Specificaţii tehnice (F4.1)

[Acest tabel va fi completat de către ofertant în coloanele 3, 4, 5, 7, iar de către autoritatea contractantă – în coloanele 2, 6, 8]

Numărul procedurii de achiziţie: **ocds-b3wdp1-MD-1594630180808 din 13 iulie 2020.**
Denumirea procedurii de achiziţie: Server pentru infrastructura de virtualizare si servicii de instalare, Soluție Antivirus si soluție de scanare vulnerabilităților, Microsoft Windows Server, Reinoirea licentei pentru firewall WatchGuard.

Nr. d/o	Cod CPV	Denumirea bunurilor	Modelul articolului	Ţara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
	1	2	3	4	5	6	7	8
		Lotul 1						
1.1	48820000-2	**Server**	**Dell EMC PowerEdge R740**	**SUA - CHINA**	**Dell Technologies Inc.**	***Cerinţe generale:*** Bunurile oferite in cadrul achiziției trebuie sa fie noi, calitative, produse de producători renumiți, bine cunoscuți internațional in domeniul TI. Configurația echipamentului trebuie sa fie compusă din componente reciproc compatibile și sa asigure funcționarea optimă a bunului in ansamblu. Produsul ofertat va trebui sa poată fi extins prin achiziția ulterioara a unui sistem de tip back-up, replicare si disaster revocovery de la același vendor pentru a exista o integrare nativa a soluției. Produsele ofertate trebuie sa se regăsească in Gartner, cadranul de lideri. Tip: Server de virtualizare pentru aplicații va avea următoarele caracteristici minime:	***Produsul Ofertat:*** **Dell EMC PowerEdge R740** Bunurile oferite în cadrul achiziției sunt noi, calitative, produse de Dell Technologies Inc., care sunt bine cunoscuți internațional în domeniul TI. Configurația echipamentului este compusa din componente reciproc compatibile și va asigura funcționarea optimă a bunului în ansamblu. Produsul ofertat va putea fi extins prin achiziția ulterioară a unui sistem de tip back-up, replicare și DISASTER RECOVERY de la același vendor pentru a exista o integrare nativă a soluției. Producatorul se regăseste în Gartner, cadranul de lideri. Tip: Server de virtualizare pentru aplicații cu următoarele caracteristici:	-

Digitally signed by Vicol Irina
Date: 2020.07.20 16:16:05 EEST
Reason: MoldSign Signature
Location: Moldova

						- Chassis: Rack mount 2U, up to 8 x 3.5" SAS/SATA Hard Drives for 2CPU Configuration; - Processor: 2 x 8 Core processor, equivalent Intel Xeon Silver 4208 2.1G, 8C/16T, 9.6GT/s, 11M Cache, Turbo, HT (85W) DDR4-2400; - Riser Config 1, 4 x 8 slots - Memory: 6x16GB RDIMM, 2933MT/s, Dual Rank; - RAID controller: min 2GB NV Cache, Write Back Cache: Flash Backed Cache. - RAID levels 0, 1, 5, 6 - RAID spans 10, 50, 60 - Online Capacity Expansion (OCE) - Online RAID Level Migration (RLM) - Auto resume after power loss during array rebuild or reconstruction/RLM - Consistency Check for background data integrity - Physical disk power management - NVRAM “Wipe” feature protects proprietary data once card is decommissioned - SED drive support - Load balancing - Fast initialization for quick array setup - Configurable stripe size up to 1MB - Patrol read for media scanning and repair - DDF compliant - Configuration on Disk (COD) - S.M.A.R.T. support - Global and dedicated hot spare with revertible hot-spare support, automatic rebuild, enclosure affinity, and emergency SATA;	- Chassis: Rack mount 2U, up to 8 x 3.5" SAS/SATA Hard Drives for 2CPU Configuration; - Processor: 2 x Intel Xeon Silver 4208 2.1G, 8C/16T, 9.6GT/s, 11M Cache, Turbo, HT (85W) DDR4-2400; - Riser Config 1, 4 x 8 slots -Memory: 6x16GB RDIMM, 2933MT/s, Dual Rank; - RAID controller: PERC H730P, 2GB NV Cache, Adapter, Write Back Cache: Flash Backed Cache. Datasheet atasat la oferta. - RAID levels 0, 1, 5, 6 - RAID spans 10, 50, 60 - Online Capacity Expansion (OCE) - Online RAID Level Migration (RLM) - Auto resume after power loss during array rebuild or reconstruction/RLM - Consistency Check for background data integrity - Physical disk power management - NVRAM “Wipe” feature protects proprietary data once card is decommissioned - SED drive support - Load balancing - Fast initialization for quick array setup - Configurable stripe size up to 1MB - Patrol read for media scanning and repair - DDF compliant - Configuration on Disk (COD) - S.M.A.R.T. support - Global and dedicated hot spare with revertible hot-spare support, automatic rebuild, enclosure affinity, and emergency SATA;	

