

ROMÂNIA
MINISTERUL APĂRĂRII NAȚIONALE
COMANDAMENTUL APĂRĂRII CIBERNETICE

Anexo nr 2/e Nr. *3A-1229* din *22.05.* 2026
București

NECLASIFICAT

Exemplarul unic

Dosar nr. _____

Termen de păstrare: 5 ani

SPECIFICAȚIE TEHNICĂ PENTRU ACHIZIȚIE

Complet pentru scanarea de vulnerabilități a rețelelor informatice

**BUCUREȘTI
2026**

CUPRINS

1. SCOP	3
2. CERINȚE	3
2.1 Cerințe privind configurația completului.....	3
2.2 Cerințe de performanță și specifice produsului <i>aplicație software-scanner</i>	3
2.3 Cerințe de performanță și specifice produsului <i>aplicație software-scanner de vulnerabilități cu suport pentru activele externe</i>	5
2.4 Cerințe licențiere.....	7
2.5 Alte cerințe	7

1. SCOP

Prezenta specificație stabilește cerințele tehnice pentru achiziționarea unui complet software a cărui componente să poată scana infrastructurile de rețea în vederea detectării vulnerabilităților de securitate existente la nivelul acestora, precum și să prezinte modalitățile și soluțiile de remediere, respectiv de eliminare a vulnerabilităților identificate la nivelul fiecărei infrastructuri de rețea scanată.

2. CERINȚE

2.1 Cerințe privind configurația completului

Nr. cerință	CERINȚA
C1.	Completul trebuie să aibă compunerea din tabelul următor:

Nr. crt.	Tip componentă	UM	Cantitate
1.	Aplicație software-scanner	buc.	6
2.	Aplicație software-scanner de vulnerabilități cu suport pentru activele externe	buc.	1

2.2 Cerințe de performanță și specifice produsului *aplicație software-scanner*

Nr. cerință	CERINȚA
C2.	Produsul software oferit trebuie să poată fi instalat pe diferite platforme de sisteme de operare și distribuții, cum ar fi: • Windows - 10, 11, Server 2012R2, Server 2016, Server 2019, Server 2022, Server 2025, platforme pe 32 sau 64 de biți; • Linux – Debian 11, 12, 13, Red Hat EL 8.8, 8.10, 9.0, 9.2, 9.4, 10, Kali 2020, Fedora 41, 42, Ubuntu 20.04, 22.04, 24.04; • Mac OS – 14, 15, 26.
C3.	Produsul trebuie să poată scana diferite sisteme de operare, dispozitive de rețea (switch-uri, routere, firewall-uri, soluții de tip storage, imprimante, scanere), diferite tipuri de hipervizoare, baze de date, tablete, telefoane mobile, servere web și componente critice de rețea pentru detectarea vulnerabilităților, amenințărilor și încălcărilor ale conformității politicilor de securitate.
C4.	Produsul trebuie să poată scana infrastructuri de rețea care folosesc adrese IP de tip IPv4 sau IPv6, precum și o rețea hibridă.
C5.	Produsul trebuie să poată scana fără să folosească credențiale ale utilizatorilor/administratorilor din infrastructura de rețea pentru a descoperi vulnerabilități ascunse sau conexiuni vulnerabile de tipul null session, precum și folosind credențiale de rețea pentru identificarea actualizărilor de aplicații software, respectiv de securitate.
C6.	Scanarea având credențiale asupra sistemelor de operare și a echipamentelor de rețea să poată fi configurată pentru diferite metode de autentificare. Acestea pot include SSH, perechi de chei SSH, SSH cu elevarea privilegiilor, Kerberos, SMB, sau altele.

