ANUNȚ DE PARTICIPARE
privind achiziționarea serviciilor informatice de securitate antivirus pentru protecția infrastructurii IT prin procedura de achiziție de valoare mică

1. Denumirea autorității contractante: Curtea de Conturi a Republicii Moldova.
2. IDNO: 1007601001330
3. Adresa: mun. Chișinău bd. Ştefan cel Mare 69
4. Numărul de telefon/fax: Tel/fax: 022-266-050
5. Adresa de e-mail și de internet a autorității contractante: ccrm@ccrm.md, www.ccrm.md
6. Adresa de e-mail sau de internet de la care se va putea obține accesul la documentația de atribuire: documentația de atribuire este anexată în cadrul procedurii în SIA RSAP
7. Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea/prestarea/executarea următoarelor bunuri /servicii/lucrări:

Nr. d/o	Cod CPV	Denumirea serviciului solicitat	U/M	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată
1.	487610000-0	**Servicii informatice de securitate antivirus pentru protecția infrastructurii IT**	buc.	1	Conform Anexei	160 000,00
Valoarea estimată a achiziției, fără TVA, lei:						**160 000,00**

8. Admiterea sau interzicerea ofertelor alternative: nu se admite.
9. Termenii și condițiile de livrare/prestare/executare solicitați: 15 zile lucrătoare de la data înregistrării contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.
10. Termenul de valabilitate a contractului: 31.12.2022.
11. Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse; se menționează informațiile solicitate (DUAE, documentație):

Nr. d/o	Denumirea documentului/cerinței	Cerințe suplimentare față de document	Obligativitatea
1.	Declarație privind valabilitatea ofertei	Conform Anexei nr. 8 din Documentația standard aprobată prin Ordinul MF nr. 115 din 15.09.2021 Confirmat prin semnătura electronică	Obligatoriu
2.	Specificații tehnice	Conform Anexei nr. 22 din Documentația standard aprobată prin Ordinul MF nr. 115 din 15.09.2021 Confirmat prin semnătura electronică	Obligatoriu
3.	Specificații de preț	Conform Anexei nr. 23 din Documentația standard aprobată prin Ordinul MF nr. 115 din 15.09.2021. Confirmat prin semnătura electronică	Obligatoriu
4.	Certificat de înregistrare a întreprinderii	Certificat/decizie de înregistrare a întreprinderii/extras din Registrul de Stat al persoanelor juridice, confirmată prin aplicarea semnăturii electronice a Participantului.	Obligatoriu
5.	Informația despre ofertant	Original cu aplicarea semnăturii electronice a Participantului	Obligatoriu

12. Criteriul de evaluare aplicat pentru adjudecarea contractului: Prețul cel mai scăzut.
13. Termenul limită de depunere/deschidere a ofertelor: până la: [ora exactă]: conform SIA RSAP *pe* [data]: conform SIA RSAP
14. Adresa la care trebuie transmise ofertele sau cererile de participare: SIA RSAP
15. Termenul de valabilitate a ofertelor: *60 zile.*
16. Locul deschiderii ofertelor: SIA RSAP, Ofertele întîrziate vor fi respinse.
17. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare: *Limba de Stat.*
18. Denumirea și adresa organismului competent de soluționare a contestațiilor: *Agenția Națională pentru Soluționarea Contestațiilor, Adresa: mun. Chișinău, bd. Ştefan cel Mare și Sfânt nr.124 (et.4), MD 2001;Tel/Fax/email: 022-820 652, 022 820-651, contestatii@ansc.md.*

Componența grupului de lucru:

Nr.	Nume, Prenume	Funcția în cadrul grupului de lucru	Semnătura
1	**Victor Munteanu**	**Conducătorul grupului de lucru**	Digitally signed by Munteanu Victor Date: 2022.10.18 13:33:32 EEST Reason: MoldSign Signature Location: Moldova
2	**Paduca Natalia**	**Membru**	Digitally signed by Paduca Natalia Date: 2022.10.18 13:29:45 EEST Reason: MoldSign Signature Location: Moldova
3	**Babără Vitalie**	**Membru**	Digitally signed by Babără Vitalie Date: 2022.10.18 11:50:28 EEST Reason: MoldSign Signature Location: Moldova
4	**Stîrcea Ustim**	**Membru**	Digitally signed by Stîrcea Ustim Date: 2022.10.18 11:51:18 EEST Reason: MoldSign Signature Location: Moldova
5	**Goriuc Teodorina**	**Membru**	
6	**Balan Violeta**	**Membru**	Digitally signed by Balan Violeta Date: 2022.10.18 11:57:27 EEST Reason: MoldSign Signature Location: Moldova
7	**Oleinic Ion**	**Secretarul grupului de lucru**	Digitally signed by Oleinic Ion Date: 2022.10.18 11:41:28 EEST Reason: MoldSign Signature Location: Moldova

Anexa

Specificația serviciilor informatice de securitate antivirus pentru protecția infrastructurii IT:

Se solicita achizitia a unei soluții corporative de tip anti-malware, care să ofere protecție, securitatea și scanarea vulnerabilităților a 150 de stații de lucru, servere fizice și virtualizate, cutii poștale pentru o perioadă de 36 luni. Produsul (soluția) să reprezinte o platformă integrată pentru managementul securității, gândita ca o soluție modulară. Produsul trebuie să conțină următoarele module:

1. Consola de management care asigura funcționalități de administrare.
2. Protecție stații și servere fizice/virtuale.
3. Protecție și securitate pentru serverele email Microsoft Exchange

1. CONSOLA DE MANAGEMENT

1.1 Instalare și configurare:

1.1.1. Pachetul de instalare necesar să fie livrat ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Consola nu va necesita o licenta suplimentara pentru sistemul de operare. Imaginea de tip template trebuie să se poată importa în Microsoft Hyper-V

1.1.2. Soluția să fie scalabilă, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeasi masina virtuală.

1.1.3. Soluția este necesar să includă aditional și un modul de balansare (load balancer) pentru cazurile în care mai multe mașini virtuale ale componentei de management sunt instalate cu acelasi rol (pentru Load Balancing și performanta/redundanta).

1.2 Cerinte generale:

1.2.1. Produsul trebuie să suporte licențierea per procesor fizic (socket). în felul acesta numărul mașinilor virtuale poate varia oricând, ele fiind protejate.

1.2.2. Soluția trebuie să includa un modul de update server prin care se asigură actualizarea de produs și a semnaturilor.

1.2.3. Soluția trebuie să permita activarea/dezactivarea actualizărilor de produs/semnaturi.

1.2.4. Soluția trebuie să permită stabilirea actualizarii automate a consolei de management prin stabilirea recurenței zilnice, săptămânale sau lunare, dar și prin stabilirea intervalului orar în care acesta se va actualiza. De asemenea, permite și trimiterea unei alerte de nefuncționalitate, cu 30 de minute înainte de actualizare.

1.2.5. Notificarile – prezente în interfața, trimise catre una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție virusi, actualizari de produs disponibile).

1.2.6. Soluția trebuie să permită instalarea serviciului de SMNP prin care se pot raporta statusul mașinilor din cadrul componenței de management.

1.2.7. Soluția trebuie să permită creare unei copii de siguranta a bazei de date a consolei de administrare, la cerere sau programată, putând fi stocată local, pe un server FTP sau în rețea.

1.3 Panou de monitorizare și raportare (Dashboard):

1.3.1. Rapoartele din panoul de monitorizare necesar să fie posibil configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport

1.3.2. Panoul central necesar să contina rapoarte pentru toate modulele suportate.

1.4 Inventarierea retelei – managementul securitatii:

1.4.1. Soluția să fie integrata cu domenii Active Directory multiple, și importa inventarul acestor platforme.

1.4.2. Soluția trebuie să permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery.

1.4.3. Soluția va oferi optiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare, adresa IP, politica aplicată, ultima dată când s-a conectat (online si/sau offline) și FQDN.
1.4.4. Soluția trebuie să permită crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descarca pachetele pentru protecția stațiilor și serverelor pe care ruleaza sistemul de operare Windows, Linux,
1.4.5. Soluția trebuie să permită instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale.
1.4.6. Soluția trebuie să permită selectarea modulelor componente atunci când se crează pachetul clientului care se instalează pe mașinile fizice/virtuale.
1.4.7. Soluția trebuie să permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antimalware.
1.4.8. Soluția trebuie să ofere posibilitatea de repornire a mașinilor fizice de la distanță.
1.4.9. Soluția trebuie să ofere informatii detaliate despre fiecare task și se fiseaza daca task-ul s-a finalizat sau nu cu succes.
1.4.10. Soluția trebuie să permită configurarea centralizată a clienților antimalware prin intermediul politicilor
1.4.11. Soluția trebuie să ofere în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi.
1.4.12. Pentru integrarea cu Active Directory, se va putea defini și intervalul (in ore) de sincronizare
1.4.13. Soluția trebuie să permită descoperirea mașinilor din Microsoft Hyper-V
1.4.14. Soluția trebuie să permită descoperirea tuturor aplicatiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare.

1.5 Politici:

1.5.1. Soluția trebuie să permită configurarea setărilor clientului antimalware prin intermediul unei singure politici ce conține setări pentru toate modulele.
1.5.2. Politica să conțina optiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web,controlul dispozitivelor, power user.
1.5.3. Soluția trebuie să permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resourse (VMware), domeniu, unitati organizationale, grupuri de securitate sau useri de active directoy.
1.5.4. Politica să poata fi schimbata automat în functie de:

- IP sau clasa de IP al stației
- Gateway-ul alocat
- DNS serverul alocat
- WINS serverul alocat
- Sufix DNS pentru conexiunea dhcp
- Clientul este/nu este în acceasi rețea cu infrastructura de management (stația de lucru poate solutiona implicit numele gazdei)
- Tipul retelei (lan, wireless)
- User-ul logat pe stație

1.6 Rapoarte:

1.6.1. Soluția trebuie să contine rapoarte care prezinta statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
1.6.2. Soluția trebuie să permită vizualizarea rapoartelor curente programate de administrator.
1.6.3. Soluția trebuie să permită exportarea rapoartelor în format .pdf și detaliile ca format .csv.
1.6.4. Soluția trebuie să permită filtrarea informatiilor continute în rapoartele trimise pe mail astfel incat doar informatiile relevante cerute de către administrator vor fi transmise pe email.

1.6.5. Soluția trebuie să includă un generator de rapoarte care ofera posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, mentinand informatiile concise și ordonate corespunzator. Astfel, soluția include interogari precum: starea terminalului, evenimente terminal, evenimente Exchange.

1.6.6. Interogarea legata de starea terminalului include informații precum:

- tip masina
- infrastructura rețelei căreia îi aparține terminalul
- datele agentului de securitate
- starea modulelor de protecție
- rolurile terminalelor.

1.6.7. Interogarea legată de evenimente terminal include informații precum:

- calculatorul ținta pe care a avut loc evenimentul
- tipul starea și configurația agentului de securitate instalat
- starea modulelor și rolurilor de protecție instalate pe agentul de securitate
- denunmirea și alocarea politicii
- utilizatorul autentificat în timpul evenimentului
- evenimente (site-uri blocate, aplicatii blocate, detecțiile etc)

1.6.8. Interogarea legata de evenimente Exchange include informații precum:

- Direcția traficului e-mail
- Evenimente de securitate (detectarea programelor de tip malware sau a fisierelor atașate)
- Măsurile implementate în fiecare situație (curațarea, stergerea, înlocuirea sau carantinarea fișierului, stergerea sau respingerea e-mail-ului)

1.7 Carantina:

1.7.1. Soluția trebuie să permită restaurarea fisierelor carantinate în locatia originală sau într-o cale configurabilă.

1.7.2. Carantina trebuie să sa fie locala, pe fiecare stația administrată și va fi administrată, fie local, fie din consola de management.

1.8 Utilizatori:

1.8.1. Administrarea trebuie să se poata face pe baza de roluri.

1.8.2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat.

- Administrator companie: administreaza arhitectura consolei de management;
- Administrator rețea: administreaza serviciile de securitate;
- Reporter: monitorizeaza și generează rapoarte.