						- Hard drives: • 4 x 4TB 7.2K RPM NLSAS 12Gbps 512n 3.5in Hot-plug Hard Drive, - Cooling system: High performance fan; - Power supply: Dual, Hot-plug, Redundant Power Supply (1+1), max 750W; - Network interfaces: • 4 x 1 Gbit Ethernet NIC ports; • 2 x 10 Gbit SFP+ NIC ports; - Ports: • Front ports: 1xVGA, 2 x USB 2.0, 1x USB 3.0, dedicated management port • Rear ports: 1xVGA, 1x Serial, 2 x USB 3.0, dedicated management network port - Diagnostic LEDs: On front panel, installed WiFi and Bluetooth module for connecting and diagnosing from mobile devices; - Server management (SM): • Must deliver advanced, agent-free local and remote server administration; • Local and remote control of system resources (manage, diagnose and monitor); • Remote power control, remote firmware updating, remote presence; • Support management interfaces IPMI2.0, WEB, WSMAN, SNMP, SSH;	Hard drives: • 4 x 4TB 7.2K RPM NLSAS 12Gbps 512n 3.5in Hot-plug Hard Drive, - Cooling system: High performance fan; - Power supply: Dual, Hot-plug, Redundant Power Supply (1+1), 750W; - Network interfaces: • Corespunde, cu 1 x Broadcom 5720 **Quad Port** 1GbE BASE-T, rNDC• 2 x 10 Gbit SFP+ NIC ports; • Corespunde, Broadcom 57412 **Dual Port** 10GbE SFP+ Adapter, PCIe Full Height - Ports: Corespunde cerintelor, data sheet cu specificatia tehnica atasata la oferta. - Diagnostic LEDs: On front panel, installed WiFi and Bluetooth module for connecting and diagnosing from mobile devices. Este inclus in configuratie iDRAC9 Enterprise si Quick Sync 2 wireless module; - Pentru Server management (SM) este inclus in configuratie iDRAC9 Enterprise care acopera toate cerintele: • Must deliver advanced, agent-free local and remote server administration; • Local and remote control of system resources (manage, diagnose and monitor); • Remote power control, remote firmware updating, remote presence; • Support management interfaces IPMI2.0, WEB, WSMAN, SNMP, SSH;	

						• LDAP user authentication, Active Directory; • "ZeroTouch deployment and provisioning" automated deployment; • Support protocols IPv4, IPv6, DNS, DDNS, DHCP; • Support of Single Sign-on and 2FA; • Notifications for alerts SNMP, Email, IPMI. • Browser based administration with, full control over the remote host server's display; keyboard, and mouse, including host OS graphical interface; • Virtual media option that provides virtual CD drive and remote image mounting; • SM & server diagnostics logging; - Rack mounting rails: ReadyRails Sliding Rails with Cable Management Arm; - Operating Systems Supported: Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server with Hyper-V, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi. - Certificates: EU Declaration of Conformity, Regulatory and Environmental compliance; - Power Efficiency: Energy Star certified; Notă: Garanția echipamentului minim 36 de luni pentru toate componentele hardware. Ofertantul trebuie sa prezinte autorizație de livrare de la producător (Manufacturer's Authorization Form).	• LDAP user authentication, Active Directory; • "ZeroTouch deployment and provisioning" automated deployment; • Support protocols IPv4, IPv6, DNS, DDNS, DHCP; • Support of Single Sign-on and 2FA; • Notifications for alerts SNMP, Email, IPMI. • Browser based administration with, full control over the remote host server's display; keyboard, and mouse, including host OS graphical interface; • Virtual media option that provides virtual CD drive and remote image mounting; • SM & server diagnostics logging; - Rack mounting rails: ReadyRails Sliding Rails with Cable Management Arm; - Operating Systems Supported: Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server with Hyper-V, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi. - Certificates: EU Declaration of Conformity, Regulatory and Environmental compliance sunt atasate cu oferta; - Power Efficiency: Energy Star certified, corespunde este mentionat in certificatul atasat; Garantia : 36 luni. MAF de la producator este atasat cu oferta.	
1.2	72000 000-5	Servicii IT: virtualizare	**Servicii IT: virtualizare**	**-**	**-**	Ofertantul va oferi servicii instalare si configurare precum: virtualizarea	Xontech Systems va acoperi toate cerintele solicitate. Certificatele	

		server consultanță, instalare/configurare software.	**server consultanță, instalare/configurare software.**			serverului pentru rularea corectă a următoarelor sisteme informaționale : • BitDefender Gravity Zone Enterprise Security; • Active Directory; • File Server; • Web Filtering pe grup de utilizatori pentru Firewall existent de model Watchguard și crearea politicilor de grup si utilizatori. Adițional, ofertantul va oferi servicii de instalare configurare si suport tehnic pentru: • Instalarea si configurarea BitDefender Enterprise Security – pentru 230 de PC-uri. • Configurarea AD - pentru cca 170 de utilizatori cu adăugarea stațiilor in Domain și migrarea informației existente. • Crearea politicilor si drepturilor de acces. • Realizarea unui raport cu lucrările efectuate in care se vor regăsi lucrările descrise mai sus; Notă: Ofertatul va oferi servicii de training administratorilor IT din cadrul instituției pentru exploatarea corecta a a tuturor serviciilor descrise mai sus Ofertantul va prezenta copia Certificatului ISO 27001:2013 şi Certificatului ISO 9001:2015 - confirmat cu aplicarea semnăturii electronice; Pentru asigurarea calității serviciilor solicitate de mai sus ofertantul va prezenta minim o persoana certificata (angajat al ofertantului) in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013; si ITIL Foundation.	solicitate de catre partea contractanta. Copiile Certificatelor solicitate sunt atasate cu oferta.	

