Anexa nr.1

Specificaţia tehnică pentru software antivirus.

№	Cerinţe	Conformat (Da/Nu)	Cometariu
Cerinţe de sistem			
1.	**Soluţia propusă trebuie să accepte sistemele de operare de mai jos:** • Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 sau o versiune ulterioară • Windows 8 Professional / Enterprise • Windows 8.1 Professional / Enterprise • Windows 10 Home / Pro / Pro pentru staţii de lucru / Educaţie / Enterprise • Windows 11 **Servere** • Windows Small Business Server 2011 Essentials / Standard (64 de biţi) • Windows MultiPoint Server 2011 (64 de biţi) • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 sau o versiune ulterioară • Windows Server 2012 Foundation / Essentials / Standard / Datacenter • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter • Windows Server 2016 Essentials / Standard / Datacenter • Windows Server 2019 Essentials / Standard / Datacenter • Windows Server 2022 **Microsoft Terminal Servere** • Microsoft Remote Desktop bazate pe Windows Server 2008 R2 SP1 • Microsoft Remote Desktop bazate pe Windows Server 2012 • Microsoft Remote Desktop bazate pe Windows Server 2012 R2 • Microsoft Remote Desktop bazate pe Windows Server 2016 • Microsoft Remote Desktop bazate pe Windows Server 2019 **Sisteme de operare Linux pe 32 de biţi:** • CentOS 6.7 şi versiuni ulterioare • Debian GNU / Linux 9.4 şi versiuni ulterioare • Debian GNU / Linux 10.1 şi versiuni ulterioare • Linux Mint 19 şi versiuni ulterioare • Mageia 4 • Red Hat Enterprise Linux 6.7 şi versiuni ulterioare • ALT Education 9 •ALT Workstation 9 •ALT Server 9 **Sisteme de operare Linux pe 64 de biţi:** • AlterOS 7.5 şi versiuni ulterioare • Amazon Linux 2 • Astra Linux Common Edition (actualizare operaţională 2.12). • Astra Linux Special Edition RUSB.10015-01 (actualizare operaţională 1.5) • Astra Linux Special Edition RUSB.10015-01 (actualizare operaţională 1.6) • Astra Linux Special Edition RUSB.10015-16 (versiunea 1) (actualizare operaţională 1.6) • CentOS 6.7 şi versiuni ulterioare • CentOS 7.2 şi versiuni ulterioare • CentOS 8.0 şi versiuni ulterioare • Debian GNU / Linux 9.4 şi versiuni ulterioare • Debian GNU / Linux 10.1 şi versiuni ulterioare • EulerOS V2.0SP2 2.2.17 • EulerOS V2.0SP5 2.5.6 • Linux Mint 19 şi versiuni ulterioare • Linux Mint 20.1 şi versiuni ulterioare • openSUSE Leap 15.0 şi versiuni ulterioare • Oracle Linux 7.3 şi versiuni ulterioare • Oracle Linux 8.0 şi versiuni ulterioare • Pardus OS 19.1 • Red Hat Enterprise Linux 6.7 şi versiuni ulterioare • Red Hat Enterprise Linux 7.2 şi versiuni ulterioare • Red Hat Enterprise Linux 8.0 şi versiuni ulterioare		

	• SUSE Linux Enterprise Server 12 SP5 și versiuni ulterioare • **SUSE Linux Enterprise Server 15 și versiuni ulterioare** • **Ubuntu 18.04 LTS și versiuni ulterioare** • Ubuntu 20.04 LTS • ALT Education 9 • ALT Workstation 9 • ALT Server 9 • GosLinux 7.2 • **Red OS 7.3** **Sisteme de operare MAC OS:** • macOS 10.14 – 12		
2.	Soluția propusă trebuie să suporte următoarele platforme virtuale: • VMware Workstation 16.1.1 Pro • VMware ESXi 7.0 Update 2a • **Microsoft Hyper-V Server 2019** • **Citrix Virtual Apps and Desktops 7 2103** • Citrix Provisioning 2012 • Citrix Hypervisor 8.2 LTSR		
3.	Soluția propusă trebuie să suporte protecția celor mai recente versiuni de sisteme de operare pe toate platformele (Windows, Linux, MacOS, iOS, Android).		
Cerințe funcționale			
2.1	**Cerințe funcționale: Antivirus**		
	Soluția propusă trebuie să fie capabilă să detecteze următoarele tipuri de amenințări: • Viruși (inclusiv polimorfi), Viermi, Troieni, Backdoors, Rootkit-uri, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Site-uri și link-uri de phishing, Zero-Day Vulnerabilities și alte programe rău intenționate și nedorite.		
	Soluția propusă trebuie să suporte interfața de scanare anti-malware (AMSI).		
	Soluția propusă trebuie să aibă capacitatea de a se integra cu Windows Defender Security Center.		
	Soluția propusă trebuie să accepte subsistemul Windows Linux.		
	Soluția propusă trebuie să ofere tehnologii de protecție de ultimă generație. De exemplu: • protecție împotriva amenințărilor fără fișiere • furnizarea de protecție pe mai multe straturi bazate pe Machine Learning (ML) și analiză comportamentală în diferite etape ale lanțului de distrugere		
	Soluția propusă trebuie să ofere scanarea memorie pentru stațiile de lucru Windows.		
	Soluția propusă trebuie să ofere Scanare memorie Kernel pentru stațiile de lucru Linux.		
