Anexa 1

Caiet de sarcini

Pentru procedura de Licitație publică

1. Denumirea beneficiarului de stat - Comisia Națională a Pieței Financiare

2. Organizatorul procedurii de achiziție - Comisia Națională a Pieței Financiare

3. Obiectul achiziției: Achiziționarea Prelungirii subscripției anuale si licențelor suplimentare a soluției corporative antivirus existente.

Specificația tehnică privind achiziționarea Prelungirii subscripției anuale si licențelor suplimentare a soluției corporative antivirus existente in cadrul CNPF pentru anul 2025

Codul CPV	Denumirea bunurilor si/sau a serviciilor	Specificația tehnică solicitată de către autoritatea contractantă
1	2	3
48761000-0	**Prelungirea subscripției anuale si licențe suplimentare a soluției corporative antivirus existente in cadrul CNPF pentru o perioadă de 12 luni.**	Soluție integrată pentru managementul securității endpoint-urilor, gândita ca o soluție modulara și scalabilă, bazata pe tehnologia Cloud, pentru a minimiza resursele locale. **Se solicită prelungirea subscriptiei anuale si licente suplimentare a soluției corporative antivirus existente in cadrul CNPF pentru o perioadă de 12 luni (Data expirarii licentelor existente 19/01/2025):** 1. **RENEWAL pentru 60 stații de lucru fizice și virtualizate existente:** (FCYBSR1GVXBQQ WithSecure Elements EPP for Computers Premium, Company Managed Renewal for 1 year Governmental). 2. **NEW pntru 20 stații de lucru fizice și virtualizate suplimentar aliniate la termenul mentionat a celor existente:** (FCYBSN1GVXBQQ WithSecure Elements EPP for Computers Premium, Company Managed License (competitive upgrade and new) for 1 year Governmental). 3. **RENEWAL pentru 40 servere fizice și virtualizate:** **(**FCRESR1GVXBQQ WithSecure Elements EPP for Servers Premium, Company Managed Renewal for 1 year Governmental). 4. **RENEWAL pentru 40 ip-uri unice.** (FCKCSR1NVXBQQ WithSecure Elements Vulnerability Management Renewal for 1 year Governmental). **Cerințe minime de calificare a ofertanților:** - Producătorul trebuie să ofere suport tehnic 24/7, prin e-mail sau telefon; - Suport tehnic local 24/7 în limba romana din partea partenerului local;

		- Autorizarea de la Producător a partenerului pentru licitatia in cauza vis-a-vis de dreptul de vânzare și de a oferi suport tehnic produselor ofertate pe teritoriul R. Moldova; - Prezentarea documentelor confirmative a minim 2 specialiști certificați pe soluția propusa. - Ofertantul va prezenta copia Certificatului ISO 27001:2013 şi Certificatului ISO 9001:2015 - certificat confirmat cu aplicarea semnăturii electronice. - Referinte de implementare in Republica Moldova in cadrul institutiilor de stat – minim 3 referinte. **Termenii și condițiIe de livrare/prestare/executare solicitat:** 10 zile lucrătoare de la data întrării in vigoare a contrcatului, care va inlcude și timpul lucrărilor de instalare, configurare și punerea în funcțiune. **<u>În cazul în care se va oferi o soluție alternativă decît cea existentă</u>, acesta trebuie să întrunească minim cerințele de mai jos, care este echivalentul soluției instalate deja în cadrul instituției:** **CONSOLA DE MANAGEMENT** **1. Cerințe generale:** 1.1. Consola de management și baza de date vor fi incluse fără a fi nevoie de softuri și licențe adiționale. 1.2. Interfața consolei de management va fi în limba engleză. 1.3. Interfața clientului de securitate, care se instalează pe stații și servere, va fi în limba română sau engleză. 1.4. Soluția va include un modul de update server prin care se asigura actualizarea de produs și a semnăturilor. 1.5. Notificări - Soluția trebuie să permită setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru următoarele acțiuni: blocat, redenumit, oprit, șters, plasat, raportat, dezinfectat, în carantină, raportat către utilizator, blocat și acțiune suplimentară solicitată de la utilizator, mutat în coșul de gunoi și ulterior expediata către o cutie poștală sau mai multe. 1.6. Soluția va permite integrarea cu un server Syslog ori SIEM pentru raportarea evenimentelor. 1.7. Soluția permite crearea unei copii de siguranța a profilului de configurație. **2. Panou de monitorizare și raportare (Dashboard):**

