Anexa nr. 22
la Documentația standard nr. 115
din „15" septembrie 2021

OFERTĂ TEHNICĂ ȘI METODOLOGIE

pentru

Sistemul informațional „Registrul de stat al incidentelor cibernetice" (SI RSIC)

Procedura de achiziție: ocds-b3wdp1-MD-1779975470972
Autoritatea contractantă: Agenția pentru Securitate Cibernetică (ASC)
Ofertant: Das Soft Plus S.R.L. (CoRLab Tech), IDNO 1019600011052
Data: 25.06.2026

Prezenta propunere tehnică răspunde 1:1 cerințelor din Caietul de sarcini (referințe CNF/CF) și nu include angajamente peste minimul solicitat. Maparea nominală cerință → soluție este consolidată în tabelul de conformitate de la finalul documentului; secțiunile de mai jos explică abordarea și raționamentul ofertantului.

1. Înțelegerea contextului

SI RSIC este registrul de stat pentru incidente, vulnerabilități și amenințări cibernetice, instituit prin HG 822/2025, în temeiul Legii 48/2023 privind securitatea cibernetică și al HG 824/2025 privind divulgarea coordonată a vulnerabilităților. Sistemul automatizează întregul ciclu — identificarea, raportarea, înregistrarea, clasificarea, analiza, gestionarea și monitorizarea incidentelor și vulnerabilităților — și facilitează schimbul securizat de informații între ASC, CERT-urile sectoriale și entitățile prevăzute de cadrul normativ. Ofertantul a analizat integral Caietul de sarcini și Anunțul de participare și își asumă livrarea în termenul ferm stabilit de autoritate, urmată de 12 luni de garanție cu SLA.

Părțile interesate și actorii. Posesorul și autoritatea contractantă este Agenția pentru Securitate Cibernetică (ASC); administrarea tehnică a MCloud și a securității de platformă revine I.P. „STISC", iar AGE oferă suportul metodologic pentru integrările cu serviciile guvernamentale. Sistemul deservește roluri cu nevoi distincte — operatorii și analiștii ASC care înregistrează, investighează și soluționează cazurile; CERT-urile sectoriale și entitățile raportoare care notifică incidente și vulnerabilități; și partenerii cu care se realizează schimb de informații conform regulilor de marcare TLP. Această separare a rolurilor stă la baza modelului de autorizare pe roluri (RBAC) și a interfețelor dedicate descrise mai jos.

Fluxul funcțional. Soluția este organizată în jurul a patru module care urmează fluxul descris în Caiet: Alertă timpurie (recepția, trierea și corelarea informațiilor despre vulnerabilități și amenințări), Incidente cibernetice (înregistrarea, investigarea, escaladarea, soluționarea și închiderea cazurilor), Schimb de informații (partajarea securizată cu CERT-urile și partenerii) și Administrare și control (roluri, taxonomii și planuri calendaristice de remediere și divulgare). Această structură stă la baza separării componentelor și a interfețelor dedicate, pentru a evita aglomerarea funcțională (CNF179).

2. Soluția propusă — arhitectură și platformă tehnologică

Arhitectură și platformă. Soluția este orientată pe servicii (SOA, conform HG 650/2023 — prestare și consum de servicii web, CNF101), cloud-ready și fără dependențe de

echipament specializat, proiectată pentru găzduire exclusiv în MCloud conform principiului „cloud-first” (HG 128/2014, CNF103, CNF104). Componentele sunt microservicii containerizate (Docker/OCI), desfășurate pe Kubernetes, cu imagini construite automat și instalabile printr-un singur chart Helm parametrizabil, identic pentru mediile Dev/Test/Prod coordonate cu I.P. „STISC”, printr-un pipeline CI/CD dedicat (CNF109, CNF128). Tehnologiile sunt stabile, larg utilizate în ramură și neproprietare, fără componente cu utilizare redusă (CNF102); persistența folosește PostgreSQL, independent tehnologic, pe serverele existente sau pe VM dedicate în MCloud (CNF110). Disponibilitatea este înaltă, cu obiective de recuperare RTO 4 ore / RPO 8 ore (CNF105), iar modelul datelor structurate prestate ca serviciu este aliniat la modelul UE (CNF100). Sistemul expune patru interfețe dedicate — portal public, aplicație internă, configurare/extragere rapoarte și administrare — pentru a separa clar fluxurile de lucru (CNF179).

