CONTRACT Nr. 45
privind achiziţia de bunuri

Obiectul achiziţiei: **Pachete software de protecţie antivirus**
Cod CPV: **48760000-3**

"07" 04 2026 mun. Chişinău

Furnizorul de bunuri	Autoritatea contractantă
IT-LAB GRUP SRL, reprezentată prin **Administrator** **Alexei CIOBAN,** care acţionează în baza **Statutului,** denumit în continuare ***Furnizor,*** pe de o parte,	**Serviciul de Protecţie şi Pază de Stat,** reprezentat prin **Director** **Alexandru HAREA,** care acţionează în baza **Legii nr.134/2008,** denumit(ă) în continuare ***Cumpărător*** pe de altă parte,

ambii (denumiţi(te) în continuare Părţi), au încheiat prezentul Contract referitor la următoarele:

a. Achiziţionarea pachetelor software de protecţie antivirus, denumite în continuare Bunuri, în conformitate cu prevederile pct.13 al Regulamentului cu privire la achiziţiile publice de valoare mică, aprobat prin Hotărârea de Guvern nr. 870 din 14.12.2022, în baza deciziei grupului de lucru al Cumpărătorului, procesul-verbal nr. 24 din 20.03.2026.

b. Următoarele documente vor fi considerate părţi componente ale Contractului:
- Specificaţia tehnică şi de preţ, conform anexei;

c. În cazul unor discrepanţe sau inconsecvenţe între documentele componente ale Contractului, documentele vor avea ordinea de prioritate enumerată mai sus.

d. În calitate de contravaloare a plăţilor care urmează a fi efectuate de Cumpărător, Furnizorul se obligă prin prezentul contract să livreze Cumpărătorului bunurile şi să înlăture defectele lor în conformitate cu prevederile Contractului sub toate aspectele.

e. Cumpărătorul se obligă prin prezentul contract să plătească Furnizorului, în calitate de contravaloare a livrării bunurilor, preţul Contractului în termenele şi modalitatea stabilite de Contract.

1. Obiectul Contractului

1.1. Furnizorul îşi asumă obligaţia de a livra bunurile conform Specificaţiei, care este parte integrantă a prezentului Contract.
1.2. Cumpărătorul se obligă, la rândul său, să achite şi să recepţioneze Bunurile livrate de Furnizor.
1.3. Calitatea Bunurilor trebuie să corespundă standardelor tehnice. Bunurile livrate în baza contractului vor respecta standardele sau alte reglementări autorizate în ţara de origine a bunurilor.

2. Termeni şi condiţii de livrare

2.1. Livrarea Bunurilor se efectuează de către Furnizor în termen de 30 zile de la înregistrarea contractului la Trezoreria de Stat a Ministerului Finanţelor.
2.2. Documentaţia de însoţire a Bunurilor include:
a) Factură .....2 ex.
b) Act de predare-primire a bunurilor .....2 ex.
2.3. Originalele documentelor prevăzute în punctul 2.2. se vor prezenta Cumpărătorului cel târziu la momentul livrării bunurilor la destinaţia finală. Livrarea bunurilor se consideră încheiată în momentul în care sunt prezentate documentele de mai sus.

3. Preţul şi condiţii de plată

3.1. Preţul Bunurilor livrate conform prezentului Contract este stabilit în lei moldoveneşti, fiind indicat Specificaţia prezentului Contract.
3.2. Suma totală a prezentului Contract, inclusiv TVA, se stabileşte în lei moldoveneşti şi constituie: **79 639 (şaptezeci şi nouă mii şase sute treizeci şi nouă) lei 20 bani MD**.
3.3. Achitarea plăţilor pentru Bunurile livrate se va efectua în lei moldoveneşti.
3.4. Metoda şi condiţiile de plată de către Cumpărător vor fi:
a) Achitarea se va efectua după livrarea şi prezentarea documentelor aferente, conform pct. 2.2. în decurs de 15 zile.
3.5. Plăţile se vor efectua prin transfer bancar pe contul de decontare al Furnizorului indicat în prezentul Contract.

