Secţiunea D - CAIET DE SARCINI
LOT I

1. Introducere

Această secţiune a documentaţiei de atribuire include ansamblul cerinţelor autorităţii contractante pe baza cărora fiecare operator economic va elabora oferta (propunerea tehnică şi propunerea financiară) pentru furnizarea produselor care fac obiectul procedurii de achiziţie.

La depunerea propunerii tehnice, pentru a facilita verificarea conformităţii acesteia cu caietul de sarcini, furnizorul va pune la dispoziţia autorităţii contractante documentele în format electronic (sau referinţe către acestea) din care să rezulte modul în care fiecare specificație solicitată prin caietul de sarcini este îndeplinită (fiecare cerinţă din caietul de sarcini va avea alăturat numele documentului, pagina şi paragraful din care rezultă cele solicitate).

Propunerea tehnică va conţine în mod obligatoriu numele produsului ofertat precum şi informaţii concludente, respectiv link-uri sau print-screen-uri care să certifice îndeplinirea cerinţelor minimale impuse.

În caz de neconcordanţă a informaţiilor din ofertă, specificaţiile oficiale publicate de producătorul echipamentului (valabile la data ofertei, pentru produsele ofertate) vor fi considerate ca referinţă, iar conţinutul acestora primează asupra detaliilor tehnice ale ofertei.

2. Contextul realizării acestei achiziţii de produse

Contractul de achiziţie publică se înscrie într-un proiect co-finanţat prin Fondul European de Dezvoltare Regională prin Programul Operaţional Competitivitate 2014-2020, Axa prioritară - Tehnologia Informaţiei si Comunicaţiilor (TIC) pentru o economie digitală competitivă, Operaţiunea Asigurarea securităţii cibernetice a sistemelor TIC şi a reţelelor informatice.

Proiectul vizează modernizarea sistemelor de securitate existente în instituţii din arcul guvernamental şi entităţi de interes public ce deţin infrastructuri IT&C cu valenţe critice pentru securitatea naţională, precum şi interoperabilitatea sistemelor desecuritate ce urmează a fi implementate şi integrate, cu sistemul informatic deja existent, în scopul susţinerii funcţionării Sistemului Naţional de Securitate Cibernetică (SNSC), în privinţa coroborării de informaţii, colaborării, analizei şi reacţiei prin mecanismul informatic de alertare rapidă şi diseminare a informaţiilor în timp real.

2.1 Informaţii despre autoritatea contractantă

Denumirea oficială: Unitatea Militară 0929 Bucureşti
Adresă:strada Franceză nr. 48-50, sector 3, Bucureşti
Cod poştal: 030105
Telefon/fax: 0377.725.476/021.313.43.88

2.2 Informaţii despre contextul care a determinat achiziţionarea produselor

Unitatea Militară 0929 Bucureşti este beneficiarul unui contract de finanţare pentru proiectul „Actualizarea şi dezvoltarea sistemului naţional de protecţie a infrastructurilor IT&C cu valenţe critice pentru securitatea naţională împotriva ameninţărilor provenite din spaţiulcibernetic”, co-finanţat prin Fondul European de Dezvoltare Regională prin Programul Operaţional Competitivitate 2014-2020.

2.3 Informații despre beneficiile anticipate de către autoritatea contractantă

Nivelul de securitate al infrastructurilor cu valențe critice pentru securitatea națională protejate în prezent este în scădere în raport cu complexitatea și frecvența atacurilor cibernetice actuale, tehnologiile de securitate existente devenind depășite de avansul amenințărilor informatice. Astfel, este necesară adaptarea acestor infrastructuri la noile nevoi și tendințe în domeniul securității cibernetice, concomitent cu creșterea și dezvoltarea capabilităților de procesare, analiză și reacție.

Soluția tehnică presupune crearea unei arhitecturi bazată pe tehnologii de securitate orientate pe utilizator, pentru care se pot granulariza politicile de securitate în funcție de necesitate, se pot identifica exact zonele în care există un atac cibernetic reușit și pot fi luate măsuri operative de eliminare a consecințelor sau izolare în vederea investigării, după caz. Integrarea hardware cu implementarea solutiilor software specifice și aplicațiilor utilizate se vor derula după următoarele etape: amplasare, instalare, punere în funcțiune, configurare, implementare și testare.

2.4 Alte iniţiative/proiecte/programe asociate cu această achiziție de produse

Prin HG nr. 271/2013 a fost aprobată Strategia de Securitate Cibernetică a României care stabilește cadrul conceptual, organizatoric și de acțiune necesar asigurării securității cibernetice și care vizează protecția infrastructurilor cibernetice în concordanță cu noile concepte și politici din domeniul apărării cibernetice elaborate și adaptate la nivelul NATO și al Uniunii Europene. Principalul obiectiv al Strategiei de Securitate Cibernetică a României l-a reprezentat crearea unui sistem național integrat - Sistemul Național de Securitate Cibernetică (SNSC) organism care are rolul de a superviza implementarea coerentă a tutror măsurilor de prevenire și reacție la atacurile cibernetice împotriva instituțiilor publice sau a companiilor private și care reunește autoritățile și instituțiile publice cu responsabilități și capabilități în domeniu.

