UNIUNEA EUROPEANA

GUVERNUL ROMÂNIEI

Programul Operaţional Competitivitate 2014–2020
– co-finanţat din Fondul European de Dezvoltare Regională –
Axa Prioritară 2 – „ Tehnologia informaţiei şi comunicaţiilor (TIC) pentru o economie digitală competitivă"

CAIET DE SARCINI

– Achiziție sistem RO-SAT –

CUPRINS

1. Obiectul contractului

Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO este beneficiarul unei finanțări nerambursabile pentru implementarea proiectului "Sistem de alertă timpurie și informare în timp real - RO-SAT", cod MySMIS2014+ 130277, în baza contractului de finanțare nr. 2/2.3.2/20.09.2019. Proiectul este cofinanțat din Fondul European de Dezvoltare Regională prin Programul Operațional Competitivitate 2014-2020, Axa Prioritară 2, Acțiunea 2.3.2 – Asigurarea securității cibernetice a sistemelor TIC și a rețelelor informatice.

Proiectul finanțat prin POC are ca obiectiv general creșterea capacității operaționale a CERT-RO în vederea asigurării capabilităților naționale de prevenire, identificare, analiză și reacție la incidentele de securitate cibernetică. Prin implementarea RO-SAT se urmărește creșterea nivelului de securitate a spațiului cibernetic național (instituții publice, companii private, utilizatori individuali), precum și creșterea capacității de răspuns la incidente de securitate cibernetică a CERT-RO. Îmbunătățirea stării de securitate prin cunoașterea, prevenirea și contracararea vulnerabilităților, riscurilor și amenințărilor la adresa securității cibernetice a organizațiilor din România este stipulată ca obiectiv al Strategiei Naționale de Securitate Cibernetică.

Contractele care fac obiectul prezentei proceduri au ca obiect **achiziția de soluții și servicii** pentru crearea sistemului RO-SAT.

Vor fi achiziționate următoarele:

I. Lot 1 – Soluții și servicii sistem RO-SAT
   a. Platformă RO-SAT
   b. SIEM
   c. Soluție knowledge management

2. Cadrul legal care guvernează relația dintre autoritatea contractantă și furnizor

Furnizorul are obligația de a respecta în executarea contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii Europene, 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.

Alte acte normative care guvernează relația dintre furnizor și autoritatea contractantă sunt:

- Legea nr. 98/2016 privind achizițiile publice, cu modificările și completările ulterioare;
- H.G. nr. 395/2016,cu modificările și completările ulterioare;
- Legea nr. 101/2016,cu modificările și completările ulterioare;
- Ordinul ANAP nr. 1068/2018 privind ghidul achizițiilor publice verzi.

În cazul în care pe parcursul derulării contractului se modifică legislația, furnizorul se obligă să se alinieze noilor reglementări tehnice și/sau legale.

3. Caracteristicile produselor/livrabilelor

Specificațiile tehnice ale produselor care fac obiectul contractelor de achiziție publică sunt menționate în prezentul caiet de sarcini. Acestea sunt minimale și obligatorii.

Nerespectarea condițiilor prevăzute în prezentul caiet de sarcini care reprezintă Anexă a contractelor, atrage răspunderea Prestatorului potrivit clauzelor contractelor dintre acesta și Autoritatea Contractantă, în conformitate cu prevederile legale, mergând până la rezilierea acestora.

4. Condiții și termene de livrare

4.1. Locul de livrare al produselor

Operatorii economici desemnați câștigători vor livra soluțiile și vor presta serviciile de integrare în locația indicată de AC în termen de 180 de zile calendaristice, de la data semnării contractului.

Produsele vor fi livrate cantitativ și calitativ în locația indicată de către autoritatea contractantă. Fiecare produs va fi însoțit de toate subansamblele/părțile componente necesare punerii și menținerii în funcțiune.

Produsele vor fi ambalate și etichetate astfel încât să se prevină orice daună sau deteriorare în timpul transportului acestora către destinația stabilită.

Ambalajul produselor trebuie să reziste manipulării accidentale, expunerii la temperaturi extreme și precipitațiilor din timpul transportului și depozitării în locuri deschise.

Toate materialele de ambalare, precum și toate materialele necesare protecției coletelor (folii de protecție, cutii etc.) vor fi preluate de către furnizor după instalarea și testarea soluțiilor cu excepția acelor ambalaje care sunt necesare a fi prezentate în vederea acordării garanției.

Transportul și toate costurile asociate sunt în sarcina exclusivă a furnizorului. Furnizorul va asigura produsele împotriva furtului, pierderii sau deteriorării intervenite pe parcursul transportului și depozitării.

Destinația de livrare este str. Italiană nr.22, et.4, sector 2, București. Livrările și instalările soluțiilor vor fi efectuate eșalonat conform unui grafic de livrare care va fi agreat de furnizor împreună cu autoritatea contractantă. Verificarea îndeplinirii obligațiilor contractuale de către autoritatea contractantă și evaluarea stadiului activităților, în sensul respectării termenelor stabilite pentru livrarea produselor care fac obiectul contractului, se face prin raportare la conținutul graficului de livrare acceptat. În cazul în care, pe parcursul duratei contractului, autoritatea contractantă constată că livrarea produselor nu respectă eșalonarea astfel cum este stabilită prin graficul de livrare, autoritatea contractantă are obligația de a solicita furnizorului să prezinte graficul actualizat, iar furnizorul are obligația de a prezenta graficul revizuit, în vederea finalizării livrării la data stabilită în contract.

Furnizorul este responsabil pentru livrarea în termenul agreat al produselor și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca nici un motiv de întârziere sau costuri suplimentare.

4.2. Valabilitate și actualizări

Acolo unde este cazul, sunt detaliate valabilitatea suportului și a actualizărilor software ale soluțiilor.

4.3. Garanție și suport

Toate produsele trebuie să fie acoperite de garanție pentru cel puțin perioada solicitată de autoritatea contractantă, conform cerințelor din prezentul caiet de sarcini.

Sistemul RO-SAT va fi instalat pe o infrastructură hardware și software ce va fi pusă la dispoziție de autoritatea contractantă. În cazul în care soluțiile ofertate conțin componente hardware garanția va trebui să acopere toate costurile rezultate din remedierea defectelor în perioada de garanție, inclusiv, dar fără a se limita la:

i. demontare, inclusiv închirierea de unelte speciale necesare pe durata intervenției;

ii. ambalaje, inclusiv furnizarea de material protector pentru transport (carton, cutii, lăzi etc.);

iii. repararea tuturor componentelor defecte sau furnizarea unor noi componente;

iv. înlocuirea părților defecte;

v. despachetarea, inclusiv curățarea spațiilor unde se efectuează intervenția;

vi. instalarea în starea inițială;

vii. testarea pentru a asigura funcționarea corectă;

viii. repunerea în funcțiune.

Soluțiile software și eventualele componente hardware oferite vor fi de ultimă generație, iar ofertantul va pune la dispoziție toate componentele hardware și licențele software necesare menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice protejate prin prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora. Nu vor fi acceptate soluții hardware sau software care la momentul depunerii ofertei sunt declarate End of Live (EoL) sau End of Sale (EoS). Ofertantul va trebui să furnizeze informații privind termenele estimate pentru EoL și EoS pentru fiecare soluție ofertată.

Furnizorul trebuie să asigure funcționarea produselor software ofertate de la data acceptanței finale pentru o durată de minim 5 ani cu suport în regim 24x7.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate soluțiilor ofertate și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

Sistemul RO-SAT, respectiv componentele software integrate în acesta, cu excepția serviciilor, precum și a soluțiilor pentru care se menționează altfel în prezentul caiet de sarcini, trebuie să poată funcționa și după expirarea licenței/licențelor, astfel încât aceasta să permită atât administrarea cât și utilizarea, folosind actualizările de securitate și de componente descărcate înainte de expirarea licenței. În cadrul ofertei tehnice se vor furniza toate detaliile necesare demonstrării realizării acestei cerințe.

NOTĂ: Toate componentele sistemului RO-SAT, cu excepția serviciilor, se vor instala on prem. Acestea vor rula pe echipamente ce vor fi puse la dispoziție de beneficiar.

4.4. Suport tehnic/SLA

Furnizorul va asigura suportul tehnic conform cerințelor incluse în caietul de sarcini. De asemenea, pentru tot sistemul se solicită cel puțin următoarele:

- Un sistem de ticketing în vederea gestionării incidentelor apărute în exploatarea sistemului;
- Relaționarea cu centrele de suport ale producătorilor soluțiilor achiziționate prin proiect;
- Servicii de suport tehnic periodic asupra soluțiilor de securitate achiziționate prin proiect ce pot cuprinde cel puțin upgrade de firmware (cel puțin de două ori pe an);
- La cerere, servicii de reconfigurare a politicilor aferente soluțiilor de securitate achiziționate prin proiect;

- La cerere, suport pentru reconfigurarea soluțiilor hardware/software livrate.
- În funcție de tipul incidentelor, furnizorul va asigura următorii timpi de răspuns și de remediere:

Componentă a sistemului	Incident **URGENT/CRITIC**			Incident **MAJOR**			Incident **MINOR**		
	Timp de răspuns	Timp remediere provizorie / temporară	Timp de remediere*	Timp de răspuns	Timp remediere provizorie / temporară	Timp de remediere*	Timp de răspuns	Timp remediere provizorie / temporară	Timp de remediere*
Hardware	4 ore	24 ore	7 zile	8 ore	48 ore	14 zile	24 ore	5 zile	30 zile
Software	4 ore	24 ore	5 zile	8 ore	48 ore	12 zile	24 ore	5 zile	30 zile

** În cazul în care software-ul de bază, aplicațiile sau tehnologiile folosite necesită corectarea unui bug și/sau construcția unui patch de la producător, timpul de remediere se va modifica cu timpul necesar producătorului să construiască patch-ul și/sau corecteze bug-ul.*

Legendă:

- Timp de răspuns: timpul scurs de la anunțul inițial înregistrat de client prin metodele de comunicare stabilite în procedura de suport tehnic (stabilită de comun acord ulterior semnării contractului de furnizare) și răspunsul primit de la echipa de suport tehnic a furnizorului către client. Răspunsul va conține termenul până la care incidentul va fi remediat, cel puțin printr-o soluție alternativă temporară. Timpul de remediere menționat în tabel se va prelungi cu durata de timp necesară pentru clarificarea incidentului.
- Timp de remediere: durata de timp de la constatarea de către furnizor a defecțiunii până la implementarea soluției finale.
- Remediere provizorie/temporară: o modificare în cadrul procedurilor sau datelor care permite desfășurarea activității utilizatorului, ca soluție care evită temporar manifestarea defectului reclamat.

Timpii prezentați în tabelul de mai sus sunt calculați din momentul în care furnizorul a fost înștiințat de apariția problemelor.

Triajul incidentelor se va face în funcție de gradul de urgență a acestora:

Denumire	**Descriere**
Urgent	Impact Major asupra funcționării sistemului. Incidentul împiedică desfășurarea activității instituției, care este serios afectată, pierderea funcționalităților devenind critică.

Critic	Impact Semnificativ asupra funcționării sistemului. Incidentul împiedică desfășurarea în condiții normale a activității. Nu sunt disponibile soluții alternative pentru funcționalitatea in cauza, dar activitatea utilizatorilor poate continua, fiind limitata la componentele neafectate ale sistemului.
Major	Impact Mediu asupra funcționării sistemului. Incidentul afectează minor funcționalitățile sistemului. Impactul asupra utilizatorilor reprezintă un inconvenient care se poate rezolva temporar prin soluții alternative ocolitoare, pentru continuarea funcționalităților.
Minor	Impact Minim asupra funcționării sistemului. Incidentul nu afectează funcționarea sistemului, putând fi tratat ca o eroare minoră care nu împiedică desfășurarea în bune condiții a activității.

În cazul incidentelor cu nivel de prioritate *„Urgent"*, furnizorul va asigura asistență 24/7 până când problema va fi rezolvată. Pentru aceasta beneficiarul va furniza o persoană de contact, disponibilă pe perioada remedierii, care să furnizeze informații, să testeze soluții și să aplice soluțiile furnizate.

La sfârșitul fiecărui caz deschis, în sistemul de ticketing, din categoriile *„Urgent"* și *„Critic"*, furnizorul va efectua o analiză a cauzelor care au dus la producerea incidentului, iar concluziile vor fi regăsite în sistemul de ticketing.

4.5. Condiții de recepție a produselor

Recepția se va face în două etape, astfel:

- Recepția cantitativă, la livrarea fizică a soluțiilor, în prezența furnizorului și a unei comisii de recepție desemnată din partea beneficiarului. Operațiunea de recepție cantitativă va fi consemnată într-un proces verbal de predare/primire.
- Recepția calitativă, după instalarea soluțiilor/licențelor în prezența furnizorului și a unei comisii de recepție desemnată din partea beneficiarului. Ofertantul va oferi/realiza instalarea soluțiilor achiziționate și configurarea suplimentară a echipamentelor, în vederea bunei funcționări a acestora, la sediul CERT-RO. Operațiunea de recepție calitativă va fi consemnată într-un proces verbal de acceptanță prin care se va constatata conformitatea cu cerințele tehnice solicitate prin prezentul caiet de sarcini și totodată conformitatea serviciilor de instalare și configurare.

Cele două operațiuni de recepție vor fi consemnate într-un proces verbal de predare/primire și respectiv acceptanță.

Dacă vreunul din bunurile inspectate sau testate nu corespunde specificațiilor din propunerea tehnică, pe baza procesului-verbal de reclamație, achizitorul are

dreptul să îl respingă, iar furnizorul are obligația ca în termenul de livrare și fără a modifica prețul contractului:

a) de a înlocui bunurile refuzate, sau
b) de a face toate modificările necesare pentru ca bunurile să corespundă specificațiilor lor tehnice.

Dreptul achizitorului de a inspecta, testa și, dacă este necesar, de a respinge nu va fi limitat sau amânat datorită faptului că bunurile au fost inspectate și testate de furnizor, cu sau fără participarea unui reprezentant al achizitorului, anterior livrării acestora la destinația finală.

5. Plata

Plata se va face cu ordin de plată, în contul de Trezorerie al furnizorului, în termen de maxim 30 zile de la primirea documentelor emise de prestator (factura fiscală) și a procesului verbal de recepție/acceptanta a produselor/serviciilor, după obținerea avizului favorabil din partea AC. Factura va trebui să conțină, în cuprinsul ei sau anexat, detalierea echipamentelor cu cantitățile și prețurile unitare/totale aferente.

Termenul de plata de 30 de zile va putea fi decalat in condițiile in care nu sunt îndeplinite condițiile prevăzute la pct. 4 din Ordinul nr. 1792/2002 sau in cazul in care apar dispoziții legale care modifica perioada de plata pentru instituțiile publice.

6. Modul de prezentare a ofertei

Operatorii economici vor include în oferta tehnică o ***matrice de conformitate*** din care să rezulte clar modul prin care se respectă fiecare dintre cerințele tehnice impuse de către beneficiar. ***Matricea de conformitate*** va fi reprezentată printr-un tabel cu două coloane în care: în prima coloană se vor trece cerințele minime tehnice pentru lotul ofertat impuse de beneficiar, în a doua coloană operatorul economic va specifica capabilitățile tehnice ale ofertei și modul concret prin care aceasta îndeplinește cerințele. Pentru a facilita verificarea conformității acesteia cu caietul de sarcini, furnizorul va pune la dispoziția autorității contractante documentele în format electronic (sau referințe către acestea) din care să rezulte modul în care fiecare specificație solicitată prin caietul de sarcini este îndeplinită (fiecare cerință din caietul de sarcini va avea alăturat numele documentului, pagina și paragraful din care rezultă cele solicitate). Matricea de conformitate va fi livrată și în format editabil.

Propunerea tehnică va conține în mod obligatoriu numele produsului ofertat precum și informații concludente, respectiv link-uri sau print-screen-uri care să certifice îndeplinirea cerințelor minimale impuse.

În caz de neconcordanță a informațiilor din ofertă, specificațiile oficiale publicate de producătorul echipamentului/soluției (valabile la data ofertei, pentru produsele ofertate) vor fi considerate ca referință, iar conținutul acestora primează asupra detaliilor tehnice ale ofertei.

7. Propunerea financiară

Propunerea financiară va cuprinde prețul ofertei, exprimat în LEI, fără TVA, și va cuprinde prețul licențelor/echipamentelor ofertate, cât și toate cheltuielile ocazionate cu livrarea, instalarea și configurarea acestora la sediul beneficiarului. ***Detalierea prețului va fi făcută la nivelul fiecărei soluții cu respectarea limitărilor de preț de la punctul "Sinteză produse solicitate" pentru categoriile ce vor fi ofertate***.

Prețul final al ofertei rezultat în urma fazei finale va fi preț ferm, neajustabil și valabil pe toata perioada de derulare a contractului până la realizarea integrală a acestuia.

8. Informații privind elaborarea propunerii tehnice

Propunerea tehnică a operatorilor economici participanți la această procedură va conține cel puțin următoarele:

- Denumirea lotului
- Denumirea produselor/livrabilelor ce vor fi ofertate.
- Cantitățile ofertate.
- Specificațiile tehnice produselor ofertate.
- Matricea de conformitate (format semnat și format editabil (DOC/DOCX/ODT))
- O schiță a modului de integrare și interconectare a soluțiilor ofertate astfel încât aceste soluții să furnizeze toate funcționalitățile solicitate în descrierea modulelor platformei RO-SAT, respectiv a soluției SIEM și a soluției de knowledge management
- O descriere exhaustivă a modului în care soluțiile ofertate vor fi integrate și interconectate astfel încât să contribuie la îndeplinirea cerințelor și specificațiilor din Caietul de Sarcini pentru fiecare modul al platformei RO-SAT, respectiv soluție SIEM si soluție de knowledge management
- Un proiect/plan de instalare în care va fi detaliat modul de livrare, instalare, configurare, integrare și testare pentru fiecare din soluțiile ofertate precum și un grafic de realizare al acestor operații

NOTĂ: după semnarea contractului proiectul/planul de instalare va fi adaptat împreună cu beneficiarul iar livrarea, instalarea, configurarea și integrarea efectivă a soluțiilor va începe numai după aprobarea proiectului/planului de instalare de către beneficiar

NOTĂ: În oferta tehnică este obligatoriu sa se declare codul produsului si denumirea producătorilor echipamentelor.

Notă privind "Marca de produs"

În conformitate cu legea privind achizițiile publice, facem următoarele precizări:

- **Acolo unde este cazul, oriunde în caietul de sarcini se întâlnesc nume, mărci, denumiri pentru anumite produse se va considera implicit adăugată mențiunea „sau echivalent".**
- **Cerințele menționate la punctele 1÷8 sunt valabile pentru tot sistemul RO-SAT.**

9. Lot 1 – Soluții și servicii sistem RO-SAT

1. **Obiectul achiziției :** Soluții și servicii sistem RO-SAT
2. **Valoare totală estimată :** 24.200.000 lei fără TVA

9.1. Sinteză produse solicitate

Soluție software/soluție hardware	Cantitate	U.M.	Preț unitar fără TVA	Valoare totală fără TVA
0	1	2	3	4
Lot 1 – Soluții și servicii sistem RO-SAT				
Platforma RO-SAT			*19.400.000,00*	*19.400.000,00*
Modulul „Darknet"				
Modulul „HoneyNet"				
Modulul „Scanner vulnerabilități"				
Modulul „Crawling website-uri"				
Modulul „OSINT"				
Modulul „Cyber Threat Intelligence"				
Modulul colectare, normalizare și îmbogățire				
Modulul „Big Data Security Analytics"				
Modulul „Security Operations Center"				
Modulul „Diseminare date" (API)				
SIEM			*4.000.000,00*	*4.000.000,00*
Soluție knowledge management			*800.000,00*	*800.000,00*
TOTAL - fără TVA				**24.200.000,00**

Ofertantul va furniza soluțiile software și echipamentele acolo unde este cazul conform specificațiilor enumerate la punctele 9.3.1 (9.3.1.1-9.3.1.10), 9.3.2, 9.3.3.

