

Specificații tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5,]

Numărul procedurii de achiziție: ocds-b3wdp1-MD-1684159833378 din 15.05.2023
Obiectul achiziției: Servicii de prevenire a pierderilor de date (DLP)

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	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
Bunuri/servicii						
Lotul 1						
Servicii de prevenire a pierderilor de date (DLP)	Trellix Data Loss Prevention Endpoint	SUA	Trellix	Cerințe funcționale față de soluția DLP (Data Loss Prevention) I. Integrare cu infrastructura IT 1. Soluția trebuie să poată rula pe: <ul style="list-style-type: none"> • Windows 10, 11 Enterprise și Professional, 32-bit sau 64-bit, • Windows Server 2012/2012R2, • Windows Server 2016, • Windows Server 2019, • Linux Ubuntu, CentOS 	Soluția oferită DLP (Data Loss Prevention) Trellix Data Loss Prevention Endpoint Subscription License sau Perpetual License I. Integrare cu infrastructura IT 1. Soluția rulează: <ol style="list-style-type: none"> 1.1 Windows 10 1803 sau mai noi Enterprise și Professional, 32-bit și 64-bit și Windows 11 64 bit 1.2 Windows Server 2012, 2012 R2, 2016, 2019, 2022 1.3 Windows 8 și 8.1 sau mai recente, Enterprise și Professional, 32-bit și 64-bit 	-

				<p>2. Soluția suportă următorul tip directory: Microsoft AD.</p> <p>3. Soluția trebuie să ofere funcționalități de instalare și deservire de la distanță pentru agenții de monitorizare.</p> <p>4. Soluția trebuie să ofere suport pentru mediile virtuale:</p> <ul style="list-style-type: none"> • VMware ESXi, • ProxMox. <p>5. Politicile trebuie să se aplice la nivel de user sau stație pe sesiuni multiple.</p> <p>II. Politici de Securitate</p> <p>1. Soluția are capacitatea de a inspecta următoarele protocoale:</p> <ul style="list-style-type: none"> • SMTP, • Telnet, • IMAP, 	<p>1.4 Windows 7 SP1 sau mai recente Enterprise si Business, 32-bit and 64-bit</p> <p>1.5 macOS Mojave, Catalina, Big Sur, Monterey.</p> <p>1.6 Linux Ubuntu, CentOS</p> <p>2. Soluția suportă următorul tip directory: Microsoft AD si Open LDAP</p> <p>3. Soluția oferă funcționalități de instalare și deservire de la distanță pentru agenții de monitorizare.</p> <p>4. Soluția oferă suport pentru mediile virtuale:</p> <ul style="list-style-type: none"> • VMware ESXi, • ProxMox. <p>5. Politicile se aplică la nivel de user sau stație pe sesiuni multiple.</p> <p>6. Soluția este capabilă să țină evidența unui număr de peste 500 de milioane de semnături ale fișierelor clasificate pe un singur server și posibilitatea de a instala un număr nelimitat de repositoare</p> <p>7. Soluția alică politici bazate pe conținut confidential pentru un număr nelimitat de tipuri de fișiere</p> <p>8. Soluția face clasificarea conținutului chiar dacă acesta este arhivat și trebuie de asemenea să suporte “nesting” (ex: arhiva zip în interiorul unei alte arhive zip)</p> <p>II. Politici de Securitate</p> <p>1. Soluția are capacitatea de a inspecta următoarele protocoale:</p> <ul style="list-style-type: none"> • SMTP, • Telnet, • IMAP, 	
--	--	--	--	--	---	--

