Anexa nr.1
la Caietul de sarcini

SPECIFICAŢII TEHNICE

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

Numărul procedurii de achiziţie nr. **ocds-b3wdp1-MD-1765269998108**
Obiectul achiziţiei: **Pachete software aferente securității informaționale**

Denumirea bunurilor	**Denumirea modelului**	**Ţara de origine**	**Producătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standar de de referinţă**
1	2	3	4	5	6	7
Lotul: Soluții EDR pentru Modernizarea și Eficientizarea Protecției Cibernetice						
Soluție de securitate cibernetică avansată pentru dispozitive tip Server/PC/ Laptop/VDI	Bitdefender GravityZone Business Security Enterprise	România	Bitdefender	**Tip**: Soluție de securitate cibernetică avansată pentru dispozitive tip Server/PC/Laptop/VDI pentru perioada 07.02.2026 – 07.02.2027 **Cantitate licențe**: Soluția trebuie să asigure protecție pentru: - 1000 dispozitive (PC/ laptop/ VDI/ Server); - 700 utilizatori; - 600 utilizatori Microsoft 365; **Cerințe Generale:** - Soluția de protecție trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST, VIRUS	**Tip**: Soluție de securitate cibernetică avansată pentru dispozitive tip Server/PC/Laptop/VDI pentru perioada 07.02.2026 – 07.02.2027 **Cantitate licențe**: Se oferă soluția Bitdefender GravityZone care va asigura protecție pentru: - 1000 dispozitive (PC/ laptop/ VDI/ Server); - 700 utilizatori; - 600 utilizatori Microsoft 365; **Cerințe Generale:** - Soluția de protecție oferită ocupă locurile de top în testele internaționale independente cu renume mondial în domeniu (certificări AV-TEST, VIRUS	

				BULLETIN'S, REAL-WORLD PROTECTION, MALWARE PROTECTION...). - Soluția trebuie să fie poziționată în topurile specializate (The Forrester Wave: Extended Detection and Response Platforms, Forrester's Analysis MITRE Engenuity ATT&CK Evaluation, MITRE ATT&CK Evaluations…). **<u>Soluția va acoperi minim următoarele cerințe și specificații tehnice:</u>** <u>Caracteristici generale</u> Soluția trebuie să reprezinte o platformă integrată pentru managementul securității, gândită ca o soluție modulară. Produsul va conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management: - Protecție stații și servere fizice și virtualizate; - Soluție de corelare evenimente pentru o vizibilitate unificată și detaliată asupra amenințărilor de securitate și răspuns rapid la amenințările avansate; - Serviciu de corelare și răspuns (XDR) la evenimente cibersecurity;	BULLETIN'S, REAL-WORLD PROTECTION, MALWARE PROTECTION...). - Soluția este poziționată în topurile specializate (The Forrester Wave: Extended Detection and Response Platforms, Forrester's Analysis MITRE Engenuity ATT&CK Evaluation, MITRE ATT&CK Evaluations…). **<u>Soluția va acoperi următoarele cerințe și specificații tehnice:</u>** <u>Caracteristici generale</u> Soluția propusă reprezintă o platformă integrată pentru managementul securității, gândită ca o soluție modulară. Produsul conține următoarele module, toate cu posibilitatea de a fi gestionate și administrate dintr-o singură consolă de management: - Protecție stații și servere fizice și virtualizate; - Soluție de corelare evenimente pentru o vizibilitate unificată și detaliată asupra amenințărilor de securitate și răspuns rapid la amenințările avansate; - Serviciu de corelare și răspuns (XDR) la evenimente cibersecurity; - Serviciu de monitorizare și protecție a identității utilizatorilor;	

				- Serviciu de monitorizare și protecție a identității utilizatorilor; - Serviciu de monitorizare și analiză a traficului din rețea și pentru a detecta amenințările avansate, mișcarea laterală și alte activități malițioase; - Serviciu pentru a monitorizare și detectare a amenințărilor în aplicațiile de productivitate de tip Software-as-a-Service (Microsoft 365); - Tehnologie de adaptare a soluției de securitate cibernetice în funcție de comportamentul utilizatorilor. <u>Consola de management</u> - Accesibilitate - atât de pe browser desktop cât și tip mobile. - Actualizare -opțiuni configurabile de actualizare consolei de management: automat și manual la necesitate. <u>Soluția de scanare centralizată</u> Soluția de scanare (pentru VDI/scanare centralizată) disponibilă de tip template și compatibilă cu următoarele hipervizoare: 1. VMware vSphere; 2. Citrix XenServer; 3. Microsoft Hyper-V. <u>Cerințe generale produs</u> Soluția trebuie să:	- Serviciu de monitorizare și analiză a traficului din rețea și pentru a detecta amenințările avansate, mișcarea laterală și alte activități malițioase; - Serviciu pentru a monitorizare și detectare a amenințărilor în aplicațiile de productivitate de tip Software-as-a-Service (Microsoft 365); - Tehnologie de adaptare a soluției de securitate cibernetice în funcție de comportamentul utilizatorilor. <u>Consola de management asigură:</u> - Este accesibilă atât de pe browser desktop cât și tip mobile. - Opțiuni de actualizare configurabile a consolei de management: automat și manual la necesitate. <u>Soluția de scanare centralizată</u> Soluția de scanare (pentru VDI/scanare centralizată) este disponibilă de tip template și este compatibilă cu următoarele hipervizoare: 1. VMware vSphere; 2. Citrix XenServer; 3. Microsoft Hyper-V. <u>Cerințe generale produs</u> Soluția întrunește opțiunile ce:	

				- permită activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management; - ofere vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi si îmbunătățiri, probleme rezolvate, probleme cunoscute; - afișeze notificările și alertele existente, să alerteze administratorul în cazul unor probleme majore (configurabile): licențiere, detecție virusi, actualizări de produs disponibile); <u>Panou de monitorizare si raportare (Dashboard)</u> - să ofere posibilitatea creării rapoartelor configurabile după tip, țintă și scop cu opțiuni specifice pentru orice tip de raport cu posibilități de adăugare/eliminare și rearanjare. - să prezinte rapoarte pentru toate modulele suportate(stare/statut/actualizare) . <u>Inventarierea rețelei – managementul securității</u> Produsul trebuie să: - se integreze cu domenii Active Directory multiple, să poată importa inventarul.	- permite activarea/dezactivarea actualizărilor automate de produs/semnături și a consolei de management; - oferă vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcții noi si îmbunătățiri, probleme rezolvate, probleme cunoscute; - afișează notificările și alertele existente, alertează administratorul în cazul unor probleme majore (configurabile): licențiere, detecție virusi, actualizări de produs disponibile); <u>Panou de monitorizare si raportare (Dashboard)</u> - oferă posibilitatea creării rapoartelor configurabile după tip, țintă și scop cu opțiuni specifice pentru orice tip de raport cu posibilități de adăugare/eliminare și rearanjare. - prezintă rapoarte pentru toate modulele suportate (stare/statut/actualizare). <u>Inventarierea rețelei – managementul securității</u> Produsul asigură: - se integreze cu domenii Active Directory multiple, poate importa inventarul.	