C7.	Scanarea internă a vulnerabilităților dintr-o infrastructură de rețea să se facă respectând cerințele PCI DSS.
C8.	Produsul trebuie să ofere scanarea de vulnerabilități a dispozitivelor dintr-o infrastructură de rețea, chiar dacă aceasta este offline, fără conectare la INTERNET.
C9.	Produsul trebuie să poată scana și detecta vulnerabilitățile a dispozitivelor de rețea (firewall, switch, routere) de la diferiți vendori, cum ar fi Cisco, Fortinet, Juniper, IBM, Palo Alto, Check Point, Sonic Wall, Sophos, Watch Guard respectiv diferite tipuri de servere de baze de date Oracle, SQL Server, MySQL, IBM DB2, SAP HANA, Sybase ASE, PostgreSQL, MongoDB, Maria DB, Redis.
C10.	Produsul trebuie să poată scana și detecta vulnerabilitățile diferitelor sisteme de operare, sisteme Microsoft Windows, Mac OS, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries, respectiv diferite soluții de virtualizare VMware ESX, ESXi, vSphere, vCenter, Microsoft Hyper-V, Citrix Xen Server.
C11.	Produsul trebuie să poată permite importul și aplicarea fișierelor de reguli de tip YARA.
C12.	Produsul trebuie să poată detecta vulnerabilități cunoscute în sisteme de operare și aplicații, configurări nesigure, patch-uri lipsa și să permită audit de conformitate pentru standarde precum PCI DSS, CIS Benchmarks sau ISO 27002.
C13.	Produsul asigura detectarea și raportarea vulnerabilităților asociate programelor malițioase (malware) – inclusiv viruși, viermi, adware, spyware și backdoor-uri, prin intermediul scanării active a sistemelor și serviciilor din rețea. Produsul identifică sistemele potențial compromise care prezintă indicatori de vulnerabilitate asociați infrastructurilor de tip botnet, detectează procesele sau servicii cu configurații nesigure și evaluează serviciile web pentru a identifica vulnerabilități care pot facilita redirectionări malițioase către conținut infectat.
C14.	Produsul trebuie să efectueze scanarea de vulnerabilități în conformitate cu diferite standarde internaționale de securitate, cum ar fi FISMA, CyberScope, GLBA, HIPAA/HITECH, SCAP.
C15.	Produsul trebuie să poată scana simultan diferite IP-uri, precum și range-uri de IP-uri sau diferite echipamente existente în cadrul unei infrastructuri de rețea.
C16.	Produsul trebuie să poată fi instalat atât într-o infrastructură de rețea conectată la INTERNET cât și într-una neconectată la INTERNET.
C17.	Produsul trebuie să execute scanări de vulnerabilități, fără instalarea de agenți pe echipamentele scanate atât în infrastructura locală a unei rețele, cât și la distanță, asupra infrastructurilor de rețea aflate în diferite locații, prin intermediul unei conexiuni VPN site-to-site terțe, în vederea identificării activelor de rețea și a echipamentelor care sunt online.
C18.	Vulnerabilitățile identificate de către produs trebuie să fie automat catalogate după criteriile de severitate și nivelul gradului de risc (Critical, High, Medium, Low, Info), conform modelului CVSS (Common Vulnerability Scoring System), în vederea determinării urgenței și prioritizării modului de remediere a acestora.
C19.	Vulnerabilitățile identificate care pot fi exploatate cu aplicații de testare (Metasploit, Core Impact și Canvas), să poată fi filtrate și detaliate din acest punct de vedere și al severității, pentru a putea fi prioritizate testările și eliminării.

C20.	La finalizarea fiecărei scanări de vulnerabilități, produsul trebuie să poată genera un raport care să poată fi personalizat în funcție de vulnerabilitățile identificate sau echipamentele scanate. Produsul trebuie să genereze raportul asemenea unui scurt rezumat pentru echipa de management a instituției sau detaliat, cu informațiile tehnice necesare personalului care administrează infrastructura de rețea pentru a putea elimina vulnerabilitățile identificate.
C21.	Rapoartele privind detaliile despre vulnerabilitățile identificate la finalizarea unei scanări, generate de către produs, să poată fi exportate cel puțin în format <i>.pdf</i> , <i>.html</i> și <i>.csv</i> .
C22.	Produsul trebuie să poată filtra vulnerabilitățile identificate după diferite criterii precum CVSS, CPE (Common Platform Enumeration), CVE (Common Vulnerabilities and Exposures), Microsoft Bulletin ID, port, protocol și altele.
C23.	Produsul trebuie să asigneze la vulnerabilitățile detectate în cadrul unei rețele, recomandările, contramăsurile și configurările de securitate, patch-urile și actualizările necesare eliminării tuturor vulnerabilităților identificate.
C24.	Produsul să poată fi administrat și utilizat printr-o interfață web securizată folosind conturi de utilizator cu drepturi simple asupra aplicației software sau cu drepturi administrative depline.
C25.	Rezultatele fiecărei scanări să poată fi salvate în diferite foldere configurate în cadrul interfeței web de utilizare a produsului oferit.
C26.	Produsul trebuie să poată scana un număr nelimitat de adrese IP sau echipamente de rețea, iar numărul diferitelor scanări de vulnerabilități executate să fie de asemenea nelimitat.

2.3 Cerințe de performanță și specifice produsului aplicație software-scanner de vulnerabilități cu suport pentru activele externe.