NOTĂ: Toate echipamentele ce se vor furniza vor fi însoțite de cablurile și accesoriile necesare montării în rack standard de 19-inch, interconectării și funcționării.

NOTĂ: Având în vedere specificitatea pieței, soluțiile ce vor fi ofertate pentru modulele platformei RO-SAT vor putea acoperi parțial una sau mai multe din funcționalitățile solicitate în aceste module. Ținând cont de acest context, în oferta tehnică ofertantul va trebui să demonstreze că soluțiile ofertate acoperă cumulat în totalitate cerințele din prezentul caiet de sarcini.

Caracteristicile tehnice minimale ale soluțiilor ce vor fi furnizate, precum și cerințele specifice (de ex. garanție, suport) sunt detaliate la punctele următoare din acest capitol.

9.2. Cerințe funcționale generale

Sistemul RO-SAT va trebui să îndeplinească următoarele cerințe funcționale:

a. Să dețină capacitatea de preluare, procesare și corelare automată a alertelor/incidentelor de securitate cibernetică din diverse tipuri de surse (honeypots, site-uri, echipamente de protecție a rețelelor, echipamente de protecție endpoint, servicii web, email etc.), în diverse formate, utilizând diferite tehnologii/protocoale de transport de date, în cantități foarte mari (aprox. 2 milioane alerte/incidente zilnic);
b. Să dispună de funcționalități de completare, analiză, corelare și normalizare automată a datelor colectate în vederea extragerii informațiilor esențiale și a statisticilor pentru stabilirea stării de securitate cibernetică la nivel național, pentru stabilirea indicatorilor de compromitere pentru diverse tipuri de amenințări cibernetice cât și pentru identificarea rapidă a organizațiilor afectate în vederea transmiterii urgente a datelor către acestea;
c. Să dispună de funcționalități de transmitere automată, rapidă, corectă, coerentă și diferențiată a alertelor de securitate cibernetică către entitățile responsabile sau cele afectate de atacurile/incidentele cibernetice;
d. Să dispună de capacitatea de schimb automat de informații, prin definirea și implementarea de politici automate de schimb/partajare cu alte platforme informatice, utilizând diferite tehnologii/protocoale de transport de date (TAXII, AMQP, XMPP, JMS etc.) și diverse metode (API, WS etc). Autentificarea la acest

API se va face prin intermediul unui API-KEY, care va putea fi generat prin accesarea la o pagină web securizată de unde partenerii (autorități, CERT/CSIRT-uri, furnizori de servicii de Internet (ISP), companii de securitate cibernetică și chiar publicul larg) se pot autentifica prin intermediul unor credentiale și al unui token software/hardware (un token unic pentru fiecare partener);

e. Să ofere posibilitatea de realizare în timp real de statistici referitoare la incidentele/alertele primite, sisteme afectate, IP-uri, ASN-uri, domenii ".ro" etc. Anumite statistici publice predefinite vor fi afișate și actualizate în timp real în cadrul unui portal web;
f. Să ofere posibilitatea de realizare a unui profil al organizației, cu un istoric al alertelor ce au vizat organizația, tipuri de vulnerabilități, relevante pentru activitatea instituției, pentru organizațiile ce se interconectează cu RO-SAT (raportare diferențiată pe profil);
g. Să ofere diverse servicii utile în activitatea de răspuns la incidente de securitate cibernetică (ex: whois, ping, DNS lookup, traceroute, reverse IP address lookup, reverse DNS, reverse NS). Se vor integra serviciile comerciale precum cele oferite de DomainTools.com sau Spyse Cybersecurity Search Engine (informații detaliate despre domeniile web) și MaxMind sau IP-API (geo-localizare a adreselor IP);
h. Să fie capabil să identifice vulnerabilități în sistemele informatice, la solicitarea terților, serviciu disponibil prin integrarea unor tehnologii de scanare (serviciul va avea un ***disclaimer*** prin care utilizatorii vor fi avertizați de posibilele consecințe negative ale scanării);
i. Să fie capabil să monitorizeze (crawling) diverse site-uri publice ce publică frecvent date referitoare la incidente de securitate cibernetică, în vederea extragerii și prelucrării acestora și includerea lor în fluxul de informații procesat de sistem;
j. Să fie capabil să identifice site-uri web cu conținut malițios, în mod automat;
k. Să fie capabil să identifice în mod automat atacuri de tip exploit automatizate asupra serviciilor de rețea;

l. Să fie capabil de recepționarea unor cantități mari de date transmise de sistemele informatice interoperabile ale partenerilor CERT-RO cât și de la alte entități;

m. Sistemul trebuie să respecte principiile de scalabilitate orizontală; de asemenea sistemul trebuie să aibă o structură modulară, care să permită dezvoltări ulterioare și adăugări de noi module;

n. Sistemul trebuie să permită furnizarea unui serviciu de tip „threat intelligence feed" către terți (abonați), prin diferite protocoale de transport (inclusiv eMail).

Sistemul RO-SAT va fi găzduit la CERT-RO. Partenerilor care vor dori interconectarea cu sistemul li se vor pune la dispoziție interfețele necesare pentru accesul în sistem, pentru transmiterea datelor cât și pentru preluarea datelor la care au acces.

Organizațiile cu care CERT-RO are încheiate protocoale de cooperare pot transmite date automat prin sisteme interoperabile (servicii web, email, VPN, formulare web etc.) sau manual, în funcție de necesitate. Accesul partenerilor în sistem se face pe bază de nume de utilizator, parola și certificat digital/token, numai după înregistrarea în prealabil a organizațiilor. În funcție de configurația fiecărui sistem în parte, accesul poate fi furnizat și prin alte metode (ex: VPN, transmitere date în baze de date tampon etc.).

Organizațiile ce nu au protocoale de cooperare cu CERT-RO pot trimite datele doar prin email sau prin interfață web (formular web), fără acces direct la sistem și fără necesitatea de identificare/autentificare.

Sistemul va dispune de o componentă special destinată managementului utilizatorilor, bazată pe protocolul LDAP și pe alte protocoale de identificare/autentificare, pentru obținerea unui grad de securitate ridicat. Sistemul va suporta integrarea cu serverele Active Directory instalate, în vederea preluării utilizatorilor.

Accesul partenerilor se face numai după identificarea și autentificarea acestora, prin intermediul unor conexiuni securizate (SSL, VPN) și prin

autentificare cu token software/hardware (un token unic pentru fiecare partener).

În vederea conectării partenerilor către sistem, se dorește punerea la dispoziție de API-uri standardizate și securizate. În acest sens, soluția trebuie să administreze API-urile pe toată durata de viață, să permită definirea de politici de acces stricte, să permită definirea de servicii web și API pentru aplicații care nu au aceste funcționalități implementate.

Sistemul trebuie să adreseze orice nevoie de management al identității, dar să ofere, de asemenea, o gamă largă de capabilități pentru a servi ca o fundație care gestionează ciclul de viață completă a tuturor identităților; sistemul trebuie să ofere modalități extinse de autentificare ale utilizatorilor (certificate/token, autentificare multifactor).

9.3. Cerințe specifice

9.3.1 Platforma RO-SAT

1. **Obiectul achiziției:** Platforma RO-SAT
2. **Valoare totală estimată :** 19.400.000 lei fără TVA

Platforma RO-SAT va funcționa ca un sistem integrat, modular, flexibil și scalabil, format din diverse module și sub-module, ce vor îndeplini numeroase funcții. Modularitatea și flexibilitatea vor oferi posibilitatea dezvoltării ulterioare de funcționalități suplimentare, care să poată apela cu ușurință modulele deja dezvoltate.

RO-SAT va fi accesibil utilizatorilor prin intermediul unei interfețe WEB intuitive, ce va oferi posibilitatea administrării sistemului și realizării majorității funcționalităților sistemului.

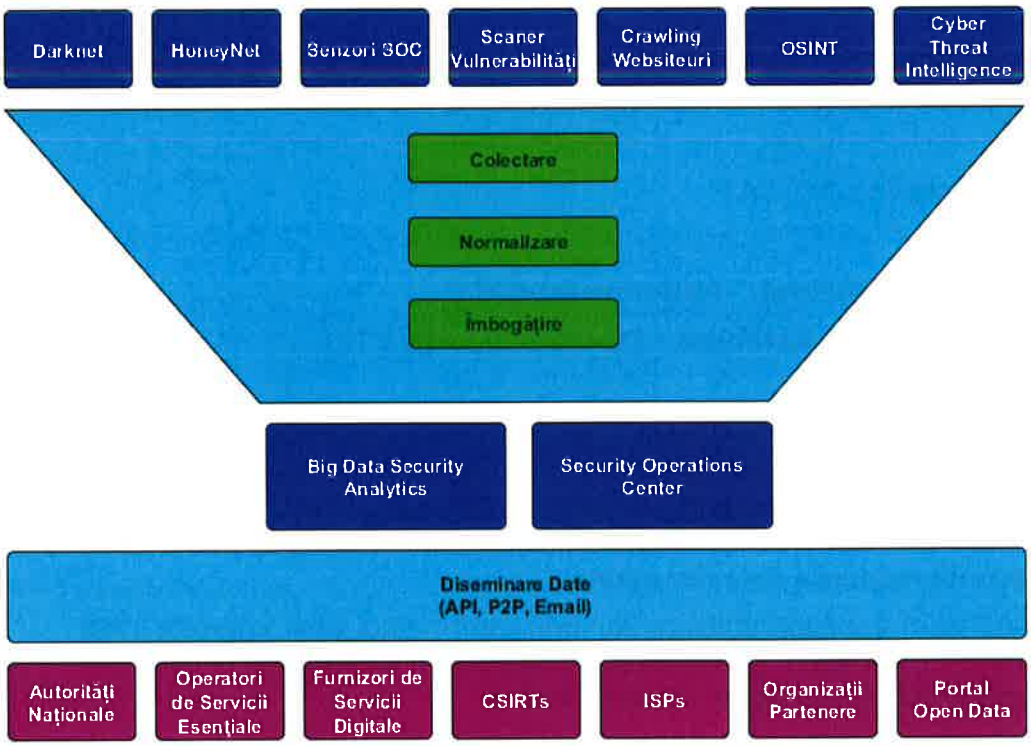
NOTĂ: Având în vedere faptul ca platforma va oferi servicii în regim 24x7, implementarea platformei va fi făcută astfel încât să poată fi asigurată continuitatea serviciilor prin intermediul unui centru de recuperare în caz de dezastru.

NOTĂ: În prezent nu a fost identificată o soluție să acopere toate funcționalitățile necesare atingerii obiectivelor proiectului. Soluțiile propuse pentru platforma ROSAT trebuie să fie COTS, cu excepția cazului

în care pe piață nu există soluții care să acopere cerințele tehnice din prezentul caiet de sarcini. Aceste soluții vor trebui configurate/personalizate astfel încât să fie asigurate toate funcționalitățile solicitate prin caietul de sarcini. Ofertantul va trebui să motiveze alegerea unei soluții nonCOTS și să demonstreze că funcționalitatea solicitată nu poate fi îndeplinită cu ajutorul unei soluții COTS.

NOTĂ: Câștigătorul va trebui să dezvolte platforma RO-SAT pornind de la soluții existente (COTS sau open-source) ce vor fi adaptate/personalizate astfel încât să fie obținut un nivel de securitate cibernetică în conformitate cu prevederile naționale și europene. Codul sursă și adaptările/personalizările vor fi documentate și vor deveni proprietatea Autorității Contractante.

În imaginea de mai jos este prezentată structura logică a funcționalităților și serviciilor ce vor trebui dezvoltate în cadrul platformei RO-SAT



NOTĂ: Senzorii SOC sunt dezvoltați de CERT-RO în cadrul altor activități. Datele furnizate de acești senzori vor trebui preluate în platforma RO-SAT fiind necesară definirea și realizarea de fluxuri de colectare, normalizare și îmbogățire a datelor obținute de senzori.

După cum reiese și din figura de mai sus, platforma RO-SAT va fi compusă dintr-o serie de module care vor genera date (evenimente, alerte, informații despre vulnerabilități, indicatori de compromitere etc.), un modul de prelucrare inițială a datelor (colectare, normalizare și îmbogățire), un modul de analiză automată a datelor colectate (Big Data Security Analytics), un modul de tip SOC (Security Operations Center) și o interfață API ce va oferi diferite nivele și profile de acces către diferite tipuri de entități: autorități, CERT/CSIRT-uri, furnizori de servicii de Internet (ISP), companii de securitate cibernetică și chiar publicul larg (printr-o interfață publică).

În imaginea de mai jos este prezentată structura logică a unui posibil mod de integrare și interconectare a soluțiilor și serviciilor platformei RO-SAT, incluzând și integrarea cu soluția SIEM ce va fi furnizată de către câștigătorul licitației. De asemenea în continuare sunt descrise și funcționalități ce vor trebui proiectate și dezvoltate de furnizor pentru a putea furniza beneficiarilor proiectului informațiile colectate și agregate în platforma RO-SAT.

Sursele principale de date sunt următoarele:

- Log-uri/evenimente/alerte echipamente și soluții hardware și software pe care va fi implementată platforma RO-SAT. Infrastructura pe care va fi implementată platforma conține următoarele tipuri de soluții și echipamente:
  - Firewall
  - ProxyWeb
  - ProxyEmail
  - WAF
  - Sandbox
  - Antivirus
- Sisteme de operare de tip Windows și Linux
- Log-urile modulului Darknet
- Log-urile modulului HoneyNet
- Datele obținute în urma scanărilor automatizate de vulnerabilități
- Datele obținute în urma scanărilor automatizate a website-urilor (crawling website-uri)
- Date extrase și agregate automat cu ajutorul modulului OSINT
- Date de tip Cyber Threat Intelligence extrase automat din feed-uri comerciale și feed-uri publice
- Log-uri colectate de la senzorii SOC

Datele colectate vor fi normalizate și îmbogățite. Vor trebui adăugate informații precum GeoIP, ASN, DNS Name, reputație, etc. Fluxurile de îmbogățire și normalizare vor fi propuse de furnizor și vor fi îmbunătățite la momentul adaptării proiectului/planului de instalare propus inițial de

furnizor. Implementarea fluxurilor de îmbogățire și normalizare va fi făcută de furnizor.

Toate datele colectate vor fi stocate într-o soluție/platformă de tip Big Data iar prin intermediul unor funcționalități de tip Big Data Security Analytics și cu ajutorul unor tehnologii de tip Machine Learning și Artificial Intelligence vor fi obținute informații suplimentare ce vor trebui să permită identificarea de pattern-uri ce pot anticipa activități specifice pregătirii unor atacuri cibernetice sau activități specifice unor atacuri aflate în derulare, dar încă nedescoperite (nedocumentate). Soluția propusă și modul general prin care se vor realiza funcționalitățile cerute vor fi detaliate de furnizor în oferta tehnică și în proiectul/planul de instalare propus în ofertă. După câștigarea licitației furnizorul va adapta fluxurile propuse în proiectul/planul de instalare conform discuțiilor pe care le va avea cu Autoritatea Contractantă, iar după aprobarea proiectului/planului de instalare le va implementa efectiv în platforma RO-SAT.

Modulul SOC - Security Operations Center va furniza în timp real informații despre situațiile care necesită intervenție/reacție rapidă a echipelor specializate din cadrul CERT-RO, astfel încât să fie asigurate stoparea atacurilor cibernetice, limitarea efectelor/pierderilor, coordonarea în vederea restabilirii funcționării normale și efectuarea investigațiilor aferente. Acesta va permite atât răspunsul automatizat (playbook-uri) la incidentele de securitate cibernetică detectate prin intermediul modulelor platformei RO-SAT cât și analiza manuală a informațiilor aferente unui incident de securitate, respectiv răspunsul manual, în baza unui sistem de ticketing integrat (case management). La momentul adaptării proiectului/planului de instalare propus în ofertă de către furnizor se va analiza și stabili dacă este oportună integrarea platformei RO-SAT cu sistemul de ticketing RTIR deținut de CERT-RO. Dacă beneficiarul va considera că este oportun furnizorul va realiza această integrare.

Modulul SOC va fi integrat de asemenea cu sistemul de afișare a alertelor video pentru a permite operatorilor vizualizarea centralizată a informațiilor furnizate de modul. Autoritatea contractantă va pune la dispoziție sistemul de afișare video urmând ca furnizorul să integreze funcțional acest sistem astfel încât operatorii platformei RO-SAT să vizualizeze alertele în timp real în mod centralizat.

Sistemul SIEM va fi folosit pentru structurarea și păstrarea datelor colectate într-o formă coerentă ce va putea fi ușor interogată. În acest sistem vor fi colectate și evidențiate atât alerte primite de la soluțiile hardware și software achiziționate pentru realizarea platformei RO-SAT (firewall-uri, proxy-uri, WAF, etc) cât și alertele primite de la senzorii SOC instalați de CERT-RO în cadrul proiectului. Acest sistem va fi integrat cu platforma RO-SAT. Modul de integrare va fi stabilit la momentul actualizării proiectului/planului de instalare propus în ofertă de către furnizor.

Furnizorul va pune la dispoziție formulare web prin intermediul cărora beneficiarii platformei RO-SAT vor completa informații precum: ip-uri, domenii/url-uri proprii, domeniul de activitate, etc (menționăm că aceste informații sunt informațiile ce vor fi solicitate minimal unui beneficiar; la momentul adaptării proiectului/planului de instalare propus inițial de furnizor vor fi stabilite toate informațiile ce vor fi completate de un beneficiar). Pe baza acestor tipuri informații furnizorul va defini și realiza fluxuri de automatizare a scanărilor de vulnerabilități și a scanărilor de website-uri/url-uri și va furniza manual/automatizat informații relevante pentru fiecare beneficiar.

Furnizorul va pune la dispoziție de asemenea și formularele de înrolare a beneficiarilor platformei și formularele de gestionare a beneficiarilor platformei.

Suplimentar furnizorul va pune la dispoziție formulare prin care va permite consultarea și extragerea manuală din platforma RO-SAT, de către beneficiari, a informațiilor relevante (IOC-uri, alerte de securitate, etc) aferente informațiilor introduse de beneficiari (ip-uri, domenii/url-uri proprii, domeniul de activitate, etc). De asemenea, furnizorul va utiliza modulul API propus pentru a permite unui beneficiar extragerea automatizată a informațiilor relevante pentru acesta. Extragerea automatizată se va face în funcție de criterii ce vor fi definite la momentul adaptării proiectului/planului de instalare propus inițial de furnizor. Dintre criterii menționăm:

- ip-uri
- domenii/url-uri proprii - domeniul de activitate
- timestamp informații
- etc

NOTĂ: informațiile ce vor fi extrase manual/automatizat vor fi furnizate la alegere beneficiarului în format JSON, CSV sau TEXT. Extragerea informațiilor va fi permisă numai după autentificarea beneficiarului.