		2.1. Rapoartele vor putea fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport. 2.2. Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. **3. Inventarierea rețelei - managementul securității:** 3.1. Se permite descoperirea mașinilor din Microsoft Hyper-V. 3.2. Se permite descoperirea stațiilor fără protecție în Active Directory. 3.3. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare și adresa IP. 3.4. Soluția va permite instalarea la distanță sau manual a clienților anti-malware pe mașini fizice/virtuale. 3.5. Soluția va permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale. 3.6. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalare de la distanță pentru endpoint-uri. 3.7. Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanță. 3.8. Soluția va oferi informații detaliate despre fiecare task și va afișa dacă task-ul s-a finalizat cu succes sau nu. 3.9. Soluția va permite configurarea centralizată a clienților anti-malware prin intermediul politicilor. 3.10. Se vor oferi în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizări, Versiunea produsului, Versiunea de semnături. 3.11. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea. **4. Politici:** 4.1. Soluția va permite configurarea setărilor clientului anti-malware prin intermediul politicilor ce conțin setări pentru toate modulele. 4.2. Politica va conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea anti-malware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user. **5. Rapoarte:** 5.1. Soluția va conține rapoarte care prezintă starea endpoint-urilor din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.

		5.2. Soluția va permite vizualizarea rapoartelor curente programate de administrator. 5.3. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. 5.4. Interogarea legata de starea terminalului include informații precum: 5.4.1. tip endpoint; 5.4.2. infrastructura rețelei căreia ii aparține endpointul; 5.4.3. datele agentului de securitate; 5.4.4. starea modulelor de protecție; 5.5. Interogarea legata de evenimente endpoint include informații precum: 5.5.1. endpoint-ul pe care a avut loc evenimentul; 5.5.2. tipul starea și configurația agentului de securitate instalat; 5.5.3. starea modulelor și rolurilor de protecție instalate pe agentul de securitate; 5.5.4. denumirea și alocarea politicii; 5.5.5. utilizatorul autentificat în timpul evenimentului; 5.5.6. evenimente (site-uri blocate, aplicații blocate, detecțiile etc); 5.5.7. Soluția trebuie să permită generarea de rapoarte grafice detaliate, cu posibilitate de export în format (docx, xml, xlsx), inclusiv cu remitere către adrese de email specificate. Posibilitatea de a configura o frecvență pentru crearea rapoartelor după (zi, săptămâna, luna, ora), rapoartele trebuie să cuprindă minim informație despre: 5.5.7.1. Vulnerabilitățile descoperite clasificate după severitate: informativ, severitate minimă, severitate medie, si severitate înalta; 5.5.7.2. Notarea severității vulnerabilităților se va face pe o notă de la 1 la 10; 5.5.7.3. Raportul va afișa descrierea pentru fiecare vulnerabilitate in parte cu unele referințe; 5.5.7.4. Recomandările propuse pentru remedierea vulnerabilității depistate; 5.5.7.5. Crearea unei statistici grafice in dependență de vulnerabilitățile depistate; 5.5.7.6. Top vulnerabilități depistate. 5.5.8. Soluția trebuie să permită crearea unor widgeturi care pot fi editate, donate sau șterse cu afișarea lor pe pagină in mod dinamic. La fel, widgeturi de bord pot fi create in forma minim de: tabel, diagramă circulară (plăcintă), histogramă, etc. 5.5.9. Tablourile de bord trebuie să conțină informații ca: vulnerabilitățile depistate care vor fi grupate după severitate/data/luna/cantitatea depistată. Cele mai grave vulnerabilități. Scanările active, scanările care sunt planificate, ultimele dispozitive scanate. 5.5.10. Soluția trebuie să permită setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru minim următoarele acțiuni: când pornește un proces de scanare, finalizarea procesului de scanare, la crearea si asignarea unui task către un utilizator existent. **6. Carantină:**