4. Condiţii de predare-primire

4.1. Bunurile se consideră predate de către Furnizor şi recepţionate de către Cumpărător dacă:
a) cantitatea Bunurilor corespunde informaţiei indicate în documentele de însoţire conform punctului 2.2. al prezentului Contract;
b) calitatea Bunurilor corespunde informaţiei indicate în Specificaţie;
c) ambalajul şi integritatea Bunurilor corespunde informaţiei indicate în Specificaţie.
4.2. Furnizorul este obligat să prezinte Cumpărătorului un exemplar original al facturii fiscale odată cu livrarea Bunurilor, pentru efectuarea plăţii. Pentru nerespectarea de către Furnizor a prezentei clauze, Cumpărătorul îşi rezervă dreptul de a majora termenul de achitare prevăzut în punctul 3.4. corespunzător numărului de zile de întârziere şi de a fi exonerat de achitarea penalităţii stabilite în punctul 10.3.

5. Standarde

5.1. Bunurile furnizate în baza contractului vor respecta standardele prezentate de către furnizor în propunerea sa tehnică.
5.2. Când nu este menţionat nici un standard sau reglementare aplicabilă se vor respecta standardele sau alte reglementări autorizate în ţara de origine a Bunurilor.

6. Obligaţiile părţilor

6.1. În baza prezentului Contract, Furnizorul se obligă:
a) să livreze Bunurile în condiţiile prevăzute de prezentul Contract;
b) să anunţe Cumpărătorul după semnarea prezentului Contract, în decurs de 5 zile calendaristice, prin telefon/fax sau mijloace electronice, despre disponibilitatea livrării Bunurilor;
c) să asigure condiţiile corespunzătoare pentru recepţionarea Bunurilor de către Cumpărător, în termenele stabilite, în corespundere cu cerinţele prezentului Contract;
d) să asigure integritatea şi calitatea Bunurilor pe toată perioada de până la recepţionarea lor de către Cumpărător.
6.2. În baza prezentului Contract, Cumpărătorul se obligă:

a) să întreprindă toate măsurile necesare pentru asigurarea recepţionării în termenul stabilit a Bunurilor livrate în corespundere cu cerinţele prezentului Contract;
b) să asigure achitarea Bunurilor livrate, respectând modalităţile şi termenele indicate în prezentul Contract.

7. Circumstanţe care justifică neexecutarea contractului

7.1. Părţile sunt exonerate de răspundere pentru neîndeplinirea parţială sau integrală a obligaţiilor conform prezentului Contract, dacă aceasta este cauzată de producerea unor cazuri de circumstanţe care justifică neexecutarea contractului (războaie, calamităţi naturale: incendii, inundaţii, cutremure de pământ, precum şi alte circumstanţe care nu depind de voinţa Părţilor).
7.2. Partea care invocă clauza circumstanţelor care justifică neexecutarea contractului este obligată să informeze imediat (dar nu mai târziu de 10 zile) cealaltă Parte despre survenirea circumstanţelor care justifică neexecutarea contractului.
7.3. Survenirea circumstanţelor care justifică neexecutarea contractului, momentul declanşării şi termenul de acţiune trebuie să fie confirmate printr-un aviz de atestare, eliberat în mod corespunzător de către organul competent din ţara Părţii care invocă asemenea circumstanţe.
7.4. În cazul în care în circumstanţele care justifică neexecutarea contractului, acesta se modifică prin acordul adiţional, inclusiv modificarea termenilor de executare, în cazul unei executări ulterioare a contractului. Când se execută pct.7.1. şi pct.7.3., părţile modifică contractul prin acord - adiţional, privind neîndeplinerea parţială sau integrală a obligaţiunilor, inclusiv modificarea termenilor în cazul suspendării şi executării ulterioare a contractului.