De ce această arhitectură și de ce CoRLab Tech. Alegerile arhitecturale nu sunt teoretice. Das Soft Plus operează deja în producție, în calitate de contractant principal, sistemul informațional național SIA eRețeta Compensată pentru CNAM — pe exact platforma tehnologică mandatată și de prezentul Caiet: microservicii containerizate pe Kubernetes în MCloud, cu integrările MPass, MConnect, MSign, MLog și MNotify funcționale în mediu de stat. La acestea se adaugă registre de stat livrate pentru instituții publice din Republica Moldova — DRG/SIRSM, CanReg (registru oncologic) și Biobanca (USMF) — care reproduc tiparul de înregistrare-clasificare-raportare specific unui registru de stat precum SI RSIC. Prin urmare, partea cea mai predispusă la eșec a acestui proiect — cele șase integrări cu platforma guvernamentală — este tocmai capacitatea pe care ofertantul a dovedit-o deja în producție, nu una de validat.

Onestitate privind componenta de specialitate. Componenta de domeniu a SI RSIC — modelele de date IODEF (incidente) și CSAF (vulnerabilități), taxonomiile MISP, evaluarea CVSS 4.0 și divulgarea coordonată conform HG 824/2025 — se bazează integral pe standarde deschise, publice (IODEF RFC 7970, CSAF/OASIS, MISP open-source, CVSS și TLP de la FIRST.org). Ofertantul le tratează ca livrabile de implementat la standard și demonstrează stăpânirea lor prin maparea explicită a modelului de date și a API-urilor la aceste standarde (secțiunile 4, 8 și tabelul de conformitate), nu printr-o pretenție de experiență CERT anterioară. Capacitatea de a livra la un standard de interoperabilitate extern este probată de alinierea CanReg la standardele europene ENCR/ECIS și de practica de proiectare securizată cu testare de penetrare premergătoare punerii în exploatare.

3. Module funcționale

3.1 Alertă timpurie (vulnerabilități și amenințări). Modulul recepționează, triază și corelează informațiile despre vulnerabilități și amenințări; oferă formularul de notificare a vulnerabilității (FNV), clasificarea și evaluarea severității și calendarul de remediere standard sau accelerat. Cazurile sunt clasificate pe ENISA Threat Taxonomy (CF101), reutilizând clasificatoarele de stat ale RM (CF912), iar o alertă poate fi triată ca pozitivă, fals-pozitivă sau degenerată într-un incident (CF107–110).

3.2 Incidente cibernetice. Modulul acoperă ciclul complet de viață al cazului — înregistrare, investigare, escaladare, soluționare și închidere — cu identificator în formatul AALLDD-XXXX (CF132), istoric complet al modificărilor și trasabilitate (CF133, CF135, CF139), suplimentarea cazului cu înregistrări adiționale și corelarea cazurilor din surse

diferite sub un caz comun (CF113, CF115). Ciclul se finalizează cu transmiterea în arhivă (CF203, CF204, CF206, CF209).

3.3 Schimb de informații. Schimbul securizat cu CERT-urile sectoriale și partenerii se face cu sincronizarea instrumentariului de ramură (MISP) și a vocabularelor standard, conform IODEF/CSAF, cu distribuirea și publicarea controlate prin marcajele TLP (FIRST.org): elementele publice se publică, modificările se notifică, iar accesul respectă nivelul TLP al cazului (CF121, CF122, CF124, CF126, CF127).

3.4 Administrare și control. Modulul gestionează rolurile și echipele (RBAC), taxonomiile și configurările, precum și planurile calendaristice pentru remediere și divulgare coordonată conform HG 824/2025. Sistemul alertează la iminența depășirii limitelor de timp ale planurilor calendaristice, ține evidența respectării acestora și jurnalizează depășirile (CF917, CF918, CF919), cu termene de remediere standard și accelerat (CF227–229, CF234, CF242).