		6.1. Soluția va permite restaurarea fișierelor din carantină în locația originala. 6.2. Carantină va fi locala, pe fiecare stație administrată și va fi administrată, fie local, fie din consola de management. **7. Utilizatori:** 7.1. Administrarea se va putea face pe baza de roluri predefinite (Administrator, Auditor) sau roluri personalizate. 7.2. Administrator companie: administrează arhitectura consolei de management și serviciile de securitate; 7.3. Auditor: monitorizează și generează rapoarte. 7.4. Utilizatorii pot fi creați în consola de management. 7.5. Se va permite configurarea detaliata a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. **8. Log-uri:** 8.1. înregistrarea acțiunilor utilizatorilor. 8.2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator. 8.3. Se va permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. **9. Actualizare:** 9.1. Se permite definirea de locații de actualizare multiple. 9.2. Se permite activarea/dezactivarea actualizărilor de produs și semnături. 9.3. Se permite actualizarea produsului într-o rețea fără acces la Internet. 9.4. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus 9.5. Soluția dispune de un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat din Cloud, fără intervenția administratorului. Astfel, administratorul va putea descarcă pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, poate descarcă pachetele pentru modul de scanare centralizata în mediile de virtualizare Hyper-V. 9.6. In cadrul serverului de actualizare, pentru o mai buna urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de scanare centralizată, se va putea vizualiza un jurnal de modificări în care sunt precizate istoric: 9.6.1. versiunea pachetului; 9.6.2. data versiunii; 9.6.3. funcții noi și îmbunătățiri; 9.6.4. probleme rezolvate;

		9.6.5. probleme cunoscute. 9.7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului anti-malware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizări de produs: 9.8. Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei 9.9. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc) 9.10. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management. 9.11. Soluția oferă posibilitatea de actualizare a aplicațiilor învechite instalate pe stațiile de lucru. **10. Certificate:** 10.1. Accesul la consola de management să se facă doar prin HTTPS. 10.2. Soluția permite afișarea în consola de management informații despre certificate: nume, autoritatea emitenta, data eliberării și data expirării certificatelor eliberate. **PROTECȚIE STAȚII ȘI SERVERE FIZICE/VIRTUALE** **11. Caracteristici generale:** 11.1. Pentru reducerea la minim a consumului de resurse, soluția anti-malware trebuie să permită instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției anti- malware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall). 11.2. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigură protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare. 11.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Anti-malware. 11.4. Pentru o mai bună protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționale). **12. Cerințe de sistem:** 12.1. Sisteme de operare pentru stații de lucru pe 32/64 biți: Windows 11, Windows 10. 12.2. Sisteme de operare pentru servere: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012.

