Caiet de Sarcini pentru achiziție „Platforma software pt. orchestrarea adaptiva si autonoma a elementelor de securitate cibernetica necesare pt. desfasurarea in siguranta a activitatilor experimentale, operationale si administrative"

Cuprins

1 Introducere

Caietul de sarcini face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Caietul de sarcini conține specificații tehnice. Acestea definesc, după caz și fără a se limita la cele ce urmează, caracteristici referitoare la nivelul calitativ, tehnic și de performanță, siguranța în exploatare, dimensiuni.

Instituțiile competente de la care furnizorii pot obține informații privind reglementările obligatorii referitoare la protecția muncii, la prevenirea și stingerea incendiilor și la protecția mediului, care trebuie respectate pe parcursul îndeplinirii contractului:

- Ministerul Muncii, Familiei, Tineretului și Solidarității Sociale;
- ; Inspectoratul Teritorial de Munca Ilfov;
- Inspectoratul pentru Situații de Urgenta „Dealul Spirii" București – Ilfov;
- Ministerul Mediului, Apelor și Pădurilor; Agenția Națională pentru Protecția Mediului; Agenția pentru Protecția Mediului Ilfov.

În cadrul acestei proceduri de atribuire, INSTITUTUL NATIONAL DE CERCETARE DEZVOLTARE PENTRU FIZICA SI INGINERIE NUCLEARA „HORIA HULUBEI" (IFIN-HH) îndeplinește rolul de Autoritatea contractantă, respectiv Achizitor în cadrul Contractului.

Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

2 Contextul realizării acestei achiziții de produse

2.1 Informații despre Autoritatea contractantă

Institutul Național de Cercetare-Dezvoltare pentru Fizică și Inginerie Nucleară "Horia Hulubei" - IFIN - HH are ca scop desfășurarea activității de cercetare științifică și dezvoltare tehnologică în domeniul fizicii şi ingineriei nucleare. Acesta este specializat să dezvolte cunoștințele în domeniul fizicii, în special a celor sub-atomice, precum și creșterea impactului domeniului nuclear în societate, prin cercetarea avansată și prin serviciile cele mai profesioniste.

Misiunea IFIN-HH este de a genera, tezauriza și disemina cunoaștere în domeniile sale de profil și de a participa activ la transferul cunoașterii și al tehnologiilor generate de aceasta, către societate.

IFIN - HH are ca obiect principal de activitate efectuarea de cercetări fundamentale, orientative și aplicative, dezvoltare tehnologică și activități productive, servicii de interes strategic în domeniul său și elaborarea proiectelor de reglementări de interes public și național care privesc asigurarea cerințelor fundamentale impuse fizicii și ingineriei nucleare.

În cadrul IFIN-HH se derulează proiectul „Extreme Light Infrastructure – Nuclear Physics" (ELI-NP), fiind în curs de a deveni un Centru European de Excelență în cercetare avansată în domeniul laserilor de mare intensitate, al interacțiunii dintre laser și materie și al surselor secundare de radiații, oferind posibilități unice la nivel mondial. Intensitatea maximă a laserilor din cadrul infrastructurii ELI-NP deține în prezent recordul mondial. Datorită caracteristicilor sale unice, această infrastructură multidisciplinară oferă posibilități noi privind studiul proceselor fundamentale observate pe durata interacțiunii dintre lumină și materie. ELI-NP este o platformă de cercetare-dezvoltare ce promovează dezvoltarea de aplicații în beneficiul societății și în cadrul căreia cercetarea aplicată va juca un rol important. Această facilitate, ELI-NP, este situată în Măgurele, județul Ilfov, România. ELI-NP găzduiește un Sistem Laser de Mare Putere (HPLS) cu două fascicule de 10 PW și va găzdui un Sistem Fascicul Gama producând

fasciculele gamma cu parametrii mult mai înalți decât cei produși în cele mai performante mașini la nivel mondial.

2.2 Informații despre contextul care a determinat achiziționarea produselor

Operarea instalațiilor și ansamblurilor experimentale din cadrul ELI-NP, respectiv desfășurarea experimentelor propriu-zise, presupun nu doar achiziția, procesarea și transferul unor volume mari de date (experimentale, teoretice, de comandă și control), ci și monitorizarea continuă și răspunsul rapid la evenimente și incidente de securitate cibernetică generate de sistemele și infrastructurile de securitate utilizate în cadrul facilității. Similar, operațiunile suport pentru operarea ELI-NP (activități de mentenanță, optimizări, reconfigurări, schimburi de informații cu terți/furnizori/parteneri) sunt însoțite de fluxuri crescute de alerte și notificări de securitate, provenind de la multiple soluții tehnice de securitate cibernetică (firewall-uri, sisteme de detectare/prevenire intruziuni, sisteme de analiză comportamentală, etc.), care trebuie procesate, corelate și investigate manual de către personalul de specialitate.

În acest context, volumul de alerte depășește capacitatea de procesare umană, studiile din industrie confirmând faptul că 70% din echipele de securitate petrec zilnic cel puțin 2,5-5 ore doar pentru triajul alertelor (înainte de a întreprinde orice acțiune concretă). În paralel, viteza și agresivitatea atacurilor cibernetice au crescut semnificativ: rapoartele actuale arată că 25% din cazuri implică exfiltrarea de date în mai puțin de 5 ore, iar 86% din atacuri au ca obiectiv perturbarea operațională (întreruperea activității, afectarea reputației sau ambele). Totodată, 42% din atacurile de tip ransomware sunt inițiate în afara orelor de program (nopți, weekend-uri, sărbători), în timp ce monitorizarea și răspunsul la incidente din cadrul ELI-NP se desfășoară în timpul orelor standard de lucru.

Această situație creează vulnerabilități majore și expuneri la riscuri operaționale și de securitate cibernetică semnificative, întrucât devine imposibilă identificarea, investigarea și răspunsul coordonat și automatizat la evenimente/incidente de securitate în timp util, mai ales în cadrul general de risc determinat de amenințările cibernetice actuale (potentat nu în ultimul rând de diseminarea și utilizarea accelerată a tehnologiilor de tip inteligență artificială în dezvoltarea și realizarea de atacuri cibernetice automatizate).

Infrastructura existentă în cadrul ELI-NP la acest moment nu dispune de capabilitățile tehnice necesare pentru orchestrarea adaptivă și autonomă a răspunsului la incidente de securitate, fiind dependentă exclusiv de intervenția manuală a personalului de specialitate pentru fiecare alertă sau incident detectat.

2.3 Informații despre beneficiile anticipate de către Autoritatea contractantă

Produsele descrise în prezentul caiet de sarcini sunt menite să contribuie la realizarea misiunii ELI-NP de a fi cea mai importantă infrastructură europeană de cercetare și dezvoltare care va facilita experimente cu câmpuri electromagnetice de intensități extrem de ridicate, permisă de dezvoltarea primului sistem laser de 10 PW din lume.

Nevoile programatice ale experimentelor viitoare, stabilite de comunitatea științifică (utilizatorul final al facilității ELI-NP) prin Cartea Albă a ELI-NP și de către Consiliul Științific Internațional Consultativ (ISAB) prin rapoartele lor anuale privind evoluția ELI-NP, au dus la implementarea mai multor zone experimentale pentru întreaga facilitate.