				- permită descoperirea PC neintegrate în Active Directory (Workgroup); - ofere opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare si adresa IP, politica aplicată, online și/sau offline și FQDN; - permită instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale; - permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale; - permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus; - ofere posibilitatea de repornire a mașinilor fizice de la distanță; - ofere informații detaliate despre fiecare task inițiat și afișarea statutului lui; - permită configurarea centralizată a clienților antivirus prin intermediul politicilor; - ofere în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.	- permite descoperirea PC neintegrate în Active Directory (Workgroup); - oferă opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare si adresa IP, politica aplicată, online și/sau offline și FQDN; - permite instalarea la distanță sau manual a clienților antivirus pe mașini fizice și virtuale; - permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale; - permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanță pentru clientul antivirus; - oferă posibilitatea de repornire a mașinilor fizice de la distanță; - oferă informații detaliate despre fiecare task inițiat și afișarea statutului lui; - permite configurarea centralizată a clienților antivirus prin intermediul politicilor; - oferă în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.	

				<u>Politici</u> Soluția trebuie să: - permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module; - conțină opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, 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 user de active directoy; - poată fi schimbată automat în funcție de: user logat, IP sau clasa de IP, Gateway alocat, DNS serverul alocat, Clientul este/nu este în accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless). <u>Monitorizare și raportare:</u> Soluția trebuie să: - permită setarea de opțiuni specifice pentru afișarea rapoartelor existente; - dețină un panou central care să afișeze statutul modulelor și	<u>Politici</u> Soluția este concepută să: - permite configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conține setări pentru toate module; - conține opțiuni specifice de activare/dezactivare și configurare a funcționalităților precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, scanarea traficului web, controlul dispozitivelor, power user; - permitãe aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unități organizaționale sau user de active directoy; - poată fi schimbată automat în funcție de: user logat, IP sau clasa de IP, Gateway alocat, DNS serverul alocat, Clientul este/nu este în accesai rețea cu infrastructura de management, Tipul rețelei (lan, wireless). <u>Monitorizare și raportare:</u> Soluția este concepută să: - permite 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; - conținâ rapoarte care prezinta statusul 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; - permită exportarea rapoartelor în format .pdf si detaliile ca format .csv; - includă un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal; - 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 ținta pe care a avut loc evenimentul, tipul starea și configurația agentului de	rapoartele lor pentru perioadele de timp specificate; - conține rapoarte care prezinta statusul mașinilor clienților, al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate; - trimite rapoarte către un număr nelimitat de adrese de email; - permite vizualizarea rapoartelor curente programate de administrator; - permite exportarea rapoartelor în format .pdf si detaliile ca format .csv; - include un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal; - oferă interogări legate de starea terminalului precum: tip mașină, infrastructură rețelei căreia aparține, datele agentului de securitate, starea modulelor de protecție, rolurile terminalelor; - oferă interogări legate de evenimente precum: calculatorul ținta pe care a avut loc evenimentul, tipul starea și configurația agentului de securitate instalat, starea	

				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); Carantină Soluția trebuie să permită restaurarea fișierelor din carantină în locația originală sau într-o cale configurabilă; Administrarea Carantinei să fie posibilă atît pe terminalul administrat cît și 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 - configurabil. Log-uri Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere	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); Carantină Soluția permite să restaureze fișierele din carantină în locația originală sau într-o cale configurabilă; Administrarea Carantinei este posibilă atât pe terminalul administrat cât și din consola de management; Utilizatori Administrarea poate fi 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 pot fi importați din Microsoft Active Directory sau creați în consola de management; Soluția oferă posibilitatea de deconectare automată a oricărui tip de utilizator după un anumit timp - configurabil. Log-uri Soluția permite înregistrarea acțiunilor utilizatorilor și oferă informații	

				informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. <u>Actualizare</u> Soluția va permite: - definirea de locații de actualizare multiple - activarea/dezactivarea actualizărilor - testarea noilor versiuni înainte de a fi instalate pe toți clienții(posibilitate de actualizare în mai multe cicluri – 1 mediu te test, 2 – mediu de producție) - definirea zonelor de test și zonelor critice de producție <u>Protecție stații și servere fizice si virtualizate – caracteristici minime</u> Soluția trebuie să: - permită instalarea personalizată a modulelor; - includă opțiune tip „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 de analiză la risk capabil să identifice și să remedieze riskurile identificate la	detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare. <u>Actualizare</u> Soluția are posibilitatea să: - definească locații de actualizare multiple - activarea/dezactivarea actualizărilor - testarea noilor versiuni înainte de a fi instalate pe toți clienții(posibilitate de actualizare în mai multe cicluri – 1 mediu te test, 2 – mediu de producție) - definească zonele de test și zonelor critice de producție <u>Protecție stații și servere fizice si virtualizate – caracteristici minime</u> Soluția este concepută să: - permite instalarea personalizată a modulelor; - include opțiune tip „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; - include protecție împotriva atacurilor zero-day de tip exploit (atacuri direcționate); - include modul de analiză la risk capabil să identifice și să remedieze riskurile identificate la	

				nivel de rețea sau sistem de operare, cu posibilitate de configurare și automatizare; - includă modul avansat de securitate bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție; - includă modul avansat de securitate pentru protecție împotriva: atacurilor direcționate (Targeted Attack), fișierelor 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 cu posibilitate de extindere a nivelului de raportare; - includă modul de sandbox, unde se vor putea trimite manual sau automat fișiere pentru a putea fi „detonate" pentru o analiză în profunzime; - includă variante de analiză a sandbox-ului tip: doar monitorizare sau blocare cu acțiuni de remediere: implicită și de siguranța. Pentru acțiunea implicită: doar raportare, dezinfecție, ștergere și transmitere în carantină. Pentru acțiunea de	nivel de rețea sau sistem de operare, cu posibilitate de configurare și automatizare; - include modul avansat de securitate bazat pe tehnologii de tip „machine learning tunabil" proiectat special pentru a detecta atacuri avansate și activități suspecte în faza pre-execuție; - include modul avansat de securitate pentru protecție împotriva: atacurilor direcționate (Targeted Attack), fișierelor suspecte si traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare menționat, i se poate stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv cu posibilitate de extindere a nivelului de raportare; - include modul de sandbox, unde se poate trimite manual sau automat fișiere pentru a putea fi „detonate" pentru o analiză în profunzime; - include variante de analiză a sandbox-ului tip: doar monitorizare sau blocare cu 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;	

				siguranța: ștergere sau permutare în carantină; - suporte "detonarea" în modulul sandbox, minim, tipurile de fișiere: 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. Acestea vor fi detectate corect chiar dacă vor fi 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 ; - ofere posibilitate de filtrare a incidentelor din interfața grafică în funcție intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac, 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	- suportă „detonarea" în modulul sandbox, pentru tipurile de fișiere: 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. Acestea vor fi detectate corect chiar dacă vor fi 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 ; - oferă posibilitate de a filtra incidentele din interfață grafică în funcție intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac, sistem de operare afectat cît și după IP, nume fișier, nume stație; - permite vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: generează o hartă de principiu a incidentului, detaliază incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, poate genera	