		12.3. Terminale Servere: Microsoft Windows Terminal/RDP Services. 12.4. Sisteme de operare linux pe baza distribuțiilor pe 64 de biți (AMD64/EM64T): ▪ AlmaLinux 8, 9 ▪ Amazon Linux 2 ▪ CentOS 7 (7.3 or newer) ▪ CentOS Stream 8 ▪ Debian 10, 11, 12 ▪ Oracle Linux 7 (7.3 or newer), 8, 9 ▪ RHEL 7 (7.3 or newer), 8, 9 ▪ Rocky Linux 8, 9 ▪ SUSE Linux Enterprise Server 12 (Service Pack 5) ▪ SUSE Linux Enterprise Server 15 (Service Pack 2 or newer) ▪ Ubuntu 18.04, 20.04, 22.04, 24.04 12.5 Sisteme de operare Security-Enhanced Linux cu urmatoarele distribuții: ▪ AlmaLinux 8, 9; ▪ CentOS 7 ; ▪ CentOS Stream 8; ▪ Debian 10, 11, 12; ▪ Oracle Linux 7, 8, 9; ▪ RHEL 7, 8, 9; ▪ Rocky Linux 8, 9. 12.6 Sisteme de operare macOS: ▪ macOS 15 "Sequoia"; ▪ macOS 14 "Sonoma"; ▪ macOS 13 "Ventura". **13. Administrare și instalare de la distanță:** 13.1. Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, browsing protection, device control, software update, application control, network location settings, automated tasks, dataguard (sandbox). 13.2. Instalarea se va putea face în mai multe moduri: 13.2.1. prin descărcarea directa a pachetului pe stația pe care se va face instalarea; 13.2.2. prin instalarea la distanta, direct din consola de management. 13.3. Instalarea clienților la distanta în alte locații decât cele în care este instalata consola de management pentru a minimiza traficul în WAN. 13.4. In consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc. 13.5. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe stații/servere.

		13.6. Consola va include o secțiune, „Audit”, unde se vor menționa toate acțiunile întreprinse in politica de securitate cu informații detaliate: logare, editare, creare etc. **14. Caracteristici și funcționalități principale ale modulului anti-malware:** 14.1. Soluția permite administratorului să stabilească acțiunea luata de produsul Anti-malware la detectarea unei amenințări noi. Astfel administratorul va putea alege intre următoarele acțiuni: 14.1.1. Acțiune implicită pentru fișiere infectate: 14.1.1.1. interzice accesul; 14.1.1.2. dezinfectează; 14.1.1.3. ștergere; 14.1.1.4. muta fișierele în carantină; 14.1.1.5. nicio acțiune; 14.1.2. Acțiune alternativa pentru fișierele infectate: 14.1.2.1. interzice accesul; 14.1.2.2. dezinfectează; 14.1.2.3. ștergere; 14.1.2.4. muta fișierele în carantină. 14.1.3. Acțiune implicită pentru fișierele suspecte: 14.1.3.1. interzice accesul; 14.1.3.2. ștergere; 14.1.3.3. muta fișierele în carantină; 14.1.3.4. nicio acțiune; 14.1.4. Acțiune alternativa pentru fișierele suspecte: 14.1.4.1. interzice accesul; 14.1.4.2. ștergere; 14.1.4.3. muta fișierele în carantină. 14.2. Scanarea automată în timp real va putea fi setata să nu scaneze arhive. 14.3. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansată încă. 14.4. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). 14.5. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP. 14.6. Configurarea cailor ce urmează a fi scanate la cerere. 14.7. Clienții anti-malware pentru stațiile de lucru să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese. 14.8. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware.

