Specificaţii tehnice (F4.1)

În cazul unei discrepanţe sau al unui conflict cu cerințele din secțiunea 2. Fișa de date a achiziției (FDA), prevederile din FDA vor prevala asupra prevederilor de mai jos.

Numărul procedurii de achiziţie nr. ocds-b3wdp1-MD-1604066688443 din 30 oct 2020

Denumirea procedurii de achiziţie: Licența pentru antivirus pentru anul 2021

Cod CPV	Denumirea bunurilor	Mode-lul artico-lului	Țara de origi-ne	Pro-ducă-torul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standa rde de referin ță
1	2	3	4	5	6	7	8
Lotul 1: Licența pentru antivirus pentru anul 2021							
48760000-3	Licența pentru antivirus pentru anul 2021	*BitDefender GravityZone Business Security*	România	România	*Tip: Subscriere anuală pentru soluția de protecție și securitate, pentru 100 locuri de muncă (PC/laptop/VDI)* I. Componente ale sistemului antivirus: A. Protecție 1. Controlul programelor active * Încredere față de programele care au o semnătură digital Pentru programe necunoscute: * Introducerea automată într-un grup (restricții slabe, restricții puternice, nesigur) * Utilizare analiza euristică pentru a determina grupul * Eliminare regulile de control ale programului care nu au accesate mai mult de un anumit număr de zile 2. File Anti-Virus * Nivel de securitate (scăzut, recomandat, ridicat) * Acțiune când se detectează o amenințare (solicitați acțiune, blocați accesul (dezinfectați / ștergeți dacă dezinfecția nu reușește)) * Tipuri de fișiere (toate fișierele, fișierele scanate după format, fișierele scanate prin extensie) * Localizare (toate unitățile detașabile, toate unitățile hard disk, toate unitățile de rețea) * Analiza semnăturii * Analiza euristică	Conform specificației tehnica anexate	Nu se aplică

Digitally signed by Cioclea Victor
Date: 2020.11.04 23:24:12 EET
Reason: MoldSign Signature
Location: Moldova

					(suprafață, medie, profundă) * Optimizarea verificării - Scanarea numai a fișierelor noi și modificate * Verificarea fișierelor compuse: - Scanare arhive - Verificare pachetele de instalare - Verificare obiecte OLE imbricate - Verificare obișnuită - opțională (despachetați fișierele compuse în fundal / despachetați fișiere compozite de dimensiuni mari) * Modul de testare (inteligent, la accesarea și schimbarea, la accesare, în timpul execuției) * Tehnologii de scanare * Suspendarea sarcinii (conform programului, la începutul programelor) este opțională 3. Firewall * Reguli pentru programe * Reguli pentru pachete * Zone (rețele disponibile) * Sistem de detectare a intruziunilor - blocarea calculatorului atacat pentru un anumit număr de minute 4. Antivirusul poștal * Nivel de securitate (scăzut, recomandat, ridicat) * Zonă de protecție (numai mesaje primite și trimise / mesaje primite) * Integrarea în sistem (POP3 trafic / SMTP / NNTP / IMAP, ICQ / MSN, MS Office Outlook plug-in, plug-in The Bat) * Metodele de verificare (a verifica link-urile pe baza Web-link-uri suspecte, verificare link-urile pe baza fishing Web-link-uri) * Analiza euristică (suprafață, medie, profundă) * Verificarea fișierelor compuse: - Posibilitatea de scanați ori ne scanare arhivele - Posibilitatea de scanați ori ne scanare obiecte cu un anumit volum * Filtru atașament (după formatul fișierului) 5.Web-antivirus * Metode de verificare (verificați linkurile către baza de		

					date a adreselor Web suspecte, verificați linkurile către baza de date a adreselor Web de fishing) * Limitați timpul cache al fragmentelor în câteva secunde. * adrese de încredere (add / change / delete / export / import) * Acțiune (cerere / bloc / permite) 6. Protecție proactivă * Analiza activității proceselor * Monitorizarea sistemului de registru 7. Anti-hacker * Reguli pentru programe * Reguli pentru pachete * Zone (rețele disponibile) * Sistem de detectarea intruziunilor Blocați computerul atacat pentru un anumit număr de mine. 8. Anti-Spy * Anti-banner (listaneagră, listaalbă) * Anti-apelare (adrese de încredere) 9. Anti-Spam * Nivelul de agresivitate (scăzut, recomandat, ridicat, blocați tot) * Integrarea în sistem (POP3 trafic / SMTP / NNTP / IMAP, ICQ / MSN, MS Office Outlook plug-in, plugin The Bat) * Metodele de verificare (a verifica link-urilepebaza Web-link-uri suspecte, verificați link-urile pe baza phishing Web-link-uri) * Algoritmi pentru recunoaștere (analiza expresiilor pe baza de date Resent Terms, utilizarea unei baze de date extinse, analiza anteturilor mesajelor PDB, recunoaștere a imaginii GSG, algoritmul de autoînvățarei Bayes pentru analiza textului) * Lista albă * Lista neagră *Instruire (prezența maestrului de formare) B. Scanare Tipuri: 1. Scanare completă 2. Scanare rapidă Specificarea: * Nivel de securitate (scăzut, recomandat, ridicat) * Acțiunecând se detectează o amenințare (cereți la sfârșitul scanării, cereți în timpul		