Comunitatea științifică așteaptă ca ELI-NP să fie o infrastructură laser de înaltă performanță, unde utilizatorii pot efectua experimente pentru cercetări de cel mai înalt nivel. Aceasta presupune un timp de lucru foarte predictibil, cu perioade minime de neoperare, pentru a efectua experimente minuțioase planificate cu ani în avans. Este imperativ necesar ca strategiile de minimizare a riscului de incapacitate operațională (inclusiv prin reducerea timpului de răspuns la incidentele de securitate cibernetică și prevenirea întreruperilor operaționale cauzate de atacuri în plan digital) să fie implementate.

În plus, în calitate de "entitate importantă" conform OUG 155/2024 (transpunerea Directivei NIS2), ELI-NP trebuie să respecte cerințe tehnice specifice, inclusiv raportarea inițială a incidentelor semnificative în maxim 24 de ore (Art. 15(7)(a)), trasabilitate (logare) a tuturor activităților (Art. 11(4)), măsuri proporționale și adecvate riscului, ținând cont de cele mai recente tehnologii și bune practici (Art. 11(2)).

3 Descrierea produselor solicitate

Produsele solicitate constau în două instanțe ale unei platforme software pentru orchestrarea adaptivă și autonomă a elementelor de securitate cibernetică (de tip SOAR – „Security Orchestration, Automation and Response", sau echivalent): una productivă (denumita in continuarea „PROD") și una pentru dezvoltare și testare (denumita „DEV-TEST"), prin care să poată fi asigurată centralizarea, automatizarea și accelerarea operațiunilor de securitate, inclusiv triajul automatizat al alertelor, îmbogățirea contextuală a informațiilor, investigarea asistată de inteligență artificială generativă și răspunsul coordonat la incidente.

Instanța DEV-TEST va permite dezvoltarea, testarea și validarea de „playbook-uri" / „runbook-uri" (sau echivalent) de orchestrare și automatizare înainte de migrarea acestora în mediul productiv (PROD), asigurând astfel securitatea și robustețea implementărilor operaționale. Licențierea va fi perpetuă pentru ambele instanțe, fără dependență de componente, resurse sau servicii externe/cloud.

Soluția trebuie să permită integrări bidirecționale extinse cu dotările tehnice de securitate cibernetică existente (multi-vendor) și să includă capabilități de management al cazurilor/incidentelor, management al vulnerabilităților și integrări specifice pentru medii de tip ICS (Industrial Control Systems) / OT (Operational Technology).

3.1 Descrierea situației actuale la nivelul Autorității contractante

Infrastructura specifică existentă în cadrul ELI-NP la acest moment nu dispune de mijloacele tehnice necesare pentru orchestrarea automată și integrată a răspunsului la evenimentele și incidentele de securitate cibernetică. Procesarea, corelarea, investigarea și răspunsul la alertele provenite de la soluțiile de securitate existente se realizează exclusiv manual, ceea ce determină:

- Întârzieri semnificative în identificarea și răspunsul la incidente (rapoarte din industrie arată că timpul median de la compromiterea inițială până la pierderea datelor este mai mic de 24 de ore, iar în unele cazuri criptarea prin ransomware apare la câteva ore după compromitere);
- Imposibilitatea procesării tuturor alertelor generate de soluțiile moderne de securitate (saturație de alerte);
- Acoperire temporală inadecvată – monitorizarea și răspunsul se desfășoară doar în timpul orelor standard de lucru, în timp ce atacurile au loc oricând (42% din atacurile de tip ransomware sunt inițiate în afara orelor de lucru).

3.2 Obiectivul general la care contribuie furnizarea produselor

Obiectivul general este reprezentat de asigurarea desfasurarii activitatilor experimentale si operationale din cadrul Proiectului ELI-NP in conditii de stabilitate, siguranta si securitate.

3.3 Obiectivul specific la care contribuie furnizarea produselor

Obiectivul specific constă în orchestrarea adaptivă și autonomă a proceselor de detectare, investigare și răspuns la evenimentele și incidentele de securitate cibernetică, prin:

- Centralizarea și automatizarea triajului alertelor provenite de la multiple soluții de securitate;
- Îmbogățirea contextuală automată a alertelor cu informații relevante din surse interne și externe;
- Investigarea asistată de tehnici bazate pe inteligență artificială generativă și motoare de recomandare bazate pe învățare automată;
- Executarea automată de acțiuni de remediere și răspuns (izolare dispozitive, blocare conturi, colectare dovezi, notificări, etc.) prin integrări bidirecționale cu dotările tehnice existente;
- Asigurarea continuității răspunsului la incidente și în afara orelor standard de lucru, prin playbook-uri automate care reduc dependența de intervenția umană imediată;
- Conformitatea cu cerințele OUG 155/2024 (NIS2), inclusiv capacitatea de raportare rapidă (sub 24h) și trasabilitatea completă a tuturor operațiunilor.

3.4 Produsele solicitate

În derularea contractului, activitatea Contractantului va fi condusă de următoarele principii:

i. Contractantul acționează în interesul Autorității contractante pe durata furnizării produselor, în condițiile și cu limitele descrise în documentația aferentă prezentei proceduri de atribuire;

ii. Contractantul acționează în sensul realizării obiectivelor prezentate pentru Contract în ceea ce privește optimizarea folosirii resurselor necesare îndeplinirii obiectivelor Contractului.

3.4.1 Platforma software pt. orchestrarea adaptiva si autonoma a elementelor de securitate cibernetica necesare pt. desfasurarea in siguranta a activitatilor experimentale, operationale si administrative

Cantitate	Unitate de măsură	Loc de livrare	Termen de livrare solicitat	Specificații tehnice SAU cerințe funcționale minime	Specificații tehnice SAU cerințe funcționale extinse	Durata minimă garanție / termen de valabilitate
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**
1	*buc.*	*IFIN-HH ELI-NP, Str. Reactoului nr. 30, Magurele, Jud. Ilfov*	*max. 3 zile de la data semnării contractului*	*cf. Anexa 1 / p. 13*	-	-

Nota 1: În conformitate cu dispozițiile art. 156 alin. (2) – (3) din Legea nr. 98/2016, specificațiile tehnice care precizează un anumit producător, o anumită origine sau un anumit procedeu care caracterizează produsele sau serviciile furnizate de un anumit operator economic și care se referă la mărci, brevete, tipuri, la o origine sau la o producție specifică vor fi interpretate și aplicate ca fiind însoțite de sintagma „sau echivalent".

Nota 2: Orice trimitere din cuprinsul prezentei documentații de atribuire (inclusiv caietul de sarcini), prin care se face trimitere la specificații tehnice și, în ordinea priorităților, la standarde naționale care transpun standarde europene, evaluări tehnice comune, specificații tehnice comune, standarde, alte sisteme tehnice de referință stabilite de organele europene de standardizare sau, în lipsa oricăreia dintre acestea, la standardele naționale, avizele tehnice naționale sau specificațiile tehnice naționale referitoare la proiectarea, calculul și execuția lucrărilor și utilizarea produselor, se citește și se interpretează ca fiind însoțită de mențiunea „sau echivalent".

3.4.2 Livrare

Termenul de livrare este de maximum 3 zile de la data semnării contractului de catre ambele parti. Un produs este considerat livrat când toate activitățile în cadrul contractului au fost realizate și este acceptat de Autoritatea contractantă (cf. capitol 6).

Produsele vor fi livrate in format electronic la adresa de email licensemanagement.cs@eli-np.ro sau, alternativ, in format fizic la locul indicat de Autoritatea contractantă in cap. 3.4.1 si in prezentul capitol.

In cazul unei livrari fizice, Contractantul va ambala si eticheta produsele furnizate astfel incat sa previna orice dauna sau deteriorare in timpul transportului acestora catre destinatia finala. Etichetarea produselor va include o referinta catre numarul sau denumirea acestora cf. prezentului Caiet de Sarcini.