		14.9. Posibilitatea de configura scanările programate să se execute cu prioritate redusă. 14.10. Pentru o protecție sporită, soluția anti-malware trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazata pe monitorizarea proceselor. 14.11. Pentru o protecție sporită, soluția anti-malware trebuie să poată scana paginile HTTP. 14.12. Pentru o mai buna gestionare a anti-malware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecția la dezinstalare. 14.13. Pentru siguranța utilizatorului, clientul va include un modul de anti-phishing. 14.14. Soluția oferă protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. 14.15. Soluția trebuie să permită instalarea serverelor de scanare externalizată în locația organizației, configurarea clienților pentru utilizarea acestora fără instalarea bazelor de date locale, trimiterea fișierelor necunoscute către serverele de scanare externalizată definite, optimizarea resurselor prin economisirea lățimii de bandă, procesării CPU și I/O-ului pe hard disk la nivelul endpoint-urilor, fără a afecta semnificativ performanța scanării fișierelor necunoscute, și să includă documentație detaliată privind funcționalitatea și implementarea. **15. Firewall:** 15.1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 15.2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 15.3. Posibilitatea de a defini rețele de încredere pentru mașina destinație. **16. Carantină:** 16.1. Produsul anti-malware să permită trimiterea automată a fișierelor din carantină către laboratoarele anti-malware ale producătorului. 16.2. Trimiterea conținutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator. 16.3. Produsul anti-malware să permită ștergerea automată a fișierelor din carantină mai vechi de o anumita perioadă, pentru a nu încărca inutil spațiul de stocare. 16.4. Posibilitatea de a restaura un fișier din carantină în locația lui originala. 16.5. Modulul de carantină va permite re-scanarea obiectelor după fiecare actualizare de semnături. 16.6. Produsul va oferi rollback pentru utilizatori la protecție împotriva ransomware-ului care va permite restabilirea fișierelor și a registrului la o stare anterioară înainte de infectarea cu ransomware. **17. Protecția datelor:**

		17.1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. **18. Controlul conținutului:** 18.1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu următoarele particularități: 18.1.1. Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini. 18.1.2. Permite controlul accesului numai la anumite pagini de Internet specificate de administrator; 18.1.3. Permite blocarea accesului la anumite aplicații definite de administrator; 18.1.4. Permite restricționarea accesului pe anumite pagini de Internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). **19. Controlul aplicațiilor:** 19.1. Pentru prevenirea infectării stațiilor și serverelor dar și pentru a permite aplicațiilor descoperite în rețea să se poată actualiza, soluția permite definirea unor programe de actualizare (Updater) care vor fi lăsate să actualizeze diferite aplicații instalate pe stații sau servere. 19.2. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv sub procese) după: 19.2.1. Target path; 19.2.2. Target SHA 1; 19.2.3. Target SHA256; 19.2.4. Target file size; 19.2.5. Target signer name; 19.2.6. Target certificate hash; 19.2.7. Target has trusted signature; 19.2.8. Parent path; 19.2.9. Parent signer name; 19.2.10. Parent certificate hash; 19.2.11. Parent has trusted signature. **20. Controlul dispozitivelor:** 20.1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 20.2. Modulul va permite controlul următoarelor tipuri de dispozitive: 20.2.1. USB Mass Storage Device;

		20.2.2. Wireless devices; 20.2.3. DVD/SC-ROM drivers; 20.2.4. Windows CE ActiveSync devices; 20.2.5. Floppy drivers; 20.2.6. Modems; 20.2.7. COM & LTP ports; 20.2.8. Printers; 20.2.9. Smart Card Readers; 20.2.10. Imaging Device (cameras and scanners) 20.2.11. IEEE 1394 Host Bus Controllers 20.2.12. IrDA Devices 20.2.13. Bluetooth Devices 20.3. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client. 20.4. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s- au configurat reguli. 20.5. Modulul va permite/bloca accesul pentru înscriere si rularea executabil. **21. Actualizare:** 21.1. Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare). **22. Scanarea vulnerabilităților infrastructurii:** 22.1. Soluția trebuie sa asigure scanarea vulnerabilităților infrastructurii (echipamente din rețea, aplicațiilor web, etc) cu posibilitatea de a fi accesată dintr-o singură interfață. 22.2. Soluția trebuie să fie capabilă să identifice atât amenințările interne cât și externe și să raporteze riscurile, să ofere o vizibilitate a vulnerabilităților într-un mod centralizat pentru toate tipurile de dispozitive conectate în rețea și care pot comunica, de exemplu: stații de lucru, servere, servere virtuale, site-uri, switch-uri, routere, aplicațiilor web, etc; 22.3. Soluția va oferi posibilitatea de a identifica toate echipamentele conectate la rețea, la fel va fi posibil de a verifica tipul de echipament, după caz: sistemul de operare instalat, IP-ul si MAC adresa, cărui domeniu aparține, vulnerabilitățile depistate, software-ul instalat pe echipament, spațiul disponibil, tipul procesorului, tipul Bios-ului. 22.4. Soluția va permite planificarea activităților după data/ora/an și de rulat scanarea vulnerabilităților pentru fiecare echipament in parte. 22.5. Soluția va pune la dispoziție un instrument care poate fi instalat pe o mașină virtuală sau pe un calculator in rețeaua pe care se dorește o scanare al vulnerabilităților sau pentru colectarea datelor echipamentelor aflate in rețea. 22.6. Soluția trebuie sa permită adăugarea unui grup de scanare in care se va indica minim: Numele grupului si persoana responsabilă, descrierea succintă a grupului.