		Lotul 2						
2.1	48761000-0	Antivirus software	**F-Secure PSB Managed Company Server Protection Premium Suite for 4 devices, 3 years**	**Finlanda**	**F-Secure Corporation**	Soluția trebuie sa asigure protecție pentru servere fizice si virtuale pentru 4 unit., cu suport inclus pe o perioada de 3 ani pentru următoarele sisteme de operare: • Microsoft® Windows Server 2008 R2; 2012; 2012 Essentials; 2012 R2; 2012 R2 Essentials; 2012 R2 Foundation; 2016 Standard; 2016 Essentials; 2016 Datacenter; 2016 Core; 2019 Standard; 2019 Essentials; 2019 Datacenter; 2019 Core; CentOS, Debian, Oracle Linux, RHCK and UEK, RHEL, SUSE Linux Enterprise Server 11 SP3, SP4, Ubuntu, etc. • soluția ofertată trebuie să fie una bazată pe tehnologia Cloud, care să ofere un management centralizat a tuturor dispozitivelor: stații de lucru, servere și dispozitive mobile; • soluția trebuie sa asigure protecție in timp real, impotriva virusilor (ransomware – crypto) cu scopul prevenirii distrugerii și modificării datelor, amenintarilor spyware, rootkit-urilor, tentativelor de intruziune, spam-urilor si a altor mesaje nedorite. • soluția trebuie să ofere actualizari automate a versiunilor noi si a hotfix-urilor; • soluția trebuie să ofere protectie impotriva virusilor si noilor amenintari necunoscute care să fie bazată pe analize euristice, de comportament și reputație; • soluția trebuie să includă patch management cu opțiuni pentru excluderi și actualizări manuale si analiza vulnerabilitatilor din retea; • soluția trebuie să ofere funcționalități de firewall, intrusion prevention si application control;	Soluția va asigura protecție pentru servere fizice si virtuale pentru 4 unit., cu suport inclus pe o perioada de 3 ani pentru următoarele sisteme de operare: • Microsoft® Windows Server 2008 R2; 2012; 2012 Essentials; 2012 R2; 2012 R2 Essentials; 2012 R2 Foundation; 2016 Standard; 2016 Essentials; 2016 Datacenter; 2016 Core; 2019 Standard; 2019 Essentials; 2019 Datacenter; 2019 Core; CentOS, Debian, Oracle Linux, RHCK and UEK, RHEL, SUSE Linux Enterprise Server 11 SP3, SP4, Ubuntu, etc. • soluția este una bazată pe tehnologia Cloud, care oferă un management centralizat a tuturor dispozitivelor: stații de lucru, servere și dispozitive mobile; • soluția asigură protecție in timp real, impotriva virusilor (ransomware – crypto) cu scopul prevenirii distrugerii și modificării datelor, amenintarilor spyware, rootkit-urilor, tentativelor de intruziune, spam-urilor si a altor mesaje nedorite. • soluția oferă actualizari automate a versiunilor noi si a hotfix-urilor; • soluția oferă protectie impotriva virusilor si noilor amenintari necunoscute care să fie bazată pe analize euristice, de comportament și reputație; • soluția include patch management cu opțiuni pentru excluderi și actualizări manuale si analiza vulnerabilitatilor din retea; • soluția oferă funcționalități de firewall, intrusion prevention si application control;	

						• soluția trebuie să asigure criptarea automată prin VPN, a întregului trafic realizat dintre dispozitivele mobile, permițând utilizarea în condiții de siguranță a Wi-Fi public și rețelelor mobile; • soluția trebuie să ofere posibilități exacte de activare si dezactivare, de configurare a funcționalităților precum: scanarea antivirus la cerere, firewall gestionat, controlul accesului la Internet, controlul aplicațiilor care să blocheze executarea aplicațiilor și scripturilor conform regulilor create sau definite de administrator., scanarea traficului web, controlul dispozitivelor; • soluția trebuie să ofere posibilitatea de aplicare a politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale sau utilizatori de AD; • soluția trebuie să ofere instalare centralizată; • soluția trebuie să ofere consolă unică de management cu instalare in cloud; • soluția trebuie să ofere functional Multi-engine anti-malware; • soluția trebuie să includă funcționalul de Patch Management, pentru a asigura actualizarea de software atît de la produsele Microsoft, cît și pentru alte aplicaţii de la terţi; • soluția trebuie să ofere funcțional de Firewall ce va permite setarea unor reguli bazate pe actiuni (blocarea sau permiterea) și direcție(intrare sau iesire) pentru controlul și monitorizarea traficului la nivel de endpoint și rețea, care sa furnizeze un nivel de securitate suplimentar, aflat deasupra regulilor utilizatorului pentru Windows Firewall și a altor reguli pentru domenii.	• soluția asigură criptarea automată prin VPN, a întregului trafic realizat dintre dispozitivele mobile, permițând utilizarea în condiții de siguranță a Wi-Fi public și rețelelor mobile; • soluția oferă posibilități exacte de activare si dezactivare, de configurare a funcționalităților precum: scanarea antivirus la cerere, firewall gestionat, controlul accesului la Internet, controlul aplicațiilor care să blocheze executarea aplicațiilor și scripturilor conform regulilor create sau definite de administrator., scanarea traficului web, controlul dispozitivelor; • soluția oferă posibilitatea de aplicare a politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale sau utilizatori de AD; • soluția oferă instalare centralizată; • soluția oferă consolă unică de management cu instalare in cloud; • soluția oferă functional Multi-engine anti-malware; • soluția include funcționalul de Patch Management, pentru a asigura actualizarea de software atît de la produsele Microsoft, cît și pentru alte aplicaţii de la terţi; • soluția oferă funcțional de Firewall ce va permite setarea unor reguli bazate pe actiuni (blocarea sau permiterea) și direcție(intrare sau iesire) pentru controlul și monitorizarea traficului la nivel de endpoint și rețea, astfel furnizând un nivel de securitate suplimentar, aflat deasupra regulilor utilizatorului pentru Windows Firewall și a altor reguli pentru domenii.	

