 1 din 12 februarie 2026

1.Date cu privire la autoritatea contractantă:

Denumirea autorității contractante	Banca Națională a Moldovei
Localitate	Republica Moldova, mun. Chișinău
IDNO	79592
Adresa	Bulevardul Grigore Vieru 1
Număr de telefon	022 822 622
Număr de fax	022 228 697
E-mail oficial	achizitii.contracte@bnm.md
Adresa de internet	www.bnm.md
Persoana de contact *(nume, prenume, telefon, e-mail)*	Silvia Dolghii, tel: 022 822 200, e-mail: silvia.dolghii@bnm.md

2.Date cu privire la procedura de atribuire:

Tipul procedurii de atribuire aplicate	☐ Cererea ofertelor de prețuri ☑ **Licitație deschisă** ☐ Negociere fără publicarea prealabilă a unui anunț de participare (NFP)* ☐ Altele: *[Indicați]*
***Temei legal pentru desfășurarea NFP** *(Legea privind achizițiile publice nr. 131/2015)*	Nu se aplică
Expunerea motivului/temeiului privind alegerea procedurii de atribuire *(în cazul aplicării altor proceduri decât licitația deschisă)*	Art. 47 din Legea nr.131 din 03.07.2015 cu privire la achizițiile publice
Procedura de achiziție repetată *(după caz, se va indica nr. procedurii/ procedurilor desfășurate anterior pentru aceiași achiziție, dar anulată/ anulate)*	Nu se aplică
Tipul obiectului contractului de achiziție/ acordului-cadru	☑ **Bunuri** ☐Servicii ☐ Lucrări
Obiectul achiziției	**Pachete software aferente securității informaționale**
Cod CPV	48730000-4
Procedura de atribuire *(se va indica din cadrul portalului guvernamental www.mtender.gov.md)*	Nr: ocds-b3wdp1-MD-1765269998108
	Link-ul: https://mtender.gov.md/tenders/ocds-b3wdp1-MD-1765269998108?tab=contract-notice
	Data publicării: **09.12.2025**
Platforma de achiziții publice utilizată	☑ **achizitii.md;** ☐ e-licitatie.md; ☐ yptender.md
Procedura a fost inclusă în planul de achiziții publice a autorității contractante	☑ **Da** ☐ Nu
	Link-ul către planul de achiziții publice publicat:

	https://bnm.md/ro/content/plan-de-achizitii-al-bnm
Anunț de intenție publicat în BAP *(după caz)*	Data: **28.01.2025** Link-ul: https://tender.gov.md/ro/system/files/bap/2014/bap_nr._7_part_i.pdf
Tehnici și instrumente specifice de atribuire *(după caz)*	☐ Acord-cadru ☐ Sistem dinamic de achiziție ☐ Licitație electronică ☐ Catalog electronic
Sursa de finanțare	☐ Buget de stat; ☐ Buget CNAM; ☐ Buget CNAS; ☐ Surse externe; ☑ Alte surse: ***Surse proprii***
Valoarea estimată *(**lei,** fără TVA)*	**1 068 333,33**

3.Clarificări privind documentația de atribuire:

(Se va completa în cazul în care au fost solicitate clarificări)

Data solicitării clarificărilor	18 .12.2025
Expunerea succintă a solicitării de clarificare	Serviciu de monitorizare și protecție În cerințe și specificații tehnice se solicită: «Serviciu de monitorizare și protecție a identității utilizatorilor» Rugăm să specificați ce inseamna protectia identității?
Expunerea succintă a răspunsului	„Protecția identității" înseamnă supravegherea continuă și corelarea automată a tuturor evenimentelor legate de conturi și autentificare din Active Directory on prem, Microsoft Entra ID/Azure AD și Microsoft Intune, pentru a detecta și opri abuzul de identități cât mai devreme în lanțul de atac. Acest lucru trebuie să fie realizat cu ajutorul senzorilor de telemetrie care să: • monitorizeaze autentificările, controalele de acces și modificările de privilegii (inclusiv atacuri de tip brute force, folosirea de bilete Kerberos furate, conectări din locații suspecte, escaladări de privilegii, utilizarea aplicațiilor cu drepturi excesive); • coreleze aceste evenimente cu alte telemetrii (din endpointuri, sau din rețea etc.) pentru a identifica rapid conturi compromise sau tentative de abuz al privilegiilor; • genereaze incidente în consola, din care administratorii pot lansa acțiuni de răspuns (de exemplu: dezactivare cont, resetare parolă, blocarea sau izolarea dispozitivului, revocarea sesiunilor, revizuirea permisiunilor aplicațiilor). La nivel de date, să fie prelucrate în principal evenimente de autentificare și acces (logon/logoff, IP uri, locație estimată, timestamp uri), identificatori de utilizator (user ID/username), informații despre