Dacă este cazul, ambalajul trebuie prevăzut astfel încât să reziste, fără limitare, manipulării accidentale, expunerii la temperaturi extreme, sării și precipitațiilor din timpul transportului și depozitării în locuri deschise. În stabilirea mărimii și greutății ambalajului Contractantul va lua în considerare, acolo unde este cazul, distanta față de destinația finală a produselor furnizate și eventuala absență a facilităților de manipulare la punctele de tranzitare.

Destinatia de livrare în format fizic este sediul Autoritatii Contractante: Institutul Național de Cercetare-Dezvoltare pentru Fizică și Inginerie Nucleară Horia Hulubei (IFIN-HH), Strada Reactorului nr. 30, Cod Postal 077125, Măgurele, județ Ilfov, Romania, cladirea ELI-NP.

3.5 Operatiuni cu titlu accesoriu

3.5.1 Instalare, punere în funcțiune, instruirea personalului

Contractantul va asigura instalarea produselor livrate pe o platforma de virtualizare hiperconvergenta (bazata pe VMware vSphere 7) a Autorității Contractante, precum si dimensionarea adecvata a resurselor alocate masinilor virtuale asociate (pentru ambele instante ale Platformei: PROD si DEV-TEST), în termenul prevazut la punctele 3.4.1 si 3.4.2 din prezentul Caiet de sarcini, respectiv de maximum 3 zile de la data semnării contractului de catre ambele parti, astfel încât acestea să fie pregătite pentru punere în funcțiune.

Punerea în funcțiune a produselor livrate, in sensul operationalizarii Platformei si integrarii funcționale a acesteia intr-un mediu informatic izolat al Autoritatii Contractante, va fi realizată de Contractant în termenul prevazut la punctele 3.4.1 si 3.4.2 din prezentul Caiet de sarcini, respectiv de maximum 3 zile de la data semnării contractului de catre ambele parti, și va consta cel puțin în următoarele:

- Instalare platforma sub forma de masina virtuala (doua instante: PROD si DEV-TEST).
- Actualizare versiunea software (incl. componente / subcomponente / module / etc.) la ultima versiune recomandata de producator pentru utilizare in medii de productie, pentru ambele instante ale platformei (PROD si DEV-TEST);
- Configurare de baza a celor doua instante (PROD si DEV-TEST):
    - Asigurare conectivitate (adrese IP, hostname, DNS, etc.)
    - Transmitere informatii jurnalizare prin Syslog la sistemul de preluare si agregare a acestor date utilizat de Autoritatea Contractanta
    - Sincronizare ceasuri / NTP
    - Control acces administrativ (i.e. la interfetele de administrare/configurare) pe baza de roluri (RBAC sau echivalent) via Microsoft Active Directory si/sau LDAP.
- Implementarea cel putin a unui scenariu de orchestrare si automatizare pe instanta DEV-TEST, in vederea validarii functionalitatii Platformei si a posibilitatilor de comunicare ale acesteia cu mijoacele specifice utilizate de Autorizatea Contractanta. Scenariul (incl. detalii privind mijloacele specifice disponibile, din motive de confidentialitate) va fi stabilit de comun acord cu personalul de specialitate al Autoritatii

Contractante dupa semnarea Contractului si va reprezenta un caz de utilizare des intalnit (de ex. gestionarea mesajelor de tip phishing sau similar).
- Hardening cel putin pentru instanta DEV-TEST, cf. documentație produs, ghiduri de bună practică, etc.

Punerea în funcțiune trebuie să fie realizată în condiții de siguranță/robustețe operațională, fără afectarea securității, performanțelor sau comportamentului rețelelor, echipamentelor și soluțiilor/platformelor la care produsele livrate sunt conectate.

Contractantul va asigura forța de muncă necesară pentru realizarea tuturor operatiunilor cu titlu accesoriu de mai sus.

Contractantul este pe deplin responsabil pentru conformitatea, calitatea și siguranța tuturor operațiunilor executate, fara a deteriora sau afecta functionarea sistemelor/echipamentelor/dotarilor existente ale Autoritatii Contractante.

Contractantul trebuie sa asigure instruirea fundamentala a personalului de specialitate al Autoritatii Contractante (min. 2 – max. 4 persoane, durata max. 1 zi) care va opera, administra si intretine Platforma, cu scopul de a asigura transferul de cunostinte necesare asigurarii unei functionari bune, robuste si sigure a acesteia, cu o asistenta minima din partea Contractantului sau independent de acesta.

De asemenea, Contractantul trebuie sa asigure instruirea de specialitate intr-o maniera independenta („self-paced", „on-demand" sau echivalent) a personalului de specialitate al Autoritatii Contractante pentru integrarea si utilizarea capabilitatilor/mecanismelor disponibile pe Platforma pentru orchestrarea adaptiva si autonoma a elementelor de securitate cibernetica, in sensul:

- Automatizarii si orchestrarii inteligente a mecanismelor tehnice multi-vendor de monitorizare si analiza a evenimentelor/indicatorilor de securitate cibernetica si de reactie tehnica la potentiale incidente cu ajutorul platformei de orchestrare de tip SOAR si a mecanismelor bazate pe tehnici de tip AI.
    - Min. 1 persoana – Max. 2 persoane
    - Curriculum de tip „SANS Institute SEC598: AI and Security Automation for Red, Blue, and Purple Teams" sau echivalent
- Integrarii mecanismelor de detectie si automatizarii actiunilor punctuale de raspuns localizat la evenimente/incidente de securitate cibernetica ce afecteaza echipamente bazate pe sisteme de operare de tip Linux, utilizand platforma de orchestrare de tip SOAR.
    - Min. 1 persoana – Max. 2 persoane
    - Curriculum de tip "SANS Institute FOR577: LINUX Incident Response and Threat Hunting" sau echivalent
- Integrarii de mijloace tehnice multi-vendor pentru asigurarea securitatii cibernetice a sistemelor/instalatiilor de control industrial si al tehnologiilor operationale (de tip ICS/OT) prin intermediul platformei de orchestrare de tip SOAR, respectiv ajustarea procedurilor („playbook-urilor") la cerintele specifice unor astfel de sisteme/instalatii/tehnilogii.
    - Min. 1 persoana – Max. 5 persoane
    - Curriculum de tip „SANS Institute ICS410: ICS/SCADA Security" sau echivalent

Tematica fiecarei instruiri si aspectele de specialitate abordate (incl. la nivel practic) in cadrul acestora trebuie ca, suplimentar fata de eventuale aspecte/functionalitati/capabilitati punctuale specifice unui anumit producator (e.g. al produselor livrate), sa trateze si sa aprofundeze (incl. la nivel practic) concepte, capabilitati, abordari si/sau metodologii general valabile (i.e. nespecifice unui anumit producator), in vederea aplicarii si utilizarii concrete a acestora in activitatile de securitate cibernetica derulate in cadrul Autoritatii Contractante, unde sunt integrate si utilizate diferite mijloace si dotari specifice provenite de la producatori diferiti.