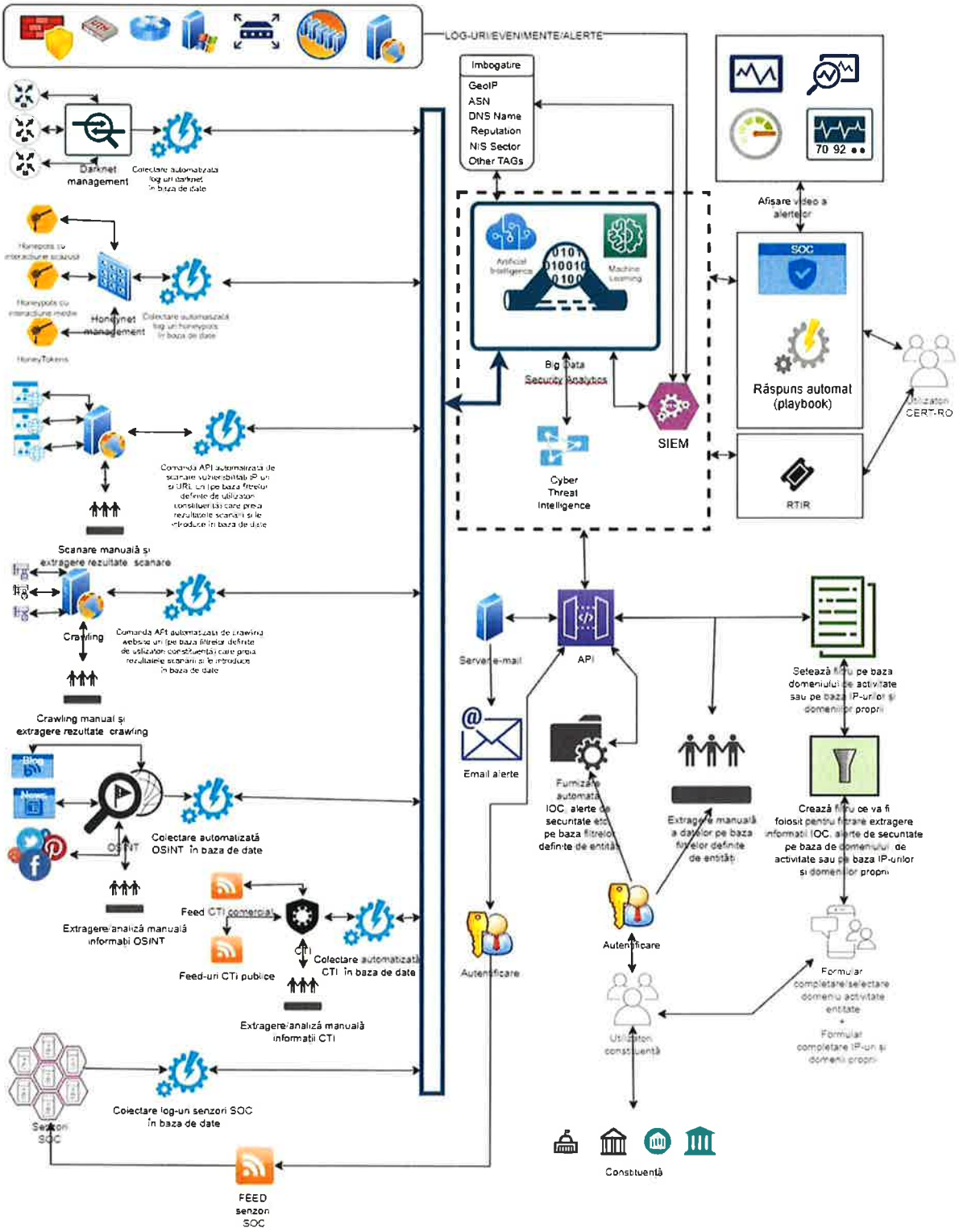
Modulul API va fi utilizat și pentru transmiterea automatizată către beneficiari prin email a unor alerte. Fluxurile de lucru și informațiile care vor fi transmise prin email vor fi de asemenea corelate/îmbunătățite la momentul adaptării proiectului/planului de instalare propus inițial de furnizor și vor trebui implementate de furnizor la nivelul platformei RO-SAT.

La nivel centralizat modulul API va trebui să permită extragerea de informații de către operatorii platformei RO-SAT. Extragerea de informații se va face fie manual, prin intermediul unor formulare ce vor fi realizate de către furnizor, fie automatizat prin utilizarea directă a interfeței API. Utilizarea modului API se va face după autentificarea operatorului. Furnizorul va trebui să definească și să realizeze aceste funcționalități. Informațiile ce vor fi extrase manual/automatizat vor fi furnizate la

alegere în format JSON, CSV sau TEXT și vor putea fi filtrate după criterii similare celor definite pentru beneficiarii platformei.

Prin intermediul modului API se va crea automatizat un feed ce va fi pus la dispoziția senzorilor SOC. De asemenea, pentru a reduce încărcarea bazei de date din punct de vedere al procesării, vor fi create automatizat feed-uri ce vor fi puse la dispoziția beneficiarilor platformei RO-SAT. Beneficiarul va putea selecta în formularul de management al contului feed-urile la care dorește să aibă acces și va putea descărca prin intermediul API-ului aceste feed-uri. Conținutul feed-urilor și fluxul de lucru va fi stabilit la momentul adaptării proiectului/planului de instalare propus inițial de furnizor. Furnizorul va trebui să implementeze în platforma RO-SAT fluxurile conform proiectului/planului de instalare final.

De asemenea la momentul actualizării proiectului/planului de instalare vor fi definite fluxurile de lucru pentru furnizarea de feed-uri de date în regim public, iar la momentul realizării platformei RO-SAT furnizorul va implementa funcționalitățile stabilite.



Structura funcțională și modul logic de integrare a modulelor platformei RO-SAT au fost detaliate unitar în cadrul punctului 9.3.1. În continuare vor fi prezentate cerințele generale și specifice pentru fiecare din modulele platformei RO-SAT (punctele 9.3.1.1. ÷ 9.3.1.10).

9.3.1.1 Modulul „Darknet"

În contextul proiectului RO-SAT, DARKNET va fi reprezentat de o platformă prin care se va putea observa și studia trafic de rețea ce reprezintă conexiuni către adrese IP neasignate vreunui sistem informatic. Acest tip de trafic este prin definiție malițios, reprezentând adesea scanări în masă ale spațiului de adrese IP pentru identificarea de sisteme vulnerabile.

Modulul Darknet este un mecanism software de monitorizare a unui spațiu continuu de adrese IP nealocate unui echipament, astfel încât aceste adrese nu pot genera trafic iar traficul care ajunge la aceste adrese este considerat ca fiind trafic ofensiv (scanări malware, scanări premergătoare atacurilor, mass scan după anumite vulnerabilități, etc.). Cu cât spațiul de adrese este mai mare, cu atât datele provenite din darknet vor fi mai relevante din punctul de vedere al monitorizării strategiilor, tacticilor și tehnicilor atacatorilor, putând evidenția de exemplu, noi campanii de exploatare a unor vulnerabilități sau care sunt serviciile și tipurile de atacuri folosite de atacatori, și ajutând la clasificarea acestora prin corelarea informațiilor obținute.

Astfel, vor fi monitorizate spațiile de adrese IP neutilizate ale CERT-RO și ale partenerilor sau beneficiarilor proiectului. Acest lucru se va realiza prin configurarea routerelor astfel încât să direcționeze către RO-SAT tot traficul de date destinat unor adrese IP nealocate.

Traficul de date astfel colectat va fi analizat automat, sau de către analiștii CERT-RO, în vederea detectării fenomenelor recente din Internet: scanări premergătoare unor atacuri, încercări de exploatare a unor vulnerabilități, răspândire de malware etc.

Modulul Darknet va permite monitorizarea unui număr flexibil de adrese IP, fiind concentrat în principal pe pachete de date TCP/UDP/ICMP, pentru a evita supraîncărcarea cu trafic de tip „ghost", care îngreunează efortul de analiză. Vor fi înregistrate cel puțin adresa sursa, portul sursa, adresa destinație și portul destinație al unui pachet, dar și amprenta temporală la nivel de an, luna, zi, ora, minut și secundă în care respectivul pachet a fost identificat.

Înregistrările obținute de modulul Darknet trebuie să poată fi exportate în format JSON, CSV sau TXT si trebuie să conțină cel puțin următoarele elemente:

- Amprenta temporală
- Ip sursă
- Port sursă
- Ip destinație
- Port destinație

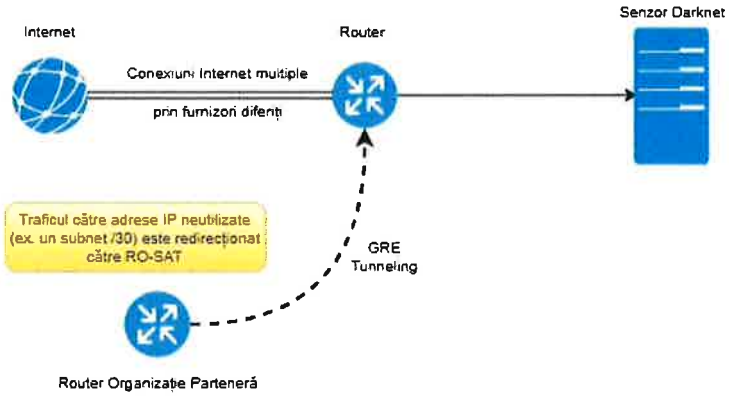


Figura de mai sus reprezintă doar o schemă de principiu a sistemului DARKNET, arhitectura finală putând să difere – spre exemplu anumite componente ar putea să fie virtualizate.

Furnizorul va oferta un modul care să permită realizarea funcționalităților descrise mai sus. Caracteristicile tehnice minimale ale modulului ce va fi ofertat sunt următoarele:

- Va permite analiza traficului de rețea către IP-uri neasignate vreunui sistem informatic
- Va dispune de o interfață de management centralizat al componentelor modulului
- Soluția va fi scalabilă și va fi integrată funcțional în platforma RO-SAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)
- Soluția va permite exportarea manuală sau automatizată a informațiilor colectate către alte baze de date.

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului

- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care modulul "Darknet" ofertat va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence"

9.3.1.2 Modulul „HoneyNet"

Modulul Honeynet va fi compus dintr-o suită de mecanisme software de tip honeypot care vor trebui să fie ca tip cel puțin din categoriile honeypot cu interacțiune scăzută, medie și înaltă și honeytoken (decepții la nivel de aplicații).

Modulul HoneyNet va consta într-o rețea de senzori de tip HoneyPot – sisteme informatice vulnerabile expuse intenționat atacurilor în vederea analizării tehnicilor și uneltelor de exploatare utilizate de atacatori. Modulul Honeynet trebuie să emuleze echipamente de rețea, servere, servicii de email și file sharing, stații de lucru (diferite sisteme de operare), echipamente industriale, dispozitive IoT, sisteme de control industrial (ICS/SCADA) dar și alte tipuri de echipamente considerate de interes pentru atacatori.

Pentru stații de lucru și servere, sistemele de operare de tip Windows ce vor trebui emulate sunt cel puțin Windows 2008, Windows 2012, Windows 2016, Windows XP Desktop, Windows 7 Desktop, de tip Windows 8 Desktop, Windows 10 Desktop. De asemenea soluția va trebui să emuleze și sisteme Linux.

NOTĂ: În cazul în care pentru implementarea honeypots vor fi necesare licențe ale sistemelor de operare sau soluțiilor emulate acestea vor fi furnizate de asemenea de ofertant, fără costuri suplimentare.

Se vor lua măsuri pentru a fi cât mai greu de identificat de către atacatori ca fiind honeypots. Se vor lua de asemenea toate măsurile necesare pentru protecția acestora, precum restaurare din snapshot atunci când integritatea este compromisă.

Modulul HoneyNet este alcătuit din doua componente: una ce nu este expusă în internet fiind vizibilă în zona DMZ, iar cea de a doua expusă în internet.

Aceste sisteme vor fi expuse în Internet prin alocarea unor adrese IP dedicate (deținute sau achiziționate de CERT-RO în acest scop), sau prin alocarea unor adrese IP neutilizate de la organizațiile partenere (GRE tunneling).

Sistemul/sistemele expuse în internet vor trebui să ruleze și să emuleze cel puțin următoarele:

- Apache HTTP
- FTP
- SSH
- VoIP
- Tomcat
- Struts 2 plugin
- SQL

La momentul actualizării proiectului/planului de instalare furnizat în cadrul ofertei se va analiza oportunitatea trecerii traficului către/dinspre honetpots printr-un firewall (pentru restricționarea anumitor conexiuni și prevenirea/stoparea unor atacuri derulate prin intermediul sistemelor honeypot compromise), ce va fi pus

la dispoziție de Autoritatea Contractantă, pentru fiecare tip de honeypot ce va fi instalat cu ajutorul modulului. De asemenea în situația în care un honeypot permite securizarea, furnizorul va analiza realizarea aceste operațiuni după ce în prealabil acestea vor fi detaliate în momentul actualizării proiectului/planului de instalare.

Honeypot-urile ce nu vor fi expuse direct în internet, vor trebui să monitorizeze cel puțin următoarele:

a) Elemente de conectivitate:

- Credentiale din memorie
- Conexiuni active
- Credentiale deceptii
- Deceptii SMB shares
- Credentiale, history, shortcuts din Browser
- Credentiale de aplicatie
- Date vulnerabile in SMB Shares

b) Servicii/aplicații:

- FTP/SFTP
- HTTP/HTTPS
- Print
- SMB
- NBNS
- SSH
- SMTP
- SWIFT Messaging
- SNMP
- Telnet
- RDP
- GIT
- mDNS
- MySQL
- Apache
- Tomcat
- Jboss
- SVN/CVS
- VPN

- Mongo DB, ES, Redis
- WinRM
- AD
- MSSQL

c) pentru echipamentele de tip ICS/SCADA:

- Modbus
- BACnet
- Siemens S7comm
- IPMI
- Common Industrial Protocol (CIP)

d) pentru echipamentele IoT/IoE:

- MQTT
- CoAP
- XMPP
- Health Level-7
- Digital Imaging & Comms in Medicine (DICOM)

Înregistrările/log-urile obținute prin intermediul modulului "HoneyNet" trebuie să poată fi exportate in format JSON, CSV sau TXT și trebuie să conțină cel puțin următoarele elemente:

- Amprenta temporală
- Ip sursă
- Port sursă
- Ip destinație
- Port destinație
- Username și parole

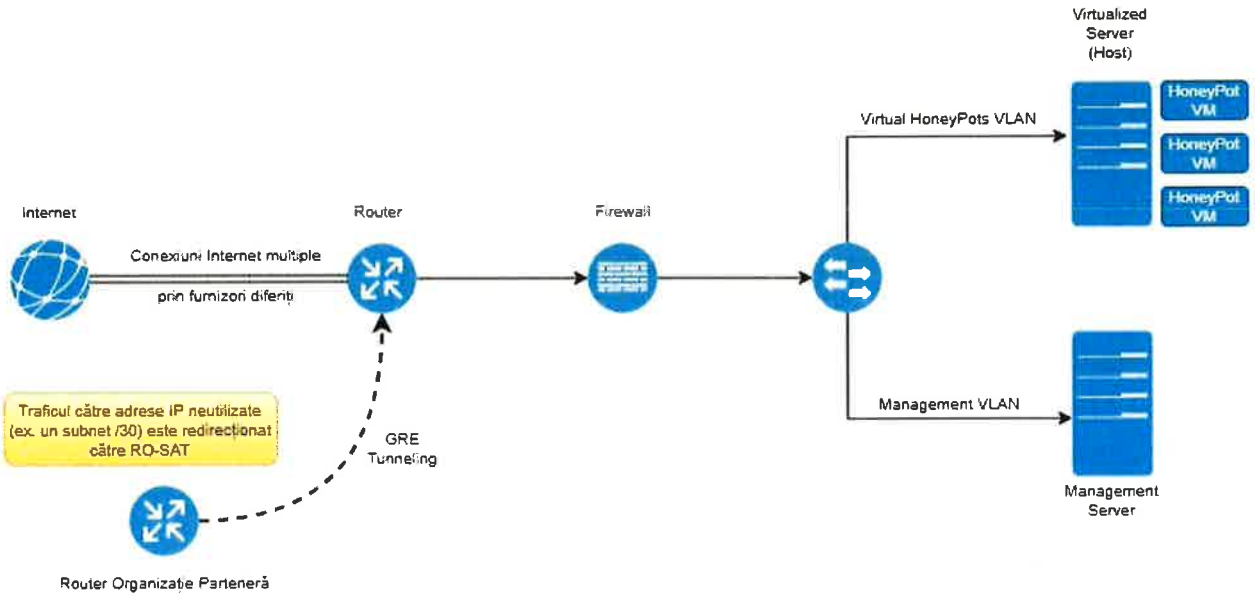


Figura de mai sus reprezintă doar o schemă de principiu a sistemului HoneyNet, arhitectura finală putând să difere.

Furnizorul va oferta un modul care să permită realizarea funcționalităților descrise mai sus. Caracteristicile tehnice minimale ale modulului ce va fi ofertat sunt următoarele:

- Modulul va fi constituit din sistemele HoneyPot și interfața de management centralizat a componentelor modulului
- Modulul va permite simularea unei game variate de sisteme și servicii informatice: echipamente de rețea, servere, servicii de email și file sharing, stații de lucru (diferite sisteme de operare), echipamente industriale, dispozitive IoT etc. Modulul HoneyNet va simula servicii vulnerabile clasice, dar și servicii specifice Internet of Things - IoT, sisteme de control industrial (ICS/SCADA)
- Soluția trebuie să permită definirea și utilizarea de honeytoken-uri
- Va dispune de o interfață de management centralizat al componentelor modulului
- Soluția va fi scalabilă și va fi integrată funcțional în platforma ROSAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)
- Soluția va permite exportarea manuală și automatizată a informațiilor colectate către alte baze de date.
- Soluția trebuie să se instaleze în 40 locații si 10 locații de test și va conține minim 500 de honeytoken-uri

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care modulul " HoneyNet" ofertat va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea

securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

9.3.1.3 Modulul „Scanner vulnerabilități"

Modulul *Scanner de vulnerabilități* trebuie să permită scanarea neintrusivă a adreselor IP și URL și trebuie să aibă în vedere:

- identificarea tehnologiilor folosite;
- identificarea versiunilor tehnologiilor folosite;
- compararea tehnologiilor și versiunilor acestora cu baze de date de vulnerabilități publice sau private și identificarea celor vulnerabile.

Nu este permisă scanarea intruzivă (prin folosirea de pachete de tip trigger pentru anumite vulnerabilități). De asemenea, soluția trebuie să permită interacțiunea prin API, atât pentru programarea și prioritizarea scanărilor, cât și pentru comunicarea rezultatelor.

Acest modul va fi utilizat pentru a verifica, în mod neintruziv, dacă anumite resurse informatice din segmentul de Internet național (IP-uri, URL-uri) sunt vulnerabile (pe baza vulnerabilităților publice sau interne – prestabilitate ca date de intrare de către specialiștii CERT-RO).

Bazele de date de vulnerabilități utilizate în cadrul acestui modul vor fi actualizate permanent (automat și manual), astfel încât să reflecte permanent nivelul de securitate cibernetică al resurselor informatice expuse în Internet la nivel național. În acest sens, modulul va trimite cereri special concepute către aceste resurse (ex. cereri HTTP/S), astfel încât din răspunsul primit să rezulte cu acuratețe cât mai mare dacă acesta sunt sau nu vulnerabile.

Înregistrările obținute de modulul *Scanner de vulnerabilități* trebuie să poată fi exportate cel puțin în formatul JSON și trebuie să conțină cel puțin următoarele informații:

- amprenta temporală a scanării;
- serviciul vulnerabil identificat;
- referință CVE (scurtă descriere a vulnerabilității, nivelul de severitate și impactul acesteia; referințe (mențiuni externe ale vulnerabilității)) sau similar (dacă există);
- recomandări de remediere a vulnerabilității.