	grupuri privilegiate și metadate tehnice despre dispozitive și politici Intune.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Consola de management În cerințe și specificații tehnice se solicită: «Consola de management: Accesibilitate - atât de pe browser desktop cât și tip mobile.» Rugăm să specificați dacă corect înțelegem că ce inseamna accesibilitate pe tip mobile este accesarea web browser prin mobile device?
Expunerea succintă a răspunsului	Prin „accesibilitate pe tip mobile” se înțelege posibilitatea de a accesa consola de management dintr-un browser web de pe un dispozitiv mobil (telefon/tabletă), cu interfață responsive/adaptată pentru ecrane mobile, fără a fi necesară o aplicație dedicată.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Politici În cerințe și specificații tehnice se solicită Politici: «Soluția trebuie să: permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module». Este necesar să fie clar de ce antivirus dispuneți?
Expunerea succintă a răspunsului	Soluțiile și platformele de securitate cibernetică folosesc acest mecanism de administrare prin politici care este un standard al industriei. Politicile au scopul de a instrui agenții software de securitate instalați local pe endpoint-uri cum să reacționeze, ce acțiuni automate să întreprindă și pe baza căror criterii să facă aceste lucruri
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Politici În cerințe și specificații tehnice se solicită Politici: „Soluția trebuie să: permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau user de active directoy;„ Rugăm să descrieți ce se are în vedere prin aplicare de pool-uri de resurse (VMware)?
Expunerea succintă a răspunsului	În soluții de Securitate cibernetică „aplicare de politici pe pool-uri de resurse (VMware)” înseamnă că, după integrarea cu VMware vCenter, pool-urile de resurse sunt importate ca obiecte de inventar în arborele inventarului agentilor instalati pe endpoint, iar politicile de securitate pot fi atașate direct acestor pool-uri care sunte prezentate în structure de tip

	arbore în sectiunea de inventor al soluției de securitate. Politica atribuită unui "resource pool" se propagă automat către toate mașinile virtuale din acel pool și este aplicată în mod dinamic oricărei VM nou create sau mutate în acel resource pool, fără intervenție manuală suplimentară. Astfel, administratorul poate utiliza pool-urile de resurse ca și „containere/foldere de politică" sau „buckets" de securitate: simpla migrare a unei VM dintr-un pool în altul schimbă implicit politica de securitate aplicată acelei VM, îndeplinind cerința privind aplicarea politicilor la nivel de resource pool VMware.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Utilizatori În cerințe și specificații tehnice se solicită Utilizatori „Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp - configurabil." Ce inseamna deconectare? Logoff/shutdown/block?
Expunerea succintă a răspunsului	În cadrul consolei soluției de securitate cibernetică „deconectare automată" înseamnă expirarea sesiunii după un timp de inactivitate configurabil, urmată de închiderea sesiunii/invalidarea token-ului și revenirea utilizatorului la ecranul de autentificare (este necesară re-autentificarea pentru a continua)."
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Protecție stații și servere fizice si virtualizate În cerințe și specificații tehnice se solicită Protecție stații și servere fizice si virtualizate – caracteristici minime «Soluția trebuie să: permită instalarea personalizată a modulelor.» Care module? De EDR?
Expunerea succintă a răspunsului	Cerința face referire la faptul că soluția permite instalarea personalizată a agentului la nivel de modul pentru toate componentele principale de securitate care vor asigura funcțiile de protecție enumerate în celelalte cerințe precum scanare euristică bazate pe semnături, protecție împotriva atacurilor zero day, etc. Modulul tip EDR poate fi și separat și instalabil selectiv, dar modelul de instalare personalizată nu se aplică exclusiv modulului EDR, ci întregului set de module disponibile/aplicabile.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Protecție stații și servere fizice si virtualizate

	În cerințe și specificații tehnice se solicită Protecție stații și servere fizice si virtualizate – caracteristici minime „să includă modul de sandbox, unde se vor putea trimite manual sau automat fișiere pentru a putea fi „detonate” pentru o analiză în profunzime.” Rugăm să specificați Sandbox de ce tip se solicit on-prem sau Cloud?
Expunerea succintă a răspunsului	Cerința indică necesitatea unui Sandbox, mai precis un serviciu de analiză comportamentală, integrat nativ cu consola de administrare și agentul software instalat local pe endpoint-uri. Fișierele suspecte de pe stațiile și serverele fizice sau virtualizate sunt trimise automat către un mediu virtual izolat, unde sunt rulate și monitorizate detaliat (fișiere, registre, procese, rețea). Pe baza verdictului întors de sandbox, soluția blochează, pune în carantină sau permite fișierul, iar administratorul are la dispoziție rapoarte detaliate (timeline, arbore de procese, clasificarea tipului de atac, IoC-uri). Verdictele sunt memorate pe hash de fișier și contribuie la actualizarea serviciului global de threat intelligence, astfel încât protecția împotriva amenințărilor noi este propagată rapid către toate endpoint-urile. Soluția de Sandbox poate fi atât onPrem cât și Cloud.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Administrare și instalare remote În cerințe și specificații tehnice se solicită „Administrare și instalare remote: Pachetele de instalare trebuie să fie configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay” (update server”);” Rugăm să oferiți în detalii care este tehnica?
Expunerea succintă a răspunsului	Soluția trebuie să ofere posibilitatea pregătirii pachetelor de instalare ale agentului ce sunt configurabile pe module, create în consola de administrare a soluției. Pentru fiecare pachet se pot selecta și combina module precum Firewall, Device Control, Content Control, Incidents/EDR Sensor, Power User și/sau a rolului de Relay (server de comunicare și update). Pachetele astfel definite se distribuie și pot fi rulate remote prin task uri „Install agent” din consola de administrare a soluției, pe stațiile descoperite în rețea, în grupurile Active Directory sau în inventarul de virtualizare. Distribuția poate fi realizată direct prin consola de administrare sau prin endpoint-uri cu rol special ce să permită distribuția, administrarea centralizată și instalarea la distanță a agenților, cu modulele indicate (din meniul de generare a pachetului de