				<ul style="list-style-type: none"> • FTP, • POP3, • IRC, • HTTP, • HTTPS, • SMB, • WSD, • TCP/IP, • LDAP, <p>de asemenea poate analiza traficul care este încapsulat în SOCKS;</p> <p>2. Soluția trebuie să suporte detectarea documentelor înregistrate/amprentate și clasificate.</p> <p>3. Soluția trebuie să aibă capacitatea de a proteja datele bazându-se pe punctul lor de origine/creare.</p> <p>4. Soluția trebuie să fie capabilă să analizeze conținutul și să aplice politici, pentru documentele în limba Română, Rusă, Engleză, Franceză.</p> <p>5. Soluția trebuie să fie capabilă să scaneze și să găsească conținut sensibil.</p>	<ul style="list-style-type: none"> • FTP, • POP3, • IRC, • HTTP, • HTTPS, • SMB, • WSD, • TCP/IP, • LDAP, <p>de asemenea poate analiza traficul care este încapsulat în SOCKS;</p> <p>2. Soluția suportă detectarea documentelor înregistrate/amprentate și clasificate.</p> <p>3. Soluția are capacitatea de a proteja datele bazându-se pe punctul lor de origine/creare.</p> <p>- Soluția este capabilă de a atribui în mod automat taguri fișierelor clasificate. Aceste taguri trebuie să fie utilizabile de aplicații third-party și alte aplicații DLP</p> <p>4. Soluția este capabilă să analizeze conținutul și să aplice politici, indiferent de limba utilizată. (Română, Rusă, Engleză, Franceză, etc)</p> <p>5. Soluția este capabilă să scaneze și să găsească conținut sensibil.</p> <p>- Agentul are capacități de analiză de conținut și blocare pentru mediile optice.</p> <p>- Soluția folosește mai puțin de 5% din procesorul în cazul utilizării intense și gradul de utilizare medie este maxim 2% în timpul funcționării normale.</p>	
--	--	--	--	--	--	--

				<p>6. Soluția trebuie să poată proteja informația confidențială care poate fi:</p> <ul style="list-style-type: none"> • scrisă pe unități USB, CD/DVD, • trimisă pe mail, • upload-ată, • copiată cu ajutorul clipboard-ului, • printată în fișier sau pe imprimantă, • scrisă pe resursele partajate în rețea, • aplicații cloud (DropBox, Google Drive, Box, iCloud, Microsoft OneDrive). <p>7. Soluția trebuie să poată oferi vizibilitate în timp real a amenințărilor pentru prevenirea pierderilor de date.</p> <p>8. Soluția trebuie să ofere protecție la nivel de „Clip board” atât pentru copy sau paste cât și pentru screen capture.</p> <p>9. Soluția trebuie să permită crearea de politici de securitate pentru dispozitivele USB de tip plug-and-play.</p> <p>10. Soluția trebuie să ofere același nivel de protecție și în regim OS Safe-Mode.</p> <p>11. Soluția trebuie să fie capabilă să facă analiză de conținut local (offline), fără a utiliza vreo altă componentă a soluției.</p>	<p>6. Soluția poate proteja informația confidențială care poate fi:</p> <ul style="list-style-type: none"> • scrisă pe unități USB, CD/DVD, • trimisă pe mail, • upload-ată, • copiată cu ajutorul clipboard-ului, • printată în fișier sau pe imprimantă, • scrisă pe resursele partajate în rețea, • aplicații cloud (DropBox, Google Drive, Box, iCloud, Microsoft OneDrive). • folosita in aplicatiile network – based • Copiata prin comanda de printscreen <p>7. Soluția oferă vizibilitate în timp real a amenințărilor pentru prevenirea pierderilor de date.</p> <p>8. Soluția oferă protecție la nivel de „Clip board” atât pentru copy sau paste cât și pentru screen capture.</p> <p>9. Soluția trebuie să permită crearea de politici de securitate pentru dispozitivele USB de tip plug-and-play.</p> <p>10. Soluția oferă același nivel de protecție și în regim OS Safe-Mode.</p> <p>11. Soluția este capabilă să facă analiză de conținut local (offline), fără a utiliza vreo altă componentă a soluției.</p>	
--	--	--	--	--	--	--