Modulul va permite introducerea automată (ex. API) și manuală a adreselor IP și a URL-urilor (individuale sau listă) ce vor fi scanate. Soluția propusă de către furnizor va dispune de mecanismele necesare automatizării introducerii adreselor IP și a URL-urilor, programării prioritizate a procesului de scanare (managementul resurselor) și introducerii rezultatelor scanării în baza de date a platformei RO-SAT.

Furnizorul va oferta un modul care să permită realizarea funcționalităților descrise mai sus. Caracteristicile tehnice minimale ale modulului ce va fi ofertat sunt următoarele:

- Va permite verificarea resurselor informatice din Internet (IP-uri, URL-uri) în scopul identificării vulnerabilităților cunoscute și nerezolvate (ex. vulnerabilități specifice WordPress, PHP etc)
- Va furniza o interfață de tip *restAPI* pentru automatizarea procesului de scanare (date de intrate – adrese IP, URL; programare prioritizată – alocarea resurselor; nivelul de recurență; date de ieșire – înregistrări în format brut, JSON sau sub formă de rapoarte)
- Va dispune de posibilități de generare a rapoartelor (manual/automat)
- Va furniza servicii de căutare în baze de date care oferă informații cu privire la echipamente (routere, camere web, echipamente VoIP, SCADA/ICS - Industrial Control Systems, etc) care sunt vulnerabile și accesibile direct din Internet
- La nivelul platformei RO-SAT furnizorul va dezvolta formulare web prin intermediul cărora beneficiarii platformei vor completa informații precum: ip-uri, domenii/url-uri proprii, domeniul de activitate, etc (menționăm că aceste informații sunt informațiile ce vor fi solicitate minimal unui beneficiar; la momentul adaptării proiectului/planului de instalare propus inițial de furnizor vor fi stabilite toate informațiile ce vor fi completate de un beneficiar). Pe baza acestor tipuri informații furnizorul va defini și realiza fluxuri de automatizare a scanărilor de vulnerabilități și va furniza manual/automatizat informații relevante pentru fiecare beneficiar (informațiile ce vor fi extrase manual/automatizat vor fi furnizate la alegere beneficiarului în format JSON, CSV sau TEXT; extragerea informațiilor va fi permisă numai după autentificarea beneficiarului)
- Soluția va fi scalabilă și va fi integrată funcțional în platforma RO-SAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)
- Soluția va permite exportarea manuală și automatizată a informațiilor colectate către alte baze de date
- Soluția va trebui să includă modalități de prioritizare predictivă a vulnerabilităților în funcție de context, nu doar de CVSS
- Soluția va analiza informații dintr-o gama larga de surse, incluzând Active Directory, configuration management databases (CMDBs), patch management systems, sisteme mobile device management (MDM) și platforme cloud
- Soluția va oferi dashboard-uri și rapoarte personalizabile

- Soluția va permite demonstrarea conformității cu standarde de industrie și reglementări, precum ISO/IEC 27001/27002, PCI, NIST Cybersecurity Framework, NIST SP 800-171 and CIS Critical Controls

- Soluția va permite instalarea unui număr nelimitat de motoare de scanare

- Licența va fi dimensionată pentru a putea scana un număr minim de 1000 IP-uri (lista IP-urilor va trebui să poată fi modificată cel puțin anual)

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care modulul " Scanner vulnerabilități" ofertat va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

9.3.1.4 Modulul „Crawling website-uri"

Acest modul va permite analiza site-urilor din aria de competență a CERT-RO (siteuri .ro sau site-uri găzduite în România) pentru identificarea malware-ului și amprentarea vulnerabilităților existente la nivelul acestora. Analiza va fi făcută neintruziv (fără acțiuni ce ar putea afecta buna funcționare a site-ului; ex: injecturi) pentru a descoperi informații care să permită detectarea și evaluarea vulnerabilităților existente. Informațiile obținute vor fi stocate în baza de date și transmise ulterior părților interesate (parteneri, posesori site etc.).

Modulul Crawling website-uri trebuie să permită scanarea simultană/în paralel a site-urilor web. De asemenea acest modul trebuie să permită opțiuni de scanare a site-urilor web în funcție de adâncime (cel puțin 3 nivele în adâncime începând de la rădăcina site-urilor web).

Modulul Crawling website-uri trebuie să permită atât analiza elementelor HTML incluse direct în pagina web, cât și a celor incluse indirect, din surse externe paginii.

Informațiile obținute vor fi analizate, agregate și stocate în baza de date a platformei RO-SAT urmând a fi utilizate ulterior.

Înregistrările obținute de Modulul „Crawling website-uri" trebuie să poată să fie exportate cel puțin în format JSON și trebuie să conțină cel puțin următoarele informații:

- Amprenta temporală a scanării
- Domeniul pe care a fost identificat atacul
- URL-ul în care a fost identificat atacul
- Tipul atacului
- Elementul HTML care a cauzat atacul

Furnizorul va oferta un modul care să permită realizarea funcționalităților descrise mai sus.

Caracteristicile tehnice minimale ale modulului ce va fi ofertat sunt următoarele:

- Soluția va permite analiza site-urilor web pentru identificarea malware-ului și amprentarea vulnerabilităților existente la nivelul acestora, în mod neintruziv
- Soluția va permite identificarea de malware obfuscat
- Soluția va furniza o interfață de tip restAPI pentru automatizarea procesului de crawling
- Soluția va dispune de posibilități de generare a rapoartelor (manual/automat)
- La nivelul platformei RO-SAT furnizorul va dezvolta formulare web prin intermediul cărora beneficiarii platformei vor completa informații precum: ip-uri, domenii/url-uri proprii, domeniul de activitate, etc (menționăm că aceste informații sunt informațiile ce vor fi solicitate minimal unui beneficiar; la momentul adaptării proiectului/planului de instalare propus inițial de furnizor vor fi stabilite toate informațiile ce vor fi completate de un beneficiar). Pe baza acestor tipuri informații furnizorul va defini și realiza fluxuri de automatizare a scanărilor de website-uri/url-uri și va furniza manual/automatizat informații relevante pentru fiecare beneficiar (informațiile ce vor fi extrase manual/automatizat vor fi furnizate la alegere beneficiarului în format JSON, CSV sau TEXT; extragerea informațiilor va fi permisă numai după autentificarea beneficiarului)
- Soluția va fi scalabilă și va fi integrată funcțional în platforma RO-SAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)
- Soluția va permite exportarea manuală și automatizată a informațiilor colectate către alte baze de date
- Soluția trebuie să adopte o structură care să permită organizarea activelor digitale expuse în internet prin folosirea unor criterii/etichete predefinite. Organizarea va putea fi făcută atât manual cât și automat. De asemenea va fi oferită opțiunea adăugării/creării de noi criterii/etichete. Soluția trebuie să poată oferi capacitatea de a aplica metadate și alte funcționalități de etichetare pentru a împărți amprenta digitală în „Organizații", „Mărci" și alte "Etichete"
- Soluția trebuie să descopere și să mențină un inventar al tuturor activelor exterioare pentru organizație și să acceseze continuu fiecare activ în mod regulat pentru a identifica orice activitate suspectă. Soluția trebuie să ofere date istorice.

- Soluția va permite obținerea de informații precum porturile deschise si scorurile CVSS ale activelor expuse în internet

- Soluția se va putea integra cu scanere de vulnerabilități și alte instrumente de management (cum ar fi Qualys, Tenable, Rapid7 sau similar)

- Soluția nu trebuie să necesite instalarea unui agent

- Soluția trebuie să furnizeze dashboard-uri și raportări personalizabile, cu capacități robuste de programare și export.

- Soluția trebuie sa ofere posibilitatea de a descoperi activele web și a le exploata așa cum o face un utilizator real (sau un atacator care efectuează recunoașterea), permițând organizației să identifice cu precizie, să monitorizeze și să gestioneze întreaga suprafață de atac expusă

- Soluția trebuie să monitorizeze active digitale expuse în internet, pentru modificări apărute, respectarea politicilor de acces sau chiar apariția unui malware.

- Alte capabilități necesare:

  - Vizualizarea detaliilor despre active, cum ar fi adresa IP, detaliile deținătorului domeniului, componentele web, CVE-urile asociate
  - Pentru asset-urile externe monitorizate va fi oferit un scor de risc pe baza indicatorilor cheie de compromitere și a stării de securitate cibernetică. Soluția trebuie să aibă capacitatea de a monitoriza evoluția si modificările acestui scor în timp (de exemplu, în ultimele 30 de zile). Ponderările, valorile și alți factori trebuie să fie ajustabili.

- Soluția trebuie să poată detecta utilizarea JavaScript pe suprafața de atac prin recunoaștere continuă

- Soluția trebuie să aibă diferite tipuri de dashboard, cum ar fi:

  - Dashboard pentru raportarea riscurilor: un scor global de risc al inventarului activelor și scorurilor organizației/organizațiilor pe subgrupele enumerate mai jos (să poată detalia în orice scor sau zonă pentru a vedea valorile care îl definesc și setul de active care au fost găsite si corespund criteriilor; să permită filtrarea după marca / organizație / tip de activ, exportabil)
  - Risk Score Delta (ex.ultimele 30 de zile)
  - Host Reputation
  - IP Reputation
  - Malware
  - Expunere CVE pe site-ul web
  - Administrarea domeniului
  - Configurare domeniu

- Găzduire și rețea
- Porturi deschise
- Politici de securitate pe site-uri web
- Configurare SSL
- Organizare SSL

- Soluția trebuie să ofere o privire de ansamblu asupra stării de securitate a organizației din punct de vedere al expunerii în internet. De asemenea, având la bază gradul de expunere externă a organizației la amenințări digitale, trebuie să poată fi furnizat un scor precis și ușor de urmărit, cu evidențierea diferențelor de la o dată la alta. Datele din spatele acestor scoruri și valori trebuie să poată fi accesate ușor. De asemenea, trebuie furnizate îndrumări/direcții de îmbunătățire (mitigation guidance) pentru a securiza activele digitale externe și pentru a îmbunătăți scorul.

- Soluția trebuie să poată corela încrucișat, în mod automat datele din diverse evenimente pentru a afișa grupuri de evenimente cu caracteristici similare.

- Soluția trebuie să acopere până la 10,000 de servere/host-uri cu capabilități generice, din care până la 1,000 de host-uri cu capabilități avansate de scanare, detaliere și identificare malware.

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care modulul " Crawling website-uri" ofertat va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor

se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

9.3.1.5 Modulul „OSINT"

Acest modul va fi utilizat pentru agregarea automată a informațiilor din surse publice (portaluri web, forumuri, blog-uri etc.) referitoare la amenințări, vulnerabilități și riscuri cibernetice- folosind surse publice si private, cum ar fi forumuri, site-uri web, social media.

Informațiile rezultate din parcurgerea surselor menționate trebuie să poată fi exportate în format JSON, CSV sau TXT. Informațiile vor fi exportate printr-o interfață de tip restAPI sau alte metode (ofertantul va descrie în oferta tehnică modul în care se va realiza acest export)

Furnizorul va oferta un modul care să permită realizarea funcționalităților descrise mai sus. Caracteristicile tehnice minimale ale modulului ce va fi ofertat sunt următoarele:

- Va permite colectarea de informații din surse publice (portaluri web, forumuri, blog-uri etc.) referitoare la amenințări, vulnerabilități și riscuri cibernetice

- Soluția va fi scalabilă și va fi integrată funcțional în platforma RO-SAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)
- Soluția va permite exportarea manuală și automatizată a informațiilor colectate către alte baze de date, printr-o interfață de tip *restAPI* sau alte metode (ofertantul va descrie în oferta tehnică modul în care se va realiza acest export) .
- Soluția trebuie să ofere acces la datele din internet de care CERT are nevoie pentru a înțelege cine este atacatorul și ce infrastructură folosește pentru a-și efectua atacurile, pentru aceasta utilizatorul folosind un indicator de compromitere (IOC) sau artefacte suspecte, cum ar fi (dar nu limitat la) un domeniu, o adresă IP sau o adresă de e-mail, înregistratorii WHOIS, informații despre certificatul SSL și Host Pairs etc.
- Soluția trebuie să ofere posibilitatea de a pivota prin seturile de date relevante unei investigații
- Soluția trebuie să permită colaborarea in cadrul unei investigații.
- Soluția trebuie să pună la dispoziție analiștilor informații privind elementele de infrastructură expuse în internet, să permită identificarea amenințărilor și automatizarea investigațiilor
- Soluția trebuie să furnizeze analiștilor informații cu caracter istoric cu scopul de a permite identificarea de conexiuni istorice între atacuri
- Soluția trebuie să ofere analiștilor posibilitatea de a adăuga IOC-uri la investigații (atât în echipă, cât și privat doar pentru un analist), precum și capacitatea de a monitoriza aceste IOC-uri pentru orice schimbare de stare sau aspect în timp. Alertarea trebuie furnizată în numeroase forme: e-mail, alertă in interfață și alertă prin API.
- Soluția trebuie să ofere posibilitatea corelării unor IOC-uri neinvestigate cu altele utilizate anterior în campaniile de atac pentru a permite o atribuire mai buna in cazul unui atac. Analiștii

trebuie să poată înțelege, TTP-urile autorilor, tipul de infrastructură pe care aceștia o folosesc pentru a derula atacul sau tipurile de site-uri compromise și utilizate pentru a derula activitățile malițioase

- Soluția trebuie să facă îmbogățirea datelor IOC analizate cu informații de tip PDNS (passive DNS), Whois, Certificate SSL și date OSINT, precum și alte seturi de date din internet, cum ar fi: Host Pairs, Trackers, Cookies, Componente WEB, Hash Malware, porturi deschise și servicii.
- Soluția trebuie să permită integrarea cu alte soluții de analiză și investigare
- Soluția trebuie sa permită integrarea cu alte soluții de securitate.
- Soluția trebuie să ofere informații avansate pentru analiști, ajutându-i să economisească timp oferind un scor reputațional al unui IOC.
- Soluția trebuie să poată oferi capabilități de furnizare și colectare de date din internet.
- Accesul la platforma trebuie asigurat pentru minim 3 utilizatori, precum si un volum minim cumulat de call-uri sau interogări API de minimum 500,000 lunar.

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care modulul "OSINT" ofertat va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

9.3.1.6 Modulul „Cyber Threat Intelligence"

Modulul de Cyber Threat Intelligence - CTI va colecta date și informații din mai multe surse, pe care le va agrega și le va transmite către platforma de analiză. În cadrul acestui modul vor fi incluse subscripții la diferite servicii de tip Cyber Threat Intelligence, unele dintre acestea fiind oferite gratuit structurilor de tip CERT, altele fiind accesibile contracost.

NOTĂ: Furnizorul va oferi cel puțin o subscripție CTI contracost ce va avea următoarele caracteristici:

- Va conține date relevante la peisajul cyber threat la nivel global
- Va conține date istorice
- Va oferi clasificări și etichetări ale datelor astfel încât interogarea datelor să poată fi făcută granular (de ex. clasificarea datelor în funcție de sectorul de activitate, țară, an, lună, zi, tip dată (IP, URL, SHA1, MD5, fișier, etc)
- Va pune la dispoziție un API care să poată fi interogat automatizat pe baza clasificărilor menționate anterior și care va permite extragerea informațiilor de tip CTI în formate consacrate (JSON, csv, text, etc)

Obiectivul principal al acestui modul este acela de a integra și corela informațiile obținute prin intermediul terminalelor SOC, al modulelor Darknet, HoneyNet, Crawling și OSINT cu cele furnizate prin intermediul subscripțiilor pentru a putea fi identificate tipurile de atacuri existente deja în spațiul cibernetic național, precum și atacatorii care le derulează, în scopul facilitării procesului de investigare și de limitare a efectelor atacurilor cibernetice.

Furnizorul va oferta un modul care să permită realizarea funcționalităților descrise mai sus. Caracteristicile tehnice minimale ale modulului ce va fi ofertat sunt următoarele:

- Va integra cel puțin o subscripție CTI Premium (comercială/contracost) (de ex. Accenture DeepSight, Anomali, Autofocus (Palo Alto Networks), Blueliv, Cofense, Crowdstrike, Flashpoint, Mandiant Advantage (FireEye), Fox-IT intel, Group IB, Intel 471, Proofpoint, Silobreaker, Sixgill etc)
- Va permite dezvoltarea (generarea) de indicatori TI (Threat Intelligence)
- Va fi instalat on premise
- Va afișa toate informațiile cunoscute și relevante aferente unui Indicator de compromitere (IoC) selectat/introdus, inclusiv scorul asociat, etichete, sursele în care este referențiat, URL-uri de referință, buletine de tip threat intelligence, campanii și alte IoC-uri asociate
- Va permite consum de TI din multiple surse fără a se limita la un produs sau producător
- Va permite clasificarea TI după tip și identificarea relevanței TI

- Va permite corelarea între fluxurile de date relevante, cum ar fi IoC-uri, campanii, actori și TTP-uri
- Va furniza automat un scor de încredere pentru IoC-uri noi fără a fi necesară o configurare manuală
- Va oferi analistului posibilitatea de a seta scoruri de încredere definite manual în plus față de scorurile de încredere derivate din analiza automată. Analistul va putea alege între cele două variante (scor manual/scor automat) pentru fiecare flux (feed) de informații în parte
- Va seta în mod automat o durată de viață pentru indicatori
- Va oferi capacitatea de a importa informații/date în sistem din interfața grafică, în următoarele formate: CSV, JSON sau XML
- Va oferi capacitatea de a importa informații/date în sistem printr-un API, în format JSON
- Va parsa informațiile dintr-o formă nestructurată a datelor provenite dintr-o altă sursă. Soluția trebuie să normalizeze datele de intrare într-un format structurat
- Va suporta parsarea informațiilor din rapoarte nestructurate trimise prin email către o căsuță de email dedicată la care soluția are acces
- Va oferi posibilitatea de a parsa automat indicatori de compromitere dintr-un e-mail de tip phishing trimis la o adresa de email dedicata
- Va oferi STIX / TAXII pentru interacțiunea cu alte soluții de CTI
- Va permite deduplicarea datelor colectate
- Va trebui să contextualizeze în mod automat orice IoC cu date precum:
    - site-uri de reputație
    - DNS pasiv
    - WHOIS
    - coordonate geografice
    - orice alte surse contextuale disponibile (ex: dacă un domeniu este DNS dinamic, dacă este găzduit de o platformă de tip hosting partajată, dacă este sinkhole, etc).
- Va permite crearea de integrări personalizate pentru fluxuri și contextualizare a datelor prin intermediul unor SDK/API-uri documentate.