				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 brețelor de securitate/ permită executarea unor comenzi în linia de comandă care se execută cu privilegii de kernel pentru eliminarea în timp real a unor	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); - poate bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV; - poate 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; - permite 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 brețelor de securitate/ permită executarea unor comenzi în linia de comandă care se execută cu privilegii de kernel pentru eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare; - permite crearea regulilor de detecție customizabilă bazată pe	

				amenințări sau colectarea de date privitoare la atacul în desfășurare; - permită crearea regulilor de detecție customizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; - permită creare regulilor de excludere customizabilă bazată pe procese, fișiere, registre si conexiuni de rețea; - permită căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre; - permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru investigare rapidă, colectare date și remedierea în timp real a breșei de securitate, reducând timpul de remediere (downtime) în cazul unui atac, executarea comenzilor în linia de comandă cu privilegii de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare <u>Cerințe de sistem</u> - Sisteme de operare pentru stații de lucru: Windows 10/11 (inclusiv Embebed și IoT), Mac OS X de la 10.12 și mai recent, Red Hat Enterprise Linux / CentOS 7 și mai	procese, fișiere, registre și conexiuni de rețea; - permite creare regulilor de excludere customizabilă bazată pe procese, fișiere, registre si conexiuni de rețea; - permite căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre; - permite deschiderea unei conexiuni remote către un endpoint potențial infectat pentru investigare rapidă, colectare date și remedierea în timp real a breșei de securitate, reducând timpul de remediere (downtime) în cazul unui atac, executarea comenzilor în linia de comandă cu privilegii de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare <u>Cerințe de sistem</u> - Sisteme de operare pentru stații de lucru: Windows 10/11 (inclusiv Embebed și IoT), Mac OS X de la 10.12 și mai recent, Red Hat Enterprise Linux / CentOS 7 și mai	

				recent, Oracle Linux 6.3 și mai recent, Ubuntu 16 și mai recent, SUSE Linux Enterprise Server 12 și mai recent, OpenSUSE 15 și mai recent, Fedora 31 și mai recent; - Sisteme de operare Windows pentru servere: Windows Server 2012/2012 R2/2016/2019/2022/2025 <u>Administrare și instalare remote</u> - Pachetele de instalare trebuie să fie configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay" (update server"); - Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management; - Din consola să fie disponibile informații despre fiecare endpoint: numele, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări; - Posibilități de creare kit pentru endpoint – tip: universal – 32/64bit, fizic/VDI, web installer/full. - Gestionare, creare și configurare grupuri pentru endpoint ce nu sunt în AD; - Posibilitate de atribuire a funcționalității de descoperire a endpoint-urilor și în afara AD, pentru oricare endpoint.	recent, Oracle Linux 6.3 și mai recent, Ubuntu 16 și mai recent, SUSE Linux Enterprise Server 12 și mai recent, OpenSUSE 15 și mai recent, Fedora 31 și mai recent; - Sisteme de operare Windows pentru servere: Windows Server 2012/2012 R2/2016/2019/2022/2025 <u>Administrare și instalare remote</u> - Pachetele de instalare permite să fie configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay" (update server"); - Permite posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management; - Din consola este disponibilă informații despre fiecare endpoint: numele, IP, sistem de operare, module instalate, politica aplicată, informații despre actualizări; - Oferă posibilitatea de creare kit pentru endpoint – tip: universal – 32/64bit, fizic/VDI, web installer/full. - Oferă posibilitatea de gestionare, creare și configurare grupuri pentru endpoint ce nu sunt în AD; - Oferă posibilitatea de atribuire a funcționalității de descoperire a endpoint-urilor și în afara AD, pentru oricare endpoint.	

				<u>Caracteristici și funcționalități principale ale modulului antivirus</u> Soluția trebuie sa permită: - stabilirea acțiunilor întreprinse de modulul antivirus la detectarea unei amenințări noi, care să cuprindă minim următoarele acțiuni: • implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune; • alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină; • acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune; • acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină; - scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de ” x” MB, definirea	<u>Caracteristici și funcționalități principale ale modulului antivirus</u> Soluția este concepută să: - stabilească acțiunile întreprinse de modulul antivirus la detectarea unei amenințări noi, care cuprinde minim următoarele acțiuni: • implicită pentru fișiere infectate: interzice accesul, dezinfectează, ștergere, mută fișierele în carantină, nici o acțiune; • alternativă pentru fișierele infectate: interzice accesul, dezinfectează, ștergere, permutare fișiere în carantină; • acțiune implicită pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină, nici o acțiune; • acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină; - ofere scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de ” x” MB,	

				nivelelor de profunzime pentru scanarea în arhive; - scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă; - scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc); - scanarea automată a emailurilor la nivelul stației 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 și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware; - setarea priorităților scanărilor programate; - configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware; - administratorului să personalizeze și motoarele de scanare, având	definirea nivelelor de profunzime pentru scanarea în arhive; - asigure scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă; - asigure scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc); - asigure scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP; - să confere configurarea căilor ce urmează a fi scanate la cerere; - produsul oferă protecție anti-spyware cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe; - ofere setarea priorităților scanărilor programate; - configurarea scanării în cloud sau pe mașina de scanare instalată în rețea și parțial scanarea locală pentru stațiile ce nu au suficiente resurse hardware; - administratorul poate să personaliza și motoarele de scanare, având posibilitatea de a	

				posibilitatea de a alege între mai multe tehnologii de scanare: scanare locală, scanarea hibrid cu motoare light, scanarea centralizată (serviciu/apliance de scanare în infrastructura proprie), scanare centralizată cu fallback* pe scanare locală, scanare centralizată cu fallback* pe scanare hibrid; - setarea a tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor; - scanarea paginilor web; - setarea a unei parole pentru protecția la dezinstalare; - modul de antiphishing; - protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată; - instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale; - utilizarea uni modul adițional de securitate bazat pe algoritmi reglabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze și blocheze atacuri de tip persistent sau targetat precum și alte	alege între mai multe tehnologii de scanare: scanare locală, scanarea hibrid cu motoare light, scanarea centralizată (serviciu/apliance de scanare în infrastructura proprie), scanare centralizată cu fallback* pe scanare locală, scanare centralizată cu fallback* pe scanare hibrid; - asigure setarea tipurilor de detecție: bazate pe semnături, bazate de comportamentul fișierelor și bazate pe monitorizarea proceselor; - asigure scanarea paginilor web; - pună la dispoziție setarea a unei parole pentru protecția la dezinstalare; - livreze un modul de antiphishing; - acorde protecție în timp real pe mașinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată; - pună la dispoziție instalarea clientului pe mașinile virtuale parte a unui pool doar pe mașina de tip template, după care se recompune pool-ul de mașini virtuale; - pună la dispoziție utilizarea modul de securitate bazat pe algoritmi reglabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze și	