8. Rezoluțiunea

8.1. Rezoluţiunea Contractului se poate realiza cu acordul comun al Părţilor.
8.2. Contractul poate fi rezolvit în mod unilateral de către:
a) Cumpărător în caz de refuz al Furnizorului de a livra Bunurile prevăzute în prezentul Contract;
b) Cumpărător în caz de nerespectare de către Furnizor a termenelor de livrare stabilite;
c) Furnizor în caz de nerespectare de către Cumpărător a termenelor de plată a Bunurilor;
d) Furnizor sau Cumpărător în caz de nesatisfacere de către una dintre Părţi a pretenţiilor înaintate conform prezentului Contract.
8.3. Cumpărătorul are dreptul de a rezolvi unilateral contractul în perioada de valabilitate a acestuia în una dintre următoarele situaţii:
a) contractantul se afla, la momentul atribuirii lui, în una dintre situaţiile care ar fi determinat excluderea sa din procedura de atribuire potrivit art.19 al Legii nr.131/2015 privind achiziţiile publice;
b) contractul a făcut obiectul unei modificări substanţiale care necesita o nouă procedură de achiziţie publică în conformitate cu art. 76 al Legii nr.131/2015 privind achiziţiile publice;
c) contractul nu ar fi trebuit să fie atribuit contractantului respectiv, având în vedere o încălcare gravă a obligaţiilor ce rezultă din Legea nr.131/2015 privind achiziţiile publice şi/sau tratatele internaţionale la care Republica Moldova este parte, care a fost constatată printr-o decizie a unei instanţe judecătoreşti naţionale sau, după caz, internaţionale.
8.4. Partea iniţiatoare a rezoluţiunii Contractului este obligată să comunice în termen de 5 zile lucrătoare celeilalte Părţi despre intenţiile ei printr-o scrisoare motivată.
8.5. Partea înştiinţată este obligată să răspundă în decurs de 5 zile lucrătoare de la primirea notificării. În cazul în care litigiul nu este soluţionat în termenele stabilite, partea iniţiatoare va iniţia rezoluţiunea.

9. Reclamaţii

9.1. Reclamaţiile privind cantitatea Bunurilor livrate sunt înaintate Furnizorului la momentul recepţionării lor, fiind confirmate printr-un act întocmit în comun cu reprezentantul Furnizorului.

9.2. Pretenţiile privind calitatea bunurilor livrate sunt înaintate Furnizorului în termen de 5 zile de la depistarea deficienţelor de calitate şi trebuie confirmate printr-un certificat eliberat de o organizaţie independentă neutră şi autorizată în acest sens.
9.3. Furnizorul este obligat să examineze pretenţiile înaintate în termen de 5 zile de la data primirii acestora şi să comunice Cumpărătorului despre decizia luată.
9.4. În caz de recunoaştere a pretenţiilor, Furnizorul este obligat, în termen de 5 zile, să livreze suplimentar Cumpărătorului cantitatea nelivrată de bunuri, iar în caz de constatare a calităţii necorespunzătoare – să le substituie sau să le corecteze în conformitate cu cerinţele Contractului.
9.5. Furnizorul poartă răspundere pentru calitatea Bunurilor în limitele stabilite, inclusiv pentru viciile ascunse.
9.6. În cazul devierii de la calitatea confirmată prin certificatul de calitate întocmit de organizaţia independentă neutră sau autorizată în acest sens, cheltuielile pentru staţionare sau întârziere sunt suportate de partea vinovată.

10. Sancţiuni

10.1. Pentru refuzul de a vinde Bunurile prevăzute în prezentul Contract Furnizorul suportă o penalitate în valoare de 1% din suma totală a contractului.
10.2. Pentru livrarea cu întârziere a Bunurilor, Furnizorul poartă plata despăgubirei în valoare de 0,1% din suma Bunurilor nelivrate, pentru fiecare zi de întârziere, dar nu mai mult de 1% din suma totală a prezentului Contract. În cazul în care întârzierea depăşeşte 15 zile calendaristice, Furnizorul prezintă Cumpărătorului o explicaţie în formă scrisă.
10.3. Pentru achitarea cu întârziere, Cumpărătorul poartă plata despăgubirei în valoare de 0,1% din suma Bunurilor neachitate, pentru fiecare zi de întârziere, dar nu mai mult de 1% din suma totală a prezentului contract.
10.4. Prima zi lucrătoare ulterioară datei ce constituie termenul limită de livrare, precum şi, termenul limită de achitare se consideră zi lucrătoare de întârziere.
10.5. Suma penalităţii calculate Furnizorului conform prezentului Contract poate fi dedusă (reţinută) de către Cumpărător din suma plăţii pentru Bunurile livrate.