						• soluția trebuie să ofere funcțional de Protecție Web: protejarea accesarilor pe site-uri bancare (Control conexiune) care să alerteze utilizatorii atunci când aceştia au o conexiune securizată către site-uri de operaţiuni bancare online şi către alte site-uri precizate care tratează informaţii sensibile; blocarea site-urilor cunoscute ca fiind dăunătoare (Navigare bazată pe reputaţie); împiedicarea accesului la site-urile nepermise (Controlul conţinutului Web); blocarea accesului la tipurile de conţinut nepermise (Filtrare tipuri de conţinut).; • soluția trebuie să ofere funcțional de Controlul conexiunilor prin securizarea plăților online si afisarea unui pop-up care blocheaza celelalte pagini si imposibilitate accesarii altor decat cea in care se efectueaza tranzactia. • soluția trebuie să ofere funcțional de scanare în timp real a tuturor obiectelor pe care le accesează utilizatorii finali, pentru depistarea programelor de tip malware și inclusiv să ofere posibilitatea de configurare și efecuare a scanării manuale; • soluția trebuie să ofere funcțional de scanare a aplicatiilor in cloud; • soluția trebuie să ofere funcțional de Scanare a semnăturilor; • soluția trebuie să includă funcțional de control a dispozitivelor externe, să ofere posibilitatea: de a seta restricţii în privinţa modului în care utilizatorii pot accesa dispozitive USB, precum dispozitive de stocare, camere USB şi imprimante; de a interzcie accesul la orice dispozitiv de stocare USB; de a stopa rularea executabilelor stocate pe astfel de dispozitive; de a seta restricţii pe grupuri de dispozitive;	• soluția oferă funcțional de Protecție Web: protejarea accesărilor pe site-uri bancare (Control conexiune) care alertează utilizatorii atunci când aceştia au o conexiune securizată către site-uri de operaţiuni bancare online şi către alte site-uri precizate care tratează informaţii sensibile; blocarea site-urilor cunoscute ca fiind dăunătoare (Navigare bazată pe reputaţie); împiedicarea accesului la site-urile nepermise (Controlul conţinutului Web); blocarea accesului la tipurile de conţinut nepermise (Filtrare tipuri de conţinut).; • soluția oferă funcțional de Controlul conexiunilor prin securizarea plăților online si afisarea unui pop-up care blocheaza celelalte pagini si imposibilitate accesarii altor decat cea in care se efectueaza tranzactia. • soluția oferă funcțional de scanare în timp real a tuturor obiectelor pe care le accesează utilizatorii finali, pentru depistarea programelor de tip malware și inclusiv să ofere posibilitatea de configurare și efecuare a scanării manuale; • soluția oferă funcțional de scanare a aplicatiilor in cloud; • soluția oferă funcțional de Scanare a semnăturilor; • soluția include funcțional de control a dispozitivelor externe, oferă posibilitatea: de a seta restricţii în privinţa modului în care utilizatorii pot accesa dispozitive USB, precum dispozitive de stocare, camere USB şi imprimante; de a interzcie accesul la orice dispozitiv de stocare USB; de a stopa rularea executabilelor stocate pe astfel de dispozitive; de a seta restricţii pe grupuri de dispozitive;	