1.8.3. Utilizatorii pot fi importati din Microsoft Active Directory sau creati în consola de management.

1.8.4. Soluția trebuie să permită configurarea detaliată a drepturilor administrative, permitând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări.

1.9 Log-uri:

1.9.1. Inregistrarea actiunilor utilizatorilor.

1.9.2. Sa fie oferite informații detaliate pentru fiecare actiune a unui utilizator.

1.9.3. Sa permită filtrarea acțiunilor utilizator după numele utilizatorului, acțiune.

1.10 Actualizare:

1.10.1. Sa permită definirea de locatii de actualizare multiple.

1.10.2. Sa permită activarea/dezactivarea actualizarilor de produs și semnături.

1.10.3. Sa permită actualizarea produsului într-o rețea fără acces la Internet.

1.10.4. Soluția să dispuna un server de actualizare (update) care va face posibila stabilirea componentelor ce vor fi descarcate automat de pe internet, fără intervenția administratorului. Astfel, administratorul va putea descarca pachetele pentru protecția stațiilor și serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac sau, poate descarca pachetele pentru modul de scanare centralizata în mediile de virtualizare Hyper-V

1.10.5. Soluția să permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitand posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare să includa 2 tipuri de actualizări de produs:

- Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei
- Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc)

1.10.6. Soluția să permită stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management.

1.11 Certificate:

1.11.1. Accesul la consola de management să se faca doar prin HTTPS.

1.11.2. Serverul web, din consola centrala de management trebuie să permită importarea de certificate digitale eliberate de o autoritate de certificare autorizată sau proprie organizației.

1.11.3. Soluția trebuie să permită afișarea în consola de management informații despre certificate: nume, autoritatea emitentă, data eliberarii și data expirarii certificatelor eliberate.

2. PROTECTIE STAȚII ȘI SERVERE FIZICE SAU VIRTUALE

2.1 Caracteristici generale minimale și eliminatorii:

2.1.1. Pentru reducerea la minim a consumului de resurse, soluția antimalware trebuie să permită instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).

2.1.2. Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includa un vaccin anti-ransomware. Acest vaccin asigura protecția împotriva tuturor amenințarilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare.

2.1.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.

2.1.4. Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includa protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de invațare automată (machine learning).

2.1.5. Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includă un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate și activitați suspecte în faza pre-executie.

2.1.6. Acest modul avansat de securitate va proteja împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecarui tip de amenințare mentionat, i se vor putea stabili, independent, un nivel de protectie dorit: permisiv, normal, agresiv.

2.1.7. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, sterge sau muta în carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide dacă dorește întâi monitorizare sau dorește și blocarea amenințărilor. Aceste acțiuni menționate, vor putea fi stabilite independent, pentru fișiere sau pentru traficul din rețea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenințările care ar fi fost detectate dacă nivelul de protecție era stabilit mai agresiv).

2.1.8. Pentru a oferi un nivel aditional de protectie a stațiilor și serverelor, soluția trebuie să includa un sandbox în cloud-ul public al producatorului acesteia.

2.1.9. Modulul de Sandbox va putea trimite automat fișiere în Sandbox-ul din cloud-ul producătorului unde vor putea fi „detonate" pentru o analiză în profunzime.

2.1.10. Modulul de Sandbox trebuie să includă două variante de analiză: doar monitorizare sau blocare. în modul monitorizare utilizatorul va putea accesa fișierul dorit, pe când în modul blocare, utilizatorului i se va bloca rularea fișierului până când Sandbox-ul din cloud-ul producatorului va da verdictul.

2.1.11. Modulul de Sandbox trebuie să includa doua tipuri de actiuni remediere: implicită și de siguranță. Pentru acțiunea implicită se va putea stabili: doar raportare, dezinfectie, stergere și carantinare. Pentru actiunea de siguranta se va putea stabili: stergere sau carantinare.

2.1.12. Modulul de Sandbox trebuie să includă și posibilitatea de trimitere manuală a fișierelor în Sandbox-ul din cloud-ul producatorului. Astfel, daca administratorul suspecteaza un fisier ca fiind malițios,îl poate trimite manual în Sandbox pentru a fi „detonat" și a afla verdictul. Va putea trimite mai multe fișiere de odată, cu posibilitate de a specifica dacă vor fi „detonate" individual sau toate în acelasi timp.