				categorii de malware sofisticat înainte de faza de execuție. Acest modul oferă următoarele funcționalități: • clasificarea tipului de atac; • abilitatea de a raporta amenințările detectate fără a le bloca; • abilitate de a ajusta agresivitatea detecției pe cel puțin 3 nivele (incluzând posibilitatea de a raporta atacuri ce ar fi fost blocate pe un nivel de agresivitate a detecției „mai ridicat" decât cel setat în mod curent în modul); • abilitatea de a acționa în mod diferit în funcție de tipul amenințării (fișier sau atac prin rețea); - posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, cînd determină că procesul este malițios; - 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;	blocheze atacuri de tip persistent sau targetat precum și alte categorii de malware sofisticat înainte de faza de execuție. Acest modul oferă următoarele funcționalități: • clasificarea tipului de atac; • abilitatea de a raporta amenințările detectate fără a le bloca; • abilitate de a ajusta agresivitatea detecției pe cel puțin 3 nivele (incluzând posibilitatea de a raporta atacuri ce ar fi fost blocate pe un nivel de agresivitate a detecției „mai ridicat" decât cel setat în mod curent în modul); • abilitatea de a acționa în mod diferit în funcție de tipul amenințării (fișier sau atac prin rețea); - pună la dispoziție posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, cînd determină că procesul este malițios; - asigure oprirea atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive; - asigure depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare;	

				- protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem" cum ar fi browser-ele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare. <u>Firewall</u> - să ofere posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate; - modulul să poată fi instalat/ activat/ dezactivat/ dezinstalat la cerere; - să permită definirea de rețele de încredere pentru mașina destinație. <u>Protecția datelor</u> Soluția trebuie să permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. <u>Controlul conținutului</u> Soluția trebuie să ofere un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: - blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, - blocarea accesului la Internet pe intervale orare,	- asigure protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem" cum ar fi browser-ele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare. <u>Firewall</u> - furnizează posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate; - modulul poate fi instalat/ activat/ dezactivat/ dezinstalat la cerere; - permite definirea de rețele de încredere pentru mașina destinație. <u>Protecția datelor</u> Soluția permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice. <u>Controlul conținutului</u> Soluția oferă un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: - blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, - blocarea accesului la Internet pe intervale orare, - blocarea paginilor de internet care conțin anumite cuvinte cheie,	

				- blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, - blocarea accesului la anumite aplicații definite de administrator, - restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). <u>Controlul dispozitivelor</u> Soluția trebuie să conțină 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 mașina client; - permite configurarea de excluderi pentru diferite tipuri de	controlul accesului numai la anumite pagini de internet specificate de administrator, - blocarea accesului la anumite aplicații definite de administrator, - restricționarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). <u>Controlul dispozitivelor</u> Soluția pune la dispoziție 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 mașina client; - permite configurarea de excluderi pentru diferite tipuri de	

				dispozitive pentru care s-au configurat reguli. <u>Evaluarea conformității:</u> Soluția trebuie să includă posibilitatea de management al conformității - framework care reflectă igiena cibernetică a utilizatorilor, fiind capabil să fie extins pentru monitorizarea și auditarea gradului de conformitate al echipamentelor și utilizatorilor cu politicile de securitate recomandate de framework-uri specializate. Produsul trebuie să ofere: - posibilitatea definirii, aplicării și urmăririi politicilor de conformitate pe stațiile de lucru, servere din infrastructura organizației. - detectarea și raportarea deviațiilor de la politicile de conformitate, cu evidențierea exactă a sistemelor nealiniate; - mecanisme automate de remediere sau recomandări pentru revenirea la starea conformă; - istoric centralizat al modificărilor și acțiunilor efectuate în contextul conformității, cu trasabilitate completă; - Interfață de administrare unificată pentru definirea regulilor, vizualizarea stării de conformitate și gestionarea excepțiilor.	dispozitive pentru care s-au configurat reguli. <u>Evaluarea conformității:</u> Soluția inslude posibilitatea de management al conformității - framework care reflectă igiena cibernetică a utilizatorilor, fiind capabil să fie extins pentru monitorizarea și auditarea gradului de conformitate al echipamentelor și utilizatorilor cu politicile de securitate recomandate de framework-uri specializate. Produsul oferă: - posibilitatea definirii, aplicării și urmăririi politicilor de conformitate pe stațiile de lucru, servere din infrastructura organizației. - detectarea și raportarea deviațiilor de la politicile de conformitate, cu evidențierea exactă a sistemelor nealiniate; - mecanisme automate de remediere sau recomandări pentru revenirea la starea conformă; - un istoric centralizat al modificărilor și acțiunilor efectuate în contextul conformității, cu trasabilitate completă; - o interfață de administrare unificată pentru definirea regulilor, vizualizarea stării de	

				<u>Evaluare dinamică a accesului:</u> Soluția trebuie să ofere următoarele funcționalități: a)Monitorizare Comportamentală Avansată și Învățare Adaptivă - să includă o fază inițială de învățare automată, pe parcursul căreia va monitoriza și analiza în mod continuu comportamentele utilizatorilor și interacțiunile cu sistemele pentru a stabili un model de referință al normalității operaționale. Durata acestei faze de învățare nu trebuie să depășească, în mod ideal, 30 de zile în absența altor surse de date relevante. O cerință importantă este capacitatea soluției de a utiliza date istorice provenite de la sisteme de detecție și răspuns la nivel de endpoint (EDR) deja existente în infrastructura Autorității Contractante. - să fie capabilă să creeze și să mențină profiluri comportamentale granulare, definite cel puțin la nivelul combinației dintre un utilizator și dispozitivul (endpoint-ul) utilizat de acesta. - să gestioneze în mod eficient situațiile în care un singur	conformitate și gestionarea excepțiilor. <u>Evaluare dinamică a accesului:</u> Soluția oferă următoarele funcționalități: a)Monitorizare Comportamentală Avansată și Învățare Adaptivă - include o fază inițială de învățare automată, pe parcursul căreia va monitoriza și analiza în mod continuu comportamentele utilizatorilor și interacțiunile cu sistemele pentru a stabili un model de referință al normalității operaționale. Durata acestei faze de învățare nu depășește 30 de zile în absența altor surse de date relevante. Soluția asigură capacitatea de a utiliza date istorice provenite de la sisteme de detecție și răspuns la nivel de endpoint (EDR) deja existente în infrastructura Autorității Contractante. - este capabilă să creeze și să mențină profiluri comportamentale granulare, definite cel puțin la nivelul combinației dintre un utilizator și dispozitivul (endpoint-ul) utilizat de acesta. - poate gestiona în mod eficient situațiile în care un singur utilizator utilizează multiple	