11. Drepturi de proprietate intelectuală

11.1. Furnizorul are obligaţia să despăgubească Cumpărătorul împotriva oricăror:
a) reclamaţii şi acţiuni în justiţie, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalaţiile sau utilajele folosite pentru/sau în legătură cu produsele achiziţionate, şi
b) daune-interese, costuri, taxe şi cheltuieli de orice natură, aferente, cu excepţia situaţiei în care o astfel de încălcare rezultă din respectarea Caietului de sarcini întocmit de către Cumpărător.

12. Dispoziţii finale

12.1. Litigiile ce ar putea rezulta din prezentul Contract vor fi soluţionate de către Părţi pe cale amiabilă. În caz contrar, ele vor fi transmise spre examinare în instanţa de judecată competentă conform legislaţiei Republicii Moldova.
12.2. Părţile contractante au dreptul, pe durata îndeplinirii contractului, să convină asupra modificării clauzelor contractului, prin acord adiţional, numai în cazul apariţiei unor circumstanţe care lezează interesele comerciale legitime ale acestora şi care nu au putut fi prevăzute la data încheierii contractului. Modificările şi completările la prezentul Contract sînt valabile numai în cazul în care au fost perfectate în scris şi au fost semnate de ambele Părţi.
12.3. Nici una dintre Părţi nu are dreptul să transmită obligaţiile şi drepturile sale stipulate în prezentul Contract unor terţe persoane fără acordul în scris al celeilalte părţi.
12.4. Prezentul Contract în cazul în care este semnat electronic, de către ambele părţi, acesta este remis în mod automat prin mijloacele electronice, dar în cazul când contractul este semnat olografic se întocmeşte în două exemplare în limba română, câte un exemplar pentru Furnizor, Cumpărător.

12.5. Prezentul Contract se consideră încheiat la data semnării şi intră în vigoare la data înregistrării la una din trezoreriile regionale ale Ministerului Finanţelor, în cazul în care sursele financiare se alocă din bugetul de stat/bugetul local, sau la data semnării sau la o altă dată ulterioară indicată în acest contract în cazul în care gestionarea surselor financiare nu se efectuează prin intermediul sistemului trezorerial.
12.6. Prezentul contract este valabil până la 31.12.2026.
12.7. Prezentul Contract reprezintă acordul de voinţă al părţilor şi se consideră semnat la data aplicării ultimei semnături de către una din părţi.
12.8. Pentru confirmarea celor menţionate mai sus, Părţile au semnat prezentul Contract în conformitate cu legislaţia Republicii Moldova.

RECHIZITELE JURIDICE, POŞTALE ŞI DE PLĂŢI ALE PĂRŢILOR

Furnizorul de bunuri **IT-LAB GRUP SRL**	**Autoritatea contractantă** **Serviciul de Protecţie şi Pază de Stat**
mun. Chişinău, str-la. Studenţilor, 2/4 of.204 IBAN: MD31ML0000000002251029397 c/fiscal: 1011600024357 B.C."Moldindconbank" S.A. Cod bancar: MOLDMD2X Cod TVA: 0608402 Tel.:+373-22-85-59-75	mun. Chişinău, str. Sfatul Ţării, 26 IBAN: MD54TRPBAA317110B00417AC c/fiscal: 1006601001104 Ministerul Finanţelor - Trezoreria de Stat Cod bancar: TREZMD2X Tel.fax.(022) 250-904, fax.250-922

SEMNĂTURILE PĂRŢILOR

Furnizorul de bunuri **IT-LAB GRUP SRL**	**Autoritatea contractantă** **Serviciul de Protecţie şi Pază de Stat**
Administrator **Alexei CIOBAN**	**Director** **Alexandru HAREA**