2.1.13. Modulul de Sandbox poate suporta „detonarea" urmatoarelor tipuri de fisiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

2.1.14. Fisierele mentionate anterior, vor putea fi detectate corect chiar dacă sunt incluse în arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

2.1.15. Modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response") capabil să identifice amenințări avansate sau atacuri în curs de desfășurare.

2.1.16. Acest modul cuprinde colectare de date și evenimente despre hardware și software aferent fiecarei stații de lucru aducând informatii detaliate referitoare la incidentele detectate, o hartă detaliată a acestora precum și actiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate - – HyperDetect. Din punct de vedere functional modulul EDR cuprinde 2 componente distincte: senzorul ce colecteaza și procesează datele respectiv partea de analiza de securitate care are ca obiect interpretarea acestora.

2.1.17. Modulul EDR trebuie să aiba capacitatea de a evalua activitatea tipica a unui endpoint din perspectiva securitatii acestuia conform tehnicilor de atac MITRE („baselining") și poate raporta orice deviație de la acest comportament sub forma unui incident

2.1.18. Modulul EDR trebuie să permită filtrarea incidentelor din interfata grafica în functie intervalul de timp, pe baza unui scor de încredere („confidence score"), indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cât și după IP, nume fișier, nume stație.

2.1.19. Modulul EDR trebuie să permită vizualizarea detaliata a incidentelor incluzând detalii specifice fiecarui nod afectat după cum urmează: tabul „rezumat" genereaza o harta de principiu a incidentului, tabul „timeline" detaliaza incidentul în functie de amprenta de timp a fiecarei acțiuni aferente incidentului, respectiv butonul „acționeaza" care poate genera un set de măsuri specifice fiecarui element din harta incidentului (kill, carantina – la nivel de nod, investigati – virus total, sandbox, google – la nivel de fisier, adaugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod).

2.1.20. Modulul EDR trebuie să poata bloca fițiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferenta incidentului sau importate folosind un fisier CSV.

2.1.21. Modulul EDR trebuie să poată excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adauga un set de fișiere malițioase într-o lista neagra pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase.

2.1.22. Modulul EDR trebuie să permită deschiderea unei conexiuni remote catre un endpoint potential infectat pentru a permite o investigare rapida a gazdei, colecta date despre atac respectiv remedia în timp real brese de securitate eliminând astfel posibile incertitudini privitoare la comportamentul potential malițios al unor fișiere/procese, reducând timpul de remediere (downtime) în cazul în care un atac a avut succes și stația ținta trebuie reconfigurata/reinstalata, permite executarea unor comenzi în linia de comanda care se executa cu privilegii de kernel ce permit eliminarea în timp real a unor amenințari sau colectarea de date privitoare la atacul în desfășurare.

2.1.23. Modulul EDR trebuie să permită creare regulilor de detecție customizabile bazate pe procese, fișiere, registri și conexiuni de rețea.
2.1.24. Modulul EDR trebuie să permită creare regulilor de excludere customizabile bazate pe procese, fișiere, registri și conexiuni de rețea.
2.1.25. Modulul EDR trebuie să permită căutarea proactiva pe stațiile de lucru protejate a indicatorilor de compormitere precum hash-uri, nume de fișiere, nume de procese, chei de registri, valori de registri.
2.1.26. Soluția trebuie să includă un modul de tip host IPS capabil să blocheze atacuri la nivel de rețea incluzand mișcarea laterală a unor categorii de malware.
2.1.27. Modulul de tip host IPS va reprezenta o sursă de telemetrie / date despre atac pentru modulul de tip EDR, acesta din urma avand abilitatea de a integra informații despre acțiunile luate de către o potențială amenințare la nivel de rețea.

2.2 Administrare și instalare remote:

2.2.1. Înainte de instalare, administratorul trebuie să poata particulariza pachetele de instalare cu modulele dorite
2.2.2. În consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc.
2.2.3. Din consola trebuie să se poată trimite o singură politică pentru configurarea integrală a clientului de pe stații/servere.
2.2.4. Consola trebuie să includa o sectiune, „Audit", unde se vor menționa toate actiunile intreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc.
2.2.5. Soluția trebuie sa-i permită administratorulului să poata crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu.
2.2.6. Soluția trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decat cele integrate în domeniu.