	instalare din consolă). În urma instalării, folosind acest pachet de instalare, pe endpoint se vor regăsi agentul cu modulele indicate.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Caracteristici și funcționalități principale ale modulului antivirus În cerințe și specificații tehnice se solicită: „Caracteristici și funcționalități principale ale modulului antivirus: instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale;” Rugăm să oferiți în detalii care este tehnica.
Expunerea succintă a răspunsului	Conceptul funcționează astfel: instalare o singură dată pe template, propagare prin clonare în pool • Consola soluția trebuie să se integreaze cu VMware vCenter și Citrix XenDesktop și să poată importa automat inventarul (datacenter, cluster, resource pool, foldere, VM-uri). • Agentul software de securitate se instalează o singură dată pe mașina „golden image”/„master image” (model), care va fi ulterior convertită în template și/sau folosită ca sursă de linked/instant clones. • Pool-ul de mașini virtuale se recreează / recompune prin clonare din acest template. • Toate VM-urile nou create din acest template pornesc cu agentul deja instalat și se înregistrează automat în consola soluției (fiecare vm – endpoint separat). • Politicile se aplică la nivel de container (datacenter/cluster/pool/folder), astfel încât orice VM nou creat în acel container moștenește automat politica de securitate asociată.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Evaluare dinamică În cerințe și specificații tehnice se solicită: „Evaluare dinamică a accesului: unelte de Piraterie Software și Hacking: Soluția trebuie să identifice prezența și utilizarea instrumentelor asociate cu pirateria sau atacurile cibernetice.” Rugăm să oferiți mai multă infprmație despe Piraterie..
Expunerea succintă a răspunsului	Soluția de protecție endpoint trebuie să poată: 1 identifica; 2 controla (blocheze/permită); 3 monitoriza, următoarele categorii de instrumente asociate pirateriei software:

	• fișiere și programe de tip cracks, keygens, activatoare/patch-uri de licență, loader-e și instalatoare „warez”, precum și packete/protectoare utilizate tipic în distribuții de software piratat; • aplicații de tip PUA (Potentially Unwanted Applications) și „potentially unsafe/riskware” asociate scenariilor de piraterie; • site-uri de tip „warez (pirated software)” și alte resurse web utilizate pentru distribuția de software piratat. Soluția trebuie să detecteze atât instrumente de hacking clare, cât și unelte dual use sau legitime folosite abuziv în atacuri, inclusiv: • malware și instrumente ofensive: exploit kits, troieni, keyloggers, rootkits, backdoor-e, RAT-uri, clienți de botnet, dump-ere de parole, password crackers, droppere de ransomware etc.; • instrumente dual use/administrative sau de pentest utilizate în atacuri (de exemplu: unelte de exfiltrare date precum Rclone, utilitare de escaladare de privilegii sau lateral movement, suite Sysinternals, TacticalRMM, gsudo și alte tool-uri legitime folosite abuziv); • instrumente de rețea și scanning/atac: port scannere, exploituri de rețea, unelte de brute force și componente implicate în trafic C2; • aplicații neproductive sau riscante utilizate în scenarii de piraterie/hacking, cum ar fi clienți de torrent/P2P, aplicații de partajare necontrolată de fișiere sau soluții de remote access neautorizate. Soluția trebuie să acopere următoarele scenarii de utilizare relevante pentru piraterie software și hacking: • prevenirea instalării și utilizării software-ului piratat: blocarea sau avertizarea accesului la site-uri warez, detectarea și blocarea/crantinarea crack-urilor, keygen-urilor și altor activatoare, precum și posibilitatea de a bloca clienți de tip P2P/torent folosiți pentru distribuția de software piratat; • semnalarea și, la necesitate, blocarea utilizării de unelte de hacking în mediul de producție: detecția și blocarea uneltelor de tip password dumper, scanner de rețea agresiv, instrumente de exfiltrare (ex. Rclone) și a altor tool-uri ofensive sau dual-use, cu posibilitatea de a alege între modurile „Detection and Prevention” (blocare) și „EDR – Report only” (doar monitorizare); • control granular al uneltelor de test/pentest: posibilitatea ca în mediile de laborator red team/pentest aceleași instrumente de atac (Kali/pentest tools, utilitare Sysinternals etc.) să fie