			<p>12. Soluția permite auditarea funcționalității agentului de endpoint.</p> <p>13. Soluția trebuie să aibă un mecanism propriu de instalare a agenților pe stațiile de lucru sau alte sisteme.</p> <p>14. Agentul de endpoint trebuie să fie compatibil, cu soluții de antivirus, firewall și antispyware third-party (de ex: Kaspersky, BitDefender, McAfee, Norton, Safeguard, Acronis, Spybot, Adaware).</p> <p>15. Soluția trebuie să permită realizarea unui proces de justificare, în cazul în care utilizatorul transmite conținut confidențial.</p> <p>16. Opțiunea de justificare a activității folosită de end-user în cadrul procesului de justificare, trebuie să poată fi validabilă sau administrabilă.</p>	<p>12. Soluția permite auditarea funcționalității agentului de endpoint.</p> <ul style="list-style-type: none"> - Soluția trebuie să permită deinstalarea agentului în mod centralizat sau în urma unui challenge/response. <p>13. Soluția are un mecanism propriu de instalare a agenților pe stațiile de lucru sau alte sisteme.</p> <ul style="list-style-type: none"> - Soluția pentru endpoint-uri are capacități de clasificare diverse ce nu depind de limbajul folosit: analiza pe termeni/cuvinte cheie, regex-uri și scor de risc, etc. <p>14. Agentul de endpoint este compatibil, cu soluții de antivirus, firewall și antispyware third-party (de ex: Bitdefender, Kaspersky, McAfee, Norton, OSCE, Zonelab, GuardianEdge, Credant, Safeguard, Ironkey, Acronis, Spybot, Adaware, etc.).</p> <ul style="list-style-type: none"> - Agentul de endpoint permite aplicarea politicilor folosind conținut înregistrat/ amprentat. <p>15. Soluția permite realizarea unui proces de justificare, în cazul în care utilizatorul transmite conținut confidențial.</p> <p>16. Opțiunea de justificare a activității folosită de end-user în cadrul procesului de justificare, poate fi validabilă sau administrabilă.</p> <ul style="list-style-type: none"> - Soluția permite utilizatorilor să devină “stakeholderi” pe un caz/eveniment, ori din inițiativa 	
--	--	--	--	---	--

				<p>17. Soluția trebuie să fie capabilă să blocheze dispozitivele portabile sau să permită doar accesul de tip read-only.</p> <p>18. Soluția trebuie să poată aplica reguli de protecție care să aibă ca criteriu cuvinte-cheie, expresii regulate și amprentă (hash-uri).</p> <p>19. Construcția regulilor trebuie să includă suport pentru logica booleană incluzând AND, OR, sau alte declarații logice.</p> <p>20. Soluția trebuie să fie capabilă să aplice următoarele acțiuni: blocare, monitorizare, notificare utilizator, menținere evidentă, criptare.</p> <p>21. Soluția trebuie să aibă abilitatea de a identifica fișierele bazându-se pe conceptul de true</p>	<p>acestora ori asignata de administrator</p> <p>17. Soluția este capabilă să blocheze dispozitivele mobile sau să permită accesul al ele doar de tip read-only sau să permită doar încărcarea dispozitivelor mobile nu și accesarea acestora.</p> <ul style="list-style-type: none"> - Soluția poate realiza reguli de protecție care să aibă ca și criteriu cuvinte-cheie. - Soluția poate realiza reguli de protecție care să aibă ca și criteriu regex-uri. <p>18. Soluția poate aplica reguli de protecție care să aibă ca criteriu cuvinte-cheie, expresii regulate și amprentă (hash-uri).</p> <ul style="list-style-type: none"> - Soluția poate realiza reguli de protecție care să aibă ca și criteriu reguli de proximitate între alte două reguli (de tip keyword, dicționar sau regex). <p>19. Construcția regulilor include suport pentru logica booleană incluzând AND, OR, sau alte declarații logice.</p> <p>20. Soluția este capabilă să aplice următoarele acțiuni: blocare, monitorizare, notificare utilizator, menținere evidentă, criptare sau aplicarea de etichete.</p> <ul style="list-style-type: none"> - Soluția permite setarea unui threshold astfel încât o regulă să nu fie activată decât după găsirea unui anumit număr de match-uri. <p>21. Soluția are abilitatea de a identifica fișierele bazându-se pe conceptul de true file type și nu doar pe extensia fișierelor.</p>	
--	--	--	--	--	---	--

				<p>file type și nu doar pe extensia fișierelor.</p> <p>22. Soluția trebuie să aibă posibilitatea rulării autonome a agentului pe endpoint în baza politicilor inițial aplicate.</p> <p>23. Soluția trebuie să fie capabilă să aplice reguli de protecție atât la nivel de grupuri /user-i definiți în</p>	<p>22. Soluția are posibilitatea rulării autonome a agentului pe endpoint în baza politicilor inițial aplicate.</p> <ul style="list-style-type: none"> - Soluția are capacitatea de a se integra cu soft de criptare 3rd party, pentru a realiza aplicarea politicilor de criptare în funcție de conținut. - Soluția dispune de cel puțin 70 de reguli de validare pentru definițiile bazate pe expresii regulate, inclusiv pentru definiția de IDNP. - Soluția permite “whitelist-area” de conținut, dispozitive, procese și utilizatori/grupuri de utilizatori din regulile de protecție - Soluția permite salvarea conținutului ce a declansat o regulă de protecție ca “evidence”. Aceste date salvate sunt recunoscute în instanță ca fiind dovezi valide. - Soluția are abilitatea de a identifica fișierele bazându-se pe conceptul de true file type și nu doar pe extensia fișierelor. - Soluția dispune de integrare nativă cu serviciu de tip CASB pentru aplicarea aceluiași reguli de protecție DLP și pe resurse manipulate în cloud - Soluția are abilitatea de a face discovery local. De asemenea ea trebuie să poată conține și o opțiune de remediere. <p>23. Soluția este capabilă să aplice reguli de protecție atât la nivel de grupuri /user-i definiți în Active</p>	
--	--	--	--	---	---	--