2.3 Caracteristici și functionalitati principale ale modulului antimalware:

2.3.1. Soluția să permită administratorului să stabileasca actiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele actiuni:

- Actiune imiplicită pentru fișiere infectate:
  - interzice accesul
  - dezinfectează
  - ștergere
  - mută fișierele în carantina
  - nicio acțiune
- Acțiune alternativă pentru fișierele infectate:
  - interzice accesul
  - dezinfectează
  - ștergere
  - muta fișierele în carantină
- Actiune imiplicita pentru fișierele suspecte:
  - interzice accesul
  - ștergere
  - muta fișierele în carantină
  - nicio acțiune
- Acțiune alternativă pentru fișierele suspecte:
  - interzice accesul
  - ștergere
  - mută fișierele în carantină

2.3.2. Scanarea automata în timp real va putea fi setata să nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fișierelor putând fi definita de administratorul solutiei,
2.3.3. Scanarea automata a emailurilor la nivelul stației de lucru pentru POP3/SMTP.
2.3.4. Clientii antimalware pentru workstație să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, certificate, extensii sau procese, incluzând amprenta (hash) în cazul fișierelor sau certificatelor.
2.3.5. Posibilitatea de configura scanarile programate să se execute cu prioritate redusă.
2.3.6. Produsul antimalware poate fi configurat să folosească scanarea în cloud, și partial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalată în rețea.
2.3.7. Pentru o protectie sporita, soluția antimalware trebuie să aiba 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazată pe monitorizarea proceselor.
2.3.8. Pentru o mai buna gestionare a antimalware instalat pe stații, produsul trebuie să includă opțiunea de setare a unei parole pentru protecția la dezinstalare.
2.3.9. Pentru siguranta utilizatorului, clientul trebuie să includă un modul de antiphishing
2.3.10. Soluția trebuie să ofere o tehnologie de tip „preventiv / vaccin" ce va actiona împotriva potentialelor atacuri de tip ransomware.
2.3.11. Soluția trebuie să ofere un set de excluziuni predefinite pentru Roluri de tip „server" Microsoft (DNS, DHCP, AD, Exchange, Sharepoint)
2.3.12. Soluția trebuie să poata detecta atacuri de tip „file-less" incluzand pe cele ce folosesc utilitare aferente sistemelor de operare de tip interpretor de script (powershell).
2.3.13. Soluția trebuie să ofere protectie înportriva atacurilor ransomware inițiate la distanță, de pe alte stații de lucru

2.4 Anti-Exploit-Avansat:

2.4.1. Sa fie posibilitatea de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive.
2.4.2. Să depisteze în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare.
2.4.3. Sa fie protejate aplicațiile utilizate frecvent și a celor de tip „sistem"

2.5 Firewall:

2.5.1. Sa fie posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
2.5.2. Sa fie abilitatea de a detecta scanarea de porturi.
2.5.3. Sa fie posibilitatea de a seta diferite profiluri de rețea
2.5.4. Sa fie abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune

2.6 Carantina:

2.6.1. Produsul antimalware trebuia să permită stergerea automată a fișierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare.
2.6.2. Posibilitatea de a restaura un fisier din carantina în locatia lui originala.
2.6.3. Modulul de carantina trebuia să permită salvarea unei copii a fisierului infectat respectiv transmiterea acestuia catre carantina înainte de a efectua orice alta acțiune asupra acestuia.

2.7 Protecția datelor:

2.7.1. Produsul trebuie să permită blocarea datelor confidentiale transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

2.8 Controlul continutului:

2.8.1. Consola să detina integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati:

- Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini.
- Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite

2.9 Controlul aplicatiilor:

2.9.1. Pentru o mai buna inventariere și administrare, soluția trebuie să includă o secțiune în consola de administrare unde se vor regăsi toate aplicatiile descoperite în rețea, grupate dupa: nume, versiune, descoperit la, gasit pe.