Instruirea de specialitate a personalului de specialitate al Autoritatii Contractante (total min. 3 persoane – max. 7 persoane) va include acces nelimitat la tot suportul de curs asociat (documentatie, materiale audio/video,

laboratoare/scenarii hands-on, licente necesare pentru parcurgerea aplicativa a aspectelor abordate, etc.) pentru o perioada de cel putin 3 luni de la momentul activarii accesului la suportul de curs, respectiv cel mai tarziu la data receptiei Platformei. Instruirea va putea fi realizata de la distanta („remote") sau cu prezenta fizica („in-person", „on site" sau echivalent). In cazul in care instruirea va fi realizata cu prezenta fizica („in-person", „on site" sau echivalent), toate costurile conexe participarii la instruire a personalului de specialitate participant vor fi asigurate de către Ofertant, acestea neputând genera costuri logistice de deplasare (transport, cazare) suplimentare pentru Autoritatea Contractantă. Data prestarii activitatilor de instruire este determinata de data la care este activat accesul la suportul de curs.

3.5.2 Access la servicii de suport/asistenta tehnica pentru remediere defecte/nefunctionalitati software

Pentru produsele livrate va fi asigurat accesul la servicii de suport/asistenta tehnica de specialitate pentru remedierea eventualelor defecte / nefuncționalități software, în conformitate cu cerințele din Anexa 1.

4 Atribuțiile și responsabilitățile Părților

4.1 Atribuțiile și responsabilitățile Contractantului

a) constituirea garanției de bună execuție în cuantumul și termenul precizat în contract;

b) îndeplinirea contractului cu respectarea termenului/termenelor de livrare asumat/asumate, respectiv maximum 3 zile de la data semnării contractului de catre ambele parti;

c) furnizarea produselor ,,Platforma software pt. orchestrarea adaptiva si autonoma a elementelor de securitate cibernetica necesare pt. desfasurarea in siguranta a activitatilor experimentale, operationale si administrative", la standardele și performanțele prezentate în propunerea tehnică;

d) asigurarea tuturor resurselor necesare derulării Contractului;

e) îndeplinirea obligațiilor de livrare, cu respectarea celor mai bune practici din domeniu, a prevederilor legale și contractuale aplicabile, astfel încât să se asigure livrarea conform cerințelor contractului

f) realizarea tuturor diligențelor necesare pentru îndeplinirea obligațiilor ce-i revin la termenul/termenele asumate prin Contract;

g) notificarea de urgență a Autorității contractante cu privire la situațiile ce pot împiedica îndeplinirea la timp și cu eficiență a obligațiilor contractuale ce-i revin;

h) alocarea de personal specializat pentru relația cu responsabilul de contract nominalizat de către Autoritatea contractantă;

i) asigurarea disponibilității informațiilor și documentelor referitoare la contract cu ocazia misiunilor de control desfășurate de Autoritatea de Management/ Organismul Intermediar sau de alte structuri cu competențe în controlul și recuperarea debitelor aferente fondurilor Uniunii Europene și/sau fondurilor publice naționale aferente acestora, după caz.

j) În cazul în care, pe întreaga durată de acces la servicii de suport/asistenta tehnica pentru remediere defecte/nefunctionalitati software, respectiv până la expirarea perioadei de valabilitate a contractului, se constată, în funcționare, orice abatere, fie de la specificațiile tehnice din caietul de sarcini, fie de la performanțele asumate în propunerea tehnică, respectiv se constată specificații tehnice sau performanțe ale produsului care sunt inferioare celor anterior menționate, constatarea abaterii se realizează prin transmiterea

de către responsabilul de contract din partea Achizitorului a unei notificări către Contractant. La primirea unei astfel de notificări, Contractantul are obligația de a constata abaterea în maximum 2 zile lucratoare de la notificare și de a remedia abaterea în termen de maxim 20 zile lucratoare de la constatare, sau în cazuri justificate, într-un alt termen agreat de Achizitor, sub sancțiunile prevăzute în contract pentru neexecutarea sau executarea necorespunzătoare a obligațiilor asumate.

4.2 Atribuțiile și responsabilitățile Autorității Contractante

a) punerea la dispoziția Contractantului a tuturor informațiilor necesare derulării contractului.

b) nominalizarea persoanei responsabile cu derularea contractului implicată în relația cu contractantul pentru asigurarea unei monitorizări efective;

c) analiza riguroasă a situațiilor notificate de către contractant, ce pot împiedica îndeplinirea la timp și cu eficientă a contractului și, în situațiile justificate, aplicarea clauzelor contractuale cu privire la prelungirea termenului/modificarea contractului;

d) numirea comisiei de recepției a produsului/produselor livrate și a operatiunilor cu titlu accesoriu acestuia/acestora;

e) efectuarea plații în termenul precizat la capitolul 7 din Caietul de Sarcini;

5 Documentații ce trebuie furnizate Autorității contractante în legătură cu produsele solicitate

Documentațiile pe care Contractantul trebuie sa le livreze Autorității contractante în cadrul contractului, pana la semnarea procesului-verbal de receptie, sunt:

a. declarația/declarații sau certificat(e) de conformitate cu specificatiile tehnice din caietul de sarcini, pentru produsele livrate;

6 Recepția produselor

Recepția tuturor produselor se va efectua în termen de maxim 2 (doua) zile lucrătoare de la primirea acestora (cf. capitol 3.4.2) la locația indicată de Autoritatea contractantă. Recepția produselor se va realiza în 2 etape, în funcție de progresul contractului, respectiv:

6.1 Recepția cantitativă a produselor

Recepția cantitativă a tuturor produselor solicitate se va realiza după furnizarea acestora în cantitatea solicitată la locația indicată de Autoritatea contractantă, pe bază de proces verbal de recepție cantitativă.

6.2 Recepția calitativă a produselor

6.2.1 Recepția calitativă a tuturor produselor, precum și a operatiunilor cu titlu accesoriu conexese va realiza după verificarea conformității cu cerințele Caietului de Sarcini și a performanțelor asumate în Propunerea Tehnică, pe baza de proces-verbal de receptie calitativa.

Procesul verbal de recepție calitativă va include unul din următoarele rezultate:

a) acceptat;

b) refuzat.

7 Modalități si condiții de plata

Modalitatea de plata:

- 30% cu titlu de avans din valoarea totala a contractului în termen de de cel mult 30 de zile de la data constituirii garanției de bună execuție și a primirii facturii fiscale emisă de Furnizor, pe baza unui instrument de garantare a restituirii avansului cu valabilitate pe întreaga durata de derulare a contractului. Plata în avans va fi recuperată prin deduceri procentuale de 30% din valoarea plăților ulterioare. Daca plata in avans nu a fost rambursată în totalitate la terminarea contractului sau înainte de rezilierea contractului, ori din diverse cazuri/motive, diferența rămasă nerambursată va deveni imediat datorată și plătibilă de către furnizor Autorității contractante.

- după livrarea, instalarea, asigurarea accesului prin punerea în funcțiune și instruirea personalului: 100% din valoarea contractului(cu recuperarea avansului de 30%) se va achita în termen de 30 de zile de la comunicarea facturii de către furnizor, însoțită de procesul verbal de recepție calitativă cu mențiunea "acceptat".

Contractantul va emite facturile conform celor antemenționate, in conformitate cu legislatia aplicabilă in vigoare. Facturile vor avea menționate numărul contractului, datele de emitere și de scadență, ale facturilor respective.