				<p>Active Directory cât și pentru user-ii locali ai sistemelor.</p> <p>24. Soluția trebuie să fie capabilă să aplice reguli de control al perifericelor chiar și atunci când nu este conectat la rețeaua companiei, cu posibilitatea de a avea politici diferite în funcție de conectivitatea la rețeaua companiei.</p> <p>25. Soluția are abilitatea de a face discovery în interiorul bazelor de e-mail stocate pe endpoint.</p> <p>26. Soluția trebuie să permită customizarea notificărilor emise în timpul funcționării și a ferestrei în care sunt scrise aceste notificări.</p> <p>27. Soluția trebuie să fie capabilă să identifice nivelul de clasificare a documentelor din marcajele vizuale și să aplice regulile de protecție pe aceste documente.</p> <p>28. Soluția trebuie să fie capabilă să protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale.</p> <p>29. Soluția trebuie să aibă opțiunea de clasificare a datelor sau integrarea cu alte produse de clasificare a datelor.</p> <p>30. Soluția trebuie să poată aplica etichete fișierelor în funcție de originea lor, informația fiind stocată securizat pentru a nu putea fi alterată de utilizator.</p> <p>31. Soluția trebuie să fie capabilă să citească informațiile de tip META stocate în fișierele Office.</p>	<p>Directory cât și pentru user-ii locali ai sistemelor.</p> <p>24. Soluția este capabilă să aplice reguli de control al perifericelor chiar și atunci când nu este conectat la rețeaua companiei, cu posibilitatea de a avea politici diferite în funcție de conectivitatea la rețeaua companiei.</p> <p>25. Soluția are abilitatea de a face discovery în interiorul bazelor de e-mail stocate pe endpoint.</p> <p>26. Soluția permite customizarea notificărilor emise în timpul funcționării și a ferestrei în care sunt scrise aceste notificări.</p> <p>27. Soluția este capabilă să identifice nivelul de clasificare a documentelor din marcajele vizuale și să aplice regulile de protecție pe aceste documente.</p> <p>28. Soluția este capabilă să protejeze documente nemarcate ce au conținut ce provine din documente clasificate cu marcaje vizuale.</p> <p>29. Soluția are opțiunea de clasificare a datelor sau integrarea cu alte produse de clasificare a datelor.</p> <p>30. Soluția poate aplica etichete fișierelor în funcție de originea lor, informația fiind stocată securizat pentru a nu putea fi alterată de utilizator.</p> <p>31. Soluția este capabilă să citească informațiile de tip META stocate în fișierele Office.</p>
--	--	--	--	---	--

				<p>32. Soluția trebuie să ofere utilizatorilor capabilități de clasificare manuala a email-ului la momentul trimiterii unui e-mail folosind clientul Outlook office.</p> <p>33. Soluția trebuie să ofere politici de securitate out-of-box care pot fi constumizate de către utilizator.</p> <p>34. Soluția trebuie să ofere posibilitatea clasificării în timp real pentru a minimiza false pozitive.</p> <p>35. Soluția trebuie să permită protejarea stațiilor de lucru mobile care sunt/nu sunt conectate la rețea.</p>	<p>32. Soluția oferă utilizatorilor capabilități de clasificare manuala a email-ului la momentul trimiterii unui e-mail folosind clientul Outlook office.</p> <p>33. Soluția oferă politici de securitate out-of-box care pot fi constumizate de către utilizator.</p> <p>34. Soluția oferă posibilitatea clasificării în timp real pentru a minimiza false pozitive.</p> <p>35. Soluția permite protejarea stațiilor de lucru mobile care sunt/nu sunt conectate la rețea.</p> <p>36. Solutia este capabilă să comunice cu alte componente de retea prin protocol Open DXL pentru blocarea incercarilor de exfiltrare de date din cadrul infrastructurii.</p> <p>37. Solutia permite clasificarea manuala a fisierelor, intr-un mod granular asigant pe grupuri, OU-uri sau useri de AD</p> <p>38. Solutia permite managementul incidentelor si cazurilor in mod granular si sa permita asignarea de useri ePO pe acestea</p> <p>39. Solutia permite obfuscarea campurilor sensibile ale incidentelor raportate, in functie de utilizator si setul de permisiuni al acestuia</p> <p>40. Solutia pune la dispozitie un utilitar de tip "wizard" pentru ghidarea administratorului in crearea politicilor initiale DLP</p>	
--	--	--	--	---	---	--