4. Interoperabilitate și integrări (m-servicii)

Servicii de platformă, dovedite în producție. SI RSIC reutilizează serviciile guvernamentale obligatorii, toate dovedite de ofertant în producție pe eRețeta Compensată: autentificare exclusiv prin MPass — acces doar pentru identități verificate (HG 1090, CNF122, CNF130); semnătură electronică și validare prin MSign (HG 405, CNF123); jurnalizare și audit prin MLog (HG 708, CNF124); notificarea părților prin MNotify (HG 376, CNF126); acces la registrele de stat prin platforma de interoperabilitate MConnect (Legea 142, CNF121); și determinarea reprezentării persoană (IDNP)–organizație (IDNO) pe baza MConnect/MPass/MPower (CNF127). Convențiile de schimb respectă XML pentru serviciile de platformă și JSON preferențial pentru API (CNF120). Autentificarea sistem-la-sistem folosește OAuth 2.0 Client Credentials Grant, cu token legat de client_id și IP și expirare configurabilă.

Notă (disclaimer terți). Disponibilitatea funcțiilor de mai sus depinde de serviciile terțe consumate (MCloud — I.P. „STISC"; m-servicii — AGE). Incidentele cauzate de indisponibilitatea acestor servicii sunt excluse din SLA asumat de Prestator.

5. Cerințe de securitate

Secure by design. Proiectarea aplică mecanismele cerute de HG 201 (CNF131), cu mecanisme de securitate documentate (CNF132) și management automatizat al secretelor și parametrilor de securitate, cu rotație fără întreruperi (CNF133, CNF141). Canalele sunt criptate, HTTPS configurat exclusiv TLS 1.3 și mai nou (CNF134); sesiunile expiră la inactivitate (implicit 10 min, configurabil, CNF135); datele de intrare sunt validate pe client și pe server (CNF136), încercările de acces eșuate sunt jurnalizate (CNF137), integritatea datelor este protejată (CNF138), iar un API de viabilitate/heartbeat expune starea componentelor (CNF139).

Apărare aplicativă și date personale. Proiectarea ține cont de OWASP Top 10 (Web, Mobile, API) și aplică privilegiul minim, cu protecție SQLi/XSS/CSRF/file-inclusion/cookie-poisoning (CNF140, CNF142) și Web Application Firewall fără reguli wildcard permisive (CNF143). Pe mediul de dezvoltare se execută scanare de vulnerabilități și teste de penetrare, cu rapoarte partajate (CNF144, CNF145), recomandări de detectare a incidentelor din loguri (CNF146), evidențierea componentelor mai vechi de 12 luni (CNF147) și scanare antimalware a atașamentelor (CNF148). Datele cu

caracter personal se reduc la setul minim (IDNP/IDNO, nume, denumire organizație), separat și cu retenție de 3 ani, urmată de ștergere (CNF149, CNF150).

6. Performanță

Ținte și mecanisme. Soluția este dimensionată pentru cel puțin 300 utilizatori concurenți (CNF151), cu timp de răspuns sub 3 secunde la operațiile uzuale (CNF152) și suport pentru cel puțin 1000 de apeluri concurente la API (CNF153). Operațiile de durată sunt procesate asincron, fără blocarea interfeței (CNF154), iar dimensiunea fișierelor încărcate este gestionată cu limite configurabile (CNF155). Se execută teste de performanță cu scenarii și rapoarte partajate cu beneficiarul (CNF156), se asigură funcționarea corectă în condiții de încărcare (CNF157) și optimizarea utilizării resurselor (CNF159). Dimensionarea TCO pe 5 ani acoperă profilul de 5.000 utilizatori, 200 procesoare și 100.000 GB (CNF115).