8 Cadrul legal care guvernează relația dintre Autoritatea contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Ofertantul devenit Contractant are obligația de a respecta în executarea Contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii enumerate în anexa X la Directiva 2014/24, respectiv:

i. Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;

ii. Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectiva;

iii. Convenția nr. 29 a OIM privind munca forțata;

iv. Convenția nr. 105 a OIM privind abolirea muncii forțate;

v. Convenția nr. 138 a OIM privind vârsta minima de încadrare în munca;

vi. Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de munca și profesie);

vii. Convenția nr. 100 a OIM privind egalitatea remunerației;

viii. Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor;

ix. Convenția de la Viena privind protecția stratului de ozon și Protocolul său de la Montreal privind substanțele care epuizează stratul de ozon;

x. Convenția de la Basel privind controlul circulației transfrontaliere a deșeurilor periculoase și al eliminării acestora (Convenția de la Basel);

xi. Convenția de la Stockholm privind poluanții organici persistenți (Convenția de la Stockholm privind POP);

xii. Convenția de la Rotterdam privind procedura de consimțământ prealabil in cunoștința de cauza, aplicabila anumitor produși chimici periculoși și pesticide care fac obiectul comerțului internațional (UNEP/FAO) (Convenția PIC), 10 septembrie 1998, și cele trei protocoale regionale ale sale.

9 Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului

Riscuri și măsuri de gestionare a riscurilor asociate furnizorului, fără a avea un caracter exhaustiv:

Riscuri	Măsuri de gestionare
Nerespectarea termenelor de realizare din culpa furnizorului	Sancțiuni pentru neîndeplinire culpabilă sau îndeplinirea defectuoasă a obligațiilor asumate prin contract
Nerespectarea termenului de livrare din motive independente de voința furnizorului	Modificarea datei de furnizare prin act adițional, pe baza de documente justificative corespunzătoare
Neconstituirea Garanției de bună execuție	Rezolutiunea contractului
Constituirea cu întârziere a Garanției de bună execuție	Prelungire termen constituire GBE, la solicitarea justificata a Furnizorului, fara a depasi 15 zile de la data semnarii Contractului
Produsul nu este însoțit la livrare de documentele specificate prevăzute în contract și în documentele anexa la contract	Recepția produselor doar după îndeplinirea obligațiilor contractuale privind furnizarea documentelor care însoțesc produsele
Dificultăți în gestionarea relației furnizorului cu subcontractanții (dacă este cazul)	Preluarea de către furnizor a parții/părților din contract aferente activității de subcontractare sau înlocuirea subcontractantului cu un nou subcontractant în condițiile prevăzute în contract
Nerespectarea prevederilor angajamentului ferm de susținere (daca este cazul)	Dreptul Achizitorului la despăgubire și/sau pretenție la daune
Nerespectarea prevederilor legale referitoare la conflictul de interese	Rezolutiunea de drept a contractului si sancțiuni contractuale
Furnizarea de produse neconforme/ Schimbarea specificațiilor contractuale sub nivelul standardelor impuse prin documentația de atribuire/ofertă	Realizarea recepției produselor cu asigurarea unei verificări riguroase a conformității specificațiilor tehnice ale produselor livrate în raport cu cerințele Caietului de sarcini și Ofertei depusă, parte din contract
Existența unor neconcordanțe între Propunerea tehnică și specificațiile Caietului de sarcini	Precizarea in contract a priorității specificaților din documentație față de Propunerea tehnică, cu excepția cazului în care parametrii tehnici din Propunerea tehnică sunt superiori celor solicitați, caz în care vor prevala prevederile din Propunerea tehnică

Riscuri și măsuri de gestionare a riscurilor asociate Achizitorului, fără a avea un caracter exhaustiv:

Riscuri	Măsuri de gestionare
Întârzieri în efectuarea plății	Sancțiuni pentru neîndeplinirea obligației de plată culpabilă sau îndeplinirea defectuoasă a obligațiilor asumate prin contract
Monitorizarea neadecvata a Contractului, respectiv a termenelor contractuale	Nominalizarea de către Achizitor a unui responsabil cu urmărirea contractului
Apariția necesității modificării unor elemente ale contractului	Prevederea de clauze contractuale care să limiteze modificarea contractului în strictă conformitate cu dispozițiile art. 221 din Legea nr. 98/2016.

Responsabil de contract,

Responsabil și Arhitect Securitate Cibernetica ELI-NP, Ing. Alexandru Vlad ȘERBĂNESCU

Șef Compartiment Securitate Cibernetica ELI-NP

Anexa 1 Platforma software pt. orchestrarea adaptiva si autonoma a elementelor de securitate cibernetica necesare pt. desfasurarea in siguranta a activitatilor experimentale, operationale si administrative

Cod	Caracteristica	Specificatie solicitata
Nr. buc.		1
Termen de livrare		max. 3 de zile de la data semnării contractului de catre ambele parti
Tip produs		Platforma software pt. orchestrarea adaptiva si autonoma a elementelor de securitate cibernetica necesare pt. desfasurarea in siguranta a activitatilor experimentale, operationale si administrative, de tip Fortinet FortiSOAR sau echivalent.
PSC	**Caracteristici specifice produs**	
.1	Functii principale: Orchestrare	Orchestrare: Reprezintă stratul de integrare și coordonare între multiple sisteme / echipamente / solutii de securitate cibernetica, unificand fluxuri de lucru prin conectarea acestor elemente individuale disparate. Referitor la funcția de Orchestrare a Platformei, aceasta trebuie să asigure/permită/includă/etc. cel puțin următoarele: 1. Centralizarea operațiunilor de securitate IT/OT prin integrarea bidirectionala, cu ajutorul unor conectori predefiniti (sau echivalent), cu produse de securitate multi-vendor. 2. Posibilitate de creare de conectori noi prin intermediul unei interefete grafice ghidate (de tip GUI wizard sau echivalent), precum si programatic de tip SDK, pentru integrarea facilă cu sisteme personalizate sau pentru care nu exista conectori predefiniti. 3. Preluarea si procesarea de informatii/alerte din orice solutie sau echipament de securitate cibernetica sau de tip IT/OT care permite preluarea programatica a acestor informatii/alerte (de ex. prin interfete de tip API). 4. Primirea si procesarea de mesaje prin protocolul Syslog (TCP și UDP) de la orice solutie sau echipament de securitate cibernetica sau de tip IT/OT care utilizeaza acest protocol. 5. Procedurarea interactiunii cu echipamente de securitate cibernetica sau de tip IT/OT prin interogări si comenzi/acțiuni (sau echivalent) 6. Librarie de soluții pentru cazuri de utilizare tipice din domeniul securitatii cibernetice (de tip „Solution Packs" sau echivalent), ce includ conectori, interogari, acțiuni/comenzi și fluxuri complete de lucru de tip „playbook" / „runbook" (sau echivalent) 7. Importul și procesarea fluxurilor de lucru în format JSON (JavaScript Object Notation) și BPMN (Business Process Model and Notation) 8. Posibilitate de creare de interfete sinoptice (de tip „dashboard" sau echivalent) complet personalizate in cadrul interfetei grafice cu utilizatorul. 9. Integrare cu sisteme de ticketing și comunicații. 10. Suport pentru segmente de rețea izolate prin utilizarea unor componente de tip agent local (sau echivalent) in cadrul fiecarui astfel de segment de retea, componente care asigură execuția de acțiuni asociate conectorilor și colectarea de date la nivel local, comunicând securizat si criptat cu platforma centrala intr-o maniera de tip outbound (exclusiv de la componenta locala la cea centrala), fără de a deschide porturi/cai de access de tip inbound (de la componenta centrala la cea locala). 11. Suport pentru utilizarea unei soluții de tip „Credential Vault" (sau echivalent) externe Platformei pentru accesarea și utilizarea securizata a datelor de acces (e.g. parole, chei API, token-uri, etc.) pentru interacțiunea cu sistemele