- Va oferi o gamă largă de fluxuri OSINT fără costuri suplimentare și fără să fie nevoie de personalizare sau configurare.
- Va oferi capabilitatea de a direcționa automat informațiile către un sistem de securitate relevant, cum ar fi produsul SIEM, și să permită filtrarea indicatorilor pe baza unui scor automat de încredere, fără a fi necesară intervenția umană.
- Va permite filtrarea output-ului pentru a minimiza TI nedorit (filtrare înainte de export)
- Va permite analistului inserarea de comentarii pe marginea amenințărilor, a indicatorilor sau a buletinelor de amenințare în scopul întregirii informațiilor disponibile.
- Va permite crearea de legături între un indicator și alte date specifice, precum threat actor sau informații referitoare la campanie.
- Va permite import de tipuri date de tip TI atât structurate cât și nestructurate
- Va permite consolidarea și expunerea atributelor din feed-urile de TI
- Va oferi capabilități de "enrichment" de date din alte surse (ex: VirusTotal, Domain Tools)
- Va oferi deduplicarea de TI din surse multiple
- Va oferi posibilitatea alocării datelor TI de indicatori de severitate și nivel de încredere al sursei
- Va avea un mecanism de categorisire și verificare a valabilității indicatorilor
- Va permite asocierea de surse multiple cu un singur indicator
- Va permite marcarea cu un timestamp (ultima apariție) a indicatorilor de tip TI pentru a identifica relevanța în funcție de durata de viată a acestora
- Va oferi capabilități de ajustare manuală a scorului indicatorilor TI
- Va permite definirea manuală a perioadei de expirare a indicatorilor
- Va pune la dispoziție un API care să permită importul de indicatori TI

- Va pune la dispoziție un API care permită extragerea informațiilor de tip TI, atât din instanța SaaS administrată de producătorul soluției, cât și din instanța on prem, aflată în locația CERT-RO. Soluția trebuie să permită filtrarea informațiilor de tip TI extrase după tipul informației, data colectării etc astfel încât să fie redusă cantitatea informației exportate
- Va permite adăugare de TI prin formate multiple precum CSV, PDF, TXT, ZIP (fișiere CSV, PDF, TXT arhivate), HTTP, EMAIL etc
- Va permite inserarea de feed-uri custom
- Va fi compatibil cu formatele și protocoalele utilizate în partajarea indicatorilor TI (ex. CybOX/STIX/TAXII)
- Va permite integrarea cu platforme comune de threat sharing (ex: MISP, Soltra)
- Va avea capabilitatea de a primi alerte de corelare (matches) pentru IoC-urile monitorizate raportate de SIEM și va furniza statistici și analize ale acestor alerte în interfața de utilizare a soluției.
- Va putea identifica și corela documentele de referință și informațiile despre amenințări în cazul oricărui indicator de compromitere (IoC).
- Va trebui să permită căutări parțiale ale indicatorului / căutări wildcard.
- Va putea corela în mod automat jurnalele istorice (log-uri) de la soluția SIEM cu IoC-urile din platforma de threat intelligence.
- Va permite recepționarea feed-urilor externe cu informații privitoare la amenințări și corelarea acestora cu informațiile provenite din infrastructura internă, pentru a detecta indicatori de compromitere (IoC).
- Va permite integrare bidirecțională cu platforme SIEM
- Va dispune de posibilități de generare de rapoarte (manual/automat)
- Va oferi dashboard-uri pentru urmărirea datelor și evenimentelor
- Va include o componentă on-premise care să asigure deținerea fizică a oricăror date private folosite de organizație. Componenta on-premise va fi instalată într-o rețea privată a beneficiarului.
- Va include și o componentă SaaS, disponibilă beneficiarului sub forma unei aplicații sau portal web, care să administreze și să gestioneze toate operațiunile de colectare, agregare și procesare de informații provenite din OSINT și soluții de

securitate terțe, fără un efort de management semnificativ de gestionare din partea beneficiarului.

- Va parsa informații nestructurate din pagini web, cum ar fi articole de știri, bloguri, platforme de socializare pentru a identifica actorii, familiile de malware și tehnicile de atac.
- IOC-urile colectate vor putea fi importate în platformă pentru analize și investigații ulterioare și vor fi comparate automat cu evenimentele și jurnalele din rețea pentru a identifica o potențială compromitere.
- Soluția va fi scalabilă și va fi integrată funcțional în platforma ROSAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)
- Soluția va permite exportarea manuală și automatizată a informațiilor colectate către alte baze de date
- Soluția trebuie să ofere posibilitatea de a limita și controla în mod granular accesul utilizatorilor la diferite funcții și obiecte.
- Soluția trebuie să ofere mijloace prin care un administrator de sistem să poată configura și gestiona utilizatorii.
- Soluția trebuie să poată fi accesată de cel puțin 3 utilizatori simultan.

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care modulul "Cyber Threat Intelligence" ofertat va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

9.3.1.7 Modulul colectare, normalizare și îmbogățire

Modulul colectare, normalizare și îmbogățire este responsabil de corelarea și analiza datelor colectate la nivelul platformei. Practic alertele sunt normalizate, standardizate și îmbogățite cu detaliile lipsă, fiind transpuse într-o bază de date, structurată conform nevoilor interne, pentru a simplifica regăsirea datelor, analiza acestora precum și identificarea anumitor corelații între atacuri.

Structura internă a bazei de date va permite importul datelor în format internațional Structured Threat Information Expression - STIX (format utilizat pentru schimbul de date despre incidentele de securitate cibernetică). Pentru operațiunile de normalizare/ clasificare/ enrichment (îmbogățire) vor fi avute în vedere următoarele:

- pentru zona de ***normalizare*** va fi urmărit modul în care pot fi creați indecșii precum și metodele de normalizare ce ar putea fi utilizate pentru fiecare tip de alertă colectată cu accent pe modul în care procesul de normalizare poate fi gestionat la nivel de utilizator;
- pentru operația/zona de ***clasificare*** va fi urmărit modul în care se pot clasifica alertele pe categorii de vulnerabilități și de risc a informațiilor clasificate. Va fi avută în vedere o taxonomie care să poată fi modificată/actualizată de către operatori în funcție de evoluția vulnerabilităților și riscurilor la nivel global;
- pentru operația de ***"enrichment"*** se va ține cont de modul în care se pot completa informațiile colectate cu date privind locația geografică și reputația, ASN, etc.

Furnizorul va oferta un modul care să permită realizarea funcționalităților descrise mai sus. Caracteristicile tehnice minimale ale modulului ce va fi ofertat sunt următoarele:

- Va asigura colectarea de la diferite surse, în formate multiple
- Va asigura translatarea datelor colectate într-un format personalizat
- Va asigura îmbogățirea datelor cu informațiile lipsă cu scopul simplificării regăsirii datelor, analiza acestora precum și identificarea anumitor corelații
- Va asigura integrarea cu modulele platformei ce vor genera date/informații ce necesită normalizare și îmbogățire (de ex. adăugarea de informații privind locația geografică și reputația, ASN etc)

- Va asigura transferul datelor colectate, normalizate și îmbogățite către modulul "Big Data Security Analytics"
- Soluția va fi scalabilă și va fi integrată funcțional în platforma ROSAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)

NOTĂ: Sursele principale de date ce vor trebui colectate, normalizate și îmbogățite sunt următoarele:

- Log-uri/evenimente/alerte echipamente și soluții hardware și software pe care va fi implementată platforma RO-SAT. Infrastructura pe care va fi implementată platforma conține următoarele tipuri de soluții și echipamente:
  - Firewall
  - ProxyWeb
  - ProxyEmail
  - WAF
  - Sandbox
  - Antivirus
- Sisteme de operare de tip Windows și Linux
- Log-urile modulului Darknet
- Log-urile modulului HoneyNet
- Datele obținute în urma scanărilor automatizate de vulnerabilități
- Datele obținute în urma scanărilor automatizate a website-urilor (crawling website-uri)
- Date extrase și agregate automat cu ajutorul modulului OSINT
- Date de tip Cyber Threat Intelligence extrase automat din feed-uri comerciale și feed-uri publice
- Log-uri colectate de la senzorii SOC

NOTĂ: Datele colectate vor fi îmbogățite cel puțin cu următoarele tipuri de informații: **GeoIP, subnet IP, deținător, adresă email abuse, ASN, DNS Name/domenii asignate IP-urilor, țară asignată, zonă/localitate, reputație IP/URL** (bazat pe CTI colectate/disponibile prin intermediul platformei RO-SAT), scor (acesta va fi definit la momentul adaptării proiectului/planului de instalare propus inițial de furnizor cu ajutorul Autorității Contractante). Ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această îmbogățire și soluțiile tehnice/serviciile ce vor fi utilizate pentru obținerea informațiilor ce vor fi utilizate pentru îmbogățire.

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care modulul "Colectare, normalizare și îmbogățire" ofertat va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;

- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

Soluția trebuie să poată funcționa și după expirarea licenței, astfel încât aceasta să permită atât administrarea cât și utilizarea, folosind actualizările de securitate și de componente descărcate înainte de expirarea licenței, cu excepția serviciilor si soluțiilor care se bazează pe informații furnizate pe bază de subscripții.

9.3.1.8 Modulul „Big Data Security Analytics"

Acest modul va utiliza tehnologii de tip Machine Learning și Artificial Intelligence pentru analiza automată a datelor colectate de modulele platformei RO-SAT într-o platformă de tip Big Data (platformă ce va fi oferită în cadrul modulului fără costuri suplimentare) precum și pentru generarea de informații despre: alerte, tendințe, tehnici de atac, unelte de atac, etc.

Obiectivul principal al acestui modul este acela de a asigura procesarea informațiilor obținute din modulele descrise anterior, astfel încât să poată fi identificate pattern-urile ce pot anticipa activități specifice pregătirii unor atacuri cibernetice sau activități specifice unor atacuri aflate în derulare, dar încă nedescoperite (nedocumentate).

Furnizorul va oferta un modul care să permită realizarea funcționalităților descrise mai sus.

Caracteristicile tehnice minimale ale modulului ce va fi ofertat sunt următoarele:

- Va pune la dispoziție o platformă de tip Big Data
- Va oferi funcționalități care să permită ingestia unui volum mare de date, și stocarea acestora pe termen lung prin utilizarea de tehnologii de tip big data
- Va oferi capabilitatea de management centralizat și monitorizarea tuturor componentelor soluției ofertate
- Va oferi acces bazat pe roluri (RBAC) pentru gestionarea drepturilor de utilizator
- Va face deduplicarea datelor ingerate
- Va oferi funcționalități de tip multi-tenant pentru managementul separat al diferiților clienți

- Va utiliza tehnologii de tip Machine Learning și Artificial Intelligence pentru analiza automată a datelor colectate și generarea de informații precum: alerte, tendințe, tehnici de atac, unelte de atac, etc
- Va oferi funcționalități care să permită interogarea și extragerea rapidă a informațiilor stocate în funcție de cerințele operaționale, punând la dispoziție tool-uri pentru explorare, analiză, vizualizare etc
- Va permite crearea de dashboard-uri personalizate (diagrame, rapoarte etc)
- Va dispune de posibilități de generare a rapoartelor (manual/automat)
- Va pune la dispoziție o interfață restAPI prin care să fie permisă introducerea/extragerea de informații din modul (cu scopul integrării celorlalte module cerute in cadrul proiectului, Honeypot, OSINT, Darknet, Vulnerability Scanning, Crawlling etc și al utilizării împreună cu alte soluții ce nu vor fi integrate în cadrul proiectului în platforma RO-SAT)
- Modulul trebuie sa asigure High Availability, cu opțiuni flexibile de păstrare și stocare a datelor
- Soluția va fi scalabilă și va fi integrată funcțional în platforma ROSAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)
- Modulul de Big Data trebuie să asigure o capacitate de ingestie a datelor de minim 2TB/zi

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanțle echipamente hardware

În cazul în care modulul "Big Data Security Analytics" ofertat va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani, în regim NBD.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

Soluția trebuie să poată funcționa și după expirarea licenței, astfel încât aceasta să permită atât administrarea cât și utilizarea, folosind actualizările de securitate și de componente descărcate înainte de expirarea licenței, cu excepția serviciilor și soluțiilor care se bazează pe informații furnizate pe bază de subscripții.

9.3.1.9 Modulul „Security Operations Center"

Acest modul va cuprinde capabilitățile de monitorizare în timp real al evenimentelor, alertelor, incidentelor pe diferite tipuri de infrastructuri esențiale (conform celor definite de Directiva NIS transpusă în Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice).

Obiectivul principal al acestui modul este acela de a furniza în timp real informații despre situațiile care necesită intervenție/reacție rapidă a echipelor specializate din cadrul CERT-RO, astfel încât să fie asigurate stoparea atacurilor cibernetice, limitarea efectelor/pierderilor, coordonarea în vederea restabilirii funcționării normale și efectuarea investigațiilor aferente.

Componentele principale sunt:

1. un sistem de afișare video a alertelor ce va fi integrat de ofertant cu platforma RO-SAT
2. o soluție de tip SOAR ce va fi integrată cu soluția SIEM (cerințele tehnice sunt specificate la punctul 9.3.2. SIEM)

NOTĂ: Autoritatea Contractantă va pune la dispoziție sistemul de afișare video

Caracteristicile tehnice minimale ale modulului ce va fi ofertat sunt următoarele:

- Soluția trebuie să permită SOC să adopte o abordare investigativă în investigarea incidentelor de securitate.
- Soluția trebuie să permită următoarele caracteristici cheie:
  a) actualizarea în permanență a contextului de business al activelor, context ce va fi pus la dispoziția analiștilor de securitate, astfel încât aceștia să poată acorda prioritate incidentelor care prezintă risc crescut pentru organizație;
  b) cadrul de colaborare și de investigare eficientă a incidentelor de securitate care să fie aliniată standardelor din industrie;

c) un cadru de lucru astfel încât atunci când un incident duce la o pierdere a datelor, organizația sa fie pregătită în avans pentru a răspunde la aceste tipuri de incidente;

d) managementul echipelor SOC pentru a rula procesul de răspuns la incidentele de securitate ca un proces de afaceri coerent și previzibil.

- Sistemul trebuie să fie agnostic și să primească alerte de la mai multe sisteme de securitate de monitorizare. Soluția ar trebui să poată primi alerte cel puțin de la soluții de tip SIEM COTS, precum Splunk, ArcSight, QRadar și RSA NetWitness.

- Soluția va permite automatizarea activităților de răspuns la incidentele de securitate cibernetică
- Soluția va permite utilizarea limbajelor de scripting Python sau JavaSript
- Soluția va permite integrarea în fluxul de automatizare cu platforme precum:
  - Instrumente de Investigații Cibernetice (de exemplu, Any.Run, CheckPoint Sandblast Appliance, CheckPoint Sandblast Cloud Services, malware, McAfee Advanced Threat Defence, Palo Alto Networks WildFire, Rekall, VMRay)
  - Platforme de comunicare (de exemplu, ActiveMQ, Cisco Webex Teams, EWS, FCM PushNotifications, Kafka)
  - Platforme SIEM

NOTĂ: Soluția oferită ar trebui să primească de asemenea alerte și de la sistemul de tip SIEM ce va fi ofertat.

  - Platforme de securitate la nivel de stație de lucru
  - Platforme de securitate la nivel de rețea
  - Active Directory (va permite extragerea următoarelor tipuri de informații: nume utilizator, nume stație de lucru, parole expirate, apartenenta la grupuri)
  - Platforme de Threat Inteligence

NOTĂ: Soluția ofertată va include cel puțin un feed PREMIUM de Threat Intelligence (ex. Accenture DeepSight, Anomali, Autofocus (Palo Alto Networks), Blueliv, Cofense, Crowdstrike, Flashpoint, Mandiant Advatage (FireEye), Fox-IT intel, Group IB, Intel 471, Proofpoint, Silobreaker, Sixgill). Acesta va fi un feed Premium diferit de cel oferit la punctul *9.3.1.6 Modulul „Cyber Threat Intelligence"* și nu poate fi un feed disponibil gratuit.

  - Platforme de analiza malware

- Soluția va pune la dispoziția administratorilor o modalitate facilă de a defini noi scripturi și integrări, în afară de cele disponibile pe platformă
- Soluția va oferi scenarii de acțiuni (playbooks) și cazuri de utilizare pre-configurate, permițând configurarea de noi scenarii într-un mod facil prin intermediul unui editor grafic disponibil în interfața grafică. Definirea de noi scenarii se va putea face de la

zero, prin modificarea scenariilor pre-configurate, sau prin folosirea de porțiuni din scenarii pre-configurate.
Scenariile de acțiuni (playbooks) vor permite definirea a următoarelor tipuri de acțiuni:

- acțiuni manuale
- acțiuni automate
- aplicare de filtre
- apelarea altor scenarii
- colectare de date
- acțiuni condiționale

- Soluția va permite rularea atât manuală a scenariilor de acțiuni, cât și automată ca urmare a identificării unui incident în cadrul platformei
- Soluția va permite documentarea automată a evenimentelor și va include detalii cu privire la desfășurarea scenariilor de acțiuni (playbooks) precum și acțiunile analiștilor legate de scenariile respective. Soluția va oferi o secțiune dedicată în interfața grafică unde vor fi prezentate aceste informații.
- Soluția va permite vizualizarea din interfața grafică a acțiunilor detaliate realizate în cadrul unui scenariu de acțiuni
- Soluția va permite asocierea activităților din cadrul unui scenariu de activități unor analiști specifici în baza rolurilor definite la nivelul platformei
- Soluția va permite repornirea unui scenariu de acțiuni din punctul în care a generat eroare sau necesită informații externe
- Soluția va permite analiștilor să intervină în fluxul unui scenariu de acțiuni cu acțiuni ad-hoc
- Soluția va permite rularea de acțiuni și a scenariilor de acțiuni (playbooks) în baza unei programări prealabile
- Soluția va permite vizualizarea istorică a activităților realizate în cadrul scenariilor de acțiuni
- Soluția va pune la dispoziția utilizatorilor un sistem de ticketing. Totodată soluția va permite integrarea cu platforme de ticketing dedicate (ex. Jira, RSA Archer, ServiceNow)
- Soluția va permite alocarea unui incident unui grup de utilizatori specifici
- Soluția va permite definirea unor timpi de răspuns (SLA) pentru evenimente specifice.
- Soluția va permite notificarea utilizatorilor în urma rulării unui scenariu de acțiuni. Notificările vor putea fi trimise prin integrarea cu platforme de tipul Okta, Slack și email
- Soluția va permite gruparea incidentelor similare în baza datelor analizate în fluxul de investigații
- Soluția va permite definirea de elemente personalizate pentru managementul incidentelor precum:
  - tipuri de incidente personalizate
  - etichete personalizate pentru incidente
  - tipuri de indicatori personalizați
  - etichete personalizate pentru indicatori

- dashboard-uri personalizate
- rapoarte personalizate

• Soluția va permite agregarea de informații din investigații anterioare
• Soluția va permite identificare de alerte redundante și gruparea acestora într-un singur ticket de incident
• Soluția va permite procesarea automată a incidentelor în baza unor fluxuri de lucru definite din interfața grafică
• Soluția va permite documentarea detaliată a incidentelor, a dovezilor identificate în urma investigațiilor, a acțiunilor utilizatorilor și a indicatorilor de compromis
• Soluția va pune la dispoziție un mecanism colaborativ care să permită interacțiunea în timp real între utilizatorii care participă la investigații
• Soluția va permite integrarea cu platforme externe colaborative care să permită interacțiunea în timp real între utilizatori
• Soluția va permite definirea de scenarii de acțiuni de tipul threat hunting pentru identificarea unor indicatori de compromis stocați local
• Soluția va permite importul de fișiere de tipul STIX, Yara, XML, CSV, JSON
• Soluția va permite exportul indicatorilor în format STIX
• Soluția va permite instalarea atât on-premise cât și în cloud
• Soluția va permite definirea de utilizatori și de roluri de utilizatori. Rolurile de utilizatori vor permite asocierea de drepturi granulare asupra zonelor diverse din platformă
• Soluția va permite definirea de integrări personalizate cu platforme terțe.
• Soluția va oferi rapoarte predefinite, disponibile în formate precum: PDF, DOC, CSV
• Soluția va permite definirea de rapoarte personalizate
• Soluția va folosi mecanisme de tip machine learning în scenarii precum:
  - Identificarea incidentelor corelate
  - Identificarea activităților următoare în baza analizei activităților istorice
  - Sugerarea analiștilor care să participe la investigații
• Soluția va permite integrarea de surse multiple de feed-uri de vulnerabilități, atât comerciale cât și de tipul "open source"
• Soluția va permite autentificarea utilizatorilor prin următoarele modalități: SAML, Active Directory, sau alte tehnologii cunoscute
• Soluția va putea fi instalată într-o configurație de tipul multi-tenant. În această configurație utilizatorii vor avea acces doar la datele lor, fără a avea posibilitate de a vizualiza datele altor utilizatori.