				utilizator utilizează multiple dispozitive, corelând activitățile pentru a oferi o imagine holistică a riscului asociat utilizatorului, nu doar riscuri izolate la nivel de dispozitiv. - să rămână activ în mod continuu de învățare și după faza inițială a mecanismului de învățare. - să detecteze și să se adapteze la schimbările în comportamentul utilizatorilor, la introducerea de noi aplicații software în mediul de lucru sau la modificări ale infrastructurii IT. b) Identificarea Proactivă și Managementul Riscurilor Asociate Vectorilor de Atac Specifici Soluția trebuie să asigure capacitatea de detecție contextuală și diferențiere între utilizările legitime și cele malițioase ale următoarelor categorii de instrumente: - binare „Living Off the Land" (LOLBins): Soluția trebuie să detecteze utilizarea anormală a utilitarelor native ale sistemului (ex. PowerShell, WMI, certutil) în scopuri neautorizate. - unelte de Tampering/Alterare a Securității: Soluția trebuie să identifice tentativele de modificare a configurațiilor de	dispozitive, corelând activitățile pentru a oferi o imagine holistică a riscului asociat utilizatorului, nu doar riscuri izolate la nivel de dispozitiv. - este activ în mod continuu de învățare și după faza inițială a mecanismului de învățare. - detectează și se adaptează la schimbările în comportamentul utilizatorilor, la introducerea de noi aplicații software în mediul de lucru sau la modificări ale infrastructurii IT. b) Identificarea Proactivă și Managementul Riscurilor Asociate Vectorilor de Atac Specifici Soluția asigură capacitatea de detecție contextuală și diferențiere între utilizările legitime și cele malițioase ale următoarelor categorii de instrumente: - binare „Living Off the Land" (LOLBins): Soluția detectează utilizarea anormală a utilitarelor native ale sistemului (ex. PowerShell, WMI, certutil) în scopuri neautorizate. - unelte de Tampering/Alterare a Securității: Soluția identifică tentativele de modificare a configurațiilor de securitate sau de	

				securitate sau de dezactivare a protecțiilor sistemului. - software de Minare a Criptomonedelor (Crypto Miners): Soluția trebuie să detecteze aplicațiile de minare neautorizată care consumă resursele sistemului. - unelte de Piraterie Software și Hacking: Soluția trebuie să identifice prezența și utilizarea instrumentelor asociate cu pirateria sau atacurile cibernetice. - unelte de Administrare la Distanță (Remote Admin Tools – RATs): Soluția trebuie să distingă între utilizarea legitimă a instrumentelor de administrare și utilizarea lor neautorizată sau malițioasă. c) Generare de Recomandări de Securitate și Opțiuni de Implementare Soluția trebuie să poată genera puțin următorul tip de recomandare, adaptată la contextul detectat: - recomandări pentru a limita sau bloca accesul anumitor utilizatori sau dispozitive la resurse specifice (aplicații, fișiere, funcționalități de sistem) atunci când comportamentul acestora deviază semnificativ de la modelul de normalitate stabilit,	dezactivare a protecțiilor sistemului. - software de Minare a Criptomonedelor (Crypto Miners): Soluția detectează aplicațiile de minare neautorizată care consumă resursele sistemului. - unelte de Piraterie Software și Hacking: Soluția identifică prezența și utilizarea instrumentelor asociate cu pirateria sau atacurile cibernetice. - unelte de Administrare la Distanță (Remote Admin Tools – RATs): Soluția oferă posibilitatea de a distinge între utilizarea legitimă a instrumentelor de administrare și utilizarea lor neautorizată sau malițioasă. c) Generare de Recomandări de Securitate și Opțiuni de Implementare Soluția poate genera următoarele recomandări adaptate la contextul detectat: - recomandări pentru a limita sau bloca accesul anumitor utilizatori sau dispozitive la resurse specifice (aplicații, fișiere, funcționalități de sistem) atunci când comportamentul acestora deviază semnificativ de la modelul de normalitate stabilit, când sunt	

				când sunt detectate activități cu risc ridicat sau când nu mai utilizează în mod activ anumite instrumente sau aplicații care, deși anterior permise, prezintă un risc inerent. - recomandările generate trebuie să fie prioritizate în mod inteligent, luând în considerare impactul potențial al implementării lor asupra reducerii globale a suprafeței de atac și/sau criticitatea riscului specific pe care îl adresează. - soluția trebuie să ofere flexibilitate în modul de aplicare a recomandărilor. Trebuie să existe opțiunea de aplicare manuală, permițând administratorilor de securitate să revizuiască și să aprobe fiecare recomandare înainte de implementare. Pentru fiecare recomandare emisă, soluția trebuie să furnizeze un set complet de informații contextuale. Acestea trebuie să includă: - descriere clară a vulnerabilității sau a riscului identificat; - estimare a impactului pe care aplicarea recomandării l-ar avea asupra reducerii suprafeței de atac; - lista profilurilor comportamentale afectate (cu detalii despre	detectate activități cu risc ridicat sau când nu mai utilizează în mod activ anumite instrumente sau aplicații care, deși anterior permise, prezintă un risc inerent. - recomandări generate care pot fi prioritizate în mod inteligent, luând în considerare impactul potențial al implementării lor asupra reducerii globale a suprafeței de atac și/sau criticitatea riscului specific pe care îl adresează. - soluția oferă flexibilitate în modul de aplicare a recomandărilor. În cadrul soluției există opțiunea de aplicare manuală, permițând administratorilor de securitate să revizuiască și să aprobe fiecare recomandare înainte de implementare. Pentru fiecare recomandare emisă, soluția furnizează un set complet de informații contextuale. Acestea includ: - descriere clară a vulnerabilității sau a riscului identificat; - estimare a impactului pe care aplicarea recomandării îl are asupra reducerii suprafeței de atac; - lista profilurilor comportamentale afectate (cu detalii despre utilizatori și dispozitivele asociate);	