				<p>41. Solutia suportă solutii terte de clasificare a datelor, precum Boldon James, Titus si Azure Information Protection</p> <p>42. Solutia permite exportul si importul politicilor, clasificarilor si regulilor create</p> <p>43. Solutia dispune de o unealta de testare a clasificarilor in consola, pentru a permite testarea match-urilor fara a fi necesara schimbarea politicilor DLP si actualizarea acestora pe clienti</p> <p>44. Solutia dispune de ghidaj pentru troubleshooting in cadrul interfetei de administrare a acesteia</p> <p>45. Solutia poate scana in fundal email-urile trimise din Outlook, pentru a nu impacta exeperienta utilizatorilor in mod negativ</p> <p>46. Solutia poate adăuga atribute costumizabile in cadrul incidentelor DLP, precum managerul utilizatorului, regiunea utilizatorului, ID, etc</p> <p>47. Solutia suportă utilizare de Rest API pentru extragerea evenimentelor de DLP si a detaliilor atribuite acestora.</p> <p>III. Consola de administrare</p> <p>1. Consola de administrare trebuie sa se poată instala pe unul din următoarele sisteme de operare pe 64 de biți:</p> <ul style="list-style-type: none"> • Microsoft Windows Sever 2016, • Microsoft Windows Sever 2012 Release 2 (R2), • Microsoft Windows Server 2012. 	<p>41. Solutia suportă solutii terte de clasificare a datelor, precum Boldon James, Titus si Azure Information Protection</p> <p>42. Solutia permite exportul si importul politicilor, clasificarilor si regulilor create</p> <p>43. Solutia dispune de o unealta de testare a clasificarilor in consola, pentru a permite testarea match-urilor fara a fi necesara schimbarea politicilor DLP si actualizarea acestora pe clienti</p> <p>44. Solutia dispune de ghidaj pentru troubleshooting in cadrul interfetei de administrare a acesteia</p> <p>45. Solutia poate scana in fundal email-urile trimise din Outlook, pentru a nu impacta exeperienta utilizatorilor in mod negativ</p> <p>46. Solutia poate adăuga atribute costumizabile in cadrul incidentelor DLP, precum managerul utilizatorului, regiunea utilizatorului, ID, etc</p> <p>47. Solutia suportă utilizare de Rest API pentru extragerea evenimentelor de DLP si a detaliilor atribuite acestora.</p> <p>III. Consola de administrare</p> <p>1. Consola poate fi instalată pe unul din următoarele sisteme de operare pe 64 de biți:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 Release 2 (R2) • Microsoft Windows Server 2012
--	--	--	--	--	--

				<p>2. Soluția trebuie să permită instalarea/dezinstalarea agentului în mod centralizat.</p> <p>3. Consola trebuie să permită pe lângă distribuirea componentelor native și împachetarea aplicațiilor de la terți și instalarea acestora pe stațiile de lucru.</p> <p>4. Consola trebuie să permită atribuirea automată a politicilor pe stații și servere în funcție de specificațiile sistemului. (Ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare).</p> <p>5. Consola de administrare trebuie să poată fi integrată cu Active Directory.</p> <p>6. Consola de administrare trebuie să poată fi instalată într-un mediu virtual.</p> <p>7. Consola de administrare trebuie să utilizeze bază de date freeware sau licența soluției să cuprindă și licența bazei de date utilizate.</p> <p>8. Consola de administrare permite instalarea unei componente de comunicare în DMZ pentru a putea permite sincronizarea sistemelor prin internet.</p>	<ul style="list-style-type: none"> • Windows Server 2008 SP2 Standard, Enterprise, Datacenter • Windows Server 2008 R2 Standard, Enterprise, Datacenter <p>2. Soluția permite instalarea/dezinstalarea agentului în mod centralizat.</p> <p>3. Consola permite pe lângă distribuirea componentelor native și împachetarea aplicațiilor de la terți și instalarea acestora pe stațiile de lucru.</p> <p>4. Consola permite atribuirea automată a politicilor pe stații și servere în funcție de specificațiile sistemului. (Ex: Platforma desktop/server, Subnet, tip procesor, sistem de operare).</p> <ul style="list-style-type: none"> - Sincronizarea dintre server și client se face atât dinspre client către server, cât și invers. <p>5. Consola de administrare poate fi integrată cu Active Directory.</p> <p>6. Consola de administrare poate fi instalată într-un mediu virtual.</p> <p>7. Consola de administrare utilizează bază de date freeware sau licența soluției să cuprindă și licența bazei de date utilizate.</p> <p>8. Consola de administrare permite instalarea unei componente de comunicare în DMZ pentru a putea permite sincronizarea sistemelor prin internet.</p> <ul style="list-style-type: none"> - Comunicarea cu serverul de administrare se poate face prin intermediul unui singur agent. 	
--	--	--	--	--	--	--