						• soluția trebuie să ofere funcțional de analiză euristică si zero day, de comportament și reputație; • soluția trebuie să ofere funcțional de Sandbox automatizat inclus – pentru analiza amănunțită prin detonarea fișierilor malițioase sau care nu pot fi protejate in baza de semnătura sau comportament; • soluția trebuie să ofere funcțional de control al aplicatiilor, prin setarea unor reguli de blocare create ca excluderi pentru a bloca un acces anume și să fie bazate: • pe actiuni precum permiterea, blocarea, sau permiterea și monitorizarea aplicațiilor; • pe evenimente precum pornire aplicație, încărcare modul, pornire program de instalare, acces la fișiere, pornire aplicație și încărcare modul; • prin stabilirea unor condiții care să poată fi selectate după atribute (cale destinație, nume fișier destinație, reputație destinație, versiune fișier destinație, cod hash pentru certificat la destinație.....etc), condiție și valoare, ce vor asigura activarea regulilor de excludere; soluția trebuie să ofere funcțional de Management API prin integrarea solutiilor terte precum: SIEM/RMM; 1.2. Cerintele tehnice vis-a-vis de administrarea solutiei: • administrarea soluției ofertate este necesara să se faca printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite creva echipamente hardware(servere de management) sau careva software special. • consola de administrare trebuie să fie capabilă de a funcționa pe orice dispozitiv și să conțină toate funționalitățile sus solicitate;	• soluția oferă funcțional de analiză euristică si zero day, de comportament și reputație; • soluția oferă funcțional de Sandbox automatizat inclus – pentru analiza amănunțită prin detonarea fișierilor malițioase sau care nu pot fi protejate in baza de semnătura sau comportament; • soluția oferă funcțional de control al aplicatiilor, prin setarea unor reguli de blocare create ca excluderi pentru a bloca un acces anume și este bazat: • pe actiuni precum permiterea, blocarea, sau permiterea și monitorizarea aplicațiilor; • pe evenimente precum pornire aplicație, încărcare modul, pornire program de instalare, acces la fișiere, pornire aplicație și încărcare modul; • prin stabilirea unor condiții care să poată fi selectate după atribute (cale destinație, nume fișier destinație, reputație destinație, versiune fișier destinație, cod hash pentru certificat la destinație.....etc), condiție și valoare, ce vor asigura activarea regulilor de excludere; • soluția oferă funcțional de Management API prin integrarea solutiilor terte precum: SIEM/RMM; **1.2. Cerintele tehnice vis-a-vis de administrarea solutiei:** • administrarea soluției se face printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite careva echipamente hardware(servere de management) sau careva software special. • consola de este capabilă de a funcționa pe orice dispozitiv și conține toate funționalitățile sus solicitate;	

						• să suporte următorele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; • interfața consolei de administare trebuie să asigure posibilitatea de funcționare în limbile: romana, rusă si engleză obligatoriu, cu capacitatea de a putea fi selectată limba dorită, în scopul unei administrări mai ușoare de către administratori; • administratorul trebuie să poată permite sau interzice utilizatorului de a activa sau dezactiva caracteristicile de securitate setate; 1.3. Cerințe vis-a-vis de funcționalul de raportare și alerte: Soluția trebuie să permită generarea de rapoarte grafice detaliate, saptămînal sau lunar, cu posibilitate de export minimum in format (csv), inclusiv cu remitere automată către adrese de email specificate, rapoartele trebuie să cuprindă minim informație despre: Clasament computere (după infecţii blocate); Top de infecţii tratate; Infecţii gestionate; Starea de protecţie; Cele mai recente actualizări pentru definiţiile de malware pe computere; Dacă s-au instalat actualizările de securitate; Soluția trebuie să permită setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru minim următoarele acțiuni: blocat, redenumit, oprit, șters, plasat, raportat, dezinfectat, în carantină, raportat către utilizator, blocat şi acţiune suplimentară solicitată de la utilizator, mutat în coșul de gunoi; Soluția trebuie să asigure posibilitatea de trimitere a alertelor in momentul declanșării prin email spevificat de administrator si sa permită setarea	• suportă următorele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; • interfața consolei de administare asigură posibilitatea de funcționare în limbile: romana, rusă si engleză cu capacitatea de a putea fi selectată limba dorită; • administratorul poate permite sau interzice utilizatorului de a activa sau dezactiva caracteristicile de securitate setate; **1.3. Cerințe vis-a-vis de funcționalul de raportare și alerte:** Soluția permite generarea de rapoarte grafice detaliate, saptămînal sau lunar, cu posibilitate de export minimum in format (csv), inclusiv cu remitere automată către adrese de email specificate, rapoartele cuprind informație despre: - Clasament computere (după infecţii blocate); - Top de infecţii tratate; - Infecţii gestionate; - Starea de protecţie; - Cele mai recente actualizări pentru definiţiile de malware pe computere; - Dacă s-au instalat actualizările de securitate; Soluția permite setarea și configurarea de alerte, declanșarea lor poate fi aplicată pentru următoarele acțiuni: blocat, redenumit, oprit, șters, plasat, raportat, dezinfectat, în carantină, raportat către utilizator, blocat şi acţiune suplimentară solicitată de la utilizator, mutat în coșul de gunoi; Soluția asigură posibilitatea de trimitere a alertelor in momentul declanșării prin email specificat de administrator si permite setarea limbii dorite in care să fie emailul (română, engleză, rusă);	