Coordonat:
A. Gheorghelaş _____
D. Tabacaru _____
A. Boţan _____

Înregistrat: nr._____

Anexă
la contractul nr. 45
din 07.04. 2026

SPECIFICAŢII DE PREŢ

Nr. d/o	Denumirea bunurilor	U.M.	Cant.	Preţ unitar fără TVA, lei	Preţ unitar cu TVA, lei	Suma cu TVA, lei
1.	Bitdefender GravityZone Business Security Premium, 12 luni	buc.	140	407,73	489,28	68 499,60
2.	Bitdefender GravityZone Business Security Enterprise, 12 luni	buc.	15	618,87	742,64	11 139,60
Total:						**79 639,20**

SPECIFICAŢII TEHNICE

Tip:

1. Soluţie de protecţie şi securitate la nivel de endpoint, reţea şi cloud pentru 140 de dispozitive;
2. Soluţie de protecţie şi securitate avansată pentru toate dispozitivele endpoint, inclusiv protecţia aplicaţiilor şi datelor sensibile pentru 15 dispozitive.

Caracteristici generale ale produsului:

Soluţia trebuie să reprezinte o platformă integrată pentru managementul securităţii, gândită ca o soluţie modulară.
Produsul va conţine următoarele module, toate cu posibilitatea de a fi gestionate şi administrate dintr-o singură consolă de management:

- Protecţie staţii şi servere fizice şi virtualizate;
- Protecţie şi securitate pentru serverele email Microsoft Exchange;
- Serviciu de corelare şi răspuns la evenimente de tip EDR („endpoint detection and response").

Consola de management:

Pachetul de instalare să fie livrat ca o maşină virtuală, care conţine toate rolurile sau serviciile necesare. Consola nu va necesita o licenţă suplimentară pentru sistemul de operare.

Consola de management să fie livrată cu o baza de date inclusă, non-relaţională fără a fi nevoie de licenţe adiţionale.
Soluţia trebuie să:

- fie scalabilă, astfel ca oricare dintre roluri sau servicii să poată fi instalate separat sau împreună pe aceeaşi sau mai multe VDI-uri;
- asigure următoarele roluri: server cu baza de date, server de comunicaţie, server de actualizare, server de web;
- includă un modul load balancer pentru performanţă şi redundanţă;
- includă mecanisme de configurare a disponibilităţii pentru serverul cu baze de date (clustering).

Cerinţe generale produs:

Soluţia trebuie să:

1. includă un unul sau mai multe module de update server prin care să asigure actualizarea componentelor şi a semnăturilor;
2. permită activarea/dezactivarea actualizărilor automate de produs/semnături şi a consolei de management;
3. transmită alerte de nefuncţionalitate, cu 30 de minute înainte de actualizare;
4. permită vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcţii noi şi îmbunătăţiri, probleme rezolvate, probleme cunoscute;
5. afişeze notificările şi alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licenţiere, detecţie viruşi, actualizări de produs disponibile);
6. permită integrarea cu un server Syslog pentru raportarea evenimentelor antivirus;
7. permită instalarea serviciului de SMNP pentru raportarea statusului maşinilor din cadrul componentei de management;
8. permită crearea unei copii de siguranţă a bazei de date a consolei de administrare, la cerere sau programat, stocata local, pe un server FTP sau în reţea.

Inventarierea reţelei – managementul securităţii:

Produsul trebuie să:

- se integreze cu domenii Active Directory multiple, VMware vCenter, Citrix Xen şi să importe inventarul acestor platforme;
- permită descoperirea maşinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM, Nutanix Prism;
- permită descoperirea staţiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery;
- ofere opţiuni de căutare, sortare şi filtrare după numele sistemului, sistem de operare şi adresa IP;
- permită instalarea la distanţă sau manual a clienţilor antivirus pe maşini fizice şi virtuale;
- permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe maşinile fizice/virtuale;
- permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanţă pentru clientul antivirus;
- ofere posibilitatea de repornire a maşinilor fizice de la distanţă;
- ofere informaţii detaliate despre fiecare task iniţiat şi afişarea statutului lui;
- permită configurarea centralizată a clienţilor antivirus prin intermediul politicilor;

- ofere în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultima actualizare, Versiunea produsului, Versiunea de semnături;
- permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea.