				utilizatori și dispozitivele asociate); - tipul de activitate vizată de recomandare (de exemplu, utilizarea unui LOLBin specific); - numele regulii de monitorizare care a stat la baza generării acelei recomandări. d) Vizibilitate Centralizată și Capacități de Raportare: Soluția trebuie să ofere o consolă de management centralizată, accesibilă printr-o interfață web securizată. Consola de management trebuie să includă un dashboard principal (tablou de bord) care să ofere o imagine de ansamblu, în timp real, asupra stării de securitate din perspectiva reducerii suprafeței de atac. <u>Dashboard-ul soluției trebui să prezinte:</u> - expunerea Suprafeței de Atac - widget expunerea Suprafeței de Atac - widget vizual (de preferință procentual) care să indice nivelul curent de expunere a suprafeței de atac și evoluția acestuia în timp. - recomandări de Top (după Impact) - o listă a celor mai importante recomandări de securitate, ordonate după impactul estimat și cu indicarea	- tipul de activitate vizată de recomandare (de exemplu, utilizarea unui LOLBin specific); - numele regulii de monitorizare care a stat la baza generării acelei recomandări. d) Vizibilitate Centralizată și Capacități de Raportare: Soluția oferă o consolă de management centralizată, accesibilă printr-o interfață web securizată. Consola de management include un dashboard principal (tablou de bord) care va oferi o imagine de ansamblu, în timp real, asupra stării de securitate din perspectiva reducerii suprafeței de atac. <u>Dashboard-ul soluției are posibilitatea să:</u> - expună suprafața de Atac - widget expunerea Suprafeței de Atac - widget vizual (de preferință procentual) care indică nivelul curent de expunere a suprafeței de atac și evoluția acestuia în timp. - recomandări de Top (după Impact) - o listă a celor mai importante recomandări de securitate, ordonate după impactul estimat și cu indicarea	

				numărului de profiluri comportamentale afectate. - incidente Detectate Corelate - widget care centralizează numărul total de incidente de securitate corelate cu categoriile de vectori de atac monitorizați. - statistici pe Categorii de Risc - widget-uri dedicate pentru principalele categorii de risc, prezentând date precum numărul de profiluri afectate, recomandările neimplementate și progresul monitorizării. Cerințe privind Funcționalitățile de Navigare și Analiză: - capacități de Drill-Down - Soluția trebuie să permită navigarea în profunzime (drill-down) din dashboard sau liste pentru vizualizarea detaliilor specifice (utilizatori, endpoint-uri, reguli). - filtrare și Căutare Avansată - Soluția trebuie să ofere opțiuni flexibile de filtrare și căutare după criterii multiple, precum numele recomandării, data, profilul comportamental, tipul de activitate și acțiunea întreprinsă. e) Administrare Centralizată și Politici de Securitate Flexibile - soluția trebuie să permită administratorilor crearea, modificarea și aplicarea de	numărului de profiluri comportamentale afectate. - incidente Detectate Corelate - widget care centralizează numărul total de incidente de securitate corelate cu categoriile de vectori de atac monitorizați. - statistici pe Categorii de Risc - widget-uri dedicate pentru principalele categorii de risc, prezentând date precum numărul de profiluri afectate, recomandările neimplementate și progresul monitorizării. Cerințe privind Funcționalitățile de Navigare și Analiză: - capacități de Drill-Down - Soluția permite navigarea în profunzime (drill-down) din dashboard sau liste pentru vizualizarea detaliilor specifice (utilizatori, endpoint-uri, reguli). - filtrare și Căutare Avansată - Soluția oferă opțiuni flexibile de filtrare și căutare după criterii multiple, precum numele recomandării, data, profilul comportamental, tipul de activitate și acțiunea întreprinsă. e) Administrare Centralizată și Politici de Securitate Flexibile - soluția permite administratorilor crearea, modificarea și aplicarea de politici de securitate detaliate.	

				politici de securitate detaliate. Aceste politici vor guverna activarea și configurarea funcționalităților de monitorizare și răspuns pe diferite grupuri de endpoint-uri, în funcție de necesitățile specifice ale departamentelor sau ale rolurilor utilizatorilor. - pentru fiecare categorie de activitate monitorizată (de exemplu, utilizarea LOLBins, instrumente de tampering, mineri de criptomonede etc.), administratorul trebuie să aibă posibilitatea de a alege unul dintre următoarele moduri de operare, oferind astfel un control granular: • monitorizarea pentru tipul respectiv de activitate este complet oprită. În acest mod, soluția nu va colecta date referitoare la acea activitate și, prin urmare, nu va genera recomandări sau alerte specifice. • colectare date despre tipul de activitate selectat, va genera automat recomandări pe baza analizei comportamentale și a regulilor definite și, cel mai important, va aplica automat aceste recomandări pentru a restricționa sau permite accesul, conform concluziilor	Aceste politici guvernează activarea și configurarea funcționalităților de monitorizare și răspuns pe diferite grupuri de endpoint-uri, în funcție de necesitățile specifice ale departamentelor sau ale rolurilor utilizatorilor. - pentru fiecare categorie de activitate monitorizată (de exemplu, utilizarea LOLBins, instrumente de tampering, mineri de criptomonede etc.), administratorul are posibilitatea de a alege unul dintre următoarele moduri de operare, oferind astfel un control granular: • monitorizarea pentru tipul respectiv de activitate este complet oprită. În acest mod, soluția colectează date referitoare la acea activitate și, prin urmare, nu va genera recomandări sau alerte specifice. • colectarea datelor despre tipul de activitate selectat, va genera automat recomandări pe baza analizei comportamentale și a regulilor definite și, cel mai important, va aplica automat aceste recomandări pentru a restricționa sau permite accesul, conform concluziilor	

				analizei. Toate acțiunile automate întreprinse de soluție în acest mod trebuie să fie jurnalizate în detaliu și disponibile pentru revizuire ulterioară de către administratori. • colectare date și generare recomandări către administratorul soluției pentru revizuire și aprobare manuală înainte de a fi efectiv implementate. Acest mod oferă un nivel suplimentar de control uman, fiind preferabil pentru situațiile mai complexe sau cu impact potențial ridicat. <u>EDR</u> Soluția trebuie să 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, care va fi capabil să: - cuprindă colectarea de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliata a acestora precum și acțiuni de remediere automate și	analizei. Toate acțiunile automate întreprinse de soluție în acest mod pot fi jurnalizate în detaliu și disponibile pentru revizuire ulterioară de către administratori. • colectare date și generare recomandări către administratorul soluției pentru revizuire și aprobare manuală înainte de a fi efectiv implementate. Acest mod oferă un nivel suplimentar de control uman, fiind preferabil pentru situațiile mai complexe sau cu impact potențial ridicat. <u>EDR</u> Soluția include modulul 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, care este capabil să: - cuprindă colectarea de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliata a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate;	

				integrare cu modulele de Sandbox și modulul avansat de securitate; - ofere senzori de colectare a datelor și componente de procesare și interpretare a acestora; - posede capacitarăți de evaluare a activitățiii tipice a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE și va raporta orice deviație de la acest comportament sub forma unui incident; - ofere vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat generînd o hartă de principiu a incidentului, detaliind incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, respectiv butonul „acționează" care poate genera un set de masuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod); - poate bloca fișiere si/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;	- oferă senzori de colectare a datelor și componente de procesare și interpretare a acestora; - posedă capacitatăți de evaluare a activitățiii tipice a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE și raportează orice deviație de la acest comportament sub forma unui incident; - oferă vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat generând o hartă de principiu a incidentului, detaliind incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, respectiv butonul „acționează" care poate genera un set de masuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod); - poate bloca fișiere si/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV; - poate excepta fișiere non-malițioase de la acțiunea de investigare sau poate	