						limbii dorite in care să fie emailul (minim română, engleză, rusă); 1.4. Alte cerințe obligatorii: Pentru soluția ofertată se solicită a fi 12 luni suport local și de 36 luni de la producător. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului. Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de ofertant, iar costul acestora trebuie să fie incluse în oferta comerciala. Pentru administratorul IT din cadrul instituției se va organiza instruiri de exploatare eficientă a sistemului. Prezentarea a minim 2 certificate tehnice pe soluția propusa. Ofertantul va prezenta copia Certificatului ISO 27001:2013 și Certificatului ISO 9001:2015 - confirmat cu aplicarea semnăturii electronice; Ofertantul va prezenta Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat. Ofertantul va avea minim o persoana certificata in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013; Ofertantul va prezenta minim 3 referințe de implementare pe piața locală a soluției ofertate.	**1.4. Alte cerințe obligatorii:** Pentru soluția ofertată se oferă 12 luni suport local de la Xontech Systems și de 36 luni de la producător. Producătorul oferă suport 24/24, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului Xontech Systems. Lucrările de instalare, configurare, punerea în funcțiune a soluției vor fi executate de ofertant, conform ofertei comerciale. Pentru administratorul IT din cadrul instituției se va organiza instruiri de exploatare eficientă a sistemului. 2 certificate tehnice a specialistilor pe soluția propusa sunt anexate la oferta. Copia Certificatului ISO 27001:2013 şi Certificatului ISO 9001:2015 - confirmat cu aplicarea semnăturii electronice sunt anexate cu oferta; Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat este atasat cu oferta. Persoana certificata in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013 , certificatul este atasat cu oferta; Ofertantul va prezenta minim 3 referințe de implementare pe piața locală a soluției ofertate.	
2.2	48900 000-7	Soluție pentru scanarea vulnerabilităților	**F-Secure Radar for 70 IP's/host for 1 year of support**	**Finlanda**	**F-Secure Corporation**	Se solicita o platforma centralizata pentru scanarea si gestionarea vulnerabilităților pentru 70 de IP-uri cu suport inclus pentru perioada 12 luni. -Platforma trebuie sa fie capabila sa identifice atât amenințările interne cat si pe cele externe si să raporteze riscurile	Se oferă o platforma centralizata pentru scanarea si gestionarea vulnerabilităților pentru 70 de IP-uri/hosturi cu suport inclus pentru perioada 12 luni. -Platforma este capabila sa identifice atât amenințările interne cat si pe cele externe	

						si reglementările conform minim PCI, GDPR, ș.a. -Produsul ofertat va trebui să poată fi extins prin achiziția ulterioară a unei soluții de antivirus, de la același producător pentru a exista o integrare nativa a soluției. Cu posibilitatea de a accesa dintr-o singură interfață fie soluția de antivirus fie soluția de scanare a vulnerabilităților. -Soluția trebuie sa asigure scanarea vulnerabilităților pentru echipamente din rețea, aplicațiilor web, site-urilor interne sau externe. - Soluția ofertată trebuie să fie una bazată pe tehnologia Cloud, care să ofere o vizibilitate a vulnerabilităților într-un mod centralizat pentru toate tipurile de dispozitive conectate in rețea si care pot comunica, de exemplu: stații de lucru, servere, servere virtuale, site-uri, switch-uri, routere, aplicațiilor web, etc; - 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, a cărui domen se atribuie, vulnerabilitățile depistate, software-ul instalat pe echipament, spațiu disponibil, tipul procesor, tip de Bios. - Soluția va permite planificarea activităților după data/ora/an si de rulat scanarea vulnerabilităților pentru fiecare echipament in parte. - 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. - Soluția trebuie sa permită adăugarea unui grup de scanare in care se va indica minim: Numele grupului si persoana	si să raporteze riscurile si reglementările conform PCI, GDPR. -Produsul ofertat poate fi extins prin achiziția ulterioară a unei soluții de antivirus, de la același producător pentru a exista o integrare nativa a soluției. Ca exemplueste produsul ofertat mai sus. Cu posibilitatea de a accesa dintr-o singură interfață fie soluția de antivirus fie soluția de scanare a vulnerabilităților. -Soluția asigură scanarea vulnerabilităților pentru echipamente din rețea, aplicațiilor web, site-urilor interne sau externe. - Soluția este una bazată pe tehnologia Cloud, care oferă o vizibilitate a vulnerabilităților într-un mod centralizat pentru toate tipurile de dispozitive conectate in rețea si care pot comunica, de exemplu: stații de lucru, servere, servere virtuale, site-uri, switch-uri, routere, aplicațiilor web, etc; - Soluția oferă posibilitatea de a identifica toate echipamentele conectate la rețea, la fel este posibil de a verifica tipul de echipament, după caz: sistemul de operare instalat, IP-ul si MAC adresa, a cărui domen se atribuie, vulnerabilitățile depistate, software-ul instalat pe echipament, spațiu disponibil, tipul procesor, tip de Bios. - Soluția permite planificarea activităților după data/ora/an si de rulat scanarea vulnerabilităților pentru fiecare echipament in parte. - Soluția 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. - Soluția permite adăugarea unui grup de scanare in care se va indica: Numele	