Politici:

Produsul trebuie să:
- permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate modulele;
- conțină opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user;
- permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau useri de active directoy;

Monitorizare și raportare:

Produsul trebuie să:
- permită setarea de opțiuni specifice pentru afișarea rapoartelor existente;
- dețină un panou central care să afișeze statutul modulelor și rapoartele lor pentru perioadele de timp specificate;
- conțină rapoarte care prezinta statutul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate;
- trimită rapoarte către un număr nelimitat de adrese de email;
- permită vizualizarea rapoartelor curente programate de administrator;
- includă un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal, evenimente Exchange;
- ofere interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor;
- ofere interogări legate de evenimente precum: calculatorul țintă 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, denumirea și alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicații blocate, detecțiile etc);
- ofere interogări de evenimente Exchange precum: direcția traficului e-mail, evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate), măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau plasarea în carantină a fișierului, ștergerea sau respingerea e-mail-ului).

Carantină:
- Produsul trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă;
- Locația, fișierele și administrarea Carantinei trebuie să fie efectuată central din consola de management;

Utilizatori:
- Administrarea este necesar să fie efectuată pe bază de roluri multiple predefinite : Administrator companie, Administrator rețea, Reporter și alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate face modificări;
- Utilizatorii să poată fi importați din Microsoft Active Directory sau creați în consola de management;
- Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp.

Log-uri:
- Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare.

Protecție stații și servere fizice și virtualizate – caracteristici minime:

Soluția antivirus trebuie să:
- permită instalarea personalizată a modulelor;
- includă un „vaccin" anti-ransomware, cu actualizări de la producător, pentru protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar daca sunt infectate și blocarea procesului de criptare;
- includă protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate);
- includă modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate și activitati suspecte în faza pre-executie;
- includă modul avansat de securitate pentru protecție împotriva: atacurilor direcționate (Targeted Attack - APT), fisierelor suspecte si traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare menționat, i se vor putea stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv includere în sandbox, ce va putea trimite manual sau automat fișiere, unde vor putea fi „detonate" pentru o analiză în profunzime;
- includă două variante de analiza a sandbox-ului: doar monitorizare sau blocare cu două tipuri de acțiuni de remediere: implicită și de siguranța. Pentru acțiunea implicită: doar raportare, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de siguranța: ștergere sau permutare în carantină;
- includă 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;

Cerințe minime a modulului de detectare, corelare și răspuns:

Acest modul trebuie să:
- cuprindă - colectare de date și evenimente despre hardware și software aferent fiecărui endpoint, aducând informații detaliate referitoare la incidentele detectate, o hartă detaliată a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate – HyperDetect;
- cuprindă componente ca senzori ce colectează și procesează datele respectiv partea de analiză de securitate care are ca obiect interpretarea acestora;
- aibă capacitatea de a evalua activitatea tipică a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și să poată raporta orice deviație de la acest comportament sub forma unui incident;
- permită filtrarea incidentelor din interfața grafică în funcție de intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cît și după IP, nume fișier, nume stație;
- permită vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: să generează o hartă de principiu a incidentului, să detalieze incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, să poată genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigare – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod);
- poată bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;
- poată excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase;
- permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru a permite o investigare rapidă a gazdei/ colectare date despre atacul respectiv/ remediere în timp real a breșelor de securitate/ permită executarea unor comenzi în linia de comandă care se execută cu privilegii de

kernel pentru eliminarea în timp real a unor ameninţări sau colectarea de date privitoare la atacul în desfăşurare;
- permită căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere, precum nume de fişiere, nume de procese, chei de registre, valori de registre;
- includă un modul de tip host IPS capabil sa blocheze atacuri la nivel de reţea incluzând mişcarea laterală a unor categorii de malware (modulul de tip host IPS să reprezinte o sursă de telemetrie / date despre atac pentru modulul de tip EDR, având abilitatea de a integra informaţii despre acţiunile luate de către o potenţială ameninţare la nivel de reţea.