Nr. cerință	CERINȚA
C27.	Produsul software oferit trebuie să poată fi instalat pe diferite platforme de sisteme de operare și distribuții, cum ar fi: • Windows - 10, 11, Server 2012R2, Server 2016, Server 2019, Server 2022, platforme pe 32 sau 64 de biți; • Linux - Debian, Red Hat, Rocky, SuSE, Ubuntu; • Mac OS – 14, 15, 26;
C28.	Produsul trebuie să poată scana diferite sisteme de operare, dispozitive de rețea (switch-uri, routere, firewall-uri, soluții de tip storage, imprimante, scanere), diferite tipuri de hipervizoare, baze de date, tablete, telefoane mobile, servere web și componente critice de rețea pentru detectarea vulnerabilităților, amenințărilor și încălcărilor ale conformității politicilor de securitate.
C29.	Produsul trebuie să permită identificarea și analiza a cel puțin cinci domenii și subdomeniilor care fac parte din structura organizației.
C30.	Produsul trebuie să permită modificarea domeniilor pentru scanare, la un interval definit de timp.
C31.	Produsul trebuie să conțină politici de audit predefinite pentru scanarea infrastructurilor de tip cloud.
C32.	Produsul trebuie să permită identificarea vulnerabilităților din etapa de dezvoltarea a cloud-ului (SDLC – Software development lifecycle)

C33.	Produsul trebuie să permită scanarea infrastructurilor cloud.
C34.	Produsul trebuie să poată scana infrastructuri de rețea care folosesc adrese IP de tip IPv4 sau IPv6, precum și o rețea hibridă.
C35.	Produsul trebuie să poată scana fără să folosească credențiale ale utilizatorilor/administratorilor din infrastructura de rețea pentru a descoperi vulnerabilități ascunse sau conexiuni vulnerabile de tipul null session, precum și folosind credențiale de rețea pentru identificarea actualizărilor de aplicații software, respectiv de securitate.
C36.	Scanarea având credențiale asupra sistemelor de operare și a echipamentelor de rețea să poată fi configurată pentru diferite metode de autentificare. Acestea pot include SSH, perechi de chei SSH, SSH cu elevarea privilegiilor, Kerberos, SMB/WMI, SNMP sau altele.
C37.	Scanarea internă a vulnerabilităților dintr-o infrastructură de rețea să se facă respectând cerințele PCI DSS.
C38.	Produsul trebuie să ofere scanarea de vulnerabilități a dispozitivelor dintr-o infrastructură de rețea, chiar dacă aceasta este offline, fără conectare la INTERNET.
C39.	Produsul trebuie să poată scana și detecta vulnerabilitățile a dispozitivelor de rețea (firewall, switch, routere) de la diferiți vendori, cum ar fi Cisco, Fortinet, Juniper, Palo Alto, Check Point, SonicWall, F5 respectiv diferite tipuri de servere de baze de date Oracle, SQL Server, MySQL, DB2, Informix / DRDA, PostgreSQL, MongoDB, Maria DB.
C40.	Produsul trebuie să poată scana și detecta vulnerabilitățile diferitelor sisteme de operare, sisteme Microsoft Windows, Mac OS, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries, respectiv diferite soluții de virtualizare VMware ESX, ESXi, vSphere, vCenter, Microsoft Hyper-V, Citrix Xen Server, și soluții de virtualizare în cloud precum EC2, Microsoft Azure, Google Cloud.
C41.	Produsul trebuie să poată permite importul și aplicarea fișierelor de reguli de tip YARA.
C42.	Produsul trebuie să poată detecta amenințări precum conexiuni de tip botnet, procese malițioase active sau nereguli privind configurarea și actualizarea produselor software de tip antivirus.
C43.	Produsul asigură detecția și raportarea programelor malițioase (malware) – inclusiv viruși, viermi, adware, spyware și backdoor-uri. Produsul identifică sistemele compromise care prezintă trafic către infrastructuri de tip botnet, monitorizează procesele active (vizibile sau ascunse) și evaluează serviciile web pentru a detecta redirectionări malițioase către conținutul infectat.
C44.	Produsul trebuie să efectueze scanarea de vulnerabilități în conformitate cu diferite standarde internaționale de securitate, cum ar fi FISMA, CyberScope, GLBA, HIPAA/HITECH, SCAP.
C45.	Produsul trebuie să poată scana simultan diferite IP-uri, precum și range-uri de IP-uri sau diferite echipamente existente în cadrul unei infrastructuri de rețea.
C46.	Produsul trebuie să poată fi instalat atât într-o infrastructură de rețea conectată la INTERNET cât și într-una neconectată la INTERNET.
C47.	Produsul trebuie să execute scanări de vulnerabilități atât în infrastructura locală a unei rețele, cât și la distanță, asupra infrastructurilor de rețea aflate în diferite locații, în vederea identificării activelor de rețea și a echipamentelor care sunt online, precum și offline.