7. Interfața utilizator

Aspect, accesibilitate și interacțiune. Aspectul vizual se coordonează iterativ cu beneficiarul (CNF170), cu wireframes, prototipuri interactive și design system livrate prin Figma. Interfața respectă WCAG 2.2 nivel AA (CNF171), este multilingvă RO (implicit)/EN/RU (CNF172), funcționează ca Progressive Web Application pe mobil (CNF173) la o lățime minimă de 1280px (CNF174) și include asistență contextuală, bookmark-uri și referințe lizibile (CNF175–177). Listele sunt paginate, cu sortare și filtrare avansată și evidențierea statutului/severității (CNF181–185), iar panoul de bord oferă KPI cards și grafice linie/bare/plăcintă, grile și tabele, configurabile și interactive (CNF186–188). Raportarea și extragerea datelor permit export în tabel electronic, CSV și HTML (precum și PDF/XLS) (CU1.03).

8. Raportare și taxonomie

Catalog semantic și taxonomii. Serviciile prestate sunt pregătite pentru integrare și publicare în catalogul semantic semantic.gov.md (CNF201), cu reutilizarea clasificatoarelor de stat ale RM (CF912). Taxonomiile MISP (MISP-taxonomies) sunt sursă primară pentru consum automat, cu posibilitatea de a exclude sau ascunde anumite taxonomii (CNF202, CNF203); valorile au spațiu de nume/predicate, cu afișare integrală sau scurtă cu tooltip (CNF204), sunt tratate ca etichete (#tag) și disponibile ca filtre (CNF205), pot fi evidențiate (culoare text/fundal), admise în câmpuri textuale și reflectate în statistici (CNF206–208). Cazurile sunt clasificate cu ENISA Threat Taxonomy (CF101); interoperabilitatea folosește IODEF v2/IODEF-SCI (incidente) și CSAF v2.1 (alerte/vulnerabilități), evaluarea conform CVSS 4.0 (CF231) și distribuirea conform TLP (CF121).

9. Testare

Strategie și acoperire. Strategia, planul și rapoartele de testare (CNF194) acoperă testarea funcțională, de regresie, de performanță (CNF156) și de securitate — scanare de vulnerabilități și teste de penetrare (CNF144–145) — cu validare în versiunile curente ale navigatoarelor libere și proprietare, Chromium și Firefox (CNF108). Testarea de securitate urmează OWASP Security Testing Guide și precede punerea în exploatare.

10. Documentare și instruire

Documentație, cod și formare. Limba de comunicare de bază este română, cu asigurarea traducerii comunicărilor și a disponibilității translatorilor pentru alte limbi (CNF191). Se livrează manuale pentru utilizatori (pe roluri) și administratori (configurare, depanare, customizare) (CNF192), tutoriale video pentru activitatea de zi cu zi (CNF193) și documente tehnice — SDD, ghid de instalare/configurare, strategia/planul și rapoartele de testare (CNF194). Codul sursă este livrat cu instrucțiuni și scripturi de compilare/instalare și configurare securizată, într-un repozitoriu Git pe MCloud (CNF195), cu referințe API pe bază de WSDL sau Swagger (CNF196). Curricula de instruire acoperă utilizatorii și administratorii (CNF197), inclusiv instruirea a 10–15 formatori desemnați de beneficiar (CNF198).

11. Licențiere, drepturi și plan de ieșire

Proprietate și independență. Ofertantul transferă codul sursă către beneficiar, cu instrucțiuni de compilare (CNF111, CNF165), și asigură licențe perpetue pentru componentele sistemului, cu excepția componentelor Open Source (CNF112). Datele aparțin beneficiarului, în formate de date deschise și pe standarde deschise (CNF113, CNF114, CNF116), API-ul este documentat (WSDL, CNF117), iar planul de transfer/ieșire elimină orice dependență nejustificată de furnizor (CNF118).

12. Mentenanță, garanție și suport

Operare și garanție. Jurnalizarea folosește o librărie mainstream (log4j/log4net), cu niveluri Critical/Error/Warning/Info/Debug și conținut detaliat (CNF161–163); stoparea grațioasă, instalarea automatizată, actualizările și copiile de rezervă sunt documentate și automatizate (CNF164–169). După recepție, ofertantul asigură garanție (mentenanță de corecție) 12 luni și disponibilitate de suport pentru următorii 5 ani, contractabil separat (CNF211, CNF212), cu soluționarea (pozitivă sau negativă) a tuturor defectelor identificate în perioada de garanție (CNF213).