				- poată excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adaugă un set de fișiere malițioase într-o listă pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase - permită vizualizarea incidentelor extinse corelate de pe mai multe endpoint-uri. <u>Senzori XDR</u> Soluția trebui sa colecteze date de la: - senzor endpoint (EDR); - senzor rețea, care să: • poată detecta rapid încercările atacatorilor de a fura date și de a le trimite în afara organizației dvs. • poată recunoaște încercările de scanare a porturilor, o tehnică comună utilizată de atacatori pentru a identifica vulnerabilitățile din infrastructura rețelei dvs. • poată detecta atacurile brute-force prin care atacatorii` încearcă să ghicească datele de autentificare pentru a obține acces neautorizat la sistemele dvs. • monitorizeze mai multe subrețele de rețea utilizând un	genera/adaugă un set de fișiere malițioase într-o listă pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase - permite vizualizarea incidentelor extinse corelate de pe mai multe endpoint-uri. <u>Senzori XDR</u> Soluția colectează date de la: - senzor endpoint (EDR); - senzor rețea, care: • poate detecta rapid încercările atacatorilor de a fura date și de a le trimite în afara organizației dvs. • poate recunoaște încercările de scanare a porturilor, o tehnică comună utilizată de atacatori pentru a identifica vulnerabilitățile din infrastructura rețelei dvs. • poate detecta atacurile brute-force prin care atacatorii` încearcă să ghicească datele de autentificare pentru a obține acces neautorizat la sistemele dvs. • monitorizează mai multe subrețele de rețea utilizând un	

				singur dispozitiv virtual Network Sensor - senzor p/u aplicații office 365 (evenimente aplicații Office 365), carte detectează: • dezactivarea protecției antiphishing Office 365. • comportament îndoielnic de creare a unui utilizator, cum ar fi un utilizator nou creat exclus de la cerințele de autentificare cu mai mulți factori. • încărcarea de documente cu macro-uri suspecte în SharePoint și OneDrive. • încărcarea de fișiere executabile în conturile Office 365. • solicitări de acces suspecte, cum ar fi acordarea accesului unui utilizator la mai multe fișiere sau directoare de pe diferite site-uri SharePoint într-o perioadă scurtă de timp. • număr neobișnuit de activități administrative sau manipulări de documente într-o anumită zi, al utilizatorului când astfel de acțiuni sunt neobișnuite pentru practicile normale ale contului de utilizator. - Senzor de identitate	singur dispozitiv virtual Network Sensor - senzor p/u aplicații office 365 (evenimente aplicații Office 365), carte detectează: • dezactivarea protecției antiphishing Office 365. • comportament îndoielnic de creare a unui utilizator, cum ar fi un utilizator nou creat exclus de la cerințele de autentificare cu mai mulți factori. • încărcarea de documente cu macro-uri suspecte în SharePoint și OneDrive. • încărcarea de fișiere executabile în conturile Office 365. • solicitări de acces suspecte, cum ar fi acordarea accesului unui utilizator la mai multe fișiere sau directoare de pe diferite site-uri SharePoint într-o perioadă scurtă de timp. • număr neobișnuit de activități administrative sau manipulări de documente într-o anumită zi, al utilizatorului când astfel de acțiuni sunt neobișnuite pentru practicile normale ale contului de utilizator. - Senzor de identitate	

				Senzorul trebuie să monitorizeze și analizeze identitățile utilizatorilor, controalele de acces și activitățile de autentificare din cadrul rețelei sau din mediul cloud. Acești senzori monitorizează continuu evenimentele legate de identitate și comportamentele conturilor, permițând identificarea potențialelor amenințări sau anomalii de securitate. Senzor de identitate p/u Active Directory, trebuie să: • detecteze activitatea asociată atacurilor care încearcă să utilizeze conturi și obiecte compromise, cuprinzând nu numai conturile utilizatorilor finali, ci și conturile de sistem și de serviciu. • detecteze atacurile care vizează protocolul de autentificare în rețea Kerberos • identifice alte activități legate de Kerberos, cum ar fi utilizarea de tichete Kerberos furate pentru a se deplasa lateral într-o rețea, solicitări de tichete cu criptare slabă (un semn comun de intenție răuvoitoare) și atacuri de reluare, care implică furtul de pachete din rețea și transmiterea lor către un serviciu sau o aplicație.	Senzorul este conceput de a monitoriza și analiza identitățile utilizatorilor, controalele de acces și activitățile de autentificare din cadrul rețelei sau din mediul cloud. Acești senzori monitorizează continuu evenimentele legate de identitate și comportamentele conturilor, permițând identificarea potențialelor amenințări sau anomalii de securitate. Senzor de identitate p/u Active Directory, sre posibilitatea de a: • detecta activitatea asociată atacurilor care încearcă să utilizeze conturi și obiecte compromise, cuprinzând nu numai conturile utilizatorilor finali, ci și conturile de sistem și de serviciu. • detecta atacurile care vizează protocolul de autentificare în rețea Kerberos • identifica alte activități legate de Kerberos, cum ar fi utilizarea de tichete Kerberos furate pentru a se deplasa lateral într-o rețea, solicitări de tichete cu criptare slabă (un semn comun de intenție răuvoitoare) și atacuri de reluare, care implică furtul de pachete din rețea și transmiterea lor către un serviciu sau o aplicație.	

				• identifice cazurile în care atacatorii înregistrează un controler de domeniu necinstit și îl utilizează pentru a injecta obiecte malițioase în alte controlere din cadrul infrastructurii Active Directory. • identifice diverse activități desfășurate de atacatori asupra obiectelor Active Directory și încercările lor de autentificare în sisteme la distanță folosind prudențiale furate. - Senzor de identitate p/u Microsoft Entra ID, trebuie să: • monitorizeze activitățile și configurațiile de autentificare, oferind informații valoroase privind metodele de autentificare a utilizatorilor și potențialele riscuri de securitate din mediul Azure AD. • colecteze și proceseze activitățile și configurațiile de autentificare, jucând un rol crucial în detectarea amenințărilor de-a lungul vectorului de atac. • urmărească și să analizeze încercările de autentificare ale utilizatorilor, inclusiv	• identifica cazurile în care atacatorii înregistrează un controler de domeniu necinstit și îl utilizează pentru a injecta obiecte malițioase în alte controlere din cadrul infrastructurii Active Directory. • identifica diverse activități desfășurate de atacatori asupra obiectelor Active Directory și încercările lor de autentificare în sisteme la distanță folosind prudențiale furate. - Senzor de identitate p/u Microsoft Entra ID, are capacitatea de a: • monitoriza activitățile și configurațiile de autentificare, oferind informații valoroase privind metodele de autentificare a utilizatorilor și potențialele riscuri de securitate din mediul Azure AD. • colecta și procesa activitățile și configurațiile de autentificare, jucând un rol crucial în detectarea amenințărilor de-a lungul vectorului de atac. • Urmări și să analiza încercările de autentificare ale utilizatorilor, inclusiv marcajele temporare, locațiile și adresele IP	