	Soluția propusă trebuie să ofere posibilitatea de a trece la modul cloud pentru protecția împotriva amenințărilor, scăzând utilizarea RAM și a **unității de disc pentru mașinile cu resurse limitate.**		
	Soluția propusă trebuie să aibă componente dedicate pentru monitorizarea, detectarea și blocarea activităților pe serverele Windows, Linux și Windows și punctele finale, pentru a proteja împotriva atacurilor de criptare de la distanță.		
	Soluția propusă trebuie să includă componente fără semnătură pentru a **detecta amenințările chiar și fără actualizări frecvente. Protecția trebuie să fie susținută de Static ML pentru pre-execuție și Dynamic ML pentru** etapele post-execuție ale lanțului de distrugere pe puncte terminale și în cloud pentru serverele și stațiile de lucru Windows.		
	Soluția propusă trebuie să ofere o analiză comportamentală bazată pe ML.		
	Soluția propusă trebuie să ofere capacitatea de a se integra cu propriile soluții Endpoint Detection and Response (EDR) și Anti-APT ale **furnizorului, pentru căutarea activă a amenințărilor și răspunsul automat la incident.**		
	Soluția propusă trebuie să suporte integrarea cu o soluție sandbox automată de detectare și prevenire a amenințărilor autonome/independente care nu depinde de soluția EDR și/sau Anti-APT a furnizorului.		
	Soluția propusă trebuie să includă capacitatea de a configura și gestiona setările paravanului de protecție încorporate în sistemele de operare		

	Windows Server şi Linux, prin consola sa de management.		
	Soluţia propusă trebuie să ofere control pentru aplicaţii şi dispozitive pentru staţiile de lucru Windows.		
	Soluţia de protecţie propusă pentru servere şi staţii de lucru trebuie să includă o componentă dedicată pentru protecţie împotriva activităţii virusului ransomware/criptor pe resursele partajate.		
	Soluţia propusă trebuie, să detecteze activităţi de tip ransomware/criptor, să blocheze automat computerul atacator pentru un interval specificat şi să **genereze informaţii despre IP-ul computerului atacator şi marca temporală şi tipul de ameninţare.**		
	Soluţia propusă trebuie să ofere o listă predefinită de excluderi de scanare pentru aplicaţiile şi serviciile Microsoft.		
	Soluţia propusă trebuie să suporte instalarea de protecţie a punctelor terminale pe servere fără a fi necesară repornirea.		
	Soluţia propusă trebuie să permită următoarele pentru puncte finale: • **Scanare manuală** • Scanare la acces • Scanare la cerere • Scanarea fişierelor comprimate • Scanare fişiere, foldere şi unităţi individuale • **Blocarea şi scanarea scripturilor** • **Garda de Registru** • Protecţie împotriva depăşirilor de buffer • Scanare în fundal/inactiv • Scanarea unităţii detaşabile la conectarea cu sistemul • Capacitatea de a detecta şi de a bloca gazdele neîncrezătoare la **detectarea activităţilor asemănătoare criptării pe resursele partajate de server.**		
	Soluţia propusă trebuie să fie protejată cu parolă pentru a preveni oprirea/închiderea procesului AV şi pentru autoprotecţie, indiferent de nivelul de autorizare a utilizatorului pe sistem.		
	Soluţia propusă trebuie să dispună de baze de date de reputaţie atât locale, cât şi globale.		
	Soluţia propusă trebuie să poată scana traficul HTTPS, HTTP şi FTP împotriva virusilor şi a programelor spion sau a oricărui alt malware.		
	Soluţia propusă trebuie să includă un firewall personal capabil, cel puţin să: • Blocheze activările la reţea ale aplicaţiilor în funcţie de clasificarea lor. • **Blocheze /permite anumite pachete, protocoale, adrese IP, porturi şi direcţie de trafic.** • Adăuge automat şi manual subreţele de reţea şi modifice permisiunile de activitate în reţea.		
	Soluţia propusă trebuie să împiedice conectarea dispozitivelor USB reprogramate care emulează tastaturi şi să permită controlul utilizării **tastaturilor de pe ecran pentru autorizare.**		
	Soluţia propusă trebuie să fie capabilă să blocheze atacurile de reţea şi să raporteze sursa infecţiei.		
	Soluţia propusă trebuie să aibă stocare locală pe punctele finale pentru a păstra copii ale fişierelor care au fost şterse sau modificate în timpul dezinfectării. Aceste fişiere trebuie să fie stocate într-un format specific care să asigure că nu reprezintă nicio ameninţare.		
	Soluţia propusă trebuie să aibă o abordare proactivă pentru a împiedica malware-ul să exploateze vulnerabilităţile existente pe servere şi staţii de lucru.		
	Soluţia propusă trebuie să suporte tehnologia AM-PPL (Anti-Malware Protected Process Light) pentru protecţie împotriva acţiunilor rău intenţionate.		
	Soluţia propusă trebuie să includă protecţie împotriva atacurilor care exploatează vulnerabilităţile din protocolul ARP pentru a falsifica adresa MAC a dispozitivului.		
	Soluţia propusă trebuie să asigure funcţionalitatea Anti-Bridging pentru staţiile de lucru Windows, pentru a preveni punţile neautorizate către reţeaua internă care ocolesc instrumentele de protecţie a perimetrului. Administratorii trebuie să poată interzice stabilirea simultană de conexiuni **prin cablu, Wi-Fi şi modem.**		
	Soluţia propusă trebuie să includă o componentă dedicată pentru scanarea		

	conexiunilor criptate.		
	Soluţia propusă trebuie să poată decripta şi scana traficul de reţea transmis prin conexiuni criptate suportate de următoarele protocoale; SSL 3.0, TLS 1.0, TLS1.1, TLS1.2, TLS 1.3.		