- Soluția va permite căutarea, prin intermediul interfeței grafice, a indicatorilor de compromis în baza etichetelor asociate, a stării acestora sau a tipului de indicator
- Soluția va permite integrarea de surse de vulnerabilități în format de date structurate (ex. JSON, CSV, STIX 1.x sau STIX 2.x) cât și nestructurate (e-mail sau RSS feeds)
- Sistemul trebuie să fie capabil să integreze surse externe de date și să le transforme în alerte pentru investigații ulterioare.
- Soluția trebuie să aibă opțiunea de a crea alerte manual.
- Soluția trebuie să se poată integra cu furnizorii de conținut
- Soluția trebuie să includă cel puțin următoarele proceduri de răspuns (playbook-uri):
    a) procedură pentru anomalii în conexiuni VPN;
    b) procedură pentru nepotrivire a protocolului și a portului;
    c) procedură Keylogger;
    d) procedură de scanare internă a porturilor;
    e) procedură de scanare externă a porturilor;
    f) procedură privind instrumente folosite de atacatori;
    g) procedură generală de detectare a malware-ului;
    h) procedură Exploit Kit;
    i) procedură email phishing;
    j) procedură investigare malware și oprire malware (containment);
    k) procedură DDOS;
    l) procedură Threat Hunting

NOTĂ: Procedurile de răspuns (playbook-uri) ce nu sunt incluse implicit în soluția ofertată vor fi dezvoltate de către ofertant pe perioada implementării soluției

- Soluția trebuie să poată fi utilizată de către operatori numai prin intermediul unei interfețe WEB.
- Soluția trebuie să aibă fluxuri de lucru predefinite pentru gestionarea unor tipuri diverse de incidente de securitate.
- Soluția trebuie să aibă diferite opțiuni de stare pentru un incident (New, Assigned, In Progress, Escalated, Resolved, Invalid).
- Soluția trebuie să aibă utilizatori predefiniți și roluri pentru gestionarea incidentelor de securitate.
- Sistemul trebuie să includă managementul centralizat al incidentelor pentru gestionarea tuturor alertelor de la instrumentele de monitorizare a securității care necesită revizuirea și triajul de către analiștii SOC.
- Procedurile de răspuns existente trebuie să poată fi importate și utilizate în soluție.
- Incidentele trebuie să fie mapate structurii organizatorice (active, facilități, procese interne etc.).

- Procedurile de intervenție în caz de incidente trebuie să poată fi gestionate în sistem.
- Procedurile de intervenție în caz de incidente trebuie să fie mapate automat la un incident bazat pe categoria acestuia.
- Sistemul trebuie să furnizeze analiza de tip „root cause" pentru investigații suplimentare și raportarea către management.
- Sistemul va trebui să aibă capabilități granulare de control al accesului bazate pe roluri (RBAC).
- Soluția trebuie să agrege alerte similare într-un singur incident.
- Sistemul trebuie să furnizeze statutul înregistrării incidentului care poate fi modificată în timpul procesului de lucru.
- Soluția va trebui să aibă funcționalități de raportare la momentul predării activității către tura următoare (workshift) pentru a furniza un rezumat al incidentelor închise, incidentele care necesită încă o monitorizare și orice alte informații.
- Soluția va dispune de cel puțin capacitatea de a colecta alerte de securitate prin intermediul mesajelor syslog.
- Soluția trebuie să aibă capacități de raportare. Sistemul va dispune de rapoarte integrate care pot fi modificate de utilizatorii finali.
- Soluția trebuie să aibă capacități pentru afișarea unor panouri de bord (dashboards), care pot fi modificate de utilizatorul final.
- Soluția trebuie să includă roluri de utilizatori diferite:

  a) SOC Manager;

  b) Incident Coordinator;

  c) L1 Handler de incidente;

  d) L2 Handler de incidente;

  e) IT Helpdesk Analyst;

  f) Manager de răspuns la incidente.

- Soluția trebuie să poată urmări toate politicile de securitate, controalele și măsurarea eficienței controalelor de securitate în SOC.
- Soluția ar trebui să aibă capacitatea de a se integra cu sistemele de gestionare a incidentelor IT operaționale.
- Soluția trebuie să aibă opțiuni de remediere cum ar fi: Crearea unui nou plan de remediere.
- Sistemul trebuie să permită documentarea proceselor standard și procedurilor care sunt urmate când se produce incidentul.
- Sistemul trebuie să dispună de chestionare de evaluare a riscurilor și de impact asupra mediului IT.
- Soluția trebuie să aibă capacitatea de a importa contexte (cum ar fi active IT, date personale, identități și impactului asupra echipamentelor și aplicațiilor critice) și informațiile despre

amenințările cibernetice (cum ar fi vectorii de atac cunoscuți și domeniile C2).

- Soluția trebuie să monitorizeze cozi de incidente pentru a se asigura că departamentul SOC își îndeplinește SLA-urile, cum ar fi MTTR (timpul mediu de soluționare) pentru incidentele de securitate.
- Baza de date a sistemului nu va necesita abilități de administrare specializate. Baza de date trebuie să fie scalabilă pentru a sprijini organizațiile de orice dimensiune.
- Sistemul să poată exporta informații către alte baze de date, depozite.
- Sistemul să ofere o metodă ușoară de încărcare a datelor privind activele pentru importurile de date unice.
- Sistemul trebuie să aibă o metodă integrată pentru a construi importuri de date programate cu sisteme externe de gestionare a activelor sau sisteme de înregistrări cu codificare minima.
- Furnizorul trebuie să ofere instruire pentru soluția ofertată.
- Soluția va fi disponibilă pentru minim 4 analiști
- Soluția va fi scalabilă și va fi integrată funcțional în platforma RO-SAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care modulul "Security Operations Center" ofertat va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani, în regim NBD.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

9.3.1.10 Modulul „Diseminare date" (API)

Prin intermediul modulului, datele corelate vor fi făcute disponibile partenerilor în funcție de responsabilitățile acestora (autorități publice, ISP-iști, furnizori de servicii digitale etc.) sau în baza prevederilor protocoalelor de cooperare bilaterale încheiate.

De asemenea, acest modul va intermedia accesul la serviciile ce vor fi definite și oferite prin platforma RO-SAT, respectiv:

1. alertare timpurie referitor la posibilitatea/iminența derulării unor atacuri
2. alerte de securitate referitoare la atacurile identificate/raportate

3. rapoarte referitoare la nivelul de amenințare cibernetică
4. statistici de securitate
5. indicatori de compromitere (IoC) care vor putea fi preluați de beneficiari/parteneri automat și/sau manual.

Soluția va include componente precum managementul interfețelor pentru parteneri, api gateway, etc care vor trebui să ofere următoarele caracteristici tehnice minime:

- Soluția trebuie să administreze API-ul pe toată durata ciclului de viață
- Soluția trebuie să permită scalare rapidă și ușoară a serviciilor expuse
- Soluția trebuie să ofere o interfață de tip portal prin care se poate face administrare de servicii web precum: definire serviciu web, actualizare și ștergere serviciu web, cerere acces pentru serviciu web
- Soluția trebuie să permită operația de translatare/mutare (ex. import/export) a politicilor de acces între mediile instalate (de la mediul de test la mediul de producție)
- Soluția trebuie să ofere capabilitatea de a compune și virtualiza API-urile
- Soluția trebuie să suporte Web Service Definition Language (WSDL) sau servicii web de tip REST
- Soluția propusă trebuie să definească politici de autentificarea și autorizare a accesului la servicii
- Soluția propusă trebuie să permită conversia XML/JSON JSON; transformarea XML/JSON JSON trebuie să fie bidirecțională - XML/JSON JSON și JSON XML/JSON
- Pentru securitatea comunicării, soluția trebuie să ofere următoarele funcționalități:
    - Controlul accesului la nivel aplicație
    - Suport pentru protocolul Secure Socket Layer (SSL) si certificate compatibile X.509
    - Suport pentru standarde deschise de control al accesului specifice serviciilor web. În funcție de tehnologia utilizată

pentru implementarea API-urilor acestea pot să includă : WS-Security, WSSecurityPolicy, XML/JSON Encryption, XML/JSON Signature, Security Assertation Markup Language (SAML), OpenID Connect.

o Transportul mesajelor XML/JSON trebuie să fie securizat (canal de comunicare criptat)

- Soluția trebuie să asigure un mod de funcționare de tip gateway fără modificarea serviciilor protejate
- Soluția trebuie să asigure definirea declarativă a politicilor de access utilizând un instrument de configurare pe baza unor primitive de activități de acces pre-definite sau personalizate
- Definirea declarativă a politicilor de acces trebuie să fie făcută utilizând o consola web-based.
- Soluția trebuie să permită auditarea selectivă a apelurilor servicii web
- Soluția va oferi capabilități de WS/API firewall și funcții de control acces pe baza de politici de acces de tip RBAC
- Soluția trebuie să permită detectarea de vulnerabilități de genul SQL-injection sau XPATH-injections
- Soluția trebuie să poată limita numărul de mesaje pe o perioadă de timp
- Soluția trebuie să poată limita numărul de conexiuni concurente către un anumit serviciu web expus
- Soluția trebuie să poată preveni atacuri de tip "replay":mesaj autentic cu credențiale valide repetat de foarte multe ori
- Soluția trebuie să aibă posibilitatea ștergerii, înlocuirii, criptării, tokenizării sau mascării de date confidențiale
- Soluția ofertată trebuie să permită detecția și mascarea datelor cu caracter personal cel puțin pentru următoarele tipuri de date structurate: Oracle, SQL Server, PostgreSQL, Sybase, DB2, MySql
- Soluția ofertată trebuie să permită mascarea datelor prin intermediul serviciilor web puse la dispoziție de producător

- Soluția trebuie să permită mascarea datelor în funcție de privilegiile utilizatorului ce accesează datele
- Soluția trebuie sa monitorizeze tranzacțiile în timp real și să permită vizualizarea statisticilor aferente
- Soluția trebuie să aibă un mecanism de alertare în cazul detectării de activități/interogări cu un volum anormal de date
- Soluția trebuie să poată oferi suport pentru criptarea/decriptarea mesajelor XML/JSON.
- Soluția trebuie să poată monitoriza și alerta în cazul în care unul sau mai multe servicii API expuse au o performanță deteriorată, sub nivelul unei limite pentru: timp de răspuns sau număr de reîncercări
- Soluția să permită prioritizarea cererilor venite de la clienți pe baza clientului, utilizatorului si atribute de servicii.
- Soluția trebuie să ofere posibilitatea de vizualizare și monitorizare a modului in care politicile de acces sunt respectate
- Soluția trebuie să ofere posibilitatea auditării cererilor și a răspunsurilor precum și a mesajelor de autentificare/autorizare.
- Soluția trebuie să se integreze ușor cu software de autentificare utilizatori
- Soluția trebuie să fie compatibilă cu standardul SAML pentru integrări cu alte produse
- Platforma tehnologică va include module care să permită citirea de date din servere de baze de date, Microsoft Sharepoint
- Soluția trebuie să implementeze tehnologiile și standardele SOA Simple Orchestration, SOA Mediation, XAMCL, WS-* sau tehnologii și standarde deschise care să permită implementarea de funcționalități similare (ex. orchestrare, mediere, transformare de date) utilizând microservicii și API-uri REST.
- Soluția trebuie să permită utilizarea websocket, XMPP, precum și Oauth, OpenID Connect pentru autentificare.
- Soluția trebuie să includă mecanisme care să permită definirea de servicii web sau API-uri REST, precum și documentarea acestora, pentru aplicații care nu au aceste funcționalități implementate.

- Soluția trebuie să permită scalarea rapidă și ușoară a serviciilor expuse pentru îmbunătățirea rapidă a performanțelor pentru perioade când se așteaptă ca traficul generat să fie intens
- Soluția trebuie să ofere posibilitatea de a integra soluții de tipul 2-factor authentication, OTP
- Componentele modulului trebuie să ruleze pe cel puțin una din distribuțiile majore de sisteme de operare prezente pe piață (Windows, Linux, Unix)
- Soluția va permite implementarea de funcționalități tip balansare a încărcării de procesare și optimizare pentru nivelele OSI Layer 4 și Layer 7 utilizând IPv4 și IPv6
- Soluția va trebui să ofere optimizarea traficului generat pe nivelul OSI Layer 7, incluzând funcționalități native pentru rolul: load-balancer pentru următoarele protocoale: HTTP/1.1, HTTP/2, HTTPS, FTP/FTPS, RADIUS inclusiv asigurarea de conexiuni multiple paralele (connection multiplexing pools) pentru îmbunătățirea transferului de date HTTP/HTTPS, permițând compresia dinamică în funcție de conținut și HTTP Caching
- Soluția va trebui să asigure următoarele funcționalități privind securitatea:
    - Posibilitatea implementării de politici în ceea ce privește banda utilizată, numărul de conexiuni și tipul solicitării (request-policy) pentru serviciile bazate pe HTTP/HTTPS
    - Posibilitatea asigurării funcționalităților de proxy pentru solicitările ce necesită autentificare tip NTLM
    - Posibilitatea implementării de funcționalități legate de limitarea numărului de cereri către serverele web
    - Posibilitatea implementării de funcționalități suplimentare de securizare a serverelor împotriva atacurilor web (SQL injection, cross-site scripting, alterarea de cookie-uri, HTTP RFC compliance)
- Soluția va permite identificarea și blocarea a cel puțin următoarelor tipuri de atacuri: SQL injection, Cross-site scripting

(XSS), Cross-Site-Request-Forgery (CSRF), Parameter tampering,Hidden-field manipulation, Session manipulation,Cookie poisoning, Stealth commanding, Backdoor and debug options, Application-buffer-overflow attacks, Brute-force attacks, Data encoding, Unauthorized navigation, SOAP- and Web-services manipulation, Web Scraping

- Soluția va implementa un mecanism de generare automată a politicilor de securitate. Acest mecanism va permite identificarea și blocarea inclusiv a atacurilor de tipul zero-day
- Soluția va permite implementarea atât a modelului negativ de securitate cât și a celui pozitiv (soluția va învăța sau va permite definirea de reguli ce vor descrie comportamentul legitim al unei aplicații sau al unui serviciu)
- Soluția va permite învățarea schemelor și structurilor XML și JSON pentru securizarea acestora
- Soluția va trebui să asigure funcționalități integrate de administrare și procesare SSL/TLS incluzând minim următoarele protocoale: SSL, SNI, TLSv1.1 și TLSv1.2, precum și funcționalități de criptare SSL – SSL Offloading și SSL Forward Proxy
- Soluția va trebui să permită implementarea a cel puțin următoarelor funcționalități de balansare:
    - o Specific OSI Layer 7 pentru rolurile: reverse-proxy și load-balancer asigurând minim următorii algoritmi de balansare: Round Robin, Weighted Round Robin, Least Connections, Least Time, Hash, IP Hash
    - o Să asigure persistența conexiunilor utilizând minim următorii algoritmi: Cookie-Insert, Session- Learn și metode de rute definite (IP sursa și parametru URL) si
    - o HTTP Caching
- Soluția va trebui să permită implementarea reverse-proxy asigurând nativ funcționalitățile de rutare în funcție de conținut și content rewriteing (URL/URI content request routing)
- Soluția va trebui să permită utilizarea echipamentului pentru aplicatii multiple prin divizarea logică pentru fiecare din site-urile

publicate pentru un număr minim de 2 Virtual Domains, fără a fi necesara licentierea suplimentara a platformei.

- Solutia va permite configurarea a minim 10 contexte virtuale prin licențiere suplimentară
- Soluția trebuie să permită implementarea de mecanisme de optimizare, accelerare, caching și compresie pentru aplicațiile monitorizate
- Soluția trebuie sa permită balansarea si optimizarea traficului la nivelul conexiunilor fizice pentru a asigura disponibilitate serviciilor protejate. Soluția va permite implementarea de protocoale de rutare dinamice, cel puțin RIP2, OSPF, BGP
- Platforma va permite gestionarea unui trafic de minim 6 Gbps. Aceasta va aloca resurse componentelor ei conform configurațiilor realizate de administrator, astfel încât sa otere capacitatea necesara de procesare pentru traficul gestionat/monitorizat (minim 6Gbps)
- Soluția va fi scalabilă și va fi integrată funcțional în platforma RO-SAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)

Modulul "Diseminare date" se va baza pe o arhitectură scalabilă și va include funcționalități specifice pentru implementarea și expunerea serviciilor web, translatarea datelor și trimiterea/extragerea de informații (alerte de securitate, indicatori de compromitere (IoC), etc) către/de către partenerii CERT-RO prin utilizarea de canale securizate.

Implementarea serviciilor se va baza pe standarde deschise - ex. HTTP/HTTPS, JSON, XML, REST, OpenID. Platforma utilizată pentru implementarea serviciilor trebuie să permită definirea de apeluri REST sincrone și asincrone.

Tehnologiile utilizate trebuie să ofere suport pentru integrarea cu baze de date de tip SQL si NoSQL.

Furnizorul va pune la dispoziție formulare web prin intermediul cărora beneficiarii platformei RO-SAT vor completa informații precum: ip-uri, domenii/url-uri proprii, domeniul de activitate, etc (menționăm că aceste informații sunt informațiile ce vor fi solicitate minimal unui beneficiar; la momentul adaptării proiectului/planului de instalare propus inițial de

furnizor vor fi stabilite toate informațiile ce vor fi completate de un beneficiar). Pe baza acestor tipuri informații furnizorul va defini și realiza fluxuri de automatizare a scanărilor de vulnerabilități și a scanărilor de website-uri/url-uri și va furniza manual/automatizat informații relevante pentru fiecare beneficiar.

Furnizorul va pune la dispoziție de asemenea și formularele de înrolare a beneficiarilor platformei și formularele de gestionare a beneficiarilor platformei.

Suplimentar furnizorul va pune la dispoziție formulare prin care va permite consultarea și extragerea manuală din platforma RO-SAT, de către beneficiari, a informațiilor relevante (IOC-uri, alerte de securitate, etc) aferente informațiilor introduse de beneficiari (ip-uri, domenii/url-uri proprii, domeniul de activitate, etc). De asemenea, furnizorul va utiliza modulul API propus pentru a permite unui beneficiar extragerea automatizată a informațiilor relevante pentru acesta. Extragerea automatizată se va face în funcție de criterii ce vor fi definite la momentul adaptării proiectului/planului de instalare propus inițial de furnizor. Dintre criterii menționăm:

- ip-uri
- domenii/url-uri proprii - domeniul de activitate
- timestamp informații
- etc

NOTĂ: informațiile ce vor fi extrase manual/automatizat vor fi furnizate la alegere beneficiarului în format JSON, CSV sau TEXT. Extragerea informațiilor va fi permisă numai după autentificarea beneficiarului.

Modulul API va fi utilizat și pentru transmiterea automatizată către beneficiari prin email a unor alerte. Fluxurile de lucru și informațiile care vor fi transmise prin email vor fi de asemenea corelate/îmbunătățite la momentul adaptării proiectului/planului de instalare propus inițial de furnizor și vor trebui implementate de furnizor la nivelul platformei RO-SAT.

La nivel centralizat modulul API va trebui să permită extragerea de informații de către operatorii platformei RO-SAT. Extragerea de informații se va face fie manual, prin intermediul unor formulare ce vor fi realizate de către furnizor, fie automatizat prin utilizarea directă a interfeței API. Utilizarea modului API se va face după autentificarea operatorului. Furnizorul va trebui să definească și să realizeze aceste funcționalități. Informațiile ce vor fi extrase manual/automatizat vor fi furnizate la alegere în format JSON, CSV și TEXT și vor putea fi filtrate după criterii similare celor definite pentru beneficiarii platformei.