	permise și monitorizate, în timp ce în mediile de producție sunt detectate și blocate.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Senzori XDR În cerințe și specificații tehnice se solicită: „Senzori XDR: solicitări de acces suspecte, cum ar fi acordarea accesului unui utilizator la mai multe fișiere sau directoare de pe diferite site-uri SharePoint într-o perioadă scurtă de timp.” Rugăm să oferiți mai multe detalii.
Expunerea succintă a răspunsului	Prin senzori specifici de analiză a telemetriei contului de Office 365 (Office 365 Mail și Office 365 Audit), soluția trebuie să detecteaze solicitări de acces suspecte, inclusiv scenarii în care același utilizator primește sau utilizează acces la un număr mare de fișiere/directoare pe mai multe site-uri SharePoint/OneDrive într-un interval scurt de timp. Detecția se bazează pe colectarea evenimentelor de acces, partajare și modificare de permisiuni din Microsoft 365 unified audit log (inclusiv Audit.SharePoint) și pe corelarea acestora cu date de identitate (Entra ID) și endpoint în motorul de corelare al incidentelor, pentru identificarea anomaliilor și a conturilor compromise. Senzorul soluției trebuie să genereze incidente corelate cu timeline detaliat al activităților, mapare a tehnicilor de atac și context de identitate, evidențiind clar accesările masive sau neobișnuite. Din aceste incidente, soluția trebuie să permită acțiuni de răspuns asupra mediului Office 365, precum dezactivarea sau resetarea contului, revocarea sesiunilor, marcarea utilizatorului ca „compromis” și acțiuni asupra fișierelor SharePoint/OneDrive (eliminarea fișierelor malițioase sau restricționarea accesului), în funcție de permisiunile de răspuns acordate.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	18.12.2025
Expunerea succintă a solicitării de clarificare	Senzor de identitate În cerințe și specificații tehnice se solicită: „Senzor de identitate: Senzorul trebuie să monitorizeze și analizeze identitățile utilizatorilor, controalele de acces și activitățile de autentificare din cadrul rețelei sau din mediul cloud. Acești senzori monitorizează continuu evenimentele legate de identitate și comportamentele conturilor, permițând identificarea potențialelor amenințări sau anomalii de securitate.” Ce se are in vedere prin controale de acces?

Expunerea succintă a răspunsului	În contextul senzorului de identitate prin „controale de acces” se înțeleg configurarea și utilizarea drepturilor de acces în infrastructura de identitate on prem și cloud – Active Directory, Microsoft Entra ID/Azure AD și Microsoft Intune – incluzând conturi, grupuri, privilegii, permisiuni de aplicații, precum și politici de acces și de dispozitiv. Senzorul de identitate trebuie să: • monitorizeze continuu aceste controale de acces (cine are ce drepturi, ce politici sunt aplicate, ce aplicații au ce permisiuni) și activitățile de autentificare asociate; • detecteaze anomalii și tentative de abuz (escaladare de privilegii, conturi compromise, permisiuni excesive, schimbări riscante de politici sau configurații Intune); • trimită evenimentele către motorul de corelare al incidentelor: pentru corelare cu alte telemetrii și generarea de incidente; • permită acțiuni rapide de răspuns din consola de administrare (de exemplu: dezactivarea contului, resetarea parolei, marcarea utilizatorului ca „compromised” în Entra ID) pentru a preveni sau limita accesul neautorizat și a restabili un nivel sigur al controalelor de acces.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	19.12.2025
Expunerea succintă a solicitării de clarificare	Politici Activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere nu este funcția de bază EDR/XDR. Rugăm, să modificați această cerință, deoarece face favoarea a vendorului de EPP care se utilizează în cadrul BNM. Rugăm să excludeți această cerință sau se fie modificată.
Expunerea succintă a răspunsului	Cerința rămâne valabilă. În cerințe e indicată necesitatea unei platforme integrate care include atât prevenție, cât și detecție și răspuns. Nu se solicită funcționalități separate, ci capabilități consolidate într-o singură soluție. Denumirea bunurilor în anunțul de participare și caietul de sarcini la cerința față de bunuri este: Soluție de securitate cibernetică avansată pentru dispozitive tip Server/PC/Laptop/VDI.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	19.12.2025
Expunerea succintă a solicitării de clarificare	Instalarea personalizată a modulelor Este acceptabil posibilitatea cu intergarea 3rd party Sandbox? Deoarece soluția completă Sandbox este soluția separată (Hardware/ VA/ Cloud).