				<p>9. Acces-ul în consola de administrare să poată fi făcut pe baza credențialelor din Active Directory.</p> <p>10. Consola de administrare trebuie să permită crearea de roluri în mod granular pentru cei ce o administrează.</p> <p>11. Toate acțiunile utilizatorilor în consola de administrare trebuie auditate.</p> <p>12. Consola trebuie să permită construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronica (E-mail).</p> <p>13. Canalul de comunicație dintre serverul de administrare și componentele distribuite pe calculatoare trebuie să fie criptat.</p> <p>14. Componenta ce asigură canalul de comunicație dintre server și stații de lucru trebuie să fie văditată din punct de vedere al securității. (Ex: FIPS, Common Criteria, Etc.)</p>	<p>- Soluția permite filtrarea evenimentelor ce sunt generate de componentele aflate pe stațiile de lucru astfel încât baza de date să nu se încarce cu informații considerate inutile.</p> <p>- Soluția permite configurarea unui mesaj de login.</p> <p>- Soluția poate folosi un proxy pentru contactarea serverului de actualizare al producătorului.</p> <p>9. Accesul în consola de administrare poate fi făcut pe baza credențialelor din Active Directory.</p> <p>Accesul în consola de management trebuie să se poată face pe baza certificatelor x509.</p> <p>10. Consola de administrare permite crearea de roluri în mod granular pentru cei ce o administrează.</p> <p>11. Toate acțiunile utilizatorilor în consola de administrare sunt auditate.</p> <p>12. Consola permite construirea unei liste de contacte în vederea folosirii acestora pentru notificări prin mesagerie electronica (E-mail).</p> <p>13. Canalul de comunicație dintre serverul de administrare și componentele distribuite pe calculatoare este criptat.</p> <p>14. Componenta ce asigură canalul de comunicație dintre server și stații de lucru este văditată din punct de vedere al securității. (Ex: FIPS, Common Criteria, Etc.)</p>	
--	--	--	--	---	--	--

				<p>15. Canalul de comunicație dintre consola și cei ce o accesează trebuie să fie criptat.</p> <p>16. Consola de administrare trebuie să poată fi accesată de pe orice computer din rețea în mod Web securizat utilizând un browser standard (Internet Explorer, Chrome, Firefox), fără necesitatea instalării de software adițional.</p> <p>17. Intervalul de transmitere a evenimentelor de pe client către server poate fi modificat.</p> <p>18. Consola trebuie să poată detecta prezența pe rețea a sistemelor noi apărute prin intermediul unor senzori.</p> <p>19. Consola trebuie să folosească un propriu index pentru a identifica și actualiza datele despre sistemele care își schimbă proprietăți precum nume, IP și configurații hardware;</p> <p>20. Consola permite automatizarea de sarcini de instalare/dezinstalare a</p>	<p>15. Canalul de comunicație dintre consola și cei ce o accesează trebuie să fie criptat.</p> <p>16. Consola de administrare este accesată de pe orice computer din rețea în mod Web securizat utilizând un browser standard (Internet Explorer, Chrome, Firefox), fără necesitatea instalării de software adițional.</p> <ul style="list-style-type: none"> - Consola de administrare poate fi accesată de pe orice computer din rețea în mod securizat, fără necesitatea instalării de software adițional. - Dacă serverul de administrare este accesat prin intermediul unei interfețe web este posibil importul unui certificat ssl generat de o autoritate locală, înlocuind astfel pe cel auto-generat. - Intervalul de sincronizare între server și componente poate fi modificat. <p>17. Intervalul de transmitere a evenimentelor de pe client către server poate fi modificat.</p> <p>18. Consola detectează prezența pe rețea a sistemelor noi apărute prin intermediul unor senzori.</p> <p>19. Consola folosește un propriu index pentru a identifica și actualiza datele despre sistemele care își schimbă proprietăți precum nume, IP și configurații hardware;</p> <p>20. Consola permite automatizarea de sarcini de instalare/dezinstalare a componentelor pe stațiile de</p>	
--	--	--	--	--	---	--