Cod	Caracteristica	Specificatie solicitata
		/ echipamentele / solutiile de securitate cibernetica orchestrate de Platforma.
.2	Functii principale: Automatizare	Automatizare: Reprezintă execuția automată a diferitelor interogari si acțiuni/comenzi definite în cadrul unui flux de lucru, eliminand/reducand efortul manual prin rularea unor procese bine definite. Referitor la funcția de Automatizare a Platformei, aceasta trebuie să asigure/permită/includă/etc. cel puțin următoarele: 1. Automatizare a task-urilor repetitive prin „playbook-uri" / „runbook-uri" (sau echivalent), cu suport pentru blocuri/module reutilizabile in cadrul mai multor „playbook-uri" / „runbook-uri". 2. Definirea și executarea de „playbook-uri" / „runbook-uri" (sau echivalent) utilizand o interfață grafică de tip drag-and-drop (fără necesitatea cunoașterii unui limbaj de programare). 3. Posibilitatea de a utiliza cel putin urmatoarele tipuri de elemente in cadrul „playbook" / „runbook": decizii logice între acțiuni, aprobări (incl. explicite de catre un factor uman), introducere manuală de date, executare cod (cel putin in limbajul Python), apelarea altor „playbook-uri" / „runbook-uri", generarea de notificări prin platforme de comunicatie. 4. Modul de simulare și testare a „playbook-urilor" / „runbook-urilor" înainte de activarea/implementarea în mediu productiv (sau echivalent) 5. Set extins de „playbook-uri" / „runbook-uri" (sau echivalent) predefinite pentru scenarii comune de investigație, remediere și răspuns 6. Mecanisme de tip CI/CD (Continuous Integration / Continuous Deployment) pentru versionarea, realizarea de snapshot-uri, revenirea rapida la stări anterioare ale unui „playbook" / „runbook" (rollback), export si import 7. Motor de generare recomandări bazat pe tehnici de tip Machine Learning, cel putin pentru: identificarea si gruparea inteligentă a alertelor si incidentelor, recomandarea de valori pentru completarea unor campuri de date relevante, recomandarea executiei unor „playbook" / „runbook" sau acțiuni (sau echivalent) 8. Functie de asistare bazat pe tehnici de tip Inteligenta Artificiala pentru ghidarea, simplificarea și automatizarea investigațiilor, acțiunilor de răspuns și a construirii de „playbook-uri" / „runbook-uri" (sau echivalent) 9. Posibilitate de a configura prioritatea de execuție pentru fiecare „playbook" / „runbook" în parte, pentru a controla ordinea în care acestea sunt executate atunci când există mai multe în coada de așteptare, pe cel putin trei niveluri (prioritate mică/medie/mare sau echivalent). 10. Mecanisme de îmbogățire automată cu informații contextuale a informatiilor/alertelor primite (de tip „Enrichment" sau echivalent), cel putin: estimare localizare geografică a unui IP (de tip GeoIP Lookup sau echivalent), reputație URL-uri si adrese IP (de tip Threat Intelligence sau echivalent), informații despre conturi de utilizatori (de tip User Context Enrichment sau ecchivalent) si dispozitive (de tip Asset Context Enrichment sau echivalent).* *NOTA: Acest punct al cerintei se refera exclusiv la prezenta/disponibilitatea unor astfel de mecanisme, nu la accesul la sursele de date necesare ca aceste mecanisme sa functioneze. Licentierea / activarea / echivalent in configuratia livrata a accestului la astfel de surse nu face obiectul acestei cerinte. 11. Funcționalitate de clasificare automată a mesajelor email pentru identificarea tentativelor de phishing pe bază de Machine Learning (sau echivalent): analiză automată a mesajelor de tip email pentru identificarea

Cod	Caracteristica	Specificatie solicitata
		tentativelor de phishing, utilizând modele pre-antrenate sau pe baza antrenării pe date locale, care furnizează recomandări de clasificare (phishing/non-phishing) afișate împreună cu scor de încredere în panoul de recomandări (sau echivalent), cu posibilitatea de a alege câmpurile analizate (cel puțin expeditor, subiect, corp mesaj) și cu integrare în mecanismele de recomandări utilizate pentru accelerarea triajului.
.3	Functii principale: Raspuns	Raspuns: Reprezintă componenta activa si executiva, constand în acțiunile tactice și imediate de control / diminuare / remediere a amenințărilor, evenimentelor sau incidentelor de securitate cibernetica Referitor la funcția de Răspuns a Platformei, aceasta trebuie să asigure/permită/includă/etc. cel puțin următoarele: 1. Trierea, îmbogățirea (enrichment) și evaluarea automată a alertelor din solutiile/echipamentele de securitate cibernetica integrate, pentru a facilita clasificarea, evaluarea și acțiunea rapidă asupra alertelor și luarea de decizii bazate pe un context bogat și actualizat. 2. Executarea automată de acțiuni de răspuns și remediere (e.g. izolare, reconfigurare reguli/filtre/politici, carantinare, scanare, etc.) 3. Gestionarea automată și închiderea alertelor de rutină/recurente 4. Maparea automată a alertelor pe framework-ul global MITRE ATT&CK (incl. MITRE ATT&CK for ICS), asociind fiecare alertă cu tacticile, tehnicile și sub-tehnicile folosite pentru a oferi utilizatorilor un context standardizat despre natura evenimentului. 5. Notificări prin canale multiple de comunicatie, cel putin: email, platforme externe de colaborare (de tip WebEx/Zoom/Teams sau echivalent), sisteme externe de ticketing, notificari in cadrul platformei 6. Include mecanisme automate și manuale pentru accelerarea distingerii între alerte legitime (care necesită acțiuni de răspuns) și alerte fals pozitive (care pot fi închise fără a întreprinde vreo acțiune), reducând astfel volumul activității manuale și reducând timpul de răspuns la amenințările reale. 7. Modul dedicat pentru managementul colaborativ al incidentelor critice (de tip „War Room" sau echivalent), reprezentand un spațiu de lucru colaborativ securizat pentru cei implicati in gestionarea incidentului, cel puțin cu următoarle funcții: acces restrictionat pe bază de invitație, gestionare task-uri/sarcini de lucru, comunicații private, raportare detaliată, jurnalizare actiuni
.4	Functii principale: Managementul incidentelor	Managementul incidentelor: Reprezinta procesul/cadrul de gestionare a întregului ciclu de viață a unii incident de securitate cibernetica Referitor la funcția Platformei de Management al Incidentelor, aceasta trebuie să asigure/permită/includă/etc. cel puțin următoarele: 1. Gestionarea centralizată a incidentelor și alertelor de securitate, atât pentru medii IT (Information Technology) cât și OT (Operational Technology/Industrial Control Systems), eliminând nevoia de a interacționa cu echipamente/soluții disparate și fragmentate. 2. Modul complet de tip „case/incident management" (sau echivalent) care permite organizarea, atribuirea (incl. in mod automat), urmarirea și coordonarea tuturor sarcinilor și activităților asociate investigării și rezolvării incidentelor de securitate, asigurând eficiență operațională și respectarea SLA-urilor (daca acestea din urmă sunt definite în cadruul Platformei)