					scanării, nu întrebați: tratați, ștergeți dacă tratamentul nu este posibil) * Modul de lansare (în fiecare zi, în fiecare zi lucrătoare, la fiecare oră, în fiecare zi a lunii) C. Actualizare * Mod de pornire: automat, după o anumită perioadă, manual * Setări proxy * Sursa de actualizare (serverele de actualizare ale companiei producătoare, servere de administrare, surse adăugătoare) * Modul de pornire: - executare sarcina cu drepturi de cont (nume de utilizator, parolă) * Distribuirea actualizărilor: -Copierea actualizărilor într-un dosar (cu indicarea de către utilizator a adresei dosarului) D. Mai multe opțiuni * Auto-apărarea programului * Dezactivarea controlului extern al programului * Protecția prin parolă * Neexecutarea sarcinilor programate atunci când rulează pe baterie * Carantină și spațiu de stocare de rezervă (nu mai mult de un anumit număr de zile de stocare a obiectelor, dimensiunea obiectelor, verificarea fișierelor în carantină după actualizare) * Posibilitatea de controlate porturi (Control toate porturile / porturile selectate) * Protecție antivirus pentru nodurile principale ale unei rețele: stații de lucru, laptopuri, servere de fișiere; * Producătorul trebuie să facă parte din grupul liderilor ori a vizionarilor în ceea ce privește protecția pentru endpoint așa cum este definit de Gartner 2019. * Produsul trebuie să salveze obiectele identificate ca fiind suspecte în carantină sau într-un director dedicat în format criptat. * Produsul trebuie să permită ca instalarea să fie efectuată pe		

					un computer local sau la distanță. Produsul trebuie să ofere suport pentru sisteme de operare Windows. * Consola de administrare a produsului trebuie sa fie instalata on-premise (nu se accepta consola web). * Produsul trebuie să permit instalarea dintr-un singur kit de instalare care să includă toate pachetele necesare pentru implementare. * Produsul trebuie să ofere administratorului posibilitatea de împiedicare a acțiunilor periculoase pentru sistemul de operare ale aplicațiilor, și să asigure controlul accesului la resursele sistemului de operare și la datele confidențiale. - Produsul trebuie să permită crearea, păstrarea și implementarea imaginilor a sistemului de operare, cu ajutorul consolei de administrare dedicată. - Produsul trebuie să permită detectarea automată a vulnerabilităților din sistemul de operare și a aplicațiilor instalate. - Produsul trebuie să permită administratorului să identifice toate încercările utilizatorului de pornire a aplicațiilor și să reglementeze lansarea aplicațiilor prin intermediul regulilor de control pentru pornirea aplicațiilor. III. Condiții suplimentare: - Furnizorul trebuie să ofere instruiri gratuite pentru 4 persoane de fiecare dată când apare o versiune nouă a soluției. În cazul în care în decursul anului nu apare nici una se efectuează cel puțin o instruire gratuită pentru 4 persoane pentru menținerea nivelului de cunoaștere a soluției de		

					securitate cu endpoint date. - În cazul unei alte soluții de securitate cu endpoint decât Kaspersky, Furnizorul trebuie să efectueze gratuit instruirea a 4 persoane în privința instalării, utilizării și administrării soluției oferite până la 10 decembrie 2020. - La necesitatea și cererea Beneficiarului, Furnizorul trebuie să efectueze gratuit auditul instalării, setărilor de securitate a soluției cu endpoint oferite și să ofere o listă de recomandări de modificare/adaptare a lor cu scopul minimizării riscurilor de securitate pentru Beneficiar	

Semnat:_____
Numele, Prenumele: Victor CIOCLEA
În calitate de: Administrator
Ofertantul: S.C. „RTS ONE” S.R.L. Adresa: mun. Chișinău, str. Mit. Bănulescu-Bodoni 59/B of. 815