SNSC a beneficiat de suport informațional/analitic/decizional necesar funcționării în urma implementării proiectului "Sistem național de protecție a

infrastructurilor IT&C de interes național împotriva amenințărilor provenite din spațiul cibernetic" – cod SMIS 48723, finanțat prin Programul Operațional Creșterea Competitivității Economice 2007-2013. Proiectul a avut ca scop consolidarea sistemelor de securitate cibernetică existente la data inițierii acestuia la nivelul infrastructurilor beneficiare, prin completarea cu tehnologiile de securitate neacoperite de sistemele existente la momentul respectiv și standardizarea tipurilor de alerte. Cu ajutorul proiectului s-a asigurat interoperabilitatea sistemelor de securitate implementate în cadrul instituțiilor publice, cu sistemul informatic al Centrului Național Cyberint (CNC), în privința colaborării, informării și reacției prin mecanismul informatic de prevenție, detecție, alertare rapidă și diseminare a informațiilor în timp real. Proiectul a contribuit la sporirea nivelului securității cibernetice naționale prin securizarea Infrastructurilor Cibernetice de Interes Național (ICIN)/ Infrastructurilor IT&C cu Valențe Critice pentru securitatea națională (IVC) și prin implementarea unui sistem de management centralizat a incidentelor de securitate (SIEM) la nivel național, fiind aplicate următoarele tehnici de securizare ce au fost implementate în cadrul tuturor IVC-urilor: prevenție, detecție, investigație și corecție. Astfel, în cadrul proiectului, în funcție de necesitățile fiecărei infrastructuri, au fost achiziționate următoarele soluții de securitate: web gateway, email gateway, UTM, endpoint security, web application firewall, SIEM, soluție de detecție a atacurilor de tip APT pentru traficul web și de email. Mediul internet, prin resursele sale hardware și software, este folosit pentru desfășurarea activității și transferul de informații între toate entitățile, de la companii, organizații și agenții guvernamentale până la utilizatorii finali. Potențial vulnerabile la atacuri cibernetice nu sunt doar mediul fizic – echipamente mobile, sisteme informatice, smartphone-uri etc. – ci și cel logic – sisteme de operare, aplicații poștă electronică, transferurile de informații sau operațiile în cloud. Studiile de specialitate relevă faptul că numărul de atacuri din ultimii ani a crescut exponențial în ceea ce privește atât volumul, cât și gradul de complexitate, conducând la un risc sporit, la costuri suplimentare și potențiale pierderi pentru instituții. Progresele tehnologice au simplificat procesele și procedurile și au permis instituțiilor să adopte noi instrumente care să le permită extinderea mijloacelor de comunicare și să structureze și să pună în aplicare servicii cu viteză crescută și flexibile. Pe de altă parte, utilizarea unor astfel de instrumente crește riscul atacurilor cibernetice, ale căror scopuri sunt în principal:

afectarea funcționării, distrugerea sau controlul ilegal al unui sistem de calcul sau infrastructură informațională;

amenințarea confidențialității, integrității și disponibilității datelor și/sau sistemelor informatice ale instituțiilor;

afectarea autenticității și non-repudierea datelor sau sustragerea informațiilor cu acces restricționat.

În ceea ce privește securitatea cibernetică din România, datele provenite în urma procesării și analizei evenimentelor de securitate la nivel CNC și CERT-RO permit formularea următoarelor afirmații:

majoritatea alertelor se referă la sisteme informatice vulnerabile (configurate necorespunzător sau nesecurizate) și la sisteme informatice infectate cu diverse variante de malware de tip botnet;

oricare dintre cele două tipuri de sisteme informatice menționate mai sus pot fi folosite ca interfață pentru desfășurarea unor atacuri asupra unor terțe ținte (din interiorul sau din afara țării), reprezentând astfel potențiale amenințări la adresa altor sisteme conectate la Internet.