		22.7. Posibilitatea de scanare prin alegerea unui șablon prestabilit care va propune scanarea sistemului după modelele: 22.7.1. Badlock detection; 22.7.2. Bash Shellshock detection; 22.7.3. GHOST detection; 22.7.4. Hearbeast detection; 22.7.5. PCI scan; 22.7.6. Scan full TCP/UDP port range; 22.7.7. Scan top-100 ports; 22.7.8. Scan top-1000 ports; 22.7.9. SSL/TLS maturity scanning; 22.8. Modul de scanare să poată fi setat după: oră, repetări zilnice, săptămânale, lunare, trimestriale, etc. 22.9. Soluția trebuie să fie administrată printr-o singură consolă, fără ca să necesite careva echipamente hardware (servere de management) sau careva software speciale. 22.10. Soluția propusă trebuie genereze un raport pe segmente din rețea pe care se dorește, cu posibilitatea selectării vulnerabilităților care vor fi afișate în raport, sortate după severitatea lor. 22.11. Soluția propusă trebuie să pună la dispoziție posibilitatea de a asigna remedierea unei vulnerabilități către un user / administrator creat in platforma de administrare. 22.12. Consola de administrare trebuie să suporte următoarele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome. 22.13. Soluția va putea afișa toată informația referitor la licența instalată și va jumaliza evenimentele și modificările aplicate de către user-ul care are accesul la portal. 22.14. In consola de administrare trebuie sa se regăsească accesul la manuale, ghiduri de instalare, ghidul de utilizare, etc, informații referitor la schimbările si actualizările soluției, portal pentru suport cu posibilitatea de a solicita ajutor de la producător. 22.15. Soluția trebuie să ofere scanări nelimitate pe parcursul perioadei de licență. **CERINȚE FAȚĂ DE SERVICIILE DE IMPLEMENTARE și CONFIGURARE** **23. Caracteristici generale:** 23.1. Ofertantul selectat va livra și instala licențele pentru soluția ofertată. 23.2. Ofertantul selectat va efectua pregătirea mediului de instalare pentru soluția propusă, după care va asigura implementarea inițială a soluției aplicative în mediul de producție și mediul de testare. 23.3. Ofertantul selectat va efectua configurarea inițială a soluției, atât pentru mediul de producție, cât și mediul de testare. Prin configurare inițială se înțelege setarea tuturor parametrilor aplicabili în corespundere cu cerințele (clientului), inclusiv configurarea și instalarea soluției ofertate, setarea politicilor și testarea înainte de a fi pusa în producție.