				marcajele temporare, locațiile și adresele IP • identifice activitățile care sugerează credențele compromise. • identifice comportamentele suspecte ale utilizatorilor, cum ar fi crearea mai multor conturi sau schimbarea numelor/emailurilor, care ar putea fi utilizate pentru uzurparea identității. • detecteze crearea de aplicații cu drepturi de acces excesiv de permisive, ceea ce poate indica o potențială încercare de escaladare a privilegiilor. Senzorul de identitate p/u Microsoft Intune, trebuie să: • monitorizeze acțiunile din cadrul mediului Intune, inclusiv modificările în ceea ce privește proprietatea dispozitivelor, atribuirea politicilor și crearea aplicațiilor Intune. • detecteze modificările în ceea ce privește proprietatea dispozitivelor, cum ar fi tranzițiile de la dispozitive deținute de companie la dispozitive personale sau viceversa.	• identifica activitățile care sugerează credențele compromise. • identifica comportamentele suspecte ale utilizatorilor, cum ar fi crearea mai multor conturi sau schimbarea numelor/emailurilor, care ar putea fi utilizate pentru uzurparea identității. • detecta crearea de aplicații cu drepturi de acces excesiv de permisive, ceea ce poate indica o potențială încercare de escaladare a privilegiilor. Senzorul de identitate p/u Microsoft Intune, are capacitatea de a: • monitoriza acțiunile din cadrul mediului Intune, inclusiv modificările în ceea ce privește proprietatea dispozitivelor, atribuirea politicilor și crearea aplicațiilor Intune. • detecta modificările în ceea ce privește proprietatea dispozitivelor, cum ar fi tranzițiile de la dispozitive deținute de companie la dispozitive personale sau viceversa. • detecta momentul în care politicile Intune sunt atribuite unor grupuri specifice	

				• detecteze momentul în care politicile Intune sunt atribuite unor grupuri specifice • identifice crearea de aplicații Intune cu atribuiri specifice, inclusiv opțiunile liniei de comandă de instalare/dezinstalare, căile fișierelor de configurare, scripturile regulilor de detectare/necesare sau numele fișierelor. - Soluția trebuie să permită aplicarea următoarelor acțiuni (automate și/sau manuale) ca măsuri de răspuns la incidente pentru acest tip de senzor: • dezactivare utilizatorului in AD • resetarea parolei utilizatorului AD • marcarea utilizatorului drept compromise • dezactivarea utilizatorului in Azure • resetarea parolei de Azure a utilizatorului <u>Power User</u> Soluția trebuie să conțină un modul pentru setări specifice – power user care să:	• identifica crearea de aplicații Intune cu atribuiri specifice, inclusiv opțiunile liniei de comandă de instalare/dezinstalare, căile fișierelor de configurare, scripturile regulilor de detectare/necesare sau numele fișierelor. - Soluția permite aplicarea următoarelor acțiuni (automate și/sau manuale) ca măsuri de răspuns la incidente pentru acest tip de senzor: • dezactivare utilizatorului in AD • resetarea parolei utilizatorului AD • marcarea utilizatorului drept compromise • dezactivarea utilizatorului in Azure • resetarea parolei de Azure a utilizatorului <u>Power User</u> Soluția este concepută cu un modul pentru setări specifice – power user care va:	

				- poată fi instalat/dezinstalat în funcție de preferința administratorului; - permită posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client; - permită administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User. <u>Protecție Anti-Tampering</u> - va permite detecția driverelor vulnerabile pe dispozitivele conectate (endpointuri) și când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrității produsului; - va permite detectarea de drivere vulnerabile pe dispozitivele conectate care pot fi exploatate de atacatori, reprezentând amenințări la adresa integrității produsului. Tehnologia trebuie să fie compatibilă cu sistemele de operare Windows și Linux; - va fi capabilă să protejeze împotriva amenințărilor noi sau erorilor umane neintenționate ce ar putea fi proiectate pentru a	- putea fi instalat/dezinstalat în funcție de preferința administratorului; - permite posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client; - permite administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User. <u>Protecție Anti-Tampering</u> - permite detecția driverelor vulnerabile pe dispozitivele conectate (endpointuri) și când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrității produsului; - permite detectarea de drivere vulnerabile pe dispozitivele conectate care pot fi exploatate de atacatori, reprezentând amenințări la adresa integrității produsului. Tehnologia este compatibilă cu sistemele de operare Windows și Linux; - este capabilă să protejeze împotriva amenințărilor noi sau erorilor umane neintenționate ce ar putea fi proiectate pentru a	

				permite acces neautorizat la kernel, ducând la compromiterea integrității poate detecta când funcțiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod malițios. <u>Actualizare</u> Soluția trebuie să ofere posibilitatea de efectuare a actualizărilor: - la nivel de stație în mod silențios (fără avertizări); - folosind unul sau mai multe servere de actualizare; - pentru locațiile la distanță prin intermediul unui client specific, care să posede și rol de server de actualizare; - gestionabil – doar local sau și servere online. **<u>Alte cerințe:</u>** Perioada de suport și menținere de la producător: - Pentru soluția ofertată se solicită a fi 12 luni pentru perioada 07.02.2026-07.02.2027; - Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanță. Notă: Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de	permite acces neautorizat la kernel, ducând la compromiterea integrității poate detecta când funcțiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod malițios. <u>Actualizare</u> Soluția oferă posibilitatea de efectuare a actualizărilor: - la nivel de stație în mod silențios (fără avertizări); - folosind unul sau mai multe servere de actualizare; - pentru locațiile la distanță prin intermediul unui client specific, care să posede și rol de server de actualizare; - gestionabil – doar local sau și servere online. **<u>Alte cerințe:</u>** Perioada de suport și menținere de la producător: - Pentru soluția ofertată se pune la dispoziție 12 luni pentru perioada 07.02.2026-07.02.2027; - Producătorul oferă suport 24/24, prin e-mail sau conectare de la distanță. Notă: Lucrările de instalare, configurare, punerea în funcțiune a	

				Ofertant, iar costul acestora trebuie să fie incluse în ofertă.	soluției sunt executate de Ofertant, iar costul acestora este inclus în ofertă.	

Digitally signed by Celonenco Vitalie
Date: 2025.12.30 19:05:07 EET
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Semnat electronic Numele, Prenumele: **CELONENCO Vitalie** În calitate de: **Administrator**

Ofertantul: **RTS ONE S.R.L.** Adresa: mun. Chișinău, str. **Mitropolit Gavriil Bănulescu-Bodoni, 59/B, of.804**