				<p>componentelor pe stațiile de lucru, de rulare a rapoartelor și de transmiterea de notificări prin mesagerie electronica.</p> <p>21. Consola trebuie să prezinte cel puțin următoarele informații despre sistemele administrate: numele sistemului, utilizatorul logat, produsele instalate, tipul de system de operare și adresa IP.</p> <p>22. Serverul de administrare trebuie să fie capabil să declanșeze acțiuni automate atunci când anumite condiții sunt îndeplinite (Ex: Generarea unui eveniment pe server, pe o stație de lucru, detectarea unui nou sistem în rețea).</p> <p>23. Consola trebuie sa permita aplicarea de politici diferite pentru sisteme pe:</p> <ul style="list-style-type: none"> • Sisteme individuale, • Grupuri de sisteme, • Sisteme din AD ce sunt același OU. <p>24. Consola trebuie să știe să lanseze automat aplicații externe și să injecteze parametrii din evenimente.</p> <p>25. Consola trebuie să permită accesarea log-ului componentei de sincronizare de pe sisteme în timp real prin intermediul unui serviciu web.</p> <p>26. Consola trebuie să permită vizualizarea incidentelor de securitate și crearea de cazuri.</p>	<p>lucru, de rulare a rapoartelor și de transmiterea de notificări prin mesagerie electronica.</p> <p>21. Consola prezintă cel puțin următoarele informații despre sistemele administrate: numele sistemului, utilizatorul logat, produsele instalate, tipul de system de operare și adresa IP. De asemenea consola se integrează cu sisteme de ticketing extern precum BMC Remedy si HP OpenView.</p> <p>22. Serverul de administrare este capabil să declanșeze acțiuni automate atunci când anumite condiții sunt îndeplinite (Ex: Generarea unui eveniment pe server, pe o stație de lucru, detectarea unui nou sistem în rețea).</p> <p>23. Consola permite aplicarea de politici diferite pentru sisteme pe:</p> <ul style="list-style-type: none"> • Sisteme individuale, • Grupuri de sisteme, • Sisteme din AD ce sunt același OU. <p>24. Consola știe să lanseze automat aplicații externe și să injecteze parametrii din evenimente.</p> <p>25. Consola permite accesarea log-ului componentei de sincronizare de pe sisteme în timp real prin intermediul unui serviciu web.</p> <p>26. Consola permite vizualizarea incidentelor de securitate și crearea de cazuri.</p>	
--	--	--	--	---	--	--

				<p>27. Consola trebuie să permită integrarea și altor aplicații/echipamente de securitate ex. (Antivirus, SandBox, Proxy, Firewall) într-o consola unica pentru a unifica administrarea acestora.</p> <p>IV. Raportarea</p> <p>1. Consola de administrare trebuie să asigure generarea de rapoarte despre nodurile administrate și despre evenimentele generate de ele.</p> <p>2. Consola trebuie să permită crearea de noi rapoarte în mod granular cu informații extrase din evenimente, sau despre sistemele administrate.</p> <p>3. Rapoartele trebuie să fie generate sub forma de tabel, lista, sumar, sau grafic istoric.</p> <p>4. Rapoartele trebuie să poată să fie exportate în format pdf, csv, html.</p> <p>5. Rapoartele trebuie să poată să fie salvate ca fișiere sau trimise prin e-mail.</p> <p>6. Rapoartele trebuie să poată să fie exportate într-un format</p>	<p>27. Consola permite integrarea și altor aplicații/echipamente de securitate ex. (Antivirus, SandBox, Proxy, Firewall) într-o consola unica pentru a unifica administrarea acestora.</p> <p>28. Consola are capabilitati de diagnoza si sa ofere recomandari si solutii pentru problemele detectate</p> <p>29. Consola suportă autentificare in regim Single Sign On (SSO) print utilizarea unei solutii de IDP</p> <p>30. Consola dispune de posibilitatea de a necesita aprobare din partea managerului pentru schimbarile politicilor si task-urilor din cadrul solutiei.</p> <p>IV. Raportarea</p> <p>1. Consola de administrare asigură generarea de rapoarte despre nodurile administrate și despre evenimentele generate de ele.</p> <p>2. Consola permite crearea de noi rapoarte în mod granular cu informații extrase din evenimente, sau despre sistemele administrate.</p> <p>3. Rapoartele sunt generate sub forma de tabel, lista, sumar, sau grafic istoric.</p> <p>4. Rapoartele pot fi exportate în format pdf, csv, html. Rapoartele pot fi personalizate cu logo-ul companiei.</p> <p>5. Rapoartele pot fi salvate ca fișiere sau trimise prin e-mail.</p> <p>6. Rapoartele pot fi exportate într-un format arhivat și expediate</p>	
--	--	--	--	---	--	--