Prin intermediul modulului API se va crea automatizat un feed ce va fi pus la dispoziția senzorilor SOC. De asemenea, pentru a reduce încărcarea bazei de date din punct de vedere al procesării, vor fi create automatizat

feed-uri ce vor fi puse la dispoziția beneficiarilor platformei RO-SAT. Beneficiarul va putea selecta în formularul de management al contului feed-urile la care dorește să aibă acces și va putea descărca prin intermediul API-ului aceste feed-uri. Conținutul feed-urilor și fluxul de lucru va fi stabilit la momentul adaptării proiectului/planului de instalare propus inițial de furnizor. Furnizorul va trebui să implementeze în platforma RO-SAT fluxurile conform proiectului/planului de instalare final.

De asemenea la momentul actualizării proiectului/planului de instalare vor fi definite fluxurile de lucru pentru furnizarea de feed-uri de date în regim public, iar la momentul realizării platformei RO-SAT furnizorul va implementa funcționalitățile stabilite.

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care modulul „Diseminare date" (API) ofertat va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani, în regim NBD.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

Soluția trebuie să poată funcționa și după expirarea licenței, astfel încât aceasta să permită atât administrarea cât și utilizarea, folosind actualizările de securitate și de componente descărcate înainte de expirarea licenței, cu excepția serviciilor si soluțiilor care se bazează pe informații furnizate pe bază de subscripții.

9.3.2 SIEM

1. **Obiectul achiziției:** SIEM
2. **Valoare totală estimată :** 4.000.000 lei fără TVA

RO-SAT va colecta, din surse multiple, date despre sisteme informatice din România implicate sau posibil implicate în diverse incidente de securitate cibernetică, respectiv: adrese IP, servere DNS, adrese de email, servicii oferite în internet, date despre diverse conexiuni sau capturi din traficul realizat, mostre de malware, vulnerabilități specifice etc. Sistemul trebuie să fie capabil să structureze toate datele pentru a le păstra într-o formă coerentă ce poate fi ușor interogată prin intermediul aceluiași sistem.

Suplimentar în soluția SIEM vor fi colectate și evidențiate separat alertele aferente soluțiilor hardware și software achiziționate pentru realizarea platformei RO-SAT (firewall-uri, routere, switch-uri etc). În mod similar vor fi colectate și evidențiate alertele primite de la senzorii SOC instalați de CERT-RO în cadrul proiectului.

NOTĂ: Implementarea soluției SIEM va fi făcută astfel încât să poată fi asigurată continuitatea serviciilor prin intermediul unui centru de recuperare în caz de dezastru.

Pentru îndeplinirea tuturor funcționalităților cerute, soluția SIEM poate fi compusa din mai multe module.

NOTĂ: Soluția SIEM propusă pentru sistemul RO-SAT trebuie să fie COTS

Soluția SIEM va trebui să ofere următoarele caracteristici tehnice minime:

- Soluția trebuie să asigure monitorizarea log-urilor și a traficului de rețea în timp real.
- Soluția se bazează pe o arhitectură de tip "big data lake"
- Soluția trebuie sa ofere posibilitatea colectării de log-uri si a traficului de rețea, iar arhitectura de stocare sa suporte stocarea datelor
- Soluția trebuie să ofere răspuns rapid/instantaneu la căutare și filtrare datorită arhitecturii platformei de tip big data
- Soluția trebuie să aibă posibilitatea de a face deduplicare la datele ingerate
- Soluția trebuie să ofere prin intermediul unei console centrale vizibilitate unificată asupra întregii infrastructuri de comunicații prin agregarea datelor primite pe baza log-urilor de la diferite sisteme, precum și detecția rapidă a incidentelor de securitate
- Soluția trebuie să ofere posibilitatea criptării transmisiei datelor între componente
- Soluția trebuie să garanteze integritatea informațiilor colectate
- Soluția trebuie să fie scalabilă și să acopere o gamă largă de implementări, de la medii mici până la medii distribuite. Soluția trebuie să aibă opțiunea de a adăuga componente fără a fi nevoie de înlocuirea hardware-ului existent, a software-ului sau a licențelor
- Soluția trebuie să ofere posibilitatea de a rula query-uri în timp real și detecția anomaliilor

- Va putea monitoriza rețele individuale sub aceeași interfață de management centralizat și să poată aplica algoritmi de Machine Learning și Artificial Intelligence separat pentru fiecare rețea individuala
- Soluția va include o bază de date cu semnături IDS. Soluția va oferi capabilitatea de reducere a numărului de alerte generate de senzorii de tip IDS prin aplicarea de algoritmi de Machine Learning și Artificial Intelligence
- Soluția va include capabilități de Sandboxing pentru detonarea și verificarea fișierelor necunoscute, precum și detecție pentru ransomware, spyware etc.
- Soluția trebuie să includă feed-uri de Threat Intel, cel puțin următoarele tip-uri: fluxuri Premium (comerciale), fluxuri open source, anti-phishing, Freemium
- Soluția trebuie să aibă mai multe tipuri de detecție încorporate corelate cu fiecare stadiu din Cybersecurity Kill Chain sau aliniate pe framework-ul Mitre Att&CK. Toate detecțiile vor fi prioritizate în baza unui scor de severitate alocat automat de algoritmul de machine learning
- Solutia trebuie sa ofere posibilitatea unei instalari flexibile, folosind echipamente hardware dedicate sau intr-un mediu virtual,
- Soluția sau cel puțin o componentă a soluției ofertate trebuie să dețină minim certificarea CC EAL 2+ sau echivalent
- Soluția trebuie sa ofere o consola unica centralizata de administrare web pentru componentele care se integreaza nativ
- Toate log-urile pot fi ingerate în platformă prin intermediul syslog și parsere dedicate specifice diferitelor tehnologii de securitate si retea, astfel încât acestea să poată fi normalizate și corelate automat
- Soluția trebuie să ofere acces la toate sursele de date, nu doar la datele colectate prin syslog
- Soluția trebuie să asigure colectarea informațiilor despre utilizatori (ex. Active Directory) prin intermediul API

- Prin inspectarea traficului de rețea în timp real, soluția trebuie să fie capabilă să detecteze anomalii sau comportament anormal și să alerteze atunci când este cazul
- Soluția trebuie să ofere capabilități de Deep Packet Inspection (DPI) pentru a identifica aplicații și a construi modele de comportament pe traficul de rețea
- Soluția va extrage din traficul analizat doar metadate relevante si date despre payload, pentru a optimiza cantitatea de date stocata
- Solutia trebuie sa includa mecanisme de tip data reduction pentru a optimiza spatiul de stocare aferent
- Soluția trebuie să suporte, dar fără a se limita la, multiple scenarii de detecție precum Application Usage Anomalies, Long App Session Anomalies, Unapproved Asset Activity, DHCP Server Anomaly, Recently Registered Domains, Non-Standard Port Anomaly, User Agent Anomaly, Bad Source Reputation etc
- Soluția trebuie să poată detecta anomalii în comportamentul echipamentelor de tip firewall
- Folosind metode de detecție incluse, soluția trebuie să poată efectua analize și să descopere anomalii în comportamentul utilizatorului
- Incidentele semnalate trebuie sa poată fi corelate cu informațiile colectate despre activitatea utilizatorilor
- Soluția trebuie să fie capabilă să colecteze informații despre endpoint-urile din rețea și să realizeze analize comportamentale
- Soluția trebuie să fie capabilă să ingereze rapoarte generate de solutiile scanare vulnerabilități și să coreleze aceste vulnerabilități în cadrul evenimentelor de securitate în desfășurare
- Soluția trebuie să descopere toate activele dintr-o infrastructura și să le grupeze în funcție de adresa MAC și IP
- Solutia trebuie sa permita adaugarea de informatii aditionale pentru endpoint-urile descoperite prin importul de fisiere CSV

- Soluția trebuie să ofere vizibilitate asupra rețelei și a serviciilor, să evidențieze modul de utilizare al aplicațiilor și să detecteze anomaliile apărute
- Soluția va facilita desfășurarea de investigații și threat hunting, punând la dispoziție, în orice moment, informații normalizate și corelate extrase rapid din data lake
- Soluția trebuie să dispună de utilitare integrate, căutări și filtre prestabilite, grafice predefinite dar să si ofere analistului posibilitatea de a le modifica sau de a crea unele noi
- Soluția trebuie să ofere capabilități avansate de căutare, inclusiv căutări corelate, care permit unui analist să agrege mai multe interogări individuale bazate pe criterii comune pentru a detecta secvențe de atac
- Toate interogările trebuie să poată fi salvate, editate, clonate de către utilizatorii platformei
- Toate rezultatele interogărilor trebuie să poată fi salvate ca dashboard-uri personalizabile
- Soluția trebuie să poată permite ca rezultatul interogărilor împreună cu acțiunile disponibile să poată fi transformate în Playbook-uri
- Soluția trebuie să ofere capabilități de răspuns automat pe baza de scenarii predefinite precum și manual, analistul având posibilitatea să acceseze direct în interfața grafică opțiunile de răspuns
- Soluția trebuie să pună la dispoziție scenarii de răspuns predefinite, bazate pe interogări automate cu acțiuni prestabilite

  Acțiunile de răspuns vor include următoarele:

  - Alerte: trimiterea de e-mail, trimiterea unui mesaj. Acțiuni: Deschiderea unui caz, Executarea unei comenzi API, crearea unui eveniment de securitate.
  - Răspunsuri: Blocarea unui IP în firewall, dezactivarea unui utilizator prin AD, rularea unui script pe un endpoint.

- Soluția trebuie sa colecteze datele in format brut cu performante ridicate de analiza in timp real
- Interfața web a soluției trebuie să suporte cel puțin următoarele opțiuni de investigare detaliată: click drill down, interogare pe o informație specifică, filtre și căutari
- Soluția trebuie sa ofere posibilitatea de a salva profile pentru vizualizarea log-urilor si pentru scopuri de investigații
- Soluția trebuie să ofere cel puțin următoarele intervale de timp pentru investigații: ultima, ora, ultimele 24 ore, ultimele 2 zile, ultimele 5 zile, toata ziua, toate datele și interval de timp personalizate
- Soluția trebuie să ofere capabilități de corelare de bază în timp real
- Soluția trebuie să ofere posibilitatea de import și export din/în sistem a regulilor de corelare printr-un back-up al configurației sistemului
- Soluția trebuie să ofere capabilități de investigare detaliată direct din pagina de sumarizare a corelării evenimentelor
- Soluția trebuie să ofere posibilitatea creării și administrării regulilor de corelare direct în interfața web, fără a fi nevoie de unelte terțe adiționale
- Soluția trebuie să ofere capabilități de alertare pentru regulile de corelare folosind cel puțin: SMTP sau SNMP și Syslog
- Soluția trebuie să ofere o interfață pentru construcția de reguli pentru rapoarte, diagrame, alerte, corelări, suficient de flexibilă și fără a fi nevoie de limbaje de scripting complexe
- Soluția trebuie să ofere suport pentru descărcarea și instalarea actualizărilor aplicației direct din consola web sau din linia de comandă
- Soluția trebuie să ofere funcții de auto monitorizare pentru verificarea stării tuturor componentelor folosind interfața web, incluzând cel puțin următorii parametrii: CPU, memoria sistemului, stare și rata de capturare

- Soluția trebuie să permită crearea de tablouri de bord personalizate
- Soluția trebuie să ofere acces pe baza de roluri
- Soluția trebuie să suporte cel puțin următoarele browsere web: Chrome, Mozilla Firefox sau Internet Explorer
- Soluția trebuie să ofere posibilitatea de a crea parsere personalizate pentru sursele de evenimente sau aplicații ce nu sunt suportate nativ de aplicație
- Soluția trebuie să ofere posibilitatea monitorizării surselor de evenimente pentru cazul în care sursa nu mai trimite evenimente sau se închide
- Soluția trebuie să ofere posibilitatea colectării log-urilor fără agent, agentul fiind folosit numai în cazurile în care colectarea fără agent nu este posibilă pentru sursa de evenimente
- Soluția trebuie să ofere funcționalități de auditare și log-uri ale sistemului
- Permite detectarea atacurilor de tip DDoS sau similare prin analiza traficului de rețea
- Soluția trebuie să ofere conectivitate externă cu serviciile de cloud ale furnizorilor pentru descărcarea informațiilor adiționale: APT, definiții Botnet, rețele malițioase, zero-day/compromitere, rapoarte suplimentare, parsere noi, reguli pentru rapoarte și diagrame
- Permite detectarea atacurilor din interior prin stabilirea unui tip al comportamentului în rețea și compararea în permanență a traficului observat în timp real cu tiparele observate în trecut
- Permite introducerea în analiză a informațiilor ce provin de la alte tipuri de tehnologii cum ar fi web-proxy, IDS/IPS, firewall sau NAC
- Oferă capabilități DPI asupra traficului folosind soluții de tip SPAN sau TAP.
- Permite generarea de rapoarte bazate pe trafic, servicii, protocoale, adrese IP, incidente de securitate sau utilizatori
- Soluția trebuie să includă informații GeoIP în scopuri de investigații

- Soluția trebuie să ofere funcționalități de raportare. Rapoartele trebuie să includă cel puțin accesul bazat pe roluri: read&write, read only, no access
- Soluția trebuie să suporte expresii regulate (de ex. RegEx), operatori logici (boolean) sau free text pentru crearea rapoartelor
- Soluția trebuie să suporte crearea de rapoarte în baza unor filtre
- Soluția trebuie să suporte o lista de variabile ce pot fi folosite la crearea rapoartelor
- Soluția trebuie să ofere diferite opțiuni pentru afișarea rapoartelor cum ar fi: tabular, area, bar, bubble, column, line, pie, step line, step area, spline area, spline
- Soluția trebuie să ofere mai multe opțiuni de afișare a graficelor
- Soluția trebuie să permită adăugarea de informații adiționale rapoartelor: header, body text și comentariu
- Soluția trebuie să ofere opțiunea de a programa rularea rapoartelor: adhoc, sau ora de ora, zilnic, săptămânal, lunar
- Soluția trebuie să ofere posibilitatea investigației detaliate (drill-down) direct din raportul generat
- Soluția trebuie să permită export-ul rapoartelor în cel puțin următoarele formate: PDF si CSV
- Soluția trebuie să ofere rapoarte, reguli și diagrame predefinite. Personalizarea rapoartelor, regulilor și diagramelor trebuie să fie posibilă
- Soluția trebuie să ofere posibilitatea de a exporta din interfața web log-urile colectate
- Soluția trebuie să permită configurarea mesajului de login în aplicație
- Soluția trebuie să permită integrarea cu alte soluții care oferă monitorizarea stațiilor și serverelor pentru analiza detaliată a amenințărilor informatice, prin intermediul unor agenți instalați local. Agentul va colecta informații despre procese, comenzi executate, manipulări de fișiere etc. Informațiile colectate de

agenți vor fi folosite de soluție pentru a detecta anomalii în comportamentul utilizatorilor, anomalii de trafic, C&C și alte tipuri de atacuri.

- Pentru a detecta amenințările la nivelul sistemului de operare, soluția propusă trebuie să efectueze analize bazate pe memoria
- Agentul trebuie să adune informații de securitate de la host, inclusiv acțiunile de rețea, nivelul de patch-uri și procesele care ruleaza in memorie.
- Soluția propusă trebuie să susțină definirea de IOC-uri (Indicatori de compromis) pe partea de server. Căutările pe baza acestor IOC-uri vor fi executate automat și vor oferi rezultate de scanare în consola server.
- Soluția propusă trebuie să permită crearea de IOC personalizate din interfața UI a consolei. Modificările IOC noi sau modificate pot fi aplicate pe baza rezultatelor scanării și pot oferi o analiză ulterioară imediata
- Soluția propusă trebuie să fie capabilă să furnizeze o corelație completă a mediului IT care să arate numărul de sisteme în care a fost găsit modulul suspect sau rău intenționat (proces, DLL etc.), fără a fi necesară efectuarea unei alte scanări.
- Furnizorul va trebuie să licențieze un număr minim de 100 de agenți

- Soluția trebuie să asigure colectarea/monitorizarea log-urilor și analiza traficului de rețea, fiind asigurate licențele necesare pentru un număr de 20000 EPS și 1 GB/s trafic

- Soluția trebuie să ofere, dacă este necesar, toate licențele, atât pentru sistemele de operare utilizate pentru implementare, cât și pentru aplicațiile terțe utilizate pentru asigurarea funcționalităților acesteia

- Soluția va fi scalabilă și va fi integrată cu platforma RO-SAT (ofertantul va descrie în oferta tehnică și în proiectul/planul de instalare furnizat modul în care se va realiza această integrare)
- Soluția ofertată trebuie să păstreze în baza de date (local) alertele de securitate pentru o perioada de 365 de zile și metadatele pe o perioadă de minim 30 de zile.

Din punct de vedere tehnic, soluția SIEM va integra cel puțin următoarele tipologii:

- Echipamente hardware precum: stații de lucru, servere, sisteme de stocare, switchuri, routere etc.;
- Echipamente de protecție a platformei RO-SAT precum: firewall, IDS/IPS, antivirus, web gateway, email gateway etc.;
- Sisteme de identificare și analiză a atacurilor, incluzând honeypots serverside, client-side (cel puțin pentru serviciul web) sau rețele de tip darknet;
- Sisteme de scanare pentru vulnerabilități web sau de rețea;
- Echipamente și software de tip SIEM care să permită corelarea informațiilor despre atacuri și diseminarea acestora;
- Sistem de backup/restaurare (echipamente, software etc.);
- Software de virtualizare;
- Sisteme de operare;
- Senzorii SOC instalați în cadrul proiectului;
- Tehnologii web utilizate pentru implementarea funcționalităților definite pentru modulele platformei RO-SAT;
- Sisteme de gestiune a bazelor de date ce pot fi utilizate pentru implementarea funcționalităților definite pentru modulele platformei ROSAT

Sursele principale de date ce vor fi integrate în SIEM sunt următoarele:

- Trafic de rețea
- Log-uri/evenimente/alerte echipamente și soluții hardware și software pe care va fi implementată platforma RO-SAT. Infrastructura pe care va fi implementată platforma conține următoarele tipuri de soluții și echipamente:
  - Firewall

- ProxyWeb
- ProxyEmail
- WAF
- Sandbox
- Antivirus

➢ Sisteme de operare de tip Windows și Linux

➢ Log-urile modulului Darknet

➢ Log-urile modulului HoneyNet

➢ Datele obținute în urma scanărilor automatizate de vulnerabilități

➢ Datele obținute în urma scanărilor automatizate a website-urilor (crawling website-uri)

➢ Date extrase și agregate automat cu ajutorul modulului OSINT

➢ Date de tip Cyber Threat Intelligence extrase automat din feed-uri comerciale și feed-uri publice

➢ Log-uri colectate de la senzorii SOC

NOTĂ: toate sursele principale de date vor fi integrate de furnizor în soluția SIEM

NOTĂ: furnizorul va analiza, va propune și va implementa pentru soluția SIEM alerte ce vor fi generate automat în urma corelării informațiilor primite de la sursele principale de date ce vor fi integrate în soluție. De asemenea furnizorul va analiza, va propune și va implementa alerte specifice pentru fiecare sursă principală de date.

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care soluția SIEM ofertată va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani, în regim NBD.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

Soluția trebuie să poată funcționa și după expirarea licenței, astfel încât aceasta să permită atât administrarea cât și utilizarea, folosind actualizările de securitate și de componente descărcate înainte de expirarea licenței, cu excepția serviciilor și soluțiilor care se bazează pe informații furnizate pe bază de subscripții.