2.9.2. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subprocese) după:

- Cale fisier: local, CD-ROM, portabil sau rețea
- Hash
- Certificat

2.10 Controlul dispozitivelor:

2.10.1. Modulul să poată fi instalat/dezinstalat în functie de preferinta administratorului.

2.10.2. Modulul să permită controlul urmatoarelor tipuri de dispozitive:

- Bluetooth Devices
- CDROM Devices
- Floppy Disk Drives
- Security Policies 153
- IEEE 1284.4
- IEEE 1394
- Imaging Devices
- Modems
- Windows Portable
- Printers
- Network Adapters
- Wireless Network Adapters
- Internal and External Storage

2.10.3. Modulul să permită configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client cum ar fi: permis/blocat/custom respectiv să poată limita accesul dispozitivelor externe la „read only" sau limita doar accesul la porturile USB ale endpoint-ului permitând orice alt tip de dispozitiv ce nu foloseste acest tip de port/interfata.

2.11 Power User:

2.11.1. Modulul trebuie să poata fi instalat/dezinstalat în functie de preferinta administratorului.

2.12 Actualizare:

2.12.1. Soluția trebuie să permită efectuarea actualizarii la nivel de stație în mod silențios (fară avertizare).

2.12.2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).

2.12.3. Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are și rol de server de actualizare.

2.12.4. Abilitatea de a împiedica punctele finale să iasă pe internet pentru a descărca actualizări.

3. PROTECȚIE ȘI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE

3.1 Cerinte minime de sistem:

3.1.1. Exchange server 2019, 2016, 2013 cu rol de Edge Transport sau Mailbox

3.1.2. Microsoft Windows Server 2008R2 sau mai nou

3.1.3. Produsul să ofere protectie antimalware, antispam (inclusiv antiphishing), precum și filtrare de atasamente și continut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea antimalware la cerere a bazelor de date Exchange.

3.1.4. Produsul să asigure scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail.

3.1.5. Actualizarea antimalware trebuie să poata fi facută automat la un interval de maxim 1 ora, precum și la cerere.
3.1.6. Produsul să ofere optiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, stergere, mutare în carantina).
3.1.7. Cu ajutorul unei baze de date complete cu semnaturi de spyware și a euristicii de detectie a acestui tip de programe, produsul va oferi protectie anti-spyware pentru a preveni furtul de date confidentiale.
3.1.8. Produsul să ofere protecție antispam, cu o bază de semnături actualizabilă prin internet.
3.1.9. Modulul antispam trebui să includa un filtru URL cu o baza de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice.
3.1.10. Produsul trebui să ofere filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje.
3.1.11. Produsul trebuie să ofere un serviciu/filtru online pentru înbunătățirea protecției împotriva valurilor de spam nou aparute.
3.1.12. Produsul să ofere posibilitatea de a defini politici de filtrare antimalware, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori.
3.1.13. Actualizarea produsului să fie configurabila și să se putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu.
3.1.14. Produsul trebui să ofere stațistici atât referitoare la scanarea antivirus cât și la scanarea antispam.
3.1.15. Produsul să se integreze în cadrul consolei de management unitar al soluției antivirus. Pentru usurința accesului la setările produsului din diferite medii de operare, produsul va avea consola de administrare web.

4. ALTE CERINȚE OBLIGATORII:

- Pentru soluția ofertată se solicită suport local și de la producător pentru 36 luni.
- Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local.
- Lucrările de instalare, configurare, punerea în funcţiune a soluției trebuie să fie executate de ofertant, iar costul acestora trebuie să fie incluse în oferta comercială.
- Se va oferi manual de instalare și administrare a produsului ofertat în limba română și engleză.
- Prezentarea a minim 2 certificate tehnice a persoanelor certificate pe produsul ofertat.
- Ofertantul va prezenta Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul ofertat.
- Ofertantul va pune la dispoziție cel puțin o persoana certificata în calitate de auditor intern pentru sistemul de management al securității informațiilor conform ISO/IEC 27001:2018 în cazul apariție problemelor de securitate;
- **Termen de livrare:** 15 zile lucrătoare de la data înregistrării contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.