	Soluţia propusă trebuie să aibă capacitatea de a exclude automat resursele web atunci când apare o eroare de scanare în timpul efectuării unei scanări a conexiunii criptate. Această excludere trebuie să fie unică pentru gazdă şi nu trebuie să fie partajată cu alte puncte finale.		
	Soluţia propusă trebuie să includă funcţionalitate de ştergere de la distanţă a datelor de pe punctul final (pentru staţii de lucru).		
	Soluţia propusă trebuie să aibă următoarele funcţionalităţi de ştergere a datelor de la distanţă: • În modul silentios • Pe hard disk-uri şi unităţi amovibile • **Pentru toate conturile de utilizator de pe computer**		
	Funcţionalitatea de ştergere a datelor de la distanţă a soluţiei propuse trebuie să suporte următoarele moduri: • Ştergerea imediată a datelor • Ştergerea datelor amânată Funcţionalitatea de ştergere a datelor de la distanţă a soluţiei propuse **trebuie să suporte următoarele metode de ştergere a datelor:** • **Ştergerea folosind resursele de operare - fişierele sunt şterse, dar** nu sunt trimise la coşul de reciclare • Ştergerea completă, fără recuperare - făcând datele practic imposibil de restabilit după ştergere		
	Soluţia propusă trebuie să includă funcţionalitatea de a şterge automat **datele dacă nu există nicio conexiune la serverul de management al punctelor finale.**		
	Soluţia propusă trebuie să accepte detectarea bazată pe semnătură, pe lângă cele asistate de cloud şi cea euristică.		
	Soluţia propusă ar trebui să aibă capacitatea de a lansa o alertă pentru a curăţa şi şterge o ameninţare detectată.		
	Soluţia propusă trebuie să aibă capacitatea de a accelera sarcinile de **scanare, omiţând acele obiecte care nu s-au schimbat de la scanarea anterioară.**		
	Soluţia propusă trebuie să aibă capacitatea de a prioritiza sarcinile de scanare personalizate şi la cerere pentru staţiile de lucru Linux.		
	Soluţia propusă trebuie să permită administratorului să excludă de la scanare fişierele/directoarele/aplicaţiile/certificatele digitale specificate, **fie la acces (protecţie în timp real), fie în timpul scanărilor la cerere.**		
	Soluţia propusă ar trebui să includă funcţionalitatea de izolare a computerelor infectate.		
	Soluţia propusă trebuie să scaneze automat unităţile detaşabile pentru a detecta programele malware atunci când acestea sunt ataşate la orice punct final. Controlul scanării trebuie să se bazeze pe dimensiunea unităţii.		
	Soluţia propusă trebuie să poată bloca utilizarea dispozitivelor de stocare **USB sau să permită accesul numai la dispozitivele permise şi să permită accesul de citire/scriere numai utilizatorilor de domeniu, pentru a reduce** furtul de date şi pentru a aplica politicile de blocare.		
	Soluţia propusă trebuie să poată face diferenţa între dispozitivele de stocare USB, imprimante, telefoane mobile şi alte periferice.		
	Soluţia propusă trebuie să poată înregistra operaţiunile de fişiere (Scrie şi **ştergere) pe dispozitivele de stocare USB. Acest lucru nu trebuie să necesite nicio licenţă sau componentă suplimentară care să fie instalată pe punctul** final.		
	Soluţia propusă trebuie să aibă capacitatea de a bloca execuţia oricărui executabil de pe dispozitivul de stocare USB.		
	Soluţia propusă trebuie să aibă capacitatea de a bloca/permite accesul **utilizatorilor la resursele web în funcţie de site-uri web, tip de conţinut, utilizator şi ora din zi.**		
	Soluţia propusă trebuie să aibă o categorie de detectare specifică pentru a bloca bannerele site-ului.		
	Soluţia propusă trebuie să ofere posibilitatea de a configura reţele Wi-Fi pe baza numelui reţelei, tipului de autentificare, tipului de criptare, astfel încât acestea să poată fi utilizate ulterior pentru a bloca sau a permite **conexiunile Wi-Fi.**		
	Soluţia propusă trebuie să accepte politici bazate pe utilizator pentru		

	controlul dispozitivelor, web şi aplicaţiilor.		
	Soluţia propusă ar trebui să permită în mod specific blocarea următoarelor dispozitive: • Bluetooth • Dispozitive mobile • Modemuri externe • CD/DVD-uri • Camere şi scanere • MTP-uri • Şi transferul de date pe dispozitive mobile		
	Soluţia propusă ar trebui să includă integrarea în cloud, pentru a oferi cele mai rapide actualizări posibile despre malware şi potenţiale ameninţări. Soluţia propusă trebuie să aibă capacitatea de a gestiona drepturile de acces ale utilizatorilor pentru operaţiunile de citire şi scriere pe CD-uri/DVD-uri, dispozitive de stocare detaşabile şi dispozitive MTP.		
	Soluţia propusă trebuie să includă filtrarea firewall după adresa locală, interfaţa fizică şi Time-To-Live (TTL) de pachete.		
	Soluţia propusă trebuie să permită administratorului să monitorizeze utilizarea de către aplicaţie a porturilor personalizate/aleatorie după lansare.		
	Soluţia propusă trebuie să accepte blocarea aplicaţiilor interzise (Deny-List) pentru a fi lansate pe punctul final şi blocarea tuturor aplicaţiilor, altele decât cele incluse în Allow-Lists.		
	Soluţia propusă trebuie să aibă o componentă de control al aplicaţiilor integrată în cloud pentru acces imediat la cele mai recente actualizări privind evaluările şi categoriile aplicaţiilor.		
	Soluţia propusă trebuie să ofere protecţie fişierelor executate în containere Windows Server.		
	Soluţia propusă trebuie să includă filtrarea programelor malware de trafic, verificarea legăturilor web şi controlul resurselor web pe baza categoriilor de cloud.		
	Componenta de control/restricţie a soluţiei propuse trebuie să includă o categorie Criptomonede şi Mining. De asemenea, trebuie să includă restricţii legale regionale predefinite pentru a se conforma legislaţiei Belgiene şi Japoneze.		
	Soluţia propusă trebuie să aibă capacitatea de a permite aplicaţii bazate pe certificatele lor de semnătură digitală, MD5, SHA256, META Data, File Path şi categoriile de securitate predefinite.		
	Soluţia propusă trebuie să aibă controale pentru descărcarea DLL şi a driverelor.		
	Soluţia propusă trebuie să accepte controlul scripturilor din PowerShell.		
	Soluţia propusă trebuie să accepte modul de testare cu generarea de rapoarte privind lansarea aplicaţiilor blocate.		
	Soluţia propusă trebuie să aibă capacitatea de a restricţiona activităţile aplicaţiei din sistem în funcţie de nivelul de încredere atribuit aplicaţiei şi de a limita drepturile aplicaţiilor de a accesa anumite resurse, inclusiv fişierele de sistem şi utilizator „Funcţionalitatea HIPS".		
	Soluţia propusă trebuie să aibă capacitatea de a controla accesul sistemului/aplicaţiei utilizatorului la dispozitivele de înregistrare audio şi video.		
	Soluţia propusă trebuie să ofere o facilitate pentru a verifica aplicaţiile enumerate în fiecare categorie bazată pe cloud.		
	Soluţia propusă trebuie să aibă capacitatea de a se integra cu un sistem Advanced Threat Protection specific furnizorului.		
	Soluţia propusă trebuie să aibă capacitatea de a reglementa automat activitatea programelor care rulează, inclusiv accesul la sistemul de fişiere şi registre, precum şi interacţiunea cu alte programe.		
	Soluţia propusă trebuie să aibă capacitatea de a şterge automat regulile de control al aplicaţiei dacă o aplicaţie nu este lansată într-un interval specificat. Intervalul trebuie să fie configurabil.		
	Soluţia propusă trebuie să aibă capacitatea de a clasifica automat aplicaţiile lansate înainte de instalarea protecţiei punctelor finale.		
	Soluţia propusă trebuie să aibă protecţie împotriva ameninţărilor de corespondenţă cu: • Filtrul de ataşamente şi capacitatea de a redenumi ataşamentele. • Scanarea mesajelor e-mail la primirea, citirea şi trimiterea.		
	Soluţia propusă trebuie să aibă capacitatea de a scana mai multe		

	redirecționări, adrese URL scurtate, adrese URL deturnate și întârzieri bazate pe timp.		
	Soluția propusă trebuie să permită utilizatorului computerului să efectueze o verificare a reputației unui fișier din meniul contextual al fișierului.		
	Soluția propusă trebuie să includă scanarea tuturor scripturilor, inclusiv a celor dezvoltate în Microsoft Internet Explorer, precum și a oricăror scripturi WSH (JavaScript, Visual Basic Script Scripturi WSH (JavaScript, Visual Basic Script etc.), lansate atunci când utilizatorul lucrează pe computer, inclusiv internetul.		
	Soluția propusă trebuie să ofere protecție împotriva malware-ului încă necunoscut pe baza analizei comportamentului acestora și a examinării modificărilor din registrul sistemului, împreună cu un motor puternic de remediere pentru a restabili automat orice modificări ale sistemului făcute de malware.		
	Soluția propusă trebuie să ofere protecție împotriva atacurilor hackerilor prin utilizarea unui firewall cu un sistem de detectare și prevenire a intruziunilor (IDS/IPS) și reguli de activitate în rețea pentru aplicații mai populare atunci când se lucrează în rețele de calculatoare de orice tip, inclusiv în rețelele wireless.		
	Soluția propusă trebuie să includă suport pentru protocolul IPv6.		
	Soluția propusă trebuie să ofere scanarea secțiunilor critice ale computerului ca sarcină de sine stătătoare.		
	Soluția propusă trebuie să încorporeze tehnologia Application Self-Protection: • protejarea împotriva gestionării neautorizate de la distanță a unui serviciu sau aplicație. • protejarea accesului la parametrii aplicației prin setarea unei parole. • prevenirea dezactivării protecției de către malware, criminali sau utilizatori amatori.		
	Soluția propusă trebuie să ofere posibilitatea de a alege ce componente de protecție împotriva amenințărilor să instaleze.		
	Soluția propusă trebuie să includă verificarea și dezinfecția antivirus a fișierelor care au fost împachetate folosind programe precum PKLITE, LZEXE, DIET, EXEPACK etc.		
	Soluția propusă trebuie să includă verificarea și dezinfectarea anti-malware a fișierelor din arhive folosind formatele RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, inclusiv fișierele protejate cu parolă.		
	Soluția propusă trebuie să protejeze împotriva programelor malware încă necunoscute aparținând familiilor înregistrate, pe baza analizei euristice.		
	Soluția propusă trebuie să includă mai multe modalități de a notifica administratorul despre evenimentele importante care au avut loc (notificare prin e-mail, anunț sonor, fereastră pop-up, intrare în jurnal).		
	Soluția propusă trebuie să permită administratorului să creeze un singur program de instalare cu configurația necesară, pentru a fi utilizat de către utilizatori care nu au cunoștințe vaste în IT.		
2.	**Cerințe funcționale: Detectare**		
	Soluția sugerată trebuie să suplimenteze informațiile de verdict din soluția Endpoint Protection cu artefacte ale sistemului despre detectare.		
	Soluția sugerată trebuie să susțină o generare automată de indicatori de amenințare (IoC) după ce apare detectarea cu capacitatea de a aplica acțiuni de răspuns.		
	Soluția trebuie să aibă capacitatea de a forța rularea scanării IoC la toate punctele finale cu aplicații EP instalate.		
	Soluția sugerată trebuie să accepte rularea de scanare IoC conform unui planificator.		
	Soluția sugerată trebuie să accepte importul de IoC terță parte în format OpenIoC pentru utilizarea sa în scanarea rețelei.		
	Soluția sugerată trebuie să accepte conservarea utilizând un set de IoC generat automat, încărcat sau extern (de la terți) pentru a detecta amenințările nedetectate mai devreme.		
	Soluția sugerată trebuie să accepte exportul IoC generat de soluție într-un fișier în format OpenIoC.		
	Cerințe funcționale: Vizibilitate		
	Soluția sugerată trebuie să genereze un card de alertă detaliat legat de amenințarea detectată la punctele finale.		

	Un card de alertă trebuie să includă cel puțin următoarele informații despre amenințarea detectată: - Graficul lanțului de dezvoltare a amenințărilor (kill chain). - Informații despre dispozitivul pe care este detectată amenințarea (nume, adresa IP, adresa MAC, lista de utilizatori, sistemul de operare). - Informații generale despre detectare, inclusiv modul de detectare. - Modificări ale registrului asociate cu detectarea. - Istoricul prezenței fișierului pe dispozitiv. Acțiunile de răspuns efectuate de aplicație.		
	Graficul lanțului de dezvoltare a amenințărilor (kill chain) trebuie să ofere informații vizuale despre obiectele implicate în alertă, de exemplu, despre procesele cheie de pe dispozitiv, conexiuni de rețea, biblioteci, registru etc.		
	Un card de alertă trebuie să prezinte o vizualizare detaliată a artefactelor sistemului și a datelor legate de alertă pentru analiza cauzei principale: - Procesul de reproducere a proceselor - Conexiuni de retea - Modificări de registru - Descărcare obiect Obiecte scăpate etc.		
	Cerințe funcționale: Raspuns		
	Soluția sugerată trebuie să accepte consola de gestionare a formularelor de răspuns „un singur clic".		
	Soluția sugerată trebuie să accepte cel puțin următoarele acțiuni de răspuns pe care un administrator le poate efectua atunci când sunt detectate amenințări:		
	Prevenirea executării obiectului		
	Soluția EDR trebuie să accepte ambele moduri: • înregistrează evenimentele despre încercări de lansare a obiectelor sau deschiderea documentelor care îndeplinesc criteriile de prevenire a execuției, dar nu blochează lansarea sau deschiderea acestor obiecte. • blochează lansarea obiectelor sau deschiderea documentelor care îndeplinesc criteriile normelor de prevenire a execuției.		
	Soluția EDR trebuie să accepte blocarea obiectelor prin hash (MD5 sau SHA256) sau după modelul de cale.		
	Soluția EDR trebuie să accepte blocarea executabilelor, scripturilor și documentelor		
	Soluția EDR trebuie să accepte notificarea utilizatorului despre opțiunea de prevenire		
	Izolarea gazdei.		
	Soluția EDR trebuie să ofere mijloace de izolare a mașinii de restul rețelei în caz de incident de securitate, păstrând în același timp comunicarea controlată cu serverul de administrare și management al agenților.		
	Soluția EDR trebuie să accepte crearea de reguli personalizate de izolare a gazdei (adică adăugarea anumitor resurse de rețea la excludere, de exemplu DNS sau selectarea profilurilor predefinite)		
	Soluția EDR trebuie să accepte readucerea manuală a gazdei online din izolare.		
	Ștergerea obiectul din gazdă sau din grupul de gazde.		
	Obținerea (descărcarea) fișierului de la o gazdă sau un grup de gazde.		
	Încheie un proces pe dispozitiv		
	Punerea în carantină un obiect		
	Soluția sugerată trebuie să suporte recuperarea obiectelor din carantină.		
	Rularea scanarea sistemului		
	Executarea la distanță a unui program / proces / comandă		
	Pornirea scanării IoC pentru un grup de gazde.		
	Soluția sugerată trebuie să suporte consola de gestionare a formularelor de răspuns „un singur clic".		
Administrare centralizată, monitorizare și actualizarea cerințelor software			
	Soluția propusă trebuie să permită instalarea de software anti-malware dintr-un singur pachet de distribuție.		
	Soluția propusă trebuie să aibă profile de instalare personalizabile în funcție de numărul de noduri protejate.		

	Soluția propusă trebuie să accepte adrese IPv6.		
	Soluția propusă trebuie să accepte verificarea în doi pași (autentificare).		
	Soluția propusă trebuie să aibă capacitatea de a citi informații din Active Directory pentru a obține date despre conturile de computer din organizație.		
	Soluția propusă trebuie să includă o consolă web încorporată pentru gestionarea punctelor finale, care nu ar trebui să necesite nicio instalare suplimentară.		
	Consola de management web a soluției propuse ar trebui să fie ușor de utilizat și trebuie să accepte dispozitive cu ecran tactil.		
	Soluția propusă trebuie să distribuie automat conturile de computer pe grup de management dacă în rețea apar computere noi. Acesta trebuie să ofere posibilitatea de a seta regulile de transfer în funcție de adresa IP, tipul sistemului de operare și locația în unitățile organizaționale din Active Directory.		
	Soluția propusă trebuie să prevadă instalarea centralizată, actualizarea și eliminarea software-ului anti-malware, împreună cu configurarea centralizată, administrarea și vizualizarea rapoartelor și informațiilor statistice despre funcționarea acestuia.		
	Soluția propusă trebuie să includă eliminarea centralizată (manuală și automată) a aplicațiilor incompatibile din centrul de administrare.		
	Soluția propusă trebuie să ofere metode flexibile pentru instalarea agentului anti-malware: RPC, GPO, un agent de administrare pentru instalare de la distanță și opțiunea de a crea un pachet de instalare autonom pentru instalare locală.		
	Soluția propusă trebuie să permită instalarea de la distanță a software-ului anti-malware cu cele mai recente baze de date anti-malware.		
	Soluția propusă trebuie să includă actualizarea automată a software-ului anti-malware și a bazelor de date anti-malware.		
	Soluția propusă trebuie să aibă facilități de căutare automată a vulnerabilităților în aplicații și în sistemul de operare pe mașinile protejate.		
	Soluția propusă trebuie să permită gestionarea unei componente care interzice instalarea și/sau rularea programelor.		
	Soluția propusă trebuie să permită gestionarea unei lucrări de control al componentelor cu dispozitive I/O externe.		
	Soluția propusă trebuie să permită gestionarea unei componente care controlează activitatea utilizatorului pe internet.		
	Soluția propusă trebuie să permită testarea actualizărilor descărcate prin intermediul software-ului de administrare centralizat înainte de a le distribui pe mașinile client și livrarea actualizărilor la locurile de muncă ale utilizatorilor imediat după primirea acestora.		
	Soluția propusă trebuie să poată implementa automat protecția infrastructurilor virtuale bazate pe VMware ESXi, Microsoft Hyper-V, platforma de virtualizare Citrix XenServer sau hypervisor.		
	Soluția propusă trebuie să permită crearea unei ierarhii de servere de administrare la un nivel arbitrar și capacitatea de a gestiona centralizat întreaga ierarhie de la nivelul superior.		
	Soluția propusă trebuie să accepte modul de servicii gestionate pentru serverele de administrare, astfel încât instanțe de server de administrare izolate logic să poată fi configurate pentru diferiți utilizatori și grupuri de utilizatori.		
	Soluția propusă trebuie să ofere acces la serviciile cloud ale furnizorului de securitate anti-malware prin intermediul serverului de administrare.		
	Soluția propusă trebuie să includă distribuirea automată a licențelor pe computerele client.		
	Soluția propusă trebuie să poată efectua inventarierea software-ului și hardware-ului instalat pe computerele utilizatorului.		
	Soluția propusă trebuie să aibă un mecanism de notificare pentru a informa utilizatorii despre evenimentele din software-ul și setările anti-malware instalate și pentru a distribui notificări despre evenimente prin e-mail.		
	Soluția propusă trebuie să permită instalarea centralizată a aplicațiilor terțe pe toate computerele sau pe anumite computere.		
	Soluția propusă trebuie să aibă capacitatea de a specifica orice computer din organizație ca centru de retransmitere a actualizărilor și a pachetelor de instalare, pentru a reduce încărcarea rețelei pe sistemul serverului		

	principal de administrare.		
	Soluția propusă trebuie să aibă capacitatea de a specifica orice computer din organizație ca centru pentru redirecționarea evenimentelor agentului anti-malware din grupul selectat de computere client către serverul de administrare centralizat, pentru a reduce încărcarea rețelei pe sistemul serverului principal de administrare. .		
	Soluția propusă trebuie să poată genera rapoarte grafice pentru evenimentele software anti-malware și date despre inventarul hardware și software, licențiere etc.		
	Soluția propusă trebuie să poată exporta rapoarte în fișiere PDF și XML.		
	Soluția propusă trebuie să asigure administrarea centralizată a stocărilor de rezervă și carantina pe toate resursele de rețea în care este instalat software-ul anti-malware.		
	Soluția propusă trebuie să prevadă crearea de conturi interne pentru autentificarea administratorilor pe serverul de administrare.		
	Soluția propusă trebuie să prevadă crearea unei copii de rezervă a sistemului de administrare cu ajutorul instrumentelor integrate ale sistemului de administrare.		
	Soluția propusă trebuie să accepte Windows Failover Cluster.		
	Soluția propusă trebuie să aibă o caracteristică de clustering încorporată.		
	Soluția propusă trebuie să includă o formă de sistem pentru a controla epidemiile virale.		
	Soluția propusă trebuie să includă controlul accesului bazat pe roluri (RBAC), iar acest lucru trebuie să permită replicarea restricțiilor pe serverele de management din ierarhie.		
	Serverul de management al soluției propuse trebuie să includă roluri de securitate predefinite pentru auditor, supervizor și ofițer de securitate.		
	Soluția propusă trebuie să aibă capacitatea de a gestiona dispozitivele mobile prin comenzi de la distanță.		
	Soluția propusă trebuie să aibă capacitatea de a șterge actualizările descărcate.		
	Soluția propusă trebuie să permită gestionarea actualizărilor Serverului de administrare din interfața aplicației.		
	Soluția propusă trebuie să ofere posibilitatea de a selecta un agent de actualizare pentru computerele client pe baza analizei rețelei.		
	Soluția propusă trebuie să arate clar informații despre distribuția vulnerabilităților între computerele gestionate.		
	Interfața de server de management a soluției propuse trebuie să accepte limba arabă.		
	Serverul de management al soluției propuse trebuie să mențină un istoric de revizuire a politicilor, sarcinilor, pachetelor, grupurilor de management create, astfel încât modificările aduse unei anumite politici/sarcini să poată fi revizuite.		
	Serverul de management al soluției propuse trebuie să aibă funcționalitate pentru a crea mai multe profiluri în cadrul unei politici de protecție cu diferite setări de protecție care pot fi active simultan pe un singur/mai multe dispozitive pe baza următoarelor reguli de activare: • Starea dispozitivului • Etichete • Active directory • Proprietari de dispozitive • Hardware		
	Soluția propusă trebuie să accepte următoarele canale de livrare a notificărilor: • E-mail • Syslog • SMS • SIEM		
	Soluția propusă trebuie să aibă capacitatea de a defini un interval de adrese IP, pentru a limita traficul clienților către serverul de management în funcție de timp și viteză.		
	Soluția propusă trebuie să aibă capacitatea de a efectua inventariere pe scripturi și fișiere .dll.		
	Soluția propusă trebuie să aibă capacitatea de a eticheta/marca computere pe baza: • Atributele rețelei o Nume		

	○ Domeniu și/sau sufix de domeniu ○ Adresa IP ○ Adresa IP către serverul de management • Locația în Active Directory ○ Unitate organizationala ○ Grup • Sistem de operare ○ Tip și versiune ○ Arhitectură ○ Numărul pachetului de service • Arhitectură virtuală • Registrul aplicațiilor ○ Numele aplicatiei ○ Versiunea aplicației ○ Producător		
	Soluția propusă trebuie să aibă capacitatea de a crea/defini setări în funcție de locația unui computer în rețea, mai degrabă decât de grupul căruia îi aparține în serverul de management.		
	Soluția propusă trebuie să aibă funcționalitatea de a adăuga un mediator de conexiune unidirecțională între serverul de management și punctul final care se conectează prin internet/rețeaua publică.		
	Soluția propusă trebuie să permită administratorului să definească setări restricționate în setările de politică/profil, astfel încât o sarcină de scanare a virușilor să poată fi declanșată automat atunci când un anumit număr de viruși este detectat într-un interval de timp definit. Valorile pentru numărul de viruși și intervalul de timp trebuie să fie configurabile.		
	Soluția propusă trebuie să aibă un tablou de bord personalizabil care să genereze și să afișeze statistici în timp real pentru punctele finale.		
	Soluția propusă trebuie să permită administratorului să personalizeze rapoartele.		
	Soluția propusă trebuie să aibă funcționalitatea de a detecta mașinile virtuale nepersistente și de a le șterge automat și datele aferente de pe serverul de management atunci când este oprită.		
	Soluția propusă trebuie să permită administratorului să stabilească o perioadă de timp după care un computer care nu este conectat la serverul de management, datele aferente acestuia sunt șterse automat de pe server.		
	Soluția propusă trebuie să permită administratorului să creeze categorii/grupuri de aplicații pe baza: • Numele aplicației • Calea aplicației • Metadatele aplicației • Certificatul aplicație digitale • Categorii de aplicații predefinite ale furnizorului • SHA • Calculatoare de referință pentru a permite/interzice execuția lor pe punctele finale.		
	Soluția propusă trebuie să permită administratorului să definească diferite condiții de schimbare a stării pentru grupuri de puncte finale din serverul de management.		
	Soluția propusă trebuie să permită administratorului să adauge instrumente personalizate/terțe de gestionare a punctelor finale în serverul de management.		
	Soluția propusă trebuie să aibă o funcție/modul încorporat pentru a colecta de la distanță datele necesare pentru depanarea de la punctele finale, fără a necesita acces fizic.		
	Soluția propusă trebuie să permită administratorului să creeze un tunel de conexiune între un dispozitiv client la distanță și serverul de management dacă portul folosit pentru conectarea la serverul de management nu este disponibil pe dispozitiv.		
	Soluția propusă trebuie să aibă o funcționalitate încorporată pentru a se conecta de la distanță la punctul final utilizând tehnologia de partajare a desktopurilor Windows. În plus, soluția trebuie să fie capabilă să mențină auditarea acțiunilor administratorului în timpul sesiunii.		
	Soluția propusă trebuie să dispună de o funcție care să permită crearea unei structuri de grupuri de administrare utilizând ierarhia Grupuri, pe baza următoarelor date: • structuri de domenii și grupuri de lucru Windows		

	• structuri ale grupurilor Active Directory • conținutul unui fișier text creat manual de către administrator		
	Soluția propusă trebuie să fie capabilă să recupereze informații despre echipamentele detectate în timpul unui sondaj de rețea. Inventarul rezultat trebuie să acopere toate echipamentele conectate la rețeaua organizației. Informațiile despre echipamente trebuie să se actualizeze după fiecare nouă interogare a rețelei. Lista echipamentelor detectate ar trebui să acopere următoarele: • dispozitive • dispozitive mobile • dispozitive de rețea • dispozitive virtuale • Componente OEM • perifericele computerului • dispozitivele conectate • telefoane VoIP • depozite de rețea Administratorul trebuie să poată adăuga manual noi dispozitive la lista de echipamente sau să editeze informații despre echipamentele care există deja în rețea. Funcționalitatea „Device is Written Off" trebuie să fie disponibilă, astfel încât astfel de dispozitive să nu fie afișate în lista de echipamente.		