Expunerea succintă a răspunsului	Arhitectura globală poate include unul sau mai multe sandbox-uri 3rd party (hardware/VA/cloud), cu condiția existenței unei integrări funcționale native sau certificate și a fluxurilor automate de analiză și răspuns. Dacă soluția de securitate cibernetică are inclus un Sandbox nativ performant, care acoperă cerințele, nu sunt necesare integrări multiple cu alte soluții de Sandbox.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	19.12.2025
Expunerea succintă a solicitării de clarificare	Instalarea personalizată a modulelor Descriere la această cerință seamănă cu IOC (indicator of Compromise). Rog, să confirmați dacă corect tractăm această cerință. Import folosind prin un fișier CSV este obligatoriu sau se permit și în alte formate?
Expunerea succintă a răspunsului	Funcția EDR de blocklist la nivel de industrie funcționează prin analiza telemetriei raw pe care doar EDR o corelează și o monitorizează. Funcția de blocare deși poate face parte și din alte module în mod limitat este o funcționalitate EDR. Formatul CSV este cel mai utilizat deoarece este universal ușor de citit, fiind o listă de identificatori precum MD5 sau SHA256 separați prin virgulă. Soluția poate bloca sau exclude fișiere/procese pe baza hash-urilor MD5/SHA256 direct din pagina incidentului, prin acțiunea de adăugare în Blocklist (reguli Application hash). Totodată, soluția poate importa și utiliza hash-uri MD5/SHA256 din fișiere CSV pentru blocarea fișierelor/proceselor, în formatul CSV standard (tip hash, valoare hash, notă opțională).
Data transmiterii	19.12.2025
Data solicitării clarificărilor	19.12.2025
Expunerea succintă a solicitării de clarificare	Firewall nu este funcția de bază EDR/XDR. Rugăm, să modificați această cerință, deoarece face favoarea a vendorului de EPP care se utilizează în cadrul BNM. Rugăm să excludeți această cerință sau se fie modificată.
Expunerea succintă a răspunsului	Funcționalitatea de firewall este solicitată ca parte a protecției endpoint integrate și nu ca soluție separată. Se acceptă implementări software la nivel de endpoint, integrate în platforma de securitate. Denumirea bunurilor în anunțul de participare și caietul de sarcini la cerința față de bunuri este: Soluție de securitate cibernetică avansată pentru dispozitive tip Server/PC/Laptop/VDI.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	19.12.2025

Expunerea succintă a solicitării de clarificare	Controlul conținutului Este cerință de soluția antivirus. Web Control nu este funcția de bază EDR/XDR. Rugăm, să modificați această cerință, deoarece face favoarea a vendorului de EPP care se utilizează în cadrul BNM.
Expunerea succintă a răspunsului	Web Control este solicitat ca mecanism de reducere a suprafeței de atac și de prevenție, integrat în soluția endpoint. Denumirea bunurilor în anunțul de participare și caietul de sarcini la cerința față de bunuri este: Soluție de securitate cibernetică avansată pentru dispozitive tip Server/PC/Laptop/VDI.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	19.12.2025
Expunerea succintă a solicitării de clarificare	Senzor de identitate Rugăm să specificați ce se are în vedere prin controale de acces?
Expunerea succintă a răspunsului	Se confirmă că prin controale de acces se înțeleg toate mecanismele de autentificare, autorizare și gestionare a privilegiilor utilizatorilor, inclusiv corelarea acestora cu evenimentele de securitate și riscul asociat.
Data transmiterii	19.12.2025
Data solicitării clarificărilor	21.12.2025
Expunerea succintă a solicitării de clarificare	Cantitatea Rugăm sa specificați cantitatea, deoarece nu este clar. Se solicita total pentru 1000 sau 2300 dispozitive?
Expunerea succintă a răspunsului	Referitor la solicitarea dumneavoastră de clarificare, vă comunicăm următoarele: În conformitate cu Anexa nr. 1 la Caietul de Sarcini, secțiunea „Cantitate licențe”, se solicită o soluție de securitate care să asigure protecția pentru un număr total de 1.000 (una mie) de dispozitive (endpoint-uri de tip PC, Laptop, VDI sau Server). Celelalte cantități menționate în specificațiile tehnice (700 utilizatori și 600 utilizatori Microsoft 365) reprezintă parametrii necesari pentru dimensionarea modulelor specifice (ex: protecția identității, protecția aplicațiilor de colaborare, etc..), în cazul în care modelul de licențiere al soluției ofertate necesită o astfel de diferențiere. Prin urmare, oferta financiară și tehnică trebuie să acopere protecția EDR/EPP pentru 1.000 de endpoint-uri, incluzând funcționalitățile solicitate pentru numărul de utilizatori specificați.
Data transmiterii	22.12.2025
Data solicitării clarificărilor	21.12.2025
Expunerea succintă a solicitării de clarificare	Licentiere Ce tip de licență se solicita?