						responsabilă, descrierea succinta a vulnerabilității. - Posibilitatea de scanare prin alegerea unui șablon prestabilit care va propunere de a scana sistemul după minim următoarele modele: TCP 0-65535 , UDP 0-1024 Badlock detection Bash Shellshock detection GHOST detection Hearbeast detection Limited TCP 0-30000, no UDP PCI scan Scan full TCP/UDP port range Scan top-100 ports Scan top-1000 ports SSL/TLS maturity scanning - Modul de scanare să poată fi setat după: oră, repetări zilnice, săptămânale, lunare, trimestriale, etc. - Soluția trebuie să ofere funcțional de Management API prin integrarea soluțiilor terțe; - Soluția trebuie să ofere posibilitatea de setare a unui logo care trebuie sa se afișeze in consola de administrare si in rapoartele de vulnerabilități exportate. - Soluția va dispune de posibilitate de autentificarea prin doi factori cu ajutorul unor soluții bazate pe TOTP (Time-based One Time Password) ca: • Use Google Authenticator, • Microsoft Authenticator, Sau altele care suporta acest algoritm. Cerințele tehnice vis-a-vis de administrarea soluției: -Administrarea soluției este necesara să se facă printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite careva echipamente hardware(servere de management) sau careva software special. -Soluția propusa trebuie sa poată genera un raport pe segmente din rețea pe care se dorește. Si va fi posibil de a selecta ce	grupului si persoana responsabilă, descrierea succinta a vulnerabilității. - Oferă posibilitatea de scanare prin alegerea unui șablon prestabilit care va propune de a scana sistemul după următoarele modele: TCP 0-65535 , UDP 0-1024 Badlock detection Bash Shellshock detection GHOST detection Hearbeast detection Limited TCP 0-30000, no UDP PCI scan Scan full TCP/UDP port range Scan top-100 ports Scan top-1000 ports SSL/TLS maturity scanning - Modul de scanare poate fi setat după: oră, repetări zilnice, săptămânale, lunare, trimestriale, etc. - Soluția oferă funcțional de Management API prin integrarea soluțiilor terțe; - Soluția oferă posibilitatea de setare a unui logo care se afișează in consola de administrare si in rapoartele de vulnerabilități exportate. - Soluția dispune de posibilitate de autentificarea prin doi factori cu ajutorul unor soluții bazate pe TOTP (Time-based One Time Password) ca: • Use Google Authenticator, • Microsoft Authenticator, Sau altele care suporta acest algoritm. Cerințele tehnice vis-a-vis de administrarea soluției: -Administrarea soluției se face printr-o singură consolă de administrare bazată pe cloud, fără ca să necesite careva echipamente hardware(servere de management) sau careva software special. -Soluția propusa poate genera un raport pe segmente din rețea pe care se dorește. Si este posibil de a selecta ce fel de	

						fel de vulnerabilități să fie afișate in raport, sortate după severitatea lor. -Soluția propusa trebuie să pună la dispoziție posibilitatea de a asigna remedierea unei vulnerabilități către un user / administrator creat in platforma de administrare. -Asignarea unui task va fi posibil prin crearea un ticket astfel se va indica unele date ca : denumire task, descrierea succinta, perioada pana când sa fie executat, prioritatea, o perioadă estimată pentru remediere, etc. -Soluția trebuie sa dispună de capacitatea de a automatiza unele procese de lucru ca: • Închiderea si redeschiderea automata a tichete-lor; • Sa trimită notificare tuturor participanților la expirarea task-ului; • Pana la expirarea termenului limita pentru executarea task-ului, soluția va notifica toți participanții. -Consola de administrare trebuie să suporte următoarele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; -Interfața consolei de administrare trebuie să asigure posibilitatea de funcționare în limba: engleză obligatoriu, cu capacitatea de a putea fi selectată alte limbi disponibile, în scopul unei administrări mai ușoare de către administratori; -Soluția va permite accesul altor useri cu drepturi de: administrator, doar vizualizare sau colegi de echipa. -Soluția va putea afișa toata informația referitor la licența instalată, jurnal de evenimente, modificările aplicate de către user-ul care are accesul la portal. -In consola de administrare trebuie sa se regăsească acces la manuale, ghiduri de instalare, ghidul de utilizare, etc, informații referitor la schimbările si	vulnerabilități să fie afișate in raport, sortate după severitatea lor. -Soluția pune la dispoziție posibilitatea de a asigna remedierea unei vulnerabilități către un user / administrator creat in platforma de administrare. -Asignarea unui task este posibil prin crearea un ticket astfel se va indica unele date ca : denumire task, descrierea succinta, perioada pana când sa fie executat, prioritatea, o perioadă estimată pentru remediere, etc. -Soluția dispune de capacitatea de a automatiza unele procese de lucru ca: • Închiderea si redeschiderea automata a tichete-lor; • Sa trimită notificare tuturor participanților la expirarea task-ului; • Pana la expirarea termenului limita pentru executarea task-ului, soluția va notifica toți participanții. -Consola de administrare suportă următoarele browsere: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari; -Interfața consolei de administrare asigură posibilitatea de funcționare în limba engleză,cu capacitatea de a putea fi selectată alte limbi disponibile, în scopul unei administrări mai ușoare de către administratori; -Soluția permite accesul altor useri cu drepturi de: administrator, doar vizualizare sau colegi de echipa. -Soluția poate afișa toata informația referitor la licența instalată, jurnal de evenimente, modificările aplicate de către user-ul care are accesul la portal. -In consola de administrare se regăseste acces la manuale, ghiduri de instalare, ghidul de utilizare, etc, informații referitor la schimbările si actualizările	