Având în vedere resursele financiare și umane limitate, precum și avansul tehnologic înregistrat de la finalizarea implementării proiectului anterior, analiza recent efectuată de către specialiștii în domeniul securității cibernetice a arătat că, față de schema de tehnologii de securitate instalate la ICIN-urile în cadrul proiectului anterior, există următoarele necesități:

îmbunătățirea unora din soluțiile de securitate existente care nu mai fac față traficului de date și noilor amenințări cibernetice;

îmbunătățirea soluțiilor și/sau tehnologiilor actuale din motive de învechire ale acestora, cu unele actuale și performante;

prelungirea licențelor de utilizare ale tehnologiilor sau echipamentelor care se află în exploatare;

adăugarea de noi tehnologii sau echipamente de același tip adaptate fiecărui IVC;

din cauza dinamicii personalului și a avansului tehnologic trebuie asigurată în mod periodic pregătirea de specialitate a personalului în domeniile securității cibernetice și a administrării serviciilor IT&C;

creșterea numărului de atacuri de tip DdoS asupra infrastructurilor IT face necesară implementarea unor soluții de filtrare cantitativă a traficului nelegitim;

crearea /dezvoltarea unor mijloace de intervenție rapidă în situația procedurii unui atac ce poate afecta IVC-urile din grupul țintă și dezvoltarea capabilităților de investigație ale atacurilor cibernetice prin construcția unui laborator mobil de analiză care să ofere funcționalități avansate de colectare de date, precum și instrumentele necesare interpretării acestora.

Toate soluțiile alese vor fi integrate/corelate cu cele utilizate în proiectul anterior, alertele generate fiind gestionate ierarhic-centralizat, primul nivel de procesare al lor fiind în cadrul IVC, iar cel de-al doilea în cadrul Centrului Național Cyberint, unde vor fi centralizate alertele din cadrul tuturor infrastructurilor beneficiare.

2.5 Cadrul general al sectorului în care autoritatea contractantăîşi desfăşoară activitatea

Proiectul implementează prevederile a două din direcţiile de acţiune stabilite prin Strategia de Securitate Cibernetică a României, respectiv:

dezvoltareacapacităţilornaţionale de management al riscului în domeniul securităţii cibernetice şi de reacţie la incidente cibernetice în baza unui „Program naţional" vizând consolidarea, la nivelul autorităţilor competente, potrivit legii, a potenţialului de cunoaştere, prevenire şi contracarare a riscurilor asociate utilizării spaţiului cibernetic simultan cu creşterea nivelului de rezilienţă al infrastructurilor cibernetice şi

promovarea şi consolidarea culturii de securitate în domeniul cibernetic prin derularea unor programe de conştientizare a administraţiei publice şi a sectorului privat cu privire la vulnerabilităţile, riscurile şi ameninţările specifice utilizării spaţiului cibernetic, inclusiv prin formarea profesională adecvată a persoanelor care îşi desfăşoară activitatea în domeniul securităţiicibernetice.

De asemenea, conform art. (34) din Directiva UE 2016/1148 a Parlamentului European şi a Consiliului privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune, Statele Membre ar trebui să fie echipate în mod adecvat, din punct de vedere al capacităţii atât tehnice, cât şi organizatorice, pentru a preveni, detecta, combate şi atenua incidentele şi riscurile la care sunt supuse reţelele şi sistemele informatice. Pentru a putea răspunde noilor provocări tehnologice şi creşterii nivelului de trafic în reţelele beneficiarilor proiectului este necesară sporirea capabilităţilor tehnice pentru soluţiile ce urmează a fi dezvoltate şi implementate încadrul instituţiilor publice.

Strategii relevante:

- Strategia Naţională privind Agenda Digitală pentru România 2020.

2.6 Factorii interesaţi şi rolul acestora

Beneficiarii direcți ai produselor ce fac obiectul achiziției sunt instituțiile guvernamentale, entități de interes public ce dețin infrastructuri IT&C cu valențe critice pentru securitatea națională (IVC) și Centrul Național Cyberint (CNC), acestea fiind implicate pe întreaga durată de concepere, dezvoltare şi implementare a proiectului precum şi în etapa de post implementare.

3. Descrierea produselor

3.1 Scopul şi obiectul contractului de achiziţie

Prin proiectul „Actualizarea şi dezvoltarea sistemului naţional de protecţie a infrastructurilor IT&C cu valenţe critice pentru securitatea naţională împotriva ameninţărilor provenite din spaţiul cibernetic", co-finanţat prin Fondul European de Dezvoltare Regională prin Programul Operaţional Competitivitate 2014-2020, se urmărește dezvoltarea, actualizarea și adaptarea tehnologiilor de securitate utilizate în prezent în scopul menținerii unui nivel corespunzător de protecție

cibernetică a infrastructurilor cu valențe critice. Tehnologiile utilizate vor fi particularizate pe necesitățile fiecărui beneficiar și vor permite o mai bună granularizare a securității per utilizator, responsabilizând structurile de tip SOC (Security Operations Center) în stabilirea politicilor de securitate, analiza informațiilor generate de sisteme și reacția în situația identificării unui eveniment cibernetic. Proiectul va permite creșterea nivelului de securizare a IVC-urilor prin implementarea sau upgradarea, după caz, a soluțiilