



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

Anexa nr. 22
la Documentația standard pentru
procedura de achiziție, cu nr. de
identificare în SIA RSAP Mtender:
ocds-b3wdp1-MD-1691570951766

SPECIFICAȚII TEHNICE

Numărul procedurii de achiziție: MTender ID: ocds-b3wdp1-MD-1691570951766

Denumirea procedurii de achiziție: **Software Antivirus**

Denumirea bunurilor	Modelul articolului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Software Antivirus	Bitdefender GravityZone Business Security Enterprise (Ultra), <i>(inclusiv serviciile de instalare, servicii de suport și training a personalului)</i>	România	România		Produs ofertă este Bitdefender GravityZone Business Security Enterprise (Ultra) ce reprezintă o platformă integrată pentru managementul securității, gândită ca o soluție modulară. Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management: <ul style="list-style-type: none">• Protecție stații și servere fizice și virtualizate;• Protecție și securitate pentru telefoanele mobile de tip smartphone cu sistem de operare iOS sau Android;• Protecție și securitate pentru serverele email Microsoft Exchange;• Serviciu de corelare și răspuns la evenimente de tip EDR („endpoint detection and response”).	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				<p>1. Soluția propusă trebuie să accepte sistemele de operare de mai jos:</p> <ul style="list-style-type: none">• 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 for Workstations / Education / Enterprise• Windows 11 <p>Servere</p> <ul style="list-style-type: none">• Windows Small Business Server 2011 Essentials / Standard (64-bit)• Windows MultiPoint Server 2011 (64-bit)• 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 <p>Microsoft Terminal Servere</p> <ul style="list-style-type: none">• Microsoft Remote Desktop Services based on Windows Server 2008 R2 SP1• Microsoft Remote Desktop Services based on Windows Server 2012• Microsoft Remote Desktop Services based on Windows Server 2012 R2	<p>1. Soluția propusă acceptă sistemele de operare de mai jos:</p> <ul style="list-style-type: none">• 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 for Workstations / Education / Enterprise• Windows 11 <p>Servere</p> <ul style="list-style-type: none">• Windows Small Business Server 2011 Essentials / Standard (64-bit)• Windows MultiPoint Server 2011 (64-bit)• 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 <p>Microsoft Terminal Servere</p> <ul style="list-style-type: none">• Microsoft Remote Desktop Services based on Windows Server 2008 R2 SP1• Microsoft Remote Desktop Services based on Windows Server 2012• Microsoft Remote Desktop Services based on Windows Server 2012 R2	
--	--	--	--	---	--	--



“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

				<ul style="list-style-type: none">• Microsoft Remote Desktop Services based on Windows Server 2016• Microsoft Remote Desktop Services based on Windows Server 2019 <p>Sisteme de operare pe 32 biți:</p> <ul style="list-style-type: none">• CentOS 6.7 și versiuni ulterioare• Debian GNU / Linux 9.4 și versiuni ulterioare• Debian GNU / Linux 10.1 și versiuni ulterioare• Linux Mint 19 și versiuni ulterioare• Mageia 4• Red Hat Enterprise Linux 6.7 și versiuni ulterioare• ALT Education 9• ALT Workstation 9• ALT Server 9 <p>Sisteme de operare pe 64 biți:</p> <ul style="list-style-type: none">• AlterOS 7.5 și versiuni ulterioare• Amazon Linux 2• Astra Linux Common Edition (actualizare operațională 2.12).• Astra Linux Special Edition RUSB.10015-01 (actualizare operațională 1.5)• Astra Linux Special Edition RUSB.10015-01 (actualizare operațională 1.6)• Astra Linux Special Edition RUSB.10015-16 (versiune 1) (actualizare operațională 1.6)• CentOS 6.7 și versiuni ulterioare• CentOS 7.2 și versiuni ulterioare• CentOS 8.0 și versiuni ulterioare	<ul style="list-style-type: none">• Microsoft Remote Desktop Services based on Windows Server 2016• Microsoft Remote Desktop Services based on Windows Server 2019 <p>Sisteme de operare pe 32 biți:</p> <ul style="list-style-type: none">• CentOS 6.7 și versiuni ulterioare• Debian GNU / Linux 9.4 și versiuni ulterioare• Debian GNU / Linux 10.1 și versiuni ulterioare• Linux Mint 19 și versiuni ulterioare• Mageia 4• Red Hat Enterprise Linux 6.7 și versiuni ulterioare• ALT Education 9• ALT Workstation 9• ALT Server 9 <p>Sisteme de operare pe 64 biți:</p> <ul style="list-style-type: none">• AlterOS 7.5 și versiuni ulterioare• Amazon Linux 2• Astra Linux Common Edition (actualizare operațională 2.12).• Astra Linux Special Edition RUSB.10015-01 (actualizare operațională 1.5)• Astra Linux Special Edition RUSB.10015-01 (actualizare operațională 1.6)• Astra Linux Special Edition RUSB.10015-16 (versiune 1) (actualizare operațională 1.6)• CentOS 6.7 și versiuni ulterioare• CentOS 7.2 și versiuni ulterioare• CentOS 8.0 și versiuni ulterioare	
--	--	--	--	---	---	--



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

			<ul style="list-style-type: none">• Debian GNU / Linux 9.4 și versiuni ulterioare• Debian GNU / Linux 10.1 și versiuni ulterioare• EulerOS V2.0SP2 2.2.17• EulerOS V2.0SP5 2.5.6• Linux Mint 19 și versiuni ulterioare• Linux Mint 20.1 și versiuni ulterioare• openSUSE Leap 15.0 și versiuni ulterioare• Oracle Linux 7.3 și versiuni ulterioare• Oracle Linux 8.0 și versiuni ulterioare• Pardus OS 19.1• Red Hat Enterprise Linux 6.7 și versiuni ulterioare• Red Hat Enterprise Linux 7.2 și versiuni ulterioare• Red Hat Enterprise Linux 8.0 și 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 <p>Sisteme de operare MAC OS:</p> <ul style="list-style-type: none">• macOS 10.14 - 12	<ul style="list-style-type: none">• Debian GNU / Linux 9.4 și versiuni ulterioare• Debian GNU / Linux 10.1 și versiuni ulterioare• EulerOS V2.0SP2 2.2.17• EulerOS V2.0SP5 2.5.6• Linux Mint 19 și versiuni ulterioare• Linux Mint 20.1 și versiuni ulterioare• openSUSE Leap 15.0 și versiuni ulterioare• Oracle Linux 7.3 și versiuni ulterioare• Oracle Linux 8.0 și versiuni ulterioare• Pardus OS 19.1• Red Hat Enterprise Linux 6.7 și versiuni ulterioare• Red Hat Enterprise Linux 7.2 și versiuni ulterioare• Red Hat Enterprise Linux 8.0 și 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 <p>Sisteme de operare MAC OS:</p> <ul style="list-style-type: none">• macOS 10.14 - 12	
--	--	--	--	--	--



“RTS ONE” S.R.L.

<https://rts.md>

+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				2. Soluția propusă trebuie să suporte următoarele platforme virtuale: <ul style="list-style-type: none">VMware Workstation 16.1.1 ProActualizarea VMware ESXi 7.0 2aMicrosoft Hyper-V Server 2019Citrix Virtual Apps and Desktops 7 2103Citrix Provisioning 2012Citrix Hypervisor 8.2 LTSR	2. Soluția propusă suportă următoarele platforme virtuale: <ul style="list-style-type: none">VMware Workstation 16.1.1 ProActualizarea VMware ESXi 7.0 2aMicrosoft Hyper-V Server 2019Citrix Virtual Apps and Desktops 7 2103Citrix Provisioning 2012Citrix 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).	3. Soluția propusă suportă protecția celor mai recente versiuni de sisteme de operare pe toate platformele (Windows, Linux, MacOS, iOS, Android).	
				Cerințe funcționale	Cerințe funcționale	
				2.1. Cerințe funcționale: Antivirus	2.1. Cerințe funcționale: Antivirus	
				Soluția propusă trebuie să fie capabilă să detecteze următoarele tipuri de amenințări: <ul style="list-style-type: none">Virusi (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 este capabilă să detecteze următoarele tipuri de amenințări: <ul style="list-style-type: none">Virusi (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 accepte Interfața de scanare anti-malware (AMSI).	Soluția propusă include Interfața de scanare anti-malware (AMSI).	
				Soluția propusă trebuie să aibă capacitatea de a se integra cu Windows Defender Security Center.	Soluția propusă are capacitatea de a se integra cu Windows Defender Security Center.	
				Soluția propusă trebuie să accepte subsistemul Windows Linux.	Soluția propusă acceptă subsistemul Windows Linux.	
				Soluția propusă trebuie să ofere tehnologii de protecție de ultimă generație. De exemplu:	Soluția propusă oferă tehnologii de protecție de ultimă generație. De exemplu: <ul style="list-style-type: none">protecție împotriva amenințărilor fără fișiere	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

			<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 Scanare memorie pentru stațiile de lucru Windows.	Soluția propusă oferă Scanare memorie pentru stațiile de lucru Windows.	
			Soluția propusă trebuie să ofere Scanare memorie Kernel pentru stațiile de lucru Linux.	Soluția propusă oferă 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 hard disk pentru mașinile cu resurse limitate.	Soluția propusă oferă posibilitatea de a trece la modul cloud pentru protecția împotriva amenințărilor, scăzând utilizarea RAM și a unității de hard disk 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 are 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 include 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 oferă analiză comportamentală bazată pe ML.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				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 oferă 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 sprijine 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 se poate integra 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 și Linux, prin consola sa de management.	Soluția propusă include capacitatea de a configura și gestiona setările paravanului de protecție încorporate în sistemele de operare Windows Server și Linux, prin consola sa de management.	
				Soluția propusă trebuie să ofere comenzi pentru aplicații și dispozitive pentru stațiile de lucru Windows.	Soluția propusă oferă comenzi pentru aplicații și dispozitive pentru stațiile de lucru Windows.	
				Soluția de protecție propuse pentru servere și stații de lucru trebuie să includă o componentă dedicată pentru protecție împotriva activității virusului ransomware/criptor pe resursele partajate.	Soluția de protecție propusă pentru servere și stații de lucru include o componentă dedicată pentru protecție împotriva activității virusului ransomware/criptor pe resursele partajate.	
				Soluția propusă trebuie, la detectarea activității de tip ransomware/criptor, să blocheze automat computerul atacator pentru un interval specificat și să genereze informații despre IP-ul computerului atacator și marca temporală și tipul de amenințare.	Soluția propusă, la detectarea activității de tip ransomware/criptor, blochează automat computerul atacator pentru un interval specificat și generează informații despre IP-ul computerului atacator și marca temporală și tipul de amenințare.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să ofere o listă predefinită de excluderi de scanare pentru aplicațiile și serviciile Microsoft.	Soluția propusă oferă o listă predefinită de excluderi de scanare pentru aplicațiile și serviciile Microsoft.	
				Soluția propusă ar trebui să sprijine instalarea de protecție a punctelor terminale pe servere fără a fi necesară repornirea.	Soluția propusă permite instalarea de protecție a punctelor terminale pe servere fără a fi necesară repornirea.	
				Soluția propusă trebuie să permită următoarele pentru puncte finale: <ul style="list-style-type: none">• Scanare manuală• Scanare la acces• Scanare la cerere• Scanarea fișierelor comprimate• Scanați fișiere, foldere și unități individuale• Blocarea și scanarea scripturilor• Garda Registrului• Protecție la depășirea tamponului• Scanare în fundal/inactiv• Scanarea unității amovibile la conexiunea cu sistemul• Capacitatea de a detecta și de a bloca gazdele neîncrezătoare la detectarea activităților asemănătoare criptării pe resursele partajate de server.	Soluția propusă permite următoarele puncte finale: <ul style="list-style-type: none">• Scanare manuală• Scanare la acces• Scanare la cerere• Scanarea fișierelor comprimate• Scanați fișiere, foldere și unități individuale• Blocarea și scanarea scripturilor• Garda Registrului• Protecție la depășirea tamponului• Scanare în fundal/inactiv• Scanarea unității amovibile la conexiunea cu sistemul• Soluția de antivirus propusă are capacitatea de a detecta și de a bloca gazdele neîncrezătoare la detectarea activităților asemănătoare criptării pe resursele partajate de server.	
				Soluția propusă ar trebui să fie protejată cu parolă pentru a preveni oprirea/închiderea procesului AV și pentru autoprotecție, indiferent de nivelul de autorizare a utilizatorului pe sistem.	Soluția propusă este protejată cu parolă pentru a preveni oprirea/închiderea procesului AV și pentru autoprotecție, indiferent de nivelul de autorizare a utilizatorului pe sistem.	
				Soluția propusă trebuie să aibă baze de date de reputație atât locală, cât și globală.	Soluția propusă dispune de baze de date de reputație atât locală, cât și globală.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să poată scana traficul HTTPS, HTTP și FTP împotriva virușilor și a programelor spion sau a oricărui alt malware.	Soluția propusă poate scana traficul HTTPS, HTTP și FTP împotriva virușilor și a programelor spion sau a oricărui alt malware.	
				Soluția propusă trebuie să includă un firewall personal capabil, cel puțin să: <ul style="list-style-type: none">• Blocheze activărilor de rețea ale aplicațiilor în funcție de clasificarea lor.• Blocheze /permite anumitor pachete, protocoale, adrese IP, porturi și direcție de trafic.• Aduge automat și manual a subrețelelor de rețea și modifice permisiunile de activitate în rețea.	Soluția propusă include un firewall personal capabil, să: <ul style="list-style-type: none">• Blocheze activărilor de rețea ale aplicațiilor în funcție de clasificarea lor.• Blocheze /permite anumitor pachete, protocoale, adrese IP, porturi și direcție de trafic.• Soluția propusă permite adăugarea automată și manuală a subrețelelor de rețea și modifice permisiunile de activitate în rețea.	
				Soluția propusă trebuie să împiedice conectarea dispozitivelor USB reprogramate care emulează tastaturi și să permită controlul utilizării tastaturilor de pe ecran pentru autorizare.	Soluția propusă poate împiedica conectarea dispozitivelor USB reprogramate care emulează tastaturi și permite controlul utilizării tastaturilor de pe ecran pentru autorizare.	
				Soluția propusă trebuie să fie capabilă să blocheze atacurile de rețea și să raporteze sursa infecției.	Soluția propusă este capabilă să blocheze atacurile de rețea și să raporteze sursa infecției.	
				Soluția propusă trebuie să aibă stocare locală pe punctele finale pentru a păstra copii ale fișierelor care au fost șterse sau modificate în timpul dezinfectării. Aceste fișiere trebuie să fie stocate într-un format specific care să asigure că nu reprezintă nicio amenințare.	Soluția propusă dispune de stocare locală pe punctele finale pentru a păstra copii ale fișierelor care au fost șterse sau modificate în timpul dezinfectării. Aceste fișiere sunt stocate într-un format specific care va asigura că nu reprezintă nicio amenințare.	
				Soluția propusă trebuie să aibă o abordare proactivă pentru a împiedica malware-ul să exploateze vulnerabilitățile existente pe servere și stații de lucru.	Soluția propusă are o abordare proactivă pentru a împiedica malware-ul să exploateze vulnerabilitățile existente pe servere și stații de lucru.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să suporte tehnologia AM-PPL (Anti-Malware Protected Process Light) pentru protecție împotriva acțiunilor rău intenționate.	Soluția propusă suportă tehnologia AM-PPL (Anti-Malware Protected Process Light) pentru protecție împotriva acțiunilor rău intenționate.	
				Soluția propusă trebuie să includă protecție împotriva atacurilor care exploatează vulnerabilitățile din protocolul ARP pentru a falsifica adresa MAC a dispozitivului.	Soluția propusă include protecție împotriva atacurilor care exploatează vulnerabilitățile din protocolul ARP pentru a falsifica adresa MAC a dispozitivului.	
				Soluția propusă trebuie să ofere funcționalitate Anti-Bridging pentru stațiile de lucru Windows pentru a preveni punțile neautorizate către rețeaua internă care ocolesc instrumentele de protecție a perimetrului. Administratorii ar trebui să poată interzice stabilirea de conexiuni simultane prin cablu, Wi-Fi și modem.	Soluția propusă oferă funcționalitate Anti-Bridging (denumită de producătorul Bitdefender Bridge mode) pentru stațiile de lucru Windows pentru a preveni punțile neautorizate către rețeaua internă care ocolesc instrumentele de protecție a perimetrului. Administratorii ar trebui să poată interzice stabilirea de conexiuni simultane prin cablu, Wi-Fi și modem.	
				Soluția propusă trebuie să includă o componentă dedicată pentru scanarea conexiunilor criptate.	Soluția propusă include o componentă dedicată pentru scanarea conexiunilor criptate.	
				Soluția propusă trebuie să poată decripta și scana traficul de rețea transmis prin conexiuni criptate suportate de următoarele protocoale; SSL 3.0, TLS 1.0, TLS1.1, TLS1.2, TLS 1.3.	Soluția propusă poate decripta și scana traficul de rețea transmis prin conexiuni criptate suportate de următoarele protocoale; SSL 3.0, TLS 1.0, TLS1.1, TLS1.2, TLS 1.3.	
				Soluția 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 și nu trebuie să fie partajată cu alte puncte finale.	Soluția propusă are capacitatea de a exclude automat resursele web atunci când apare o eroare de scanare în timpul efectuării unei scanări a conexiunii criptate. Această excludere este unică pentru gazdă și nu este partajată cu alte puncte finale.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să includă funcționalitate de ștergere de la distanță a datelor de pe punctul final (pentru stații de lucru).	Soluția propusă include funcționalitatea de ștergere de la distanță a datelor de pe punctul final (pentru stații de lucru).	
				Soluția propusă trebuie să aibă următoarele funcționalități de ștergere a datelor de la distanță: <ul style="list-style-type: none">• În modul silentios• Pe hard disk-uri și unități amovibile• Pentru toate conturile de utilizator de pe computer	Soluția propusă are următoarele funcționalități de ștergere a datelor de la distanță: <ul style="list-style-type: none">• În modul silentios• Pe hard disk-uri și unități amovibile Pentru toate conturile de utilizator de pe computer	
				Funcționalitatea de ștergere a datelor de la distanță a soluției propuse trebuie să accepte următoarele moduri: <ul style="list-style-type: none">• Ștergerea imediată a datelor• Ștergerea datelor amânată• Funcționalitatea de ștergere a datelor de la distanță a soluției propuse trebuie să accepte următoarele metode de ștergere a datelor:<ul style="list-style-type: none">• Ștergerea folosind resursele de operare - fișierele sunt șterse, dar nu sunt trimise la coșul de reciclare• Ștergerea completă, fără recuperare - făcând datele practic imposibil de restabilit după ștergere	Soluția propusă dispune de funcționalitatea de ștergere a datelor de la distanță a soluției propuse care acceptă următoarele moduri: <ul style="list-style-type: none">• Ștergerea imediată a datelor• Ștergerea datelor amânată• Soluția propusă dispune de funcționalitatea de ștergere a datelor de la distanță a soluției propuse care acceptă următoarele metode de ștergere a datelor:<ul style="list-style-type: none">• Ștergerea folosind resursele de operare - fișierele sunt șterse, dar nu sunt trimise la coșul de reciclare• Ștergerea completă, fără recuperare - făcând datele practic imposibil de restabilit după ștergere	
				Soluția propusă trebuie să includă funcționalitate pentru a șterge automat datele dacă nu există nicio conexiune la serverul de management al punctelor finale.	Soluția propusă include funcționalitate pentru a șterge automat datele dacă nu există nicio conexiune la serverul de management al punctelor finale.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să accepte detectarea bazată pe semnătură, pe lângă cele asistate de cloud și euristică.	Soluția propusă poate detecta pe bază pe semnătură, pe lângă cele asistate de cloud și euristică.	
				Soluția propusă ar trebui să aibă capacitatea de a lansa o alertă pentru, curăța și șterge o amenințare detectată.	Soluția propusă are capacitatea de a lansa o alertă pentru, curăța și șterge o amenințare detectată.	
				Soluția propusă ar trebui să aibă capacitatea de a accelera sarcinile de scanare, omitând acele obiecte care nu s-au schimbat de la scanarea anterioară.	Soluția propusă dispune de capacitatea de a accelera sarcinile de scanare, omitând acele obiecte care nu s-au schimbat de la scanarea anterioară.	
				Soluția propusă ar trebui să aibă capacitatea de a prioritiza sarcinile de scanare personalizate și la cerere pentru stațiile de lucru Linux.	Soluția propusă dispune de capacitatea de a prioritiza sarcinile de scanare personalizate și la cerere pentru stațiile de lucru Linux.	
				Soluția propusă trebuie să permită administratorului să excludă de la scanare fișierele/directoarele/aplicațiile/certIFICATELE digitale specificate, fie la acces (protecție în timp real), fie în timpul scanărilor la cerere.	Soluția propusă permite administratorului să excludă de la scanare fișierele/directoarele/aplicațiile/certIFICATELE digitale specificate, fie la acces (protecție în timp real), fie în timpul scanărilor la cerere.	
				Soluția propusă ar trebui să includă funcționalitatea de izolare a computerelor infectate.	Soluția propusă include funcționalitatea de izolare a computerelor infectate.	
				Soluția propusă trebuie să scaneze automat unitățile amovibile pentru malware atunci când sunt atașate la orice punct final. Controlul scanării ar trebui să se bazeze pe dimensiunea unității.	Soluția propusă poate să scaneze automat unitățile amovibile pentru malware atunci când sunt atașate la orice punct final. Controlul scanării se bazează pe dimensiunea unității.	
				Soluția propusă trebuie să poată bloca utilizarea dispozitivelor de stocare USB sau să permită accesul numai la dispozitivele permise și să permită accesul de citire/scriere numai utilizatorilor de domeniu, pentru a reduce furtul de date și pentru a aplica politicile de blocare.	Soluția propusă poate bloca utilizarea dispozitivelor de stocare USB sau permiterea accesului numai la dispozitivele permise și permite accesul de citire/scriere numai utilizatorilor de domeniu, pentru a reduce furtul de date și pentru a aplica politicile de blocare.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să poată face diferența între dispozitivele de stocare USB, imprimante, telefoane mobile și alte periferice.	Soluția propusă poate să facă diferența între dispozitivele de stocare USB, imprimante, telefoane mobile și alte periferice.	
				Soluția propusă trebuie să poată înregistra operațiunile de fișiere (Scrie și ștergere) pe dispozitivele de stocare USB. Acest lucru nu ar trebui să necesite nicio licență sau componentă suplimentară care să fie instalată pe punctul final.	Soluția propusă poate înregistra operațiunile de fișiere (Scrie și ștergere) pe dispozitivele de stocare USB. Aceasta nu necesită nicio licență sau componentă suplimentară care să fie instalată pe punctul final.	
				Soluția propusă trebuie să aibă capacitatea de a bloca execuția oricărui executabil de pe dispozitivul de stocare USB.	Soluția propusă are capacitatea de a bloca execuția oricărui executabil de pe dispozitivul de stocare USB.	
				Soluția propusă trebuie să aibă capacitatea de a bloca/permite accesul utilizatorilor la resursele web în funcție de site-uri web, tip de conținut, utilizator și ora din zi.	Soluția propusă are capacitatea de a bloca/permite accesul utilizatorilor la resursele web în funcție de site-uri web, tip de conținut, utilizator și ora din zi.	
				Soluția propusă trebuie să aibă o categorie de detectare specifică pentru a bloca bannerele site-ului.	Soluția propusă dispune de o categorie de detectare specifică pentru a bloca bannerele site-ului.	
				Soluția propusă trebuie să ofere posibilitatea de a configura rețele Wi-Fi pe baza numelui rețelei, tipului de autentificare, tipului de criptare, astfel încât acestea să poată fi utilizate ulterior pentru a bloca sau a permite conexiunile Wi-Fi.	Soluția propusă oferă posibilitatea de a configura rețele Wi-Fi pe baza numelui rețelei, tipului de autentificare, tipului de criptare, astfel încât acestea pot fi utilizate ulterior pentru a bloca sau a permite conexiunile Wi-Fi.	
				Soluția propusă trebuie să accepte politici bazate pe utilizator pentru controlul dispozitivelor, web și aplicațiilor.	Soluția propusă acceptă politici bazate pe utilizator pentru controlul dispozitivelor, web și aplicațiilor.	
				Soluția propusă ar trebui să permită în mod specific blocarea următoarelor dispozitive: <ul style="list-style-type: none">• Bluetooth• Dispozitive mobile• Modemuri externe	Soluția propusă permite în mod specific blocarea următoarelor dispozitive: <ul style="list-style-type: none">• Bluetooth• Dispozitive mobile• Modemuri externe	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				<ul style="list-style-type: none">• CD/DVD-uri• Camere și scanere• MTP-uri• Și transferul de date pe dispozitive mobile	<ul style="list-style-type: none">• CD/DVD-uri• Camere și scanere• MTP-uri• Și transferul de date pe dispozitive mobile	
				Soluția propusă ar trebui să includă integrarea în cloud, pentru a oferi cele mai rapide actualizări posibile despre malware și potențiale amenințări. Soluția propusă trebuie să aibă capacitatea de a gestiona drepturile de acces ale utilizatorilor pentru operațiunile de citire și scriere pe CD-uri/DVD-uri, dispozitive de stocare detașabile și dispozitive MTP.	Soluția propusă include integrarea în cloud, pentru a oferi cele mai rapide actualizări posibile despre malware și potențiale amenințări. Soluția propusă are capacitatea de a gestiona drepturile de acces ale utilizatorilor pentru operațiunile de citire și scriere pe CD-uri/DVD-uri, dispozitive de stocare detașabile și dispozitive MTP.	
				Soluția propusă trebuie să includă filtrarea firewall după adresa locală, interfața fizică și Time-To-Live (TTL) de pachete.	Soluția propusă include filtrarea firewall după adresa locală, interfața fizică și Time-To-Live (TTL) de pachete.	
				Soluția propusă trebuie să permită administratorului să monitorizeze utilizarea de către aplicație a porturilor personalizate/aleatorie după lansare.	Soluția propusă permite administratorului să monitorizeze utilizarea de către aplicație a porturilor personalizate/aleatorie după lansare.	
				Soluția propusă trebuie să accepte blocarea aplicațiilor interzise (Deny-List) pentru a fi lansate pe punctul final și blocarea tuturor aplicațiilor, altele decât cele incluse în Allow-Lists.	Soluția propusă poate bloca aplicațiile interzise (Deny-List) pentru a fi lansate pe punctul final și blocarea tuturor aplicațiilor, altele decât cele incluse în Allow-Lists.	
				Soluția propusă trebuie să aibă o componentă de control al aplicațiilor integrată în cloud pentru acces imediat la cele mai recente actualizări privind evaluările și categoriile aplicațiilor.	Soluția propusă dispune de o componentă de control al aplicațiilor integrată în cloud pentru acces imediat la cele mai recente actualizări privind evaluările și categoriile aplicațiilor.	
				Soluția propusă trebuie să ofere protecție fișierelor executate în containere Windows Server.	Soluția propusă oferă protecție fișierelor executate în containere Windows Server.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să includă filtrarea programelor malware de trafic, verificarea legăturilor web și controlul resurselor web pe baza categoriilor de cloud.	Soluția propusă dispune de filtrarea programelor malware de trafic, verificarea legăturilor web și controlul resurselor web pe baza categoriilor de cloud.	
				Componenta de control/restricție a soluției propuse trebuie să includă o categorie Criptomonede și Mining. De asemenea, trebuie să includă restricții legale regionale predefinite pentru a se conforma legislației belgiene și japoneze.	Componenta de control/restricție a soluției propuse include o categorie Criptomonede și Mining. În același timp, includă restricții legale regionale predefinite pentru a se conforma legislației belgiene și japoneze.	
				Soluția propusă trebuie să aibă capacitatea de a permite aplicații bazate pe certificatele lor de semnătură digitală, MD5, SHA256, META Data, File Path și categoriile de securitate predefinite.	Soluția propusă are capacitatea de a permite aplicații bazate pe certificatele lor de semnătură digitală, MD5, SHA256, META Data, File Path și categoriile de securitate predefinite.	
				Soluția propusă trebuie să aibă controale pentru descărcarea DLL și a driverelor.	Soluția propusă include controale pentru descărcarea DLL și a driverelor.	
				Soluția propusă trebuie să accepte controlul scripturilor din PowerShell.	Soluția propusă poate accepta controlul scripturilor din PowerShell.	
				Soluția propusă trebuie să accepte Modul de testare cu generarea de rapoarte privind lansarea aplicațiilor blocate.	Soluția propusă acceptă Modul de testare cu generarea de rapoarte privind lansarea aplicațiilor blocate.	
				Soluția propusă trebuie să aibă capacitatea de a restricționa activitățile aplicației din sistem în funcție de nivelul de încredere atribuit aplicației și de a limita drepturile aplicațiilor de a accesa anumite resurse, inclusiv fișierele de sistem și utilizator „Funcționalitatea HIPS”.	Soluția propusă dispune de capacitatea de a restricționa activitățile aplicației din sistem în funcție de nivelul de încredere atribuit aplicației și de a limita drepturile aplicațiilor de a accesa anumite resurse, inclusiv fișierele de sistem și utilizator „Funcționalitatea HIPS”.	
				Soluția propusă trebuie să aibă capacitatea de a controla accesul sistemului/aplicația utilizatorului la dispozitivele de înregistrare audio și video.	Soluția propusă oferă capacitatea de a controla accesul sistemului/aplicația utilizatorului la dispozitivele de înregistrare audio și video - Video & Audio Protections	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să ofere o facilitate pentru a verifica aplicațiile enumerate în fiecare categorie bazată pe cloud.	Soluția propusă oferă facilitatea de a verifica aplicațiile enumerate în fiecare categorie bazată pe cloud.	
				Soluția propusă trebuie să aibă capacitatea de a se integra cu un sistem Advanced Threat Protection specific furnizorului.	Soluția propusă dispune de capacitatea de a se integra cu un sistem Advanced Threat Protection specific furnizorului.	
				Soluția propusă trebuie să aibă capacitatea de a reglementa automat activitatea programelor care rulează, inclusiv accesul la sistemul de fișiere și registre, precum și interacțiunea cu alte programe.	Soluția propusă are capacitatea de a reglementa automat activitatea programelor care rulează, inclusiv accesul la sistemul de fișiere și registre, precum și interacțiunea cu alte programe.	
				Soluția propusă trebuie să aibă capacitatea de a șterge automat regulile de control al aplicației dacă o aplicație nu este lansată într-un interval specificat. Intervalul trebuie să fie configurabil.	Soluția propusă are capacitatea de a șterge automat regulile de control al aplicației dacă o aplicație nu este lansată într-un interval specificat. Intervalul trebuie să fie configurabil.	
				Soluția propusă trebuie să aibă capacitatea de a clasifica automat aplicațiile lansate înainte de instalarea protecției punctelor finale.	Soluția propusă are capacitatea de a clasifica automat aplicațiile lansate înainte de instalarea protecției punctelor finale.	
				Soluția propusă trebuie să aibă protecție împotriva amenințărilor de corespondență cu: <ul style="list-style-type: none">• Filtrul de atașamente și capacitatea de a redenumi atașamentele.• Scanarea mesajelor e-mail la primirea, citirea și trimiterea.	Soluția propusă dispune de protecție împotriva amenințărilor de corespondență cu: <ul style="list-style-type: none">• Filtrul de atașamente și capacitatea de a redenumi atașamentele.• Scanarea mesajelor e-mail la primirea, citirea și trimiterea.	
				Soluția propusă trebuie să aibă capacitatea de a scana mai multe redirectionări, adrese URL scurtate, adrese URL deturnate și întârzieri bazate pe timp.	Soluția propusă are capacitatea de a scana mai multe redirectionări, adrese URL scurtate, adrese URL deturnate și întârzieri bazate pe timp.	
				Soluția propusă trebuie să permită utilizatorului computerului să efectueze o	Soluția propusă permite utilizatorului computerului să efectueze o verificare a	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				verificare a reputației unui fișier din meniul contextual al fișierului.	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 include 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 oferă 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 oferă 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 include suportul pentru protocolul IPv6.	
				Soluția propusă trebuie să ofere scanarea secțiunilor critice ale computerului ca sarcină de sine stătătoare.	Soluția propusă oferă scanarea secțiunilor critice ale computerului ca sarcină de sine stătătoare.	
				Soluția propusă trebuie să încorporeze tehnologia Application Self-Protection:	Soluția propusă este încorporată cu tehnologia Application Self-Protection care poate să:	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

			<ul style="list-style-type: none">• protejarea împotriva gestionării neautorizate de la distanță a unui serviciu de aplicație.• protejarea accesului la parametrii aplicației prin setarea unei parole.• prevenirea dezactivării protecției de către malware, criminali sau utilizatori amatori.	<ul style="list-style-type: none">• protejeze împotriva gestionării neautorizate de la distanță a unui serviciu de aplicație.• protejeze accesul la parametrii aplicației prin setarea unei parole;• prevină dezactivarea 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 oferă posibilitatea de a alege ce componente de protecție împotriva amenințărilor să instaleze.	
			Soluția propusă trebuie să includă verificarea și dezinfectia antivirus a fișierelor care au fost împachetate folosind programe precum PKLITE, LZEXE, DIET, EXEPACK etc.	Soluția propusă include verificarea și dezinfectia 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 include 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 poate 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 include 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	Soluția propusă permite administratorului să creeze un singur program de instalare cu	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

			necesară, pentru a fi utilizat de utilizatorii care nu cunosc cunoștințele IT.	configurația necesară, pentru a fi utilizat de utilizatorii care nu cunosc cunoștințele IT.	
			2. Cerințe funcționale: Detectare	2. Cerințe funcționale: Detectare	
			Soluția sugerată trebuie să suplimenteze informațiile de verdict din soluția Endpoint Protection cu artefacte ale sistemului despre detectare.	Soluția propusă poate 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 propusă poate efectua 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 de antivirus propusă are 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 de antivirus propusă poate accepta 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 de antivirus propusă poate accepta 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 de antivirus propusă poate accepta 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.	Soluția de antivirus propusă poate accepta exportul IoC generat de soluție într-un fișier în format OpenIoC.	
			Cerințe funcționale: Vizibilitate	Cerințe funcționale: Vizibilitate	
			Soluția sugerată trebuie să genereze un card de alertă detaliat legat de amenințarea detectată la punctele finale	Soluția propusă poate genera un card de alertă detaliat legat de amenințarea detectată la punctele finale	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				<p>Un card de alertă trebuie să includă cel puțin următoarele informații despre amenințarea detectată:</p> <ul style="list-style-type: none">• 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. <p>Acțiunile de răspuns efectuate de aplicație.</p>	<p>Un card de alertă include cel puțin următoarele informații despre amenințarea detectată:</p> <ul style="list-style-type: none">• 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. <p>Acțiunile de răspuns efectuate de aplicație.</p>	
				<p>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.</p>	<p>Graficul lanțului de dezvoltare a amenințărilor (kill chain) oferă informații vizuale despre obiectele implicate în alertă, de exemplu, despre procesele cheie de pe dispozitiv, conexiuni de rețea, biblioteci, registru etc.</p>	
				<p>Un card de alertă trebuie să prezinte o vizualizare detaliată a artefactelor sistemului și a datelor legate de alertă pentru analiza cauzei principale:</p> <ul style="list-style-type: none">• Procesul de depunere a icrelor• Conexiuni de rețea• Modificări de registru• Descărcare obiect• Obiecte scăpate etc.	<p>Un card de alertă prezintă o vizualizare detaliată a artefactelor sistemului și a datelor legate de alertă pentru analiza cauzei principale:</p> <ul style="list-style-type: none">• Procesul de depunere a icrelor• Conexiuni de rețea• Modificări de registru• Descărcare obiect• Obiecte scăpate etc.	
				Cerințe funcționale: Răspuns	Cerințe funcționale: Răspuns	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția sugerată trebuie să accepte consola de gestionare a formularelor de răspuns „un singur clic”.	Soluția propusă acceptă 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:	Soluția propusă acceptă cel puțin următoarele acțiuni de răspuns pe care un administrator le poate efectua atunci când sunt detectate amenințări:	
				Prevenirea executării obiectului	Prevenirea executării obiectului	
				Soluția EDR trebuie să accepte ambele moduri: <ul style="list-style-type: none">• înregistrează evenimentele despre încercări de lansare a obiectelor sau a 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 acceptă ambele moduri: <ul style="list-style-type: none">• înregistrarea evenimentele despre încercări de lansare a obiectelor sau a documentelor care îndeplinesc criteriile de prevenire a execuției, dar nu blochează lansarea sau deschiderea acestor obiecte.• blocarea lansării 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 acceptă blocarea obiectelor prin hash (MD5 sau SHA256) sau după modelul de cale.	
				Soluția EDR trebuie să accepte blocarea executabilelor, scripturilor și documentelor	Soluția EDR acceptă blocarea executabilelor, scripturilor și documentelor	
				Soluția EDR trebuie să accepte notificarea utilizatorului despre opțiunea de prevenire	Soluția EDR acceptă notificarea utilizatorului despre opțiunea de prevenire	
				Izolarea gazdei.	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 oferă 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.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				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 acceptă 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.	Soluția EDR acceptă readucerea manuală a gazdei online din izolare.	
				Ștergerea obiectului din gazdă sau din grupul de gazde.	Șterge obiectul din gazdă sau din grupul de gazde.	
				Obținerea (descărcarea) fișierului de la o gazdă sau un grup de gazde.	Obține (descărcarea) fișierul de la o gazdă sau un grup de gazde.	
				Încheie un proces pe dispozitiv.	Încheie un proces pe dispozitiv.	
				Punerea în carantină un obiect	Pune în carantină un obiect	
				Soluția sugerată trebuie să sprijine recuperarea obiectelor din carantină.	Soluția propusă permite recuperarea obiectelor din carantină.	
				Rularea scanarea sistemului	Rularea scanarea sistemului	
				Executarea de la distanță a unui program / proces / comandă	Executarea de la distanță a unui program / proces / comandă	
				Pornirea scanării loC pentru un grup de gazde.	Pornirea scanării loC pentru un grup de gazde.	
				Soluția sugerată trebuie să accepte consola de gestionare a formularelor de răspuns „un singur clic”.	Soluția propusă acceptă consola de gestionare a formularelor de răspuns „un singur clic”.	
				Administrare centralizată, monitorizare și actualizare a cerințelor software	Administrare centralizată, monitorizare și actualizare a cerințelor software	
				Soluția propusă trebuie să permită instalarea de software anti-malware dintr-un singur pachet de distribuție.	Soluția propusă permite 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 dispune de profile de instalare personalizabile în funcție de numărul de noduri protejate.	
				Soluția propusă trebuie să accepte adrese IPv6.	Soluția propusă acceptă adrese IPv6.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să accepte verificarea în doi pași (autentificare).	Soluția propusă acceptă 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 are 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.	Soluția propusă include o consolă web încorporată pentru gestionarea punctelor finale, care nu necesită 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.	Consola de management web a soluției propuse este ușor de utilizat și poate accepta 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 poate distribui automat conturile de computer pe grup de management dacă în rețea apar computere noi. Soluția oferă 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 este dotată cu 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 include eliminarea centralizată (manuală și automată) a aplicațiilor incompatibile din centrul de administrare.	



“RTS ONE” S.R.L.

<https://rts.md>

+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să ofere metode flexibile pentru instalarea agentului anti-malware: RPC, GPO, un agent de administrare pentru instalare la distanță și opțiunea de a crea un pachet de instalare autonom pentru instalare locală.	Soluția propusă oferă metode flexibile pentru instalarea agentului anti-malware: RPC, GPO, un agent de administrare pentru instalare la distanță și opțiunea de creare a unui 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 permite 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 include 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 dispune de 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 permite 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 permite 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 permite 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	Soluția propusă permite 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	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				ale utilizatorilor imediat după primirea acestora.	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 poate 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 permite 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 acceptă modulul 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 oferă acces la serviciile cloud ale furnizorului de securitate anti-malware prin intermediul serverului de administrare.	
				Soluția propusă trebuie să includă distribuția automată a licențelor pe computerele client.	Soluția propusă include distribuția automată a licențelor pe computerele client.	
				Soluția propusă trebuie să poată efectua inventarierea software-ului și hardware-ului instalat pe computerele utilizatorului.	Soluția propusă poate 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 are 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.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să permită instalarea centralizată a aplicațiilor terțe pe toate computerele sau pe anumite computere.	Soluția propusă permite 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 are 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 are 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 poate 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 poate 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 asigură 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	Soluția propusă dispune de funcționalitate de crearea de conturi interne pentru	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				administratorilor pe serverul de administrare.	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 dispune de funcționalitate de creare a 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 acceptă Windows Failover Cluster.	
				Soluția propusă trebuie să aibă o caracteristică de clustering încorporată.	Soluția propusă dispune de funcționalitate de clustering încorporată.	
				Soluția propusă trebuie să includă o formă de sistem pentru a controla epidemiile virale.	Soluția propusă dispune de funcționalitate de sistem pentru a controla epidemiile virale.	
				Soluția propusă trebuie să includă controlul accesului bazat pe rol (RBAC), iar acest lucru trebuie să permită replicarea restricțiilor pe serverele de management din ierarhie.	Soluția propusă include controlul accesului bazat pe rol (RBAC), iar acest lucru permite replicarea restricțiilor pe serverele de management din ierarhie.	
				Serverul de management al soluției propuse trebuie să includă roluri de securitate predefinite pentru auditor, supervisor și ofițer de securitate.	Serverul de management al soluției propuse include roluri de securitate predefinite pentru auditor, supervisor și ofițer de securitate.	
				Soluția propusă trebuie să aibă capacitatea de a gestiona dispozitivele mobile prin comenzi de la distanță.	Soluția propusă are capacitatea de a gestiona dispozitivele mobile prin comenzi de la distanță.	
				Soluția propusă trebuie să aibă capacitatea de a șterge actualizările descărcate.	Soluția propusă are capacitatea de a șterge actualizările descărcate.	
				Soluția propusă trebuie să permită gestionarea actualizărilor Serverului de administrare din interfața aplicației.	Soluția propusă permite gestionarea actualizărilor Serverului de administrare din interfața aplicației.	
				Soluția propusă trebuie să ofere posibilitatea de a selecta un agent de	Soluția propusă oferă posibilitatea de a selecta un agent de actualizare pentru computerele client pe baza analizei rețelei.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				actualizare pentru computerele client pe baza analizei rețelei.		
				Soluția propusă trebuie să arate clar informații despre distribuția vulnerabilităților între computerele gestionate.	Soluția propusă descifrează informații despre distribuția vulnerabilităților între computerele gestionate.	
				Interfața de server de management a soluției propuse trebuie să accepte limba arabă.	Interfața de server de management a soluției propuse acceptă inclusiv 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 dispune de 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: <ul style="list-style-type: none">• Starea dispozitivului• Etichete• Active directory• Proprietari de dispozitive• Hardware	Serverul de management al soluției propuse are 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: <ul style="list-style-type: none">• Starea dispozitivului• Etichete• Active directory• Proprietari de dispozitive• Hardware	
				Soluția propusă trebuie să accepte următoarele canale de livrare a notificărilor: <ul style="list-style-type: none">• E-mail• Syslog• SMS• SIEM	Soluția propusă acceptă următoarele canale de livrare a notificărilor: <ul style="list-style-type: none">• E-mail• Syslog• SMS• SIEM	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				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 are 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 are capacitatea de a efectua inventariere pe scripturi și fișiere .dll.	
				Soluția propusă trebuie să aibă capacitatea de a eticheta/marca computere pe baza: <ul style="list-style-type: none">• Atributele rețelei<ul style="list-style-type: none">- Nume- Domeniu și/sau Sufix de domeniu- Adresa IP- Adresa IP către serverul de management• Locația în Active Directory<ul style="list-style-type: none">- Unitate organizațională- Grup• Sistem de operare<ul style="list-style-type: none">- Tip și versiune- Arhitectură- Numărul pachetului de service• Arhitectură virtuală• Registrul aplicațiilor<ul style="list-style-type: none">- Numele aplicației- Versiunea aplicației- Producător	Soluția propusă are capacitatea de a eticheta/marca computere pe baza: <ul style="list-style-type: none">• Atributele rețelei<ul style="list-style-type: none">- Nume- Domeniu și/sau Sufix de domeniu- Adresa IP- Adresa IP către serverul de management• Locația în Active Directory<ul style="list-style-type: none">- Unitate organizațională- Grup• Sistem de operare<ul style="list-style-type: none">- Tip și versiune- Arhitectură- Numărul pachetului de service• Arhitectură virtuală• Registrul aplicațiilor<ul style="list-style-type: none">- Numele aplicației- 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 are 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.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				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 dispune de 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 permite administratorului să definească setări restricționate în setările de politică/profil, astfel încât o sarcină de scanare a virușilor care poate declanșa 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 poate fi configurabil.	
				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 are un tablou de bord personalizabil care să genereze și afișeze statistici în timp real pentru punctele finale.	
				Soluția propusă trebuie să permită administratorului să personalizeze rapoartele.	Soluția propusă permite 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 are 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 și datele aferente acestuia sunt șterse automat de pe server.	Soluția propusă permite administratorului să stabilească o perioadă de timp după care un computer care nu este conectat la serverul de management și datele aferente acestuia sunt șterse automat de pe server.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				<p>Soluția propusă trebuie să permită administratorului să creeze categorii/grupuri de aplicații pe baza:</p> <ul style="list-style-type: none">• Numele aplicației• Calea aplicației• Metadatele aplicației• Certificat aplicației digitale• Categorii de aplicații predefinite ale furnizorului• SHA• Calculatoare de referință <p>pentru a permite/interzice execuția lor pe punctele finale.</p>	<p>Soluția propusă permite administratorului să creeze categorii/grupuri de aplicații pe baza:</p> <ul style="list-style-type: none">• Numele aplicației• Calea aplicației• Metadatele aplicației• Certificat aplicației digitale• Categorii de aplicații predefinite ale furnizorului• SHA• Calculatoare de referință <p>pentru permiterea/interzicerea execuției lor pe punctele finale.</p>	
				<p>Soluția propusă trebuie să permită administratorului să definească diferite condiții de schimbare a stării pentru grupuri de puncte finale din serverul de management.</p>	<p>Soluția propusă permite administratorului să definească diferite condiții de schimbare a stării pentru grupuri de puncte finale din serverul de management.</p>	
				<p>Soluția propusă trebuie să permită administratorului să adauge instrumente personalizate/terțe de gestionare a punctelor finale în serverul de management.</p>	<p>Soluția propusă permite administratorului să adauge instrumente personalizate/terțe de gestionare a punctelor finale în serverul de management.</p>	
				<p>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.</p>	<p>Soluția propusă dispune de o funcție/modul încorporat pentru a colecta de la distanță datele necesare pentru depanarea de la punctele finale, fără a necesita acces fizic.</p>	
				<p>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.</p>	<p>Soluția propusă permite 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.</p>	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				<p>Soluția propusă trebuie să aibă funcționalitate încorporată pentru a se conecta de la distanță la punctul final folosind tehnologia de partajare a desktopului Windows. În plus, soluția trebuie să fi capabilă să mențină auditarea acțiunilor administratorului în timpul sesiunii.</p>	<p>Soluția propusă are funcționalitate încorporată pentru a se conecta de la distanță la punctul final folosind tehnologia Remote Shell. În plus, soluția este capabilă să mențină auditarea acțiunilor administratorului în timpul sesiunii.</p>	
				<p>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:</p> <ul style="list-style-type: none">• structuri ale domeniilor și ale grupuri de lucru Windows• structuri ale grupurilor Active Directory• conținutul unui fișier text creat manual de administrator	<p>Soluția propusă dispune de o funcție care să permită crearea unei structuri de grupuri de administrare utilizând ierarhia Grupuri, pe baza următoarelor date:</p> <ul style="list-style-type: none">• structuri ale domeniilor și ale grupuri de lucru Windows• structuri ale grupurilor Active Directory <p>conținutul unui fișier text creat manual de administrator</p>	
				<p>Soluția propusă trebuie să fie capabilă să recupereze informații despre echipamentele detectate în timpul unui sondaj de rețea. Inventarul rezultat ar trebui să acopere toate echipamentele conectate la rețeaua organizației. Informațiile despre echipament ar trebui să se actualizeze după fiecare nou sondaj de rețea. Lista echipamentelor detectate ar trebui să acopere următoarele:</p> <ul style="list-style-type: none">• dispozitive• dispozitive mobile• dispozitive de rețea• dispozitive virtuale• Componente OEM• perifericele computerului• dispozitivele conectate	<p>Soluția propusă este capabilă să recupereze informații despre echipamentele detectate în timpul unui sondaj de rețea. Inventarul rezultat acoperă toate echipamentele conectate la rețeaua organizației. Informațiile despre echipament ar trebui să se actualizeze după fiecare nou sondaj de rețea. Lista echipamentelor detectate acoperă următoarele:</p> <ul style="list-style-type: none">• dispozitive• dispozitive mobile• dispozitive de rețea• dispozitive virtuale• Componente OEM• perifericele computerului• dispozitivele conectate• telefoane VoIP	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

			<ul style="list-style-type: none">• telefoane VoIP• depozite de rețea <p>Administratorul trebuie să poată adăuga manual noi dispozitive la lista de echipamente sau să editeze informații despre echipamentele care există deja în rețea.</p> <p>Funcționalitatea „Device is Written Off” trebuie să fie disponibilă, astfel încât astfel de dispozitive să nu fie afișate în lista de echipamente.</p>	<ul style="list-style-type: none">• depozite de rețea <p>Administratorul poate adăuga manual noi dispozitive la lista de echipamente sau să editeze informații despre echipamentele care există deja în rețea.</p> <p>Funcționalitatea „Device is Written Off” este disponibilă, astfel încât astfel de dispozitive să nu fie afișate în lista de echipamente.</p>	
			Soluția propusă trebuie să încorporeze un singur agent de distribuție/relev 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 este încorporată cu un singur agent de distribuție/relev 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/relev pentru a transmite/transferă sau proxy cererile de reputație a amenințărilor de la punctele finale către serverul de management.	Soluția propusă este încorporată cu un singur agent de distribuție/relev 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 acceptă descărcarea fișierelor diferențiate, mai degrabă decât pachetele complete de actualizare.	
			Soluția propusă trebuie să accepte OPEN API și să includă linii directe pentru integrarea cu sisteme externe terțe.	Soluția propusă acceptă OPEN API și să includă linii directe 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 include un instrument încorporat pentru a efectua diagnostice de la distanță și a colecta jurnale de depanare fără a necesita acces fizic la computer.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să includă Controlul accesului bazat pe roluri (RBAC) cu roluri predefinite personalizabile.	Soluția propusă include 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.	Serverul de management principal/primar/părinte al soluției propuse poate transmite actualizări și servicii de reputație în cloud.	
				Rapoartele soluției propuse trebuie să includă informații despre fiecare amenințare și tehnologia care a detectat-o.	Rapoartele soluției propuse includ 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.	Raportul privind soluția propusă include 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 de sănătate etc. a punctelor finale gestionate de la serverele de management secundare	Serverul de management primar al soluției propuse poate prelua informații detaliate de raportare privind starea de sănătate 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 include 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 poate 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 permite migrarea rapidă de la consola de management locală la consola de management bazată pe cloud a furnizorului.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția propusă trebuie să includă suport pentru implementarea bazată pe cloud prin: <ul style="list-style-type: none">• Amazon Web Services• Microsoft Azure	Soluția propusă include suport pentru implementarea bazată pe cloud prin: <ul style="list-style-type: none">• Amazon Web Services• Microsoft Azure	
				Soluția propusă trebuie să ofere mecanisme de actualizare a bazei de date anti-malware, inclusiv: <ul style="list-style-type: none">• Mai multe moduri de actualizare, inclusiv canale de comunicare globală prin protocolul HTTPS, resurse partajate în rețeaua locală și suporturi detașabile.• Verificarea integrității și autenticității actualizărilor prin intermediul unei semnături digitale electronice.	Soluția propusă oferă mecanisme de actualizare a bazei de date anti-malware, inclusiv: <ul style="list-style-type: none">• Mai multe moduri de actualizare, inclusiv canale de comunicare globală 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.	Soluția propusă acceptă Single Sign On (SSO) folosind NTLM și Kerberos.	
				Administrare și raportare EDR	Administrare și raportare EDR	
				Soluția sugerată trebuie să accepte comunicarea securizată între consola de management și punctele finale cu agentul EDR	Soluția propusă acceptă 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 propusă acceptă 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.	Soluția propusă are caracteristici/module încorporate 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.	Aplicația EDR dispune de un mecanism de autoapărare pentru a preveni modificarea intrărilor sale de fișiere/componente de sistem etc.	



“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				Soluția EDR trebuie să aibă un mecanism de autoapărare pentru a preveni modificarea intrărilor sale de fișiere / componente de sistem etc.	Soluția EDR dispune de un mecanism de autoapărare pentru a preveni modificarea intrărilor sale de fișiere / componente de sistem etc.	
				Cerințe pentru documentația soluției. O documentație pentru software-ul EDR, inclusiv instrumentele de administrare, trebuie să includă cel puțin un ajutor online pentru administratori.	Cerințe pentru documentația soluției. Documentație pentru software-ul EDR, inclusiv instrumentele de administrare, care include 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	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, sunt oferite Ofertant, iar costul acestora este inclus în ofertă; Servicii de intervenție în mod continuu 24h/zi – 7zile/săptămână pentru alerte cibernetice ce conțin următoarele activități: - Efectuarea de interogări de bază pentru a aduna informații suplimentare legate de incidentul de securitate - Echipa de support al Societății cu Răspundere Limitată „RTS ONE” se va conecta la consola de management a clientului și vom actualiza progresul / rezolvarea incidentelor de Securitate	



“RTS ONE” S.R.L.

<https://rts.md>

+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				<ul style="list-style-type: none">- 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, recomandă 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 local va prioritiza și gestiona escaladarea incidentelor validate catre IS Posta Moldovei Autorizarea de la producător - Manufacture Authorization Letter.	<ul style="list-style-type: none">- Echipa de support al Societății cu Răspundere Limitată „RTS ONE” va investiga evenimentele de securitate și va escalada la nivelul 2 de intervenție- Echipa de support al Societății cu Răspundere Limitată „RTS ONE” va asigura gestionarea și prioritizarea alertelor, gestionarea răspunsurilor la incidente și escaladarea acestora- Echipa de support al Societății cu Răspundere Limitată „RTS ONE” va asista personalul superior al utilizatorilor finali în probleme de securitate, daca va fi necesar.- Echipa de support al Societății cu Răspundere Limitată „RTS ONE” va valida atacurile, evalua impactul, recomandă contramăsurile și va lucra în implementarea soluției de mitigare și răspuns.- Echipa de support al Societății cu Răspundere Limitată „RTS ONE” va emite recomandări de ajustare a produsului/ tehnologiei de securitate către IS Posta Moldovei- Echipa de support al Societății cu Răspundere Limitată „RTS ONE” va colabora cu părțile interesate ale Clientului pentru a asigura rezolvarea în timp util a problemelor de securitate ridicate și critice- Echipa de support al Societății cu Răspundere Limitată „RTS ONE” va prioritiza și gestiona escaladarea incidentelor validate catre IS Posta Moldovei	
--	--	--	--	---	---	--



🏢 "RTS ONE" S.R.L.

🔗 <https://rts.md>

☎ (+373) 22 101 777

✉ office@rts.one

📍 str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

					Autorizarea de la producător - Manufacture Authorization Letter. – se anexează la prezenta Specificație tehnică	
--	--	--	--	--	---	--

Semnat:

Numele, Prenumele: **CELONENCO Vitalie**

Ofertantul: **Societatea cu Răspundere Limitată „RTS ONE”**

În calitate de: **Administrator**

Adresa: **mun.Chișinău, str.Mitropolit Gavriil Bănulescu-Bodoni,
59/B, of.815**