Expunerea succintă a răspunsului	În conformitate cu cerințele din Caietul de Sarcini, se solicită o licențiere de tip Subscripție (Subscription) pe o perioadă determinată de 12 luni (07.02.2026 – 07.02.2027). Licența ofertată trebuie să fie complet funcțională pentru numărul total de endpoint-uri solicitat și să includă obligatoriu, pe toată durata contractului: 1. Dreptul de utilizare a soluției software (agenți și consolă de management); 2. Accesul la toate modulele funcționale descrise în specificațiile tehnice; 3. Actualizări automate de securitate (semnături, baze de date, indicatori de compromitere); 4. Actualizări de versiune a produsului (software upgrades) lansate de producător în această perioadă; 5. Suport tehnic din partea producătorului.
Data transmiterii	22.12.2025

4.Modificări operate în documentația de atribuire: n/a

(Se va completa în cazul în care au fost operate modificări)

Rezumatul modificărilor	**-**
Publicate în BAP/alte mijloacelor de informare *(după caz)*	-
Termen-limită de depunere și deschidere a ofertelor prelungit *(după caz)*	-

5.Până la termenul-limită (data 31 decembrie 2025, ora 08:48), a depus oferta 1 (unu) operator economic:

Nr.	Denumirea operatorului economic	IDNO	Asociații/ administratorii
1.	**RTS ONE SRL**	1018600009979	SC REȚELE TERESTRE SRL (NICOLAEV VIRGINIA), CIOCLEA PETRU, CIOCLEA OLGA / CELONENCO VITALIE

6. Informații privind ofertele depuse și documentele de calificare și aferente DUAE prezentate de către operatorii economici:

Denumire document	Denumirea operatorului economic
	RTS ONE SRL
Documentele ce constituie oferta	
Propunerea tehnică	*prezentat*
Propunerea financiară	*prezentat*
DUAE	*prezentat*
Garanția pentru ofertă	*prezentat*
Documente de calificare	
Declarație privind valabilitatea ofertei	*prezentat*
Declarația privind respectarea regimului de incompatibilități prevăzute la art. 16 alin. (6) din Legea nr. 131/2015	*prezentat*

Declarația privind lipsa conflictului de interese	*prezentat*
Dovada înregistrării persoanei juridice, în conformitate cu prevederile legale din ţara în care ofertantul este stabilit	*prezentat*
Existența contului bancar	*prezentat*
Situațiile financiare	*prezentat*
Certificat care confirmă neaplicarea sancţiunilor penale (cazier judiciar) faţă de ofertant	*prezentat*
Demonstrarea experienței operatorului economic în domeniul de activitate aferent obiectului contractului ce urmează a fi atribuit	*prezentat*
Prezentarea actelor care atestă dreptul de livrare/prestare a bunurilor/serviciilor	*prezentat*
Deținerea certificatelor sau alte documente ce atestă respectarea/ îndeplinirea standardelor de asigurare a calității și/sau a standardelor de protecție a mediului	*nu a prezentat*

*(Informația privind denumirea documentelor prezentate se va indica în conformitate cu cerințele din documentația de atribuire și se va consemna prin: **prezentat, neprezentat, nu corespunde** (în cazul când documentul a fost prezentat, dar nu corespunde cerințelor de calificare)*

7. Informația privind corespunderea ofertelor cu cerințele solicitate:

Denumirea lotului	**Denumirea operatorului economic**	**Prețul ofertei, MDL** (fără TVA)	**Cantitate și unitate de măsură**	**Corespunderea cu cerințele de calificare**	**Corespunderea cu specificațiile tehnice**
Soluții EDR pentru Modernizarea și Eficientizarea Protecției Cibernetice	RTS ONE SRL	820 420,00	1 bucata	+	+

** În cazul utilizării licitației electronice se va indica prețul ofertei finale (Informația privind "Corespunderea cu cerințele de calificare" și "Corespunderea cu specificațiile tehnice" , se va consemna prin: „+" în cazul corespunderii și prin „-" în cazul necorespunderii).*

8. Pentru elucidarea unor neclarități sau confirmarea unor date privind corespunderea ofertei cu cerințele stabilite în documentația de atribuire (inclusiv justificarea prețului anormal de scăzut) s-a solicitat:

Data solicitării	**Operatorul economic**	**Informația solicitată**	**Rezumatul răspunsului operatorului economic**
06.01.2026	RTS ONE SRL	Clarificare privind prezentarea componenței soluției ofertate, lista completă a componentelor/ licențelor/serviciilor incluse precum și a cantităților care vor acoperi funcționalul solicitat pentru 1000	Operatorul economic a confirmat că componența soluției ofertate și corelarea acesteia cu funcționalitățile solicitate, pentru acoperirea 1000 endpoints, 700 utilizatori și 600 utilizatori Microsoft 365. 1. Soluția ofertată