SLA și control al schimbării. Pentru defectele critice: preluare în maximum 2 ore, soluționare în maximum 6 ore, raportare orară a progresului (CNF214); pentru cele non-critice: confirmare în maximum 8 ore, soluționare în maximum 5 zile lucrătoare (CNF215). Există un mecanism pentru solicitări de modificare în perioada de garanție (CNF216), iar planul de dare în exploatare se pregătește și se coordonează cu beneficiarul (CNF217).

13. Echipa de proiect

Acoperirea rolurilor-cheie. Caietul de sarcini (pag. 87) cere ca echipa de proiect să includă cel puțin cele 9 roluri-cheie — manager de proiect, analist de business/sistem, arhitect software, expert securitate cibernetică, specialist integrare cu servicii guvernamentale partajate, specialist DevOps/deployment MCloud, QA/test automation, expert UX/UI și specialist instruire — și ca oferta să prezinte profilurile acestor specialiști și nivelul lor de experiență. Oferta nominalizează câte un profil distinct pentru fiecare dintre cele 9 roluri, prezentat în Declarația privind personalul de specialitate (Anexa 14), confirmată prin semnătura electronică a ofertantului. Experiența pe platforma guvernamentală și pe registre de stat (eRețeta Compensată, CanReg, Biobanca) este confirmată prin scrisorile de recomandare ale beneficiarilor și prin contractele din Anexa 12; la solicitarea autorității contractante se prezintă copiile contractelor de muncă.

14. Riscuri și managementul schimbării

Riscuri principale și măsuri. Riscul principal de termen îl reprezintă coordonarea integrărilor cu serviciile de platformă guvernamentală (aspecte organizaționale, contractuale și tehnice). Măsuri: alocarea de personal experimentat care a livrat deja aceste integrări în producție, inițierea timpurie a clarificărilor și coordonării cu I.P. „STISC" și AGE și puncte de contact dedicate. Al doilea risc ține de adoptarea standardelor de domeniu (IODEF/CSAF/MISP/CVSS); el este atenuat prin tratarea acestora ca livrabile la standard deschis, cu mapare documentată a modelului de date și validare timpurie cu beneficiarul. Riscurile sunt gestionate printr-un registru de riscuri și un mecanism de control al schimbării.

15. Tabel de conformitate (cerințe Caiet de sarcini → soluție oferită)

Maparea nominală a principalelor cerințe funcționale (CF) și nefuncționale (CNF) la soluția oferită:

Cod cerință	Cerința din Caietul de sarcini	Cum este acoperită în soluția oferită
CNF100	Aliniere model de date la modelul UE (date structurate prestate ca serviciu)	Modelul de date este aliniat la vocabularele UE pentru datele structurate publicate ca serviciu; mapare documentată în SDD.
CNF101	Arhitectură SOA (HG 650/2023) — prestare/consum de servicii web	Arhitectură orientată pe servicii: microservicii cu API documentat (OpenAPI), prestare și consum de servicii web.
CNF102	Tehnologii stabile, neproprietare, larg utilizate	Stack open-source/mainstream (containere OCI, Kubernetes, PostgreSQL); fără componente cu utilizare redusă sau proprietare.
CNF103 / CNF104	Soluție Cloud-Ready, găzduire în MCloud (HG 128/2014)	Cloud-first, fără dependență de hardware specializat; desfășurare exclusiv în MCloud prin chart Helm parametrizabil.
CNF105	Disponibilitate înaltă, RTO 4h / RPO 8h	Componente redundante (min. 2 instanțe), copii de rezervă automatizate; obiective de recuperare RTO 4h / RPO 8h.
CNF108	Validare pe Chromium și Firefox	Testare funcțională în versiunile curente Chromium și Firefox (plus Edge/Safari).
CNF109 / CNF128	Containerizare Docker/Kubernetes; medii Dev/Test/Prod, CI/CD cu STISC	Imagini Docker automatizate; pipeline CI/CD coordonat cu I.P. „STISC", build la tag de versiune, registru securizat.
CNF110	Bază de date independentă tehnologic	PostgreSQL pe servere existente sau VM dedicate în MCloud, pentru performanță maximă.
CNF111–118 / CNF165	Cod sursă, licențe perpetue, date deschise, plan de ieșire	Transfer cod sursă editabil + instrucțiuni de compilare; licențe perpetue (excepție Open Source); fără dependență nejustificată de furnizor.
CNF115	Dimensionare TCO 5 ani (5.000 utilizatori / 200 CPU / 100.000 GB)	TCO bottom-up pe 5 ani, anexat ofertei financiare.
CNF120 / CNF121	XML servicii platformă, JSON pentru API; MConnect (Legea 142)	XML pentru m-servicii, JSON preferențial pentru API public; acces la registre prin MConnect.
CNF122 / CNF130	Autentificare exclusiv prin MPass (HG 1090)	Acces doar pentru identități verificate MPass; maparea atributelor MPass la roluri.
CNF123	Semnătură electronică prin MSign (HG 405)	Semnare și validare prin MSign.
CNF124	Jurnalizare și audit prin MLog (HG 708)	Evenimentele de business jurnalizate securizat în MLog.