9.3.3 Soluție de knowledge management

1. **Obiectul achiziției:** Soluție de knowledge management
2. **Valoare totală estimată :** 800.000 lei fără TVA

Soluția este o soluție de suport a sistemului RO-SAT ce va fi utilizată pentru instruirea utilizatorilor și administratorilor sistemului, angajați ai CERT-RO beneficiarul platformei. Nu este necesară integrarea cu platforma RO-SAT și cu soluția SIEM.

Ofertantul va furniza o soluție software de knowledge management, instruire online sau asistată și testare care să ofere cumulat următoarele caracteristici tehnice minime:

- Să fie ușor accesibilă, eficientă și să permită ca un număr mare de utilizatori (cel puțin 100), răspândiți în locații diverse, să primească acces rapid la materiale de suport cu privire la modul corect de utilizare a sistemului RO-SAT
- Soluția va permite adăugarea ulterioară de materiale
- Soluția va cuprinde materiale care să permită specialiștilor CERT-RO însușirea tehnicilor de administrare și utilizare a platformei RO-SAT
- Soluția poate cuprinde și link-uri de acces către resurse de pe platforma vendorului, care vor putea fi accesate pe perioada de valabilitate a suportului pentru modulele respective
- Soluția va oferi o aplicație de management al instruirii (instruire on-line cu sau fără trainer)
- Soluția va include un modul de organizare a conținutului, un modul de administrare a utilizatorilor, un modul de rulare a conținutului, unul de testare a cunoștințelor și unul de raportare
    - Modulul de administrare a utilizatorilor va permite adăugarea, editarea și ștergerea conturilor acestora. De asemenea, modulul trebuie să poată crea grupuri de utilizatori din fiecare categorie iar pentru fiecare grup să poată stabili cursurile pe care le poate accesa și drepturile pe care utilizatorii din grup le au asupra acestora (vizualizarea materialelor de curs sau editarea materialelor de curs). Această funcționalitate trebuie să fie disponibilă și la nivel de utilizator, astfel încât să se poată specifica pentru un utilizator cursurile la care are acces

NOTĂ: Autoritatea contractantă are în vedere trei categorii de utilizatori: cursanți, instructori, administratori

- Aplicația trebuie să asigure accesul securizat al utilizatorilor. Fiecare utilizator trebuie să fie înregistrat în cadrul soluției cu un identificator unic care să permită atribuirea tuturor datelor legate de activitatea și rezultatele obținute în cadrul cursurilor pe care le parcurge.
- Modulul de organizare al conținutului trebuie să permită organizarea materialelor după modelul unei biblioteci on-line. Modul de organizare a conținutului trebuie să fie ușor de utilizat, facil de navigat. Trebuie să permită organizarea și sortarea conținutului în funcție de tematică pentru ca acesta să fie ușor de găsit și optimizarea căutărilor în funcție de cuvinte cheie și tag-uri
- Modulul trebuie să permită importul de resurse didactice, inclusiv în format multimedia sau de documentare pe care să le organizeze în funcție de tematică și să le pună la dispoziția utilizatorilor în funcție de drepturile acestora.
- În cadrul modulului, resursele didactice trebuie să poată fi reorganizate sau șterse de către utilizatorii care au drepturi în acest sens.
- Modulul de organizare a conținutului trebuie să permită adăugarea de resurse în format video (de ex. mp4, wmv, mkv, mov) și în format text pe aceeași pagină.
- Modulul de rulare a conținutului educațional include facilitățile necesare pentru vizualizarea conținutului. Modulul trebuie să asigure rularea în bune condiții a materialelor de curs multimedia, a materialelor video / video-tutorial sau a celor de tip prezentare ori document. Modulul trebuie să ofere utilizatorilor instrumentele necesare pentru a urmări materialele de instruire în condiții optime.
- Pentru formatul video vor exista facilități de vizualizare a conținutului în browser. În cazul materialelor de curs în format video modulul trebuie să ofere utilizatorilor comenzile necesare pentru a urmări materialele de instruire

în condiții optime. Comenzile trebuie să fie ușor de reperat și de folosit.

- Comenzile pentru rularea conținutului trebuie să fie ușor de reperat și de folosit, iar interfața trebuie să asigure legătură facilă cu biblioteca.
- Modulul trebuie să permită rularea materialelor de curs folosind cel puțin următoarele browsere: Internet Explorer/Edge, Google Chrome sau Firefox.
- Pe lângă posibilitatea de adăugare a materialelor de curs, soluția va permite și adăugarea de materiale de evaluare sub forma de chestionare/teste pentru verificarea nivelului de cunoștințe dobândit în urma parcurgerii cursurilor.
- Modulul de raportare trebuie să asigure cel puțin o evidență a numărului de materiale de instruire parcurse per utilizator, datele la care au fost parcurse, rezultatele testelor susținute de utilizatorul respectiv în urma unui anumit curs și va permite publicarea datelor respective ca rapoarte ușor de consultat, sub formă grafică.

NOTĂ: Soluția ofertată va trebui să acopere prin funcționalități activitățile definite la capitolul *9.4. Instalarea și punerea în funcțiune a soluțiilor ofertate - punctul d)Training/predare soluții livrate*

NOTĂ: Întreaga documentație de utilizare și administrare a sistemului RO-SAT, va fi livrată în format electronic odată cu produsul în sine. De asemenea, acestea vor fi incluse și în soluția de knowledge management) pentru a facilita accesul la respectivele documente. De asemenea în soluția de knowledge management vor fi incluse și documentele specificate la capitolul 9.5.Licențe, manuale și documentație

Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității contractante în cadrul contractului sunt cel puțin următoarele:

- Licențe/alte documente necesare/folosite la activarea produsului
- Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

- Documentația de utilizare

Ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Garanție și suport

Garanție echipamente hardware

În cazul în care Soluția de knowledge management ofertată va conține o componentă hardware, furnizorul va trebui să asigure funcționarea produselor hardware de la data instalării pentru o durată de minim 5 ani.

În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare.

În cazul defectării echipamentului hardware, ofertantul îl va repara sau înlocui conform termenelor de SLA de la momentul raportării. În situația în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanție similară cu a produsului înlocuit. Înlocuirea și operaționalizarea componentelor sistemelor se va realiza fără alte costuri din partea beneficiarului (înlocuire componente defecte, reinstalări, reconfigurări, transport etc.).

Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data acceptanței finale pentru o durată de minim 5 ani.

Suportul tehnic include acces gratuit la pachetele de actualizare a firmware-ului și a software-urilor asimilate hardware-ului și la documentația necesară aplicării actualizărilor respectiv:

- remedieri în cazul problemelor de funcționalitate (bug fix), actualizări în cazul problemelor de securitate ale produsului în sine (security updates), actualizări de funcționalitate în cadrul unei versiuni sau în cazul versiunilor majore. Actualizările ce vizează depanarea unor probleme identificate că afectează securitatea firmware-ului și a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului;
- îndrumări și recomandări în ceea ce privește procesul de actualizare și suport în cazul apariției de situații neprevăzute în timpul actualizărilor;
- suport pentru aplicarea de soluții de funcționare alternative (workaround) în cazul apariției de defecțiuni a căror rezolvare nu este încă inclusă în pachetele de remediere sau schimbării producătorului soluției;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menținerii tuturor funcționalităților solicitate pentru asigurarea securității sistemelor informatice privind prevenirea, detecția și eliminarea amenințărilor și/sau vulnerabilităților specifice acestora, inclusiv pentru informațiile de tip „threat intelligence".

Soluția trebuie să poată funcționa și după expirarea licenței, astfel încât aceasta să permită atât administrarea cât și utilizarea, folosind actualizările de securitate și de componente descărcate înainte de expirarea licenței, cu excepția serviciilor si soluțiilor care se bazează pe informații furnizate pe bază de subscripții.

9.4. Instalarea și punerea în funcțiune a soluțiilor ofertate – detalii suplimentare

Instalarea și punerea în funcțiune a soluțiilor ofertate va avea la bază un proiect/plan de instalare în care va fi detaliat modul de livrare, instalare, configurare și testare pentru toate soluțiile ofertate, precum și graficul de realizare al acestor operații.

NOTĂ: după semnarea contractului proiectul/planul de instalare furnizat de ofertant în oferta tehnică va fi adaptat împreună cu Autoritatea Contractantă. Livrarea, instalarea, configurarea și integrarea efectivă a soluțiilor va începe numai după aprobarea proiectului/planului de instalare de către Autoritatea Contractantă.

NOTĂ: Pentru realizarea sistemului RO-SAT Autoritatea Contractantă va pune la dispoziție platforma hardware necesară și software de virtualizare și management al mașinilor virtuale. În cadrul sistemului RO-SAT furnizorul va pune la dispoziție, fără costuri suplimentare toate sistemele de operare, și licențele aferente acestora astfel încât sistemul RO-SAT să funcționeze conform cerințelor funcționale și arhitecturii propuse.

Mai jos sunt detaliate etapele conform cărora se va derula instalarea și punerea în funcțiune a soluțiilor ce vor fi livrate.

a) Realizarea Documentației de instalare

Împreună cu Beneficiarul se va agrea de comun acord formatul documentului și procedurile de etichetare a soluțiilor în cadrul unor discuții tehnico-procedurale preliminare. Documentația de instalare asociată fiecărei soluții ce va fi integrată va conține obligatoriu informații privind:

- Numele şi codul soluției;
- Persoane de contact, atât din partea Beneficiarului, cat si din partea Furnizorului;
- Resursele hardware necesare;
- Diagrama conexiunilor logice între soluțiile ce vor fi integrate;

- Fluxurile de date, modalitățile de îmbogățire, interconectare soluții

b) Configurarea echipamentelor și instalarea soluțiilor software

Toate soluțiile vor fi configurate de către Furnizor conform soluției tehnice agreate cu Beneficiarul în urma workshop-urilor comune.

Planul de adresare IP pentru testarea soluțiilor instalate va fi agreat de Furnizor împreună cu Beneficiarul. Furnizorul va configura adresele IP de producție pe soluții, după instalarea acestora și va efectua testele de verificare necesare.

Responsabilitatea Furnizorului se va răsfrânge doar asupra soluțiilor livrate de acesta si va presupune activități legate de integrarea soluțiilor în sistemele informatice existente.

Toate soluțiile vor fi instalate și configurate în conformitate cu cerințele Beneficiarului. O parte din cerințe sunt furnizate în prezentul caiet de sarcini. Celelalte cerințe vor rezulta în urma discuțiilor tehnice preliminare, discuții ce vor avea ca rezultat proiectul/planul de instalare actualizat ce va trebui aprobat de către Beneficiar.

c) Testare

Furnizorul va pregăti planuri de testare pentru toate soluțiile livrate și instalate. Beneficiarul va examina și aproba planurile de testare pregătite de Furnizor. După aprobarea planurilor de testare furnizorul împreună cu beneficiarul va derula testele stabilite. În cazul în care vor fi descoperite probleme acestea vor fi remediate de Furnizor iar testarea va fi reluată.

Planurile de testare trebuie să urmeze o metodologie standard în domeniu.

Planurile de testare trebuie să includă, după caz:

- teste funcționale
- teste de arhitectură, teste non-funcționale
- teste de conexiune
- teste de conectivitate și interoperabilitate
- testele de conectare și utilizare pentru site-urile locale și remote
- teste de raportare care sa reflecte starea de funcționare a sistemului
- teste de securitate, conform bunelor practici in domeniu
- teste de backup și restaurare

Testele non-funcționale trebuie să acopere cerințele de disponibilitate, scalabilitate, fiabilitate, robustețe, salvare și restaurare, recuperarea în caz de dezastru, estimări capacitate și planificare, performanța, managementul configurațiilor, extensibilitate/flexibilitate, siguranță în funcționare, securitate, managementul și monitorizarea sistemului, managementul căderilor în sistem, contingența, operarea, conectivitatea și calitatea serviciilor.

Beneficiarul se va asigura că Furnizorul a efectuat cu succes următoarele activități, cu rezultatele lor respective:

- toate componentele necesare au fost livrate corespunzător și instalate;
- toate elementele furnizate sunt pe deplin funcționale;
- sesiunile de knowledge transfer au fost livrate;
- toate documentele necesare, manuale, CD-uri de instalare și licențele legate de acest proiect au fost livrate;
- în procesul de implementare a sistemului se vor genera raportări care să reflecte starea de funcționare a sistemului

Suplimentar, interfețele web precum și orice alte componente ale platformei vor fi testate din punct de vedere al funcționalității atât de contractor cât și de beneficiar, înainte de preluarea sistemului.

d) Training soluții livrate

Sistemul RO-SAT va fi operat de specialiștii Direcției Tehnice din cadrul CERT-RO. După implementarea proiectului, contractorul va livra manuale complete de folosire (pașii de urmat de către utilizatori în vederea exploatării produsului), mentenanță și administrare (instalarea, administrarea zilnică, instalarea upgrade-urilor și dezinstalarea/reinstalarea), tutoriale video disponibile prin intermediul modulului de Knowledge Management asupra folosirii și administrării aplicațiilor și a platformei livrate.

Programele de instruire destinate personalului Autorității contractante care va avea în sarcină sistemul cuprind administrarea sistemului, mentenanța, operarea sistemului IT si securitatea sistemului.

Scopul acestor programe de instruire este de a asigura operarea sistemului informatic și administrarea componentelor software de bază, baze de date și a aplicațiilor.

Instruirea trebuie să se realizeze folosind scenarii reale, situații cu care utilizatorul se va întâlni în activitatea de zi cu zi. Materialele de instruire trebuie să fie ușor de folosit, explicite și eficiente.

Pentru fiecare componentă a sistemului RO-SAT furnizorul va realiza un modul de instruire a utilizatorilor și un modul de instruire a administratorilor de sistem.

Fiecare modul de curs va cuprinde o secțiune de prezentare a utilizării/administrării componentei din sistemul RO-SAT alături de o secțiune de testare a cunoștințelor asimilate.

Pentru fiecare material de instruire, furnizorul va stabili și va valida împreună cu beneficiarul obiectivele educaționale pe care utilizatorul trebuie să le atingă în urma parcurgerii instruirii. Obiectivele trebuie să fie formulate precis, să fie aliniate cu cerințele beneficiarului, iar îndeplinirea lor să poată fi verificată prin intermediul testelor care vor însoți fiecare modul de instruire.

Prezentarea modului de operare a fiecărui modul din aplicație trebuie să fie explicită și eficientă. Prezentarea se va realiza folosind mediul de lucru în care va acționa ulterior utilizatorul, comenzile, interfețele și ordinea etapelor din procedura de operare.

Instruirea va conține și exemplificări practice făcute cu ajutorului sistemului RO-SAT instalat. Exemplificările practice vor fi concepute astfel încât să nu afecteze funcționarea sistemului RO-SAT.

Parcurgerea materialului de prezentare și a celui de fixare (testare) se vor contabiliza și vor fi publicate în cadrul modulului de raportare al modulului de Knowledge Management. Utilizatorului i se vor indica materialele parcurse. Administratorii soluției vor avea o evidență a volumului de conținut parcurs de către fiecare utilizator și vor putea publica datele respective sub forma unui raport.

Pentru evaluarea măsurii în care utilizatorii au atins obiectivele urmărite în cadrul fiecărei sesiuni de instruire, soluția va include baterii de testare. Testele trebuie să servească obiectivele educaționale care corespund modulului de instruire respectiv. Testele trebuie să verifice doar itemii care sunt prezentați în cadrul modulului de instruire de care sunt legate. Numărul de teste din fiecare baterie e stabilit de furnizor, în funcție de tematica și de obiectivele fiecărui modul de instruire. Pentru fiecare obiectiv trebuie să existe cel puțin un item de testare care să arate dacă acesta a fost atins.

Testele utilizate pentru evaluare trebuie să fie variate, fiind obligatoriu să se folosească minim 5 tipuri diferite de teste. Testele se vor servi de text, imagini sau video pentru a verifica de o manieră cât mai fidelă nivelul de pregătire al utilizatorilor. Pe parcursul rezolvării, utilizatorul trebuie să aibă posibilitatea de a reveni și a modifica răspunsuri până la finalizarea testului. La final, testele vor oferi utilizatorului feedback cu privire la corectitudinea soluțiilor date și la punctajul obținut.

Suportul de instruire aferent platformei va fi pus la dispoziția beneficiarului in platforma de knowledge management cu cel puțin 10 zile înainte de data desfășurării sesiunilor de instruire. Materialele de instruire vor fi în limba română sau engleză.

Knowledge transfer-ul către administratorii și utilizatorii platformei RO-SAT va fi coordonat și prestat de către personalul furnizorului.

În acest sens se va utiliza soluția de knowledge management ofertată la punctul 9.3.3 Soluție de knowledge management sau alte platforme agreate de furnizor cu mențiunea că în acest caz suportul de curs va trebui introdus și în platforma de knowledge management.

Knowledge transfer-ul administratorilor sistemului RO-SAT are în vedere dobândirea cunoștințelor necesare:

- administrării utilizatorilor și permisiunilor asociate acestora;
- administrării și particularizării soluțiilor;
- consultării jurnalelor de auditare a accesului și operațiunilor desfășurate în cadrul sistemului;
- întreținerii/mentenanței soluțiilor.

Knowledge transfer-ul utilizatorilor sistemului RO-SAT va avea în vedere deprinderea cunoștințelor privind:

- utilizarea generală a sistemului;
- adăugarea/modificarea/ștergerea datelor în cadrul sistemului;
- definirea/generarea de rapoarte în funcție de rol (definire rapoarte/generare rapoarte).

Toate materialele în format electronic – însoțite de documente suport – vor fi publicate de furnizor în soluția de knowledge management.

Toate sesiunile de instruire prestate de personalul furnizorului vor fi înregistrate video și audio și vor constitui dovada prestării activităților respective.

La sfârșitul fiecărei sesiuni de instruire, aferentă unei soluții din sistemul RO-SAT, se vor elabora documentele:

- Prezenta la curs/diploma de participare (după caz);
- Raport activitate de instruire realizat de către instructor.

e) Predare sistem RO-SAT

După finalizarea sesiunilor de instruire aferente fiecărei soluții implementate în sistemul RO-SAT, sistemul va fi predat Beneficiarului.

Predarea sistemului RO-SAT va presupune schimbarea parolelor și detaliilor de conectare pentru toate soluțiile instalate. Această operațiune va fi efectuată de Beneficiar cu suportul Furnizorului.

9.5. Licențe, manuale și documentație

Furnizorul va pune la dispoziția autorității contractante toate licențele/alte documente necesare/folosite la activarea produselor instalate în cadrul sistemului RO-SAT.

Pentru sistemul RO-SAT realizat furnizorul va pune la dispoziție următoarele manuale și documentații:

- documentațiile tehnice furnizate de producători ale soluțiilor ofertate și instalate
- manuale de instalare și configurare ale soluțiilor ofertate și instalate
- manuale de administrare a sistemului RO-SAT
- manuale de utilizare a componentelor sistemului RO-SAT
- documentația funcțională a componentelor sistemului RO-SAT
- documentația tehnică a componentelor sistemului RO-SAT

- alte manuale/documentații stabilite în urma perioadei de analiză, dezvoltare sau urmare derulării activităților de realizare ale sistemului RO-SAT

Furnizorul va pune la dispoziția beneficiarului toate manualele și documentațiile în limba română, cu excepția documentațiilor tehnice ale soluțiilor, furnizate de producători, care pot fi în limba engleză.

Întreaga documentație de utilizare și administrare a sistemului RO-SAT, va fi livrată în format electronic odată cu produsul în sine. De asemenea, acestea vor fi incluse și în portal (soluția de knowledge management, instruire asistată și testare) pentru a facilita accesul la respectivele documente.