Data solicitării	Operatorul economic	Informația solicitată	Rezumatul răspunsului operatorului economic
		endpoints, 700 utilizatori, 600 utilizatori Microsoft 365. Inclusiv, solicitarea de a preciza care din componentele/modulele din cadrul soluției ofertate acoperă funcționalitățile solicitate prin caietul de sarcini: EDR, XDR, monitorizarea și analiza traficului de rețea, monitorizarea/protecția identităților, monitorizarea aplicațiilor Microsoft 365, corelarea evenimentelor de securitate, precum și alte module sau servicii relevante menționate în documentația de atribuire, astfel încât să poată fi verificată conformitatea soluției ofertate.	Soluția ofertată este Bitdefender GravityZone Business Security Enterprise, platformă unificată de securitate endpoint și XDR, care include senzori XDR nativi pentru endpoint, rețea, identitate și aplicații de productivitate, precum și modulul GravityZone PHASR pentru evaluare dinamică a accesului și reducerea suprafeței de atac. 2. Componența și cantități: - GravityZone Business Security Enterprise – 1000 endpoints; - Senzori XDR Endpoint & Network – incluși în licența Enterprise; - Senzor XDR pentru identitate (Identity Security) – 700 utilizatori; - Protecție Microsoft 365 (Exchange Online, OneDrive, SharePoint) – 600 utilizatori; - GravityZone PHASR (Proactive Hardening and Attack Surface Reduction) – 1000 endpoints; - Servicii profesionale (implementare, configurare, instruire) – inclus. Soluția Bitdefender GravityZone Business Security Enterprise îndeplinește integral cerințele funcționale din caietul de sarcini pentru volumele solicitate, printr-o arhitectură unificată EDR/XDR, asigurând acoperirea completă a funcționalităților cerute la nivel de endpoint, identitate, rețea și aplicații de productivitate.
		Clarificare cu referire la criteriul de performanță indicat la pct. 4.1 ”Experiență în livrări EDR/XDR (ultimii 3 ani)”, precum și Declarația de la distribuitor prezentată în acest sens în ofertă, vă rugăm să clarificați și să	Operatorul economic pentru demostrarea criteriului de performanță indicat la pct.4.1. „Experiență în livrări EDR/XDR (ultimii 3 ani)”, în calitate de furnizor și implementator principal, a comunicat că, în conformitate cu Anexa nr.12 „DECLARAŢIE privind lista principalelor livrări/ prestări efectuate în ultimii 3 ani de activitate” prezentate în cadrul

Data solicitării	Operatorul economic	Informația solicitată	Rezumatul răspunsului operatorului economic
		demonstrați îndeplinirea cerinței, respectiv: - Existența a minimum 3 proiecte EDR/XDR implementate cu succes în ultimii 3 ani; - Încadrarea implementărilor prezentate în perioada ultimilor 3 ani; - Caracterul EDR/XDR al soluțiilor implementate; - Rolul ofertantului în cadrul proiectelor (implementator principal / integrator / furnizor) - Relevanța implementărilor în raport cu instituții publice, financiare, bănci sau infrastructuri critice. Precum și clarificări la criteriul de performanță indicat la pct. 4.2 „Implementări ale soluției propuse în instituții critice din UE (ultimii 3 ani)", precum și Declarația producătorului prezentată în ofertă, în acest sens, vă rugăm să clarificați și să demonstrați îndeplinirea integrală a acestei cerințe, inclusiv sub aspectul: - Existenței a minimum 3 implementări distincte în Uniunea Europeană, realizate în ultimii 3 ani, în instituții publice, financiare sau bănci; - Dimensiunii implementărilor (minimum 1000 endpoints);	licitației publice, principalele 3 proiecte implementate cu funcționalitățile de EDR/XDR sunt: a) Secretariatul Parlamentului Republicii Moldova – instituție publică; b) I.M.S.P. CENTRUL NATIONAL DE ASISTENTA MEDICALA URGENTA – instituție publică; c) O.C.N. MICROINVEST S.R.L. – organizație financiară. pentru demostrarea criteriului de performanță indicat la pct.4.2. „Implementări ale soluției propuse în instituții critice din UE (ultimii 3 ani)" OE a prezentat o scrisoare din partea Producatorului Bitdefender in care a mentionat ca Implementările au fost realizate în Uniunea Europeană, în instituții publice, unități esențiale sau instituții financiare, cu volum de minimum 1.000 endpoint-uri/licențe, utilizând soluții Bitdefender Enterprise și/sau componente EDR/XDR, după cum urmează, pe baza informațiilor publice disponibile: 1. AOU Bologna – Policlinico Sant'Orsola (Italia), Domeniu: instituție publică – sănătate (unitate esențială). Soluție: Bitdefender GravityZone Business Security Enterprise – GOV Volum: 5.700 licențe EDR/XDR: EDR integrat (menționat explicit în documentația publică) Patria Bank S.A. (România) Domeniu: instituție financiară – bancă Soluție: Bitdefender GravityZone Business Security Enterprise Volum: 1.100 endpoint-uri EDR/XDR: EDR Link: https://www.bitdefender.com/content/dam/bitdefender/business/case-studies/patria-bank/Bitdefender-CaseStudy-PatriaBank.pdf