Cerinţe de sistem:
- Sisteme de operare pentru staţii de lucru: Windows 7/8.1/10 (inclusiv Embebed şi IoT), Mac OS X 10.11. şi mai recent, Red Hat Enterprise Linux / CentOS 6 şi mai recent, Oracle Linux 6.3 şi mai recent, Ubuntu 14.04 şi mai recent, SUSE Linux Enterprise Server 11 şi mai recent, OpenSUSE 42 şi mai recent, Fedora 25 şi mai recent, Debian 8.0 şi mai recent;
- Sisteme de operare Windows pentru servere: Windows Server 2008/2008 R2/2012/2012 R2/2016/2019.

Administrare şi instalare remote:
- Pachetele de instalare trebuie să fie configurabile cu modulele necesare: advanced threat control, anti-exploit, firewall, network protection respectiv content control, device control, power user, patch management, full disk encryption, EDR sensor, exchange protection respectiv „relay" (cu sau fară „patch caching server");
- Să existe posibilitatea de instalare manuală, sau automată la distanţă, direct din consola de management.

Consola de administrare trebuie să:
- includă secţiune, „Audit", unde se vor păstra toate acţiunile întreprinse de administratori şi utilizatori ai consolei, cu informaţii detaliate: logare, editare, creare, delogare, permutare etc;
- ofere posibilitatea de a crea pachetele de instalare de tip web installer sau kit full
- permită selectarea clientului care va realiza descoperirea staţiilor din reţea, altele decît cele integrate în domen;
- permită creare grupuri/subgrupuri, pentru endpoint-uri din reţea dar care nu sunt integrate domen;
- permită raportarea staţiilor care sunt protejate respectiv neprotejate de către soluţie;
- suporte definirea de portlet-uri (reprezentari grafice) configurabile.

Caracteristici şi funcţionalităţi principale ale modulului antivirus:

Produsul trebuie sa permită:
- stabilirea acţiunilor întreprinse de modulul antivirus la detectarea unei ameninţări noi. Astfel administratorul va putea alege între următoarele acţiuni:
  1. implicită pentru fişiere infectate: interzice accesul, dezinfectează, ştergere, mută fişierele în carantină, nici o acţiune;
  2. alternativă pentru fişierele infectate: interzice accesul, dezinfectează, ştergere, permutare fişiere în carantină;
  3. acţiune implicită pentru fişierele suspecte: interzice accesul, ştergere, mută fişierele în carantină, nici o acţiune;
  4. acţiune alternativă pentru fişierele suspecte: interzice accesul, ştergere, mută fişierele în carantină;
- scanarea automată în timp real cu setarea excepţiilor, definirea unor liste de excludere de la scanarea în timp real şi la cerere a anumitor directoare, discuri, fişiere, extensii sau procese, să nu scaneze arhive sau fişiere mai mari de « x » MB, definirea nivelelor de profunzime pentru scanarea în arhive;
- scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicaţii cu potenţial periculos protejând sistemul de virusii necunoscuţi prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă;
- scanarea oricărui suport de stocare a informaţiei (CD-uri, harduri externe, unităţi partajate etc);
- scanarea automată a emailurilor la nivelul staţiei de lucru pentru POP3/SMTP;
- configurarea căilor ce urmează a fi scanate la cerere;
- cu ajutorul unei baze de date complete cu semnături de spyware şi a euristicii de detecţie a acestui tip de programe, produsul va trebui să ofere protecţie anti-spyware;
- setarea priorităţilor scanărilor programate;
- configurarea scanării în cloud sau pe maşina de scanare instalată în reţea şi parţial scanarea locală pentru staţiile ce nu au suficiente resurse hardware;
- administratorului să personalizeze şi motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: scanare locală, scanarea hibrid cu motoare light, scanarea centralizată în Cloud-ul privat, scanare centralizată cu fallback* pe scanare locală, scanare centralizată cu fallback* pe scanare hibrid;
- setarea a tipurilor de detecţie: bazate pe semnături, bazate de comportamentul fişierelor şi bazate pe monitorizarea proceselor;
- scanarea paginilor web;
- setarea a unei parole pentru protecţia la dezinstalare;
- modul de antiphishing;
- protecţie în timp real pe maşinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalată;
- instalarea clientului pe maşinile virtuale parte a unui pool doar pe maşina de tip template, după care se recompune pool-ul de maşini virtuale;
- utilizarea uni modul adiţional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze şi blocheze atacuri de tip persistent sau targetat precum şi alte categorii de malware sofisticat înainte de faza de execuţie. Acest modul oferă următoarele funcţionalităţi:
  a) Clasificarea tipului de atac;
  b) Abilitatea de a raporta ameninţările detectate fără a le bloca;
  c) Abilitate de a ajusta agresivitatea detecţiei pe cel puţin 3 nivele (incluzând posibilitatea de a raporta atacuri ce ar fi fost blocate pe un nivel de agresivitate a detecţiei „mai ridicat" decât cel setat in mod curent in modul);
  d) Abilitatea de a acţiona in mod diferit in funcţie de tipul ameninţării (fişier sau atac prin reţea);
- posibilitatea de restaurare a fişierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, cînd determină că procesul este malitios;
- oprirea atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive;
- depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare;
- protejarea aplicaţiilor utilizate frecvent şi a celor de tip „sistem" cum ar fi browserele, aplicaţiile de tip office sau reader, procesele critice aferente sistemelor de operare.