Cod	Caracteristica	Specificatie solicitata
		3. Gruparea inteligentă a alertelor în incidente pe bază de algoritmi de tip Machine Learning și criterii configurabile sau specifice (e.g. aceeași adresă IP sursă/destinație, atribute comune, etc.), facilitând reducerea complexității operaționale și asigurând o structurare coerentă a incidentelor de investigat. 4. Reprezintă o interfață unificată pentru managementul tichetelor, eliminând/reducând semnificativ necesitatea utilizatorului de a comuta între multiple platforme. 5. Generare de reprezentari grafice de tip graf (sau echivalent) pentru afisarea si evidentierea relațiilor/interconexiunilor între diferite elemente dintr-o investigație de securitate (e.g. alerte, incidente, indicatori, active, utilizatori, vulnerabilități, etc.), facilitand o vizualizare si intelegere rapida a modului in care sunt legate componentele unui incident și a secvenței de compromitere. 6. Jurnalizarea si vizualizarea acțiunilor altor utilizatori in contextul unui incident. 7. Posibilitate de colaborare între utilizatorii Platformei, cu evidențierea modificărilor/actualizărilor aduse diferitelor elemente („playbook-uri" / „runbook-uri", alerte, incidente, sarcini, etc.) și realizarea de comentarii/observații. 8. Inventarierea activelor digitale prin conectarea la sisteme externe de tip CMDB (Configuration Management Database, sau echivalent), respectiv agregarea si vizualizarea informatiilor asociate acestora in contextul unui incident. 9. Posibilitate de atribuie automata a incidentelor și sarcinilor la utilizatorii potriviți pe bază de prioritate sau număr de sarcini deja aflate în coada de lucru a acestora (backlog), eliminând alocarea manuală și asigurând o distribuție echilibrată a încărcării. 10. Ofera atat interfete sinoptice și rapoarte preconfigurate, cat si posibilitatea crearii unora personalizate, precum si posibilitatea de generare/actualizare automată (programată) a acestor rapoarte.
.5	Compatibilitate cu tehnologii de securitate cibernetica	Platforma trebuie sa ofere mecanisme native de conectare si integrare (de tip „connector" sau echivalent) cel putin pentru colectarea de date si executarea de actiuni cf. celor enumerate mai jos (sau echivalent), si cel putin pentru urmatoarele platforme/solutii/echipamente utilizate de Autoritatea Contractanta: a. Firewall-uri: Fortinet FortiGate (incl. suport pt. operare in mod multi-VDOM, in maniera Profile-based sau Policy-based) 1. Block IP Address, Unblock IP Address, Get Blocked IP Addresses 2. Block Application, Unblock Application, Get Blocked Applications 3. Block URL, Unblock URL, Get Blocked URLs 4. Get Addresses, Create Address, Update Address, Delete Address 5. Get Address Groups, Create Address Group, Update Address Group, Delete Address Group 6. Get Services , Create Service, Update Service, Delete Service 7. Get Service Groups, Create Service Group, Update Service Group, Delete Service Group 8. Update Policy 9. Execute Command

Cod	Caracteristica	Specificatie solicitata
		b. Platforma management centralizat firewall-uri: Fortinet FortiManager (incl. suport pt. operare in maniera multi-ADOM, cu multiple VDOM-uri per ADOM, utilizand modul de lucru „workspace" sau „workflow"): 1. Cu efect la nivel de ADOM individual i. Get Blocked IP Addresses, Block IP Address, Unblock IP Address ii. Install Policy, Re-install Policy, Get Installation Policy Package Status iii. Create Address, Get Addresses List, Update Address, Delete Address iv. Create Address Group, Get Address Groups List, Update Address Group, Delete Address Group v. Create Custom Service, Get Custom Services List, Update Custom Service, Delete Custom Service vi. Get Service Categories List, Create Service Group, Get Service Groups List, Update Service Group, Delete Service Group vii. Get Blocked URLs, Block URL, Unblock URL 2. Cu efect la nivelul tuturor ADOM-urilor/GLOBAL i. Get Blocked IP Addresses, Block IP Address, Unblock IP Address ii. Create Address, Get Addresses List, Update Address, Delete Address iii. Create Address Group, Get Address Groups List, Update Address Group, Delete Address Group iv. Create Custom Service, Get Custom Services List, Update Custom Service, Delete Custom Service v. Get Service Categories List, Create Service Group, Get Service Groups List, Update Service Group, Delete Service Group vi. Get Blocked URLs, Block URL, Unblock URL 3. Assign Global Policy Package 4. Interogare FortiManager ca baza de date locala FortiGuard Distribution Server / FDS pentru serviciile cu acces pe baza de abonament FortiGuard Distribution Network / FDN: i. WebFilter URL Lookup (categorisire URL-uri) ii. AntiSpam Lookup (validarea adrese IP drept surse cunoscuta de mesajelor e-mail de tip „spam") c. Platforme de management centralizat al identitatii, autentificare multi-factor si de tip Single Sign-On: Fortinet FortiAuthenticator 1. Get Local User List, Get Specific Local User, Update Local User Status (Activate/Deactivate) 2. Get LDAP User List, Get Specific LDAP User, Update LDAP User Status (Activate/Deactivate)

Cod	Caracteristica	Specificatie solicitata
		d. Platforma pentru centralizare, stocare si analiza date jurnalizare: cel putin Fortinet FortiAnalyzer (incl. suport pt. operare in maniera multi-ADOM, cu multiple VDOM-uri per ADOM) 1. Get Incident, Get Incident for Multiple ADOMs, Count Incidents for Multiple ADOMs, Update Incident, Get Events For Incident, Get Incident Assets, Add Incident Attachment, Get Incident Attachments, Update Incident Attachment 2. Get Event, Get Event for Multiple ADOMs, Count Events for Multiple ADOMs, Get Event Logs 3. Get Outbreak Alerts Summary 4. Run Report, Get Report File, Get Executed Report List 5. Get Endpoint Information 6. Execute an API Request e. Software monitorizare stare sisteme informatice: PRTG 1. Get Sensor Status, Pause Sensor, Resume Sensor f. Platforma ticketing: Request Tracker 1. Create Ticket, Comment Ticket, Get Ticket Properties, Update Ticket Suplimentar, platforma trebuie sa ofere mecanisme native de conectare si integrare (de tip „connector" sau echivalent) cel putin pentru colectarea de date si/sau executarea de actiuni cel putin pentru urmatoarele tipuri de platforme/solutii/echipamente/protocoale/etc. (sau echivalent, dupa caz): g. Platforme partajare informatii despre amenintari cibernetice: MISP h. Soluții de tip endpoint security i. Soluții de tip email security j. Platforme de tip SIEM k. Solutie configurare centralizata sisteme Microsoft: Microsoft SCCM l. Baze de date: MySQL, PostreSQL, MongoDB, Miscrosoft SQL m. Platforme de analiză și vizualizare log-uri: Graylog, Elastic Search n. Servere de fisiere, cel putin prin protocoalele SMB/SAMBA si SCP o. Servere de email, cel putin prin protocoalele IMAP si SMTP p. Protocolul SSH, pentru executarea de comenzi pe alte sisteme
.6	Compatibilitate infrastructura	- Platforma trebuie sa poata fi instalata si sa ruleze ca o masina virtuala pe platforma de virtualizare hiperconvergenta VMware (vSphere versiunile 7 si 8) utilizata de Autoritatea Contractanta. - Platforma trebuie sa poata importa si utiliza infrastructuri de certificate digitale de tip root („Root CA certificate" sau echivalent) si intermediare („Intermediate CA certificate" sau echivalent). - Platforma trebuie sa poata fi accesata si utilizata prin intermediul unui reverse proxy.