				<p>arhivat și expediate automat pe e-mail unor destinații presetate.</p> <p>7. Consola trebuie să permită să evalueze evenimentele primite de la stațiile de lucru și filtrarea lor pentru o mai bună identificare a informațiilor relevante.</p> <p>8. Să se poată genera rapoarte utilizând:</p> <ul style="list-style-type: none"> • Log-ul de audit administrativ, • Detalii despre sistemele administrate (detalii de configurare, hardware, utilizator), • Evenimente de sisteme, • Informații despre politicile și sarcinile aplicate sistemelor, • Informații furnizate de senzori. <p>V. Solicități suplimentare</p> <p>1. Oferta trebuie să acopere 100 de stații de lucru.</p> <p>2. Ofertantul trebuie să posede oficiu de suport local, iar timpul de suport să fie 8/24 ore și 5/7 zile.</p> <p>3. Oferta trebuie să includă și serviciile de instalare și configurare.</p> <p>4. Ofertantul trebuie să fie partener oficial al furnizorului de servicii DLP.</p> <p>5. Ofertantul trebuie să aibă în state minim doi specialiști tehnici certificați pe produsul propus.</p> <p>6. Ofertantul la solicitarea cumpărătorului (după necesitate) să fie pregătit pentru a prezenta funcționalitățile produsului instalat, pe o platformă de testare, înainte de scurgerea timpului de anunțare a învingătorului.</p>	<p>automat pe e-mail unor destinații presetate.</p> <p>7. Consola permite să evalueze evenimentele primite de la stațiile de lucru și filtrarea lor pentru o mai bună identificare a informațiilor relevante.</p> <p>8. Pot fi generate rapoarte utilizând:</p> <ul style="list-style-type: none"> • Log-ul de audit administrativ, • Detalii despre sistemele administrate (detalii de configurare, hardware, utilizator), • Evenimente de sisteme, • Informații despre politicile și sarcinile aplicate sistemelor, • Informații furnizate de senzori. <p>V. Solicități suplimentare</p> <p>1. Oferta comercială este pentru 100 stații de lucru.</p> <p>2. Dispunem de oficiu de suport local, iar timpul de suport să fie 8/24 ore și 5/7 zile.</p> <p>3. Oferta comercială include și serviciile de instalare și configurare.</p> <p>4. Compania RSD este partener oficial al companiei Trellix.</p> <p>5. Prezentăm CV-ul la doi specialiști tehnici angajați ai RSD-ului, certificați pe soluțiile Trellix.</p> <p>6. La solicitarea suntem pregătiți pentru a prezenta funcționalitățile produsului instalat, pe o platformă de testare, înainte de scurgerea timpului de anunțare a învingătorului.</p>	
--	--	--	--	--	--	--

				7. Oferta să conțină costul utilizării soluției pentru un an calendaristic și nelimitat (dacă există acest tip de licență). 8. În dependență tipul licenței achiziționate (anuală sau pentru totdeauna), suportul trebuie să fie inclus în oferta de preț.	7. Oferta comercială conțină costul utilizării soluției pentru un an calendaristic (subscripție) și nelimitat (Perpetual) 8. În dependență tipul licenței achiziționate (anuală sau pentru totdeauna), suportul este inclus în oferta comercială.	
Total lot 1						
TOTAL						

Numele, Prenumele: Bîrsan Vitalie

În calitate de: Administrator

Ofertantul: ICS Reliable Solutions Distributor SRL

Adresa: Mun. Chișinău str. Alexandru cel Bun 85