Data solicitării	Operatorul economic	Informația solicitată	Rezumatul răspunsului operatorului economic
		- Nivelului de utilizare a soluției (EDR / XDR / alte componente relevante); - Concordanței implementărilor cu soluția EDR/XDR ofertată în cadrul prezentei proceduri	3. Casa Națională de Asigurări de Sănătate (CNAS) – procedura SCN1152801 (România) Domeniu: instituție publică – sănătate (unitate esențială) Soluție: Bitdefender GravityZone Enterprise Volum: minimum 1.630 – maximum 5.330 licențe (acord-cadru) EDR/XDR: Enterprise (capabilități EDR/XDR conform gamei GravityZone) Link: https://www.e-licitatie.ro/pub/notices/rfq-invitation/v2/view/100213591 4. Ministerul Afacerilor Externe al României (MAE) – procedura SCN1161658 (România) Domeniu: instituție publică centrală – administrație publică Soluție: Bitdefender GravityZone Business Security Enterprise Volum: 2.000 licențe EDR/XDR: Enterprise (EDR inclus conform gamei de produs) Link: https://e-licitatie.ro/pub/notices/ca-notices/view-c/100553051

9. Ofertanții respinși/descalificați: n/a

Denumirea operatorului economic	Motivul respingerii/descalificării
-	-

10.Modalitatea de evaluare a ofertelor:

Pentru fiecare lot ☑

Pentru mai multe loturi cumulate □

Pentru toate loturile □

Alte limitări privind numărul de loturi care pot fi atribuite aceluiași ofertant: *[Indicați]*

Justificarea deciziei de a nu atribui contractul pe loturi:

_____

11.Criteriul de atribuire aplicat:

Preţul cel mai scăzut□

Costul cel mai scăzut □

Cel mai bun raport calitate-preţ ☑

Cel mai bun raport calitate-cost □

(În cazul în care în cadrul procedurii de atribuire sunt aplicate mai multe criterii de atribuire, se vor indica toate criteriile de atribuire aplicate și denumirea loturilor aferente)

12.Informaţia privind factorii de evaluare aplicați: n/a

(Se va completa pentru loturile care au fost atribuite în baza criteriilor: cel mai bun raport calitate-preţ sau cel mai bun raport calitate-cost)

Factorii de evaluare		Valoarea din ofertă	Punctajul calculat
Lotul: Soluții EDR pentru Modernizarea și Eficientizarea Protecției Cibernetice			
RTS ONE SRL			**Total:100**
Evaluarea financiară	70	820 420,00	70,00
Evaluarea criteriilor de performanță	30	-	30,00

13.Reevaluarea ofertelor: n/a

(Se va completa în cazul în care ofertele au fost reevaluate repetat)

Motivul reevaluării ofertelor	
Modificările operate	

14.În urma examinări, evaluării și comparării ofertelor depuse în cadrul procedurii de atribuire s-a decis:

Atribuirea contractului de achiziție publică:

Denumirea lotului	Denumirea operatorului economic	Cantitate și unitate de măsură	Prețul unitar, (fără TVA)	Prețul total, (fără TVA)	Prețul total, (inclusiv TVA)
Lotul: Soluții EDR pentru Modernizarea și Eficientizarea Protecției Cibernetice					
Soluție de securitate cibernetică avansată pentru dispozitive tip Server/PC/Laptop/ VDI	**RTS ONE SRL**	1 buc.	820 420,00	820 420,00	984 504,00
TOTAL:				**820 420,00**	**984 504,00**

Anularea procedurii de achiziție publică: nu se aplică.

Argumentare: nu se aplică.

15. Componența grupului de lucru instituit prin ordinul nr.335 din 18.11.2019, cu modificările ulterioare:

Nr.	Nume, Prenume	Funcția în cadrul grupului de lucru	Semnătura
1.	**ȘCHENDRA Constantin**	**Președinte a grupului de lucru**	
2.	**PISARENCO Olga**	**Președinte adjunct al grupului de lucru**	

3.	**GAGEA Radu**	**Președinte adjunct al grupului de lucru**	
4.	**VRANCEAN Andjana**	**Membră al grupului de lucru**	
5.	**DANILĂ Ștefan**	**Membru al grupului de lucru**	
6.	**UNGUREAN Valeriu**	**Membru al grupului de lucru**	
7.	**ȘUȘU Elena**	**Membră a grupului de lucru**	
8.	**DOLGHII Silvia**	**Secratară a grupului de lucru**	