Cod cerință	Cerința din Caietul de sarcini	Cum este acoperită în soluția oferită
CNF126 / CNF127	Notificare prin MNotify (HG 376); reprezentare IDNP–IDNO	Notificări prin MNotify; determinarea reprezentării persoană-organizație prin MConnect/MPass/MPower.
CNF131–134 / CNF141	Secure-by-design (HG 201), management secrete, TLS 1.3	Mecanisme de securitate documentate; management automatizat al secretelor; HTTPS exclusiv TLS 1.3+.
CNF135–138	Expirare sesiune, validare intrări, jurnalizare eșecuri, integritate	Expirare sesiune la inactivitate (10 min configurabil); validare client+server; jurnalizarea acceselor eșuate; protecția integrității datelor.
CNF139	API de viabilitate / heartbeat	Endpoint de heartbeat pentru monitorizarea stării componentelor.
CNF140 / CNF142 / CNF143	OWASP Top 10; SQLi/XSS/CSRF; WAF fără reguli wildcard	Aliniere OWASP Top 10 (Web/Mobile/API); protecții explicite; WAF fără reguli permisive.
CNF144 / CNF145	Scanare vulnerabilități și teste de penetrare	Scanare + pen-test pe mediul de dezvoltare, cu rapoarte partajate cu beneficiarul.
CNF146 / CNF147 / CNF148	Detectare incidente din loguri; componente curente; antimalware atașamente	Recomandări de detectare din loguri; evidențierea componentelor mai vechi de 12 luni; scanare antimalware a atașamentelor.
CNF149 / CNF150	Protecția datelor personale (set redus, retenție 3 ani)	Set minim (IDNP/IDNO, nume, organizație), separare, retenție 3 ani apoi ștergere.
CNF151 / CNF152	≥300 utilizatori concurenți; răspuns <3s	Arhitectură dimensionată pentru ≥300 utilizatori concurenți; răspuns <3s la operațiile uzuale.
CNF153 / CNF154 / CNF155	≥1000 apeluri API concurente; procesare asincronă; limite fișiere	≥1000 apeluri concurente la API; operațiile de durată procesate asincron; limite configurabile de fișier.
CNF156 / CNF157 / CNF159	Teste de performanță; funcționare sub încărcare; optimizare	Scenarii și rapoarte de performanță partajate; funcționare corectă sub încărcare; utilizare eficientă a resurselor.
CNF161–169	Loguri mainstream; stopare grațioasă; instalare/backup automatizate	log4j/log4net cu niveluri Critical→Debug; oprire grațioasă; instalare, actualizări și backup documentate și automatizate.
CNF170–177	Aspect coordonat; WCAG 2.2 AA; multilingv RO/EN/RU; PWA ≥1280px	Design coordonat iterativ (Figma); WCAG 2.2 nivel AA; RO/EN/RU; PWA, lățime minimă 1280px; asistență contextuală.
CNF181–188 / CU1.03	Liste, filtrare, panou de bord, export date	Liste paginate/sortare/filtrare; KPI cards și grafice configurabile; export tabel electronic, CSV, HTML (plus PDF/XLS).
CNF191–198	Limba RO, manuale, tutoriale video, SDD, cod sursă, API ref, instruire	Comunicare în RO; manuale utilizator/admin; tutoriale video; SDD/ghiduri; cod sursă în Git pe MCloud; API Reference (WSDL/Swagger); curicula + 10–15 formatori.
CNF201–208	Catalog semantic; taxonomii MISP; etichete, filtre, statistici	Pregătire pentru semantic.gov.md; taxonomii MISP cu excludere/spațiu de nume; #tag-uri ca filtre; evidențiere și reflectare în statistici.
CNF211–217	Garanție 12 luni + suport 5 ani; SLA; control modificări	Garanție 12 luni + disponibilitate suport 5 ani; SLA critice 2h/6h, non-critice 8h/5 zile lucrătoare; mecanism de control al schimbării.
CF101 / CF912	Clasificare ENISA Threat Taxonomy; reutilizare clasificatoare RM	Modulul Alertă timpurie clasifică pe taxonomia ENISA, reutilizând clasificatoarele de stat publicate pe semantic.gov.md.
CF102 / CF128 / CF129	Import/încărcare/actualizare în format CSAF	Încărcare, descărcare și actualizare alerte și vulnerabilități în format CSAF v2.1.