	Soluția propusă trebuie să încorporeze un singur agent de distribuție/releu pentru a suporta cel puțin 10.000 de puncte finale pentru livrarea de protecție, actualizări, patch-uri și pachete de instalare către site-uri la distanță.		
	Soluția propusă trebuie să încorporeze un singur agent de distribuție/releu pentru a transmite/transferă sau proxy cererile de reputație a amenințărilor de la punctele finale către serverul de management.		
	Soluția propusă trebuie să accepte descărcarea fișierelor diferențiate, mai degrabă decât pachetele complete de actualizare.		
	Soluția propusă trebuie să accepte OPEN API și să includă linii directoare pentru integrarea cu sisteme externe terțe.		
	Soluția propusă trebuie să includă un instrument încorporat pentru a efectua diagnostice de la distanță și a colecta jurnale de depanare fără a necesita acces fizic la computer.		
	Soluția propusă trebuie să includă Controlul accesului bazat pe roluri (RBAC) cu roluri predefinite personalizabile.		
	Serverul de management principal/primar/părinte al soluției propuse trebuie să poată transmite actualizări și servicii de reputație în cloud.		
	Rapoartele soluției propuse trebuie să includă informații despre fiecare amenințare și tehnologia care a detectat-o.		
	Raportul privind soluția propusă trebuie să includă detalii despre componentele de protecție a punctelor terminale care sunt sau nu sunt instalate pe dispozitivele client, indiferent de profilul de protecție aplicat/existent pentru aceste dispozitive.		
	Serverul de management primar al soluției propuse trebuie să poată prelua informații detaliate de raportare privind starea tehnică etc. a punctelor finale gestionate de la serverele de management secundare.		
	Soluția propusă trebuie să includă opțiunea pentru client fie de a implementa o consolă de management locală, fie de a utiliza consola de management bazată pe cloud furnizată de furnizor.		
	Soluția propusă trebuie să se poată integra cu consola de management bazată pe cloud a furnizorului pentru gestionarea punctelor finale fără costuri suplimentare.		
	Soluția propusă trebuie să permită migrarea rapidă de la consola de management locală la consola de management bazată pe cloud a furnizorului.		
	Soluția propusă trebuie să includă suport pentru implementarea bazată pe cloud prin: • Amazon Web Services • Microsoft Azure		
	Soluția propusă trebuie să ofere mecanisme de actualizare a bazei de date anti-malware, inclusiv: • Modalități multiple de actualizare, inclusiv canale de comunicare globale prin protocolul HTTPS, resurse partajate în rețeaua locală		

	și suporturi detașabile. • **Verificarea integrității și autenticității actualizărilor prin intermediul unei semnături digitale electronice.**		
	Soluția propusă trebuie să accepte Single Sign On (SSO) folosind NTLM și Kerberos.		
	Administrare și raportare EDR		
	Soluția sugerată trebuie să accepte comunicarea securizată între consola de management și punctele finale cu agentul EDR		
	Soluția sugerată trebuie să accepte gestionarea agentului EDR prin interfața de linie de comandă		
	Soluția sugerată trebuie să aibă caracteristică/modul încorporat pentru a colecta datele necesare pentru depanare, fără a necesita un acces fizic la punctul final.		
	Aplicația EDR trebuie să aibă un mecanism de autoapărare pentru a preveni modificarea intrărilor sale de fișiere/componente de sistem etc.		
	Soluția trebuie să permită crearea de conturi cu roluri diferite, utilizate pentru a administra soluția, pentru a monitoriza alertele sau pentru a revizui modificările. Soluția trebuie să fie capabilă să trimită notificări prin e-mail atunci când sunt generate anumite tipuri de alerte de securitate.		
	Cerințe pentru documentația soluției. O documentație pentru software-ul **EDR, inclusiv instrumentele de administrare, trebuie să includă cel puțin un ajutor online pentru administratori.**		
	Suport local de la Ofertant; Lucrările de instalare, configurare, punerea în funcțiune a soluției și asigurarea suportului la definirea/configurarea politicilor inițiale Training Beneficiarului - min. 3 persoane; **Furnizarea documentației de instalare, (passport system și sistemul de administrare;** **Configurare, restabilire a serviciului oferit + Training + documentația,** trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă; Servicii de intervenție în mod continuu 24h/zi – 7zile/săptămână pentru alerte cibernetice ce conțin următoarele activități: **- Efectuarea interogări de bază pentru a aduna informații suplimentare legate de incidentul de securitate** - Echipa de support local se va conecta la consola de management a acestuia și va actualiza progresul / rezolvarea incidentelor de Securitate - Echipa de support local va investiga evenimentele de securitate și va escalada la nivelul 2 de intervenție **- Echipa de support local va asigura gestionarea și prioritizarea alertelor, gestionarea răspunsurilor la incidente și escaladarea acestora** - Echipa de support local va asista personalul superior al utilizatorilor finali în probleme de securitate, daca va fi necesar. - Echipa de support local va valida atacurile, evalua impactul, recomanda contramăsurile și va lucra în implementarea soluției de mitigare și răspuns. **- Echipa de support local va emite recomandări de ajustare a produsului/ tehnologiei de securitate către IS Posta Moldovei** - Echipa de support local va colabora cu părțile interesate ale Clientului pentru a asigura rezolvarea în timp util a problemelor de securitate ridicate și critice - Echipa de support locală va prioritiza și gestiona escaladarea **incidentelor validate catre IS Posta Moldovei** **Autorizarea de la producător - Manufacture Authorization Letter.**		

Șef Direcției Tehnologii Informaționale **Victor TVERDOHLEB**