						actualizările soluției, comunitate, portal pentru suport cu posibilitatea de a solicita ajutor de la producător. -bord pot fi create in forma de minima de: tabel, plăcinta, histograma, etc. - Tablourile de bord trebuie să conțină informații ca: vulnerabilitățile depistate care vor fi grupate după severitate/data/luna/cantitatea depistata. Cele mai grave vulnerabilati. Scanările active. Scanările care sunt planificate. Ultimele dispozitive scanate. Soluția trebuie să permită setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru minim următoarele acțiuni: când startează un proces de scanare, finalizare procesului de scanare, la crearea si asignarea unui task către un utilizator existent. Cerințe vis-a-vis de funcționalul de raportare și alerte: - Soluția trebuie să permită generarea de rapoarte grafice detaliate, săptămânal sau lunar, cu posibilitate de export minimum in format (csv, docx și xml), inclusiv cu remitere automată către adrese de email specificate, rapoartele trebuie să cuprindă minim informație despre: - Vulnerabilitățile descoperite clasificate după severitate: informativ, severitate minima, severitate medie, si severitate înalta. - Notarea severității vulnerabilităților se va face pe notă de la 1 la 10 - Raportul va afișa descriere pentru fiecare vulnerabilitate in parte cu unele referințe. - Recomandările propuse pentru remedierea vulnerabilității depistate. - Crearea unei statistici grafice in dependenta de vulnerabilitățile depistate - Top vulnerabilități depistate.	soluției, comunitate, portal pentru suport cu posibilitatea de a solicita ajutor de la producător. - Tablourile de bord pot fi create in forma de: tabel, plăcinta, histograma, etc. - Tablourile conțin informații ca: vulnerabilitățile depistate care vor fi grupate după severitate/data/luna/cantitatea depistata. Cele mai grave vulnerabilati. Scanările active. Scanările care sunt planificate. Ultimele dispozitive scanate. Soluția permite setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru următoarele acțiuni: când startează un proces de scanare, finalizare procesului de scanare, la crearea si asignarea unui task către un utilizator existent. Cerințe vis-a-vis de funcționalul de raportare și alerte: - Soluția permite generarea de rapoarte grafice detaliate, săptămânal sau lunar, cu posibilitate de export minimum in format (csv, docx și xml), inclusiv cu remitere automată către adrese de email specificate, rapoartele cuprind informație despre: - Vulnerabilitățile descoperite clasificate după severitate: informativ, severitate minima, severitate medie, si severitate înalta. - Notarea severității vulnerabilităților se va face pe notă de la 1 la 10 - Raportul va afișa descriere pentru fiecare vulnerabilitate in parte cu unele referințe. - Recomandările propuse pentru remedierea vulnerabilității depistate. - Crearea unei statistici grafice in dependenta de vulnerabilitățile depistate - Top vulnerabilități depistate.	

						Soluția trebuie să permită crearea unor tablouri de bord care pot fi editate, clonate sau șterse cu afișarea lor pe pagina in mod dinamic. La fel, tablourile de bord pot fi create in forma de minima de: tabel, plăcinta, histograma, etc. - Tablourile de bord trebuie să conțină informații ca: vulnerabilitățile depistate care vor fi grupate după severitate/data/luna/cantitatea depistata. Cele mai grave vulnerabilati. Scanările active. Scanările care sunt planificate. Ultimele dispozitive scanate. Soluția trebuie să permită setarea și configurarea de alerte, declanșarea lor să poată fi aplicată pentru minim următoarele acțiuni: când starteaza un proces de scanare, finalizare procesului de scanare, la crearea si asignarea unui task către un utilizator existent. Alte cerințe obligatorii: Pentru soluția ofertată se solicită suport 12 luni de la producător. Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de ofertant, iar costul acestora trebuie să fie incluse în oferta comerciala. Va prezenta un raport privind vulnerabilitățile depistate si remedierile propuse. Pentru administratorul IT din cadrul instituției se va organiza instruiri de exploatare eficientă a sistemului. Prezentarea a minim 2 certificate tehnice pe soluția propusa. Ofertantul va prezenta copia Certificatului ISO 27001:2013 şi Certificatului ISO 9001:2015 - confirmat cu aplicarea semnăturii electronice; Ofertantul va prezenta Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat.	- Aceste cerinte sau descris mai sus, probabil se repeta. Alte cerințe obligatorii: Pentru soluția ofertată se oferă suport 12 luni de la producător. Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să vor fi executate de ofertant, iar costul acestora este inclus în oferta comerciala. Ofertantul Va prezenta un raport privind vulnerabilitățile depistate si remedierile propuse. Pentru administratorul IT din cadrul instituției se va organiza instruiri de exploatare eficientă a sistemului. 2 certificate tehnice pe soluția propusa sunt anexate la ofertă. Copia Certificatului ISO 27001:2013 şi Certificatului ISO 9001:2015 - confirmat cu aplicarea semnăturii electronice este atasat la oferta; Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat este anexat cu oferta. Persoana certificata(angajat al ofertantului) in calitate de auditor intern	

						Ofertantul va avea minim o persoana certificata(angajat al ofertantului) in calitate de auditor intern pentru sistemul de management al securității informaționale conform ISO 27001:2013;	pentru sistemul de management al securității informaționale conform ISO 27001:2013, certificatul este anexat cu oferta;	
		Lotul 3						
3.	48900000-7	Microsoft Windows Server	**WinSvrSTDCore SNGL LicSAPk OLP 16Lic NL CoreLic**	**SUA**	**Microsoft**	Microsoft Windows Server Standard Core 2019 care sa acopere 16 core.	WinSvrSTDCore SNGL LicSAPk OLP 16Lic NL CoreLic	
		Lotul 4						
4	48900000-7	Renew WatchGuard Standard Support pentru 12 luni	**Renewal Watchguard Firebox M270 with Basic Security for 1 year**	**SUA**	**WatchGuard Technologies**	Se solicita reinoirea licentei pentru WatchGuard de tip Firebox M270, se solicita licenta de tip Basic Security Suite.	Renewal Watchguard Firebox M270 with Basic Security for 1 year.	
		TOTAL						

Semnat:

Nume: **Irina Vicol**
În calitate de: **Administrator**
Ofertantul: **Xontech Systems SRL**
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova.
Data: “20” iulie 2020