Cod cerință	Cerința din Caietul de sarcini	Cum este acoperită în soluția oferită
CF104 / CF105	Date obiecte „alertă” și „vulnerabilitate”	Structuri de date aliniate modelului, populate inclusiv din documentele atașate.
CF107–110 / CF113 / CF115	Triere alertă (pozitivă/fals-pozitivă); degenerare în incident; corelare	Fluxuri de triere și degenerare a alertei în incident; corelare manuală/automată a cazurilor sub un caz comun.
CF121 / CF122 / CF124 / CF126 / CF127	Distribuire și publicare conform TLP; sincronizare	Control al accesului conform TLP (FIRST.org); publicarea elementelor publice; notificarea modificărilor.
CF132 / CF133 / CF135 / CF139	Identificator caz AALLDD-XXXX; atribute și istoric caz	Generarea automată a identificatorului; trasabilitate completă a atributelor, istoricului și modificărilor.
CF203 / CF204 / CF206 / CF209	Escaladare, evidențiere, arhivare, închidere incident	Ciclu de viață complet al incidentului, cu transmitere în arhivă.
CF227–229 / CF234 / CF242	Calendare de remediere; termene de divulgare coordonată	Notificări incomplete în max 2 zile; cazuri critice în max 2 ore; calendar accelerat; respectarea termenelor HG 824/2025.
CF231 / CF232 / CF236	Evaluare CVSS 4.0; raport final de remediere	Calcul scor și clasificare CVSS 4.0, cu informarea raportorului; raport final cu teste de validare.
CF917 / CF918 / CF919	Urmărirea limitelor calendaristice	Alertare la iminența depășirii termenelor, evidența respectării și jurnalizarea depășirilor.
CF249 / CNF179	Prezentarea datelor; interfețe dedicate	Vizualizare structurată, paginată, filtrabilă; interfețe dedicate (portal public, aplicație internă, rapoarte, administrare).
IODEF / CSAF / CVSS / TLP / MISP / EUVD	Standarde de interoperabilitate	IODEF v2/IODEF-SCI (incidente), CSAF v2.1 (vulnerabilități), CVSS 4.0, TLP, MISP-taxonomies, EUVD — implementate ca livrabile la standard.

Semnat: _____ Numele, Prenumele: Butucea Afanasie În calitate de: Administrator

Ofertantul: Das Soft Plus S.R.L. (brand CoRLab Tech), IDNO 1019600011052

Adresa: MD-2001, str. Lev Tolstoi 74, ap. 78, mun. Chișinău, Republica Moldova

Digitally signed by Butucea Afanasie
Date: 2026.06.25 14:20:15 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