Cod	Caracteristica	Specificatie solicitata
		- Pentru platforma trebuie furnizat un inventar al tuturor fluxurilor de comunicatie (protocol, port si element/componenta sursa/destinatie) necesare functionarii individuale.
.7	Utilizare	Platforma trebuie sa ofere o interfata grafica pentru utilizatori, care sa includa fluxuri de utilizare ghidate (de tip „wizzard" sau echivalent) pentru facilitarea și accelerarea proceselor de utilizare/configurare, respectiv pentru reducerea complexității în utilizare și a riscului de eroare umană, incluzând cel puțin: - Flux de utilizare ghidat pentru configurarea colectării datelor din surse externe (de tip „Data Ingestion Wizard" sau echivalent), inclusiv maparea datelor colectate cu atribute locale și programarea colectarii datelor; - Flux de utilizare ghidat pentru export-ul și import-ul de configurații (e.g. module, interfete sinoptice / dashboard-uri, „playbook-uri"/„runbook-uri", etc.) - Flux de utilizare ghidat pentru crearea și configurarea conectorilor noi.
.8	Administrare	Referitor la administrarea Platformei, aceasta trebuie să asigure/permită/includă/etc. cel puțin următoarele: - Administrare prin interfata web si de tip linie de comanda (SSH) - Functie de transmitere a informatiilor de jurnalizare (de tip „log forwarding" sau echivalent) prin protocolul Syslog. - Utilizatori si profiluri de utilizatori cu drepturi de acces configurabile (incl. la nivel de „playbook", „runbook" sau echivalent), de tip „Role Based Access Control" sau echivalent. Unui utilizator trebuie sa ii poata fi alocate unul sau mai multe roluri. - Permite autentificare/autorizare prin LDAP si RADIUS; - Permite autentificarea multi-factor si autorizarea de tip SSO/SAML cu „Platforma de management centralizat al identitatii, autentificare multi-factor si de tip Single Sign-On" utilizata de Autoritatea Contractanta (Fortinet FortiAuthenticator). - Permite integrari/automatizari/echivalent prin interfata de tip API sau echivalent
.9	Functionare in regim de cluster (sau echivalent)	Produsul ofertat trebuie sa poata oferi, printr-o licentiere suplimentara ulterioara, posibilitatea de a functiona atat intr-o configuratie de tip activ-activ (incl. "load-balancing", pentru scalabilite d.p.d.v. performante oferite) sau activ-pasiv (pentru asigurarea unui nivel ridicat de redundanta), sau echivalent. Functionarea in oricare dintre aceste moduri trebuie sa fie posibila fara reconfigurarea nodului/instantei initiale (de ex. fara externalizarea bazei de date, etc.) sau echivalent. Licentierea / activarea / echivalent in configuratia livrata a acestor functii nu se solicita prin prezentul Caiet de Sarcini si nu face obiectul prezentei proceduri de atribuire. Licentierea / activarea / echivalent in configuratia livrata a acestor functii trebuie sa poata fi realizata, intr-o maniera perpetua (cf. pct. LIC.1) cel putin pana la momentul expirarii „Accessului la servicii de suport/asistenta tehnica pentru remediere defecte/nefunctionalitati software" (cf. pct. TSS.2).

Cod	Caracteristica	Specificatie solicitata
LIC	**Licentiere**	
.1	Modalitate/tip licentiere mediu PRODUCTIV si mediu DEZVOLTARE-TESTARE	- Licentierea va include doua medii / instante separate ale Platformei: o Pentru mediul productiv, operational: o (1) instanta o Pentru mediul de dezvoltare si testare: o (1) instanta - Licentierea va fi perpetua pentru toate functiile Platformei in configuratia livrata, in ambele medii / pentru ambele instante, fara incetarea functionarii acestora dupa expirarea perioadei de acces la serviciile de suport/asistenta tehnica. Dupa expirarea accesului la aceste servicii, Platforma trebuie sa continue sa functioneze in configuratia ofertata. - Fara dependenta operationala de componente, resurse sau servicii externe sau de tip "cloud", in ambele medii / pentru ambele instante.
.2	Capacitate licențiată mediu PRODUCTIV	- Platforma va permite utilizarea concomitentă de către cel puțin 5 (cinci) utilizatori. Numarul de utilizatori simultani trebuie sa poate fi crescut, printr-o licentiere suplimentara ulterioara (dacă este necesară), la un total de cel putin 10 (zece) utilizatori concomitenti fara modificarea modalitatii/tipului de licentiere de la pct. LIC.1 (licentierea / activarea / echivalent acestor utilizatori simultani suplimentari nu se solicita prin prezentul Caiet de Sarcini si nu face obiectul prezentei proceduri de atribuire). - Platforma va permite definirea unui numar de cel puțin 100 (o sută) de utilizatori. - Platforma va permite, d.p.d.v. licentiere, crearea unui numar neliminat de „playbook-uri", „runbook-uri" sau echivalent. Licentierea nu va limita numarul de actiuni/operatiuni individuale continute in cadrul fiecarui „playbook", „runbook" sau echivalent. - Platforma va permite, d.p.d.v. licentiere, executarea unui numar neliminat atat de „playbook-uri", „runbook-uri" sau echivalent, cat si de actiuni/operatiuni individuale continute in cadrul acestora.
.3	Capacitate licențiată mediu DEZVOLTARE-TESTARE	- Platforma va permite utilizarea concomitentă de către cel puțin 2 (doi) utilizatori. - Platforma va permite, d.p.d.v. licentiere, crearea unui numar neliminat de „playbook-uri", „runbook-uri" sau echivalent. Licentierea nu va limita numarul de actiuni/operatiuni individuale continute in cadrul fiecarui „playbook", „runbook" sau echivalent. - Platforma va permite, d.p.d.v. licentiere, executarea unui numar de cel putin 1000 (o mie) de actiuni/operatiuni individuale pe zi in cadrul „playbook-urilor", „runbook-urilor" supuse dezvoltarii si testarii (sau echivalent).
TSS	**Acces la servicii de suport/asistenta tehnica pentru remediere defecte/nefunctionalitati software**	
.1	Acces	Accesul va include cel putin urmatoarele elemente (putand fi realizate si prin servicii de suport/asistenta tehnica incluse in oferta standard a producatorului, acolo unde sunt comercializate ca atare / dupa caz): - Posibilitatea de raportare a defectelor/nefunctionalitatilor/incidentelor functionale prin portal web, sistem de chat on-line, e-mail sau telefon, respectiv de transmitere a solicitarilor referitoare la probleme tehnice survenite in functionare (e.g. deschidere de tichete in caz de bug-uri sau alte probleme similare, etc.); - Acces la servicii suport/asistenta tehnica (cel putin de tip „24x7" / 24 ore pe zi, 7 zile pe saptamana) prin personal calificat pentru identificarea si

Cod	Caracteristica	Specificatie solicitata
		remedierea defectiunilor de functionare (incl. eventualele interventii cu personal calificat, la nevoie), de tip "next business day" (preluare si raspuns initial) sau echivalent/superior; - Acces la servicii suport/asistenta tehnica specializata (de tipul „Best Practice Service" sau echivalent) care să acopere remedierea problemelor in functionare/nefunctionalitatilor la integrarea Platformei cu sisteme/echipamente/solutii terte de securitate cibernetica suportate, furnizarea de elemente de cod și de configurație pentru remediere, precum și bune practici pentru evitarea reaparitiei de probleme/nefunctionalitati similare. - Acces la elementele software asociate (incl. versiuni actualizate care contin patch-uri, etc.) strict necesare exclusiv in vederea remedierii, precum si la documentatia tehnica si baza de cunostinte („knowledge base" sau echivalent) asociate.
.2	Durata acces	Cel putin 3 ani de la data semnării procesului verbal de recepție calitativă acceptat.