Firewall:
- sa ofere posibilitatea de a configura reguli de firewall pentru aplicaţii sau conectivitate;
- modulul să poată fi instalat/dezinstalat la cerere;
- să permită definirea de reţele de încredere pentru maşina destinaţie;

Protecţia datelor:
- Produsul trebuie să permite blocarea datelor confidenţiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.

Controlul conţinutului:

Produsul trebuie să ofere un modul integrat dedicat controlului accesului la Internet cu următoarele particularităţi: blocarea accesului la Internet pentru

anumite maşini client sau grupuri de maşini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conţin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicaţii definite de administrator, restricţionarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

Controlul aplicaţiilor:

Pentru administrare şi inventariere eficientă produsul trebuie să deţină un modul care va oferi posibilitatea de a:

- efectua descoperirea aplicaţiilor utilizate pe staţiile utilizatorilor grupate după: nume, versiune, descoperit la, găsit pe;
- regăsi toate procesele descoperite în reţea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe;
- bloca rularea anumitor aplicaţii sau procese definite de administrator (inclusiv subprocese) după: cale fişier: local, CD-ROM, portabil sau reţea, hash , certificat.

Controlul dispozitivelor:

Produsul trebuie să conţină un modul pentru controlul dispozitivelor care:

- poate fi instalat/dezinstalat conform setărilor stabilite;
- permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage;
- permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la maşina client;
- permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

Power User:

Produsul trebuie să conţină un modul pentru setări specifice – power user care să:

- poată fi instalat/dezinstalat în funcţie de preferinţa administratorului;
- permită posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa şi modifica setările clientului antivirus dintr-o consola disponibilă local pe maşina client;
- permită administratorului soluţiei să suprascrie din consola setările aplicate de utilizatorii Power User.

Actualizare:

Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:

- la nivel de staţie în mod silenţios (fără avertizări);
- folosind unul sau mai multe servere de actualizare;
- pentru locaţiile la distanţă prin intermediul unui client antivirus care are şi rol de server de actualizare.

Alte cerinţe:

Perioada de suport şi menţinere de la producător:

1. Pentru soluţia ofertată se solicită a fi 12 luni din data activării licentelor;
2. Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanţă.

SEMNĂTURILE PĂRŢILOR

Furnizorul de bunuri **IT-LAB GRUP SRL**	**Autoritatea contractantă** **Serviciul de Protecţie şi Pază de Stat**
Administrator **Alexei CIOBAN**	**Director** **Alexandru HAREA**

Coordonat:
V. Dodica