C48.	Vulnerabilitățile identificate de către produs trebuie să fie automat catalogate după criteriile de severitate și nivelul gradului de risc (Critical, High, Medium, Low, Info), conform modelului CVSS (Common Vulnerability Scoring System), în vederea determinării urgenței și prioritizării modului de remediere a acestora.
C49.	Vulnerabilitățile identificate care pot fi exploatate cu aplicații de testare (Metasploit, Core Impact și Canvas), să poată fi filtrate și detaliate din acest punct de vedere și al severității, pentru a putea fi prioritizate testării și eliminării.
C50.	La finalizarea fiecărei scanări de vulnerabilități, produsul trebuie să poată genera un raport care să poată fi personalizat în funcție de vulnerabilitățile identificate sau echipamentele scanate. Produsul trebuie să genereze raportul asemenea unui scurt rezumat pentru echipa de management a instituției sau detaliat, cu informațiile tehnice necesare personalului care administrează infrastructura de rețea pentru a putea elimina vulnerabilitățile identificate.
C51.	Rapoartele privind detaliile despre vulnerabilitățile identificate la finalizarea unei scanări, generate de către produs, să poată fi exportate cel puțin în format <i>.pdf</i> , <i>.html</i> și <i>.csv</i> .
C52.	Produsul trebuie să poată filtra vulnerabilitățile identificate după diferite criterii precum CVSS, CPE (Common Platform Enumeration), CVE (Common Vulnerabilities and Exposures), Microsoft Bulletin ID, port, protocol și altele.
C53.	Produsul trebuie să asigneze la vulnerabilitățile detectate în cadrul unei rețele, recomandările, contramăsurile și configurările de securitate, patch-urile și actualizările necesare eliminării tuturor vulnerabilităților identificate.
C54.	Produsul să poată fi administrat și utilizat printr-o interfață web securizată folosind conturi de utilizator cu drepturi simple asupra aplicației software sau cu drepturi administrative depline.
C55.	Rezultatele fiecărei scanări să poată fi salvate în diferite foldere configurate în cadrul interfeței web de utilizare a produsului oferat.
C56.	Produsul trebuie să poată scana un număr nelimitat de adrese IP sau echipamente de rețea, iar numărul diferitelor scanări de vulnerabilități executate să fie de asemenea nelimitat.

2.4 Cerințe licențiere

Nr. cerință	CERINȚA
C57.	Licența pentru produsele <i>Aplicație software-scanner</i> și <i>Aplicație software-scanner de vulnerabilități cu suport pentru activele externe</i> oferate din complet va fi de tipul cod de activare și cu subscripție pe minim 60 de luni, de la data recepției de către beneficiar.
C58.	Licențele trebuie să poată fi instalate și offline, într-o rețea fără conexiune la internet.

2.5 Cerințe privind garanția produsului

Nr. cerință	CERINȚA
C59.	Garanția produsului trebuie să fie de minim 60 de luni de la data recepției produsului.
C60.	Nu se acceptă condiționarea acordării garanției produsului de acordarea accesului ofertantului la produsul instalat în rețele private ale beneficiarului.

C61.	Pentru produsul software oferit garanția trebuie să includă: - acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora funcție de severitate; - dreptul de a face update-uri și upgrade-uri, gratuite, la toate componentele produsului software incluse în această achiziție, dacă pe perioada garanției apar astfel de situații.
------	---

2.6 Cerințe privind recepția produsului

Nr. cerință	CERINȚA
C62.	Recepția produsului se va desfășura în acord cu prevederilor contractuale și va conține o recepție calitativă și o recepție cantitativă.
C63.	Recepția se va realiza la sediul beneficiarului din str. Drumul Taberei 7-9, Sector 6, București, în prezența reprezentanților beneficiarului și contractantului.
C64.	În cadrul activității de recepție se vor parcurge următoarele etape: - verificarea livrării licențelor produsului; - verificarea funcționării produsului în acord cu prevederile cerințelor tehnice prevăzute în prezentul document, de către o comisie de recepție formată din angajați ai beneficiarului.
C65.	La finalul recepției cantitative se va întocmi un proces de recepție, care va avea ca referință și Procesul verbal al recepției calitative, prin care se va finaliza activitatea de recepție.

2.7 Cerințe privind documentația de instalare și utilizare

Nr. cerință	CERINȚA
C66.	Documentația de instalare și utilizare trebuie pusă la dispoziție în format electronic sau prin specificarea link-ului din internet unde se regăsește.

2.8 Alte cerințe

Nr. cerință	CERINȚA
C67.	Produsul oferit trebuie să fie nou, nefolosit și să încorporeze toate îmbunătățirile recente din documentația tehnică și de fabricație.
C68.	Produsul propus nu trebuie să includă un produs EoL (<i>End of Life</i>) și/sau EoS (<i>End of Sale</i>) la data depunerii ofertei.
C69.	Specificațiile tehnice și de calitate ale produsului oferit trebuie, obligatoriu, susținute de documentații originale: prospecte, foi de catalog sau documentații în format electronic.
C70.	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.