		23.4. în baza rezultatelor de la etapa de design. Ofertantul selectat va implementa toate configurările / customizările agreate și darea în exploatare a soluției. 23.5. Ofertantul selectat va efectua instalarea soluției ofertate în întreaga infrastructură a Comisiei Naționale a Pieței Financiare, inclusiv la toți utilizatorii finali (instalarea se va considera încheiată în momentul când toți utilizatorii vor avea instalat agentul și calculatorul va primi cel puțin o actualizare a bazelor și a agentului). 23.6. La sfârșitul etapei. Ofertantul va face o demonstrație a soluției și a modulelor care au fost acoperite, fapt care va servi drept unul din criteriile de acceptanță ale etapei de implementare. 23.7. După acceptanța finală a soluției, va fi activată în mod automat opțiunea de garanție post- implementare și suport. Perioada de garanție post-implementare și suport va fi de 1 an calendaristic de la data activării acestei opțiuni. 23.8. Serviciile de garanție post-implementare și suport se referă la serviciile oferite de către Ofertantul selectat adițional la serviciile de mentenanță și suport a licențelor, oferite direct de către producătorul licențelor. 23.9. Serviciile de garanție post-implementare și suport, vor include următoarele componente: 23.9.1. Gestionarea serviciului de actualizare a serverelor la ultimele actualizări oferite de producător; 23.9.2. Gestionarea incidentelor de securitate apărute pe perioada suportului activ; 23.9.4. Solicitări de analiza și corecție a politicilor de securitate în cadrul companiei implementate. **24. Cerințele față de serviciile de instruire** 24.1. În cadrul proiectului, Ofertantul va organiza sesiuni de instruire și transfer de cunoștințe pentru grupurile țintă în vederea formării setului de cunoștințe necesar pentru a permite echipei instruite să preia menținerea și configurarea ulterioară a soluției, în conformitate cu necesitățile utilizatorilor. 24.2. Instruirea se va organiza pentru diferite grupuri țintă la sediul Cumpărătorului. 24.3. Administrator - 3 persoane. 24.4. în acest sens, Ofertantul va prezenta ca parte a ofertei, un plan de instruire, în care se va indica ce tipuri de instruiri va efectua Ofertantul, pentru ce categorie de utilizatori, precum și cuprinsul/agenda acestor instruiri. 24.5. în afara instruirilor ce țin de utilizarea soluției, Ofertantul trebuie să efectueze și sesiuni de instruire pentru echipa de mentenanță din partea Cumpărătorului, în scopul asigurării unui nivel adecvat de cunoștințe și competențe, pentru a putea utiliza eficient instrumentele de configurare și dezvoltare disponibile în cadrul soluției.

		24.6. în cadrul serviciilor de implementare, pentru a asigura transferul necesar de cunoștințe către echipa Cumpărătorului, Ofertantul va fi de acord ca cel puțin o persoană să asiste la lucrările de parametrizare/configurare, stabilite de comun acord de către Părți. 24.7. Ofertantul selectat la etapa de încheiere a contractului, va trebui să elaboreze și să convină cu Cumpărătorul următoarele elemente ale componentei de instruire: 24.7.1. Strategia Ofertantului cu privire la instruire și programul de formare; 24.7.2. Structura și componența pachetului de cursuri pentru formare și a manualelor de studiu pentru fiecare categorie de utilizator; 24.7.3. Metodologia și procedurile de evaluare și control al eficienței și suficienței sesiunilor de instruire. 24.8. în cadrul sesiunilor de instruire, Ofertantul va pune la dispoziția Cumpărătorului întreg setul de documentație al soluției care să cuprindă cel puțin următoarele componente: 24.8.1. Ghidurile administratorilor; 24.8.2. Ghidurile de instalare și configurare; 24.8.3. Fișierele surse pentru toate configurările și customizările realizate pe parcursul proiectului. **25. Licențe:** 25.1. 80 endpoints (fizice si virtualizate), 12 luni subscripție; 25.2. 40 servers (fizice si virtualizate). 12 luni subscripție; 25.3. 40 IP unice (interne, externe, web), 12 luni subscripție.

Remarcă:

Având în vedere conjunctura actuală, ce ține de securitatea statului, precum și necesitatea de a asigura compatibilitatea sistemului antivirus cu celelalte sisteme IT, utilizate de către CNPF și de către alte autorități publice, nu pot fi acceptate soluții Antivirus, elaborate în Federația Rusă sau de elaboratori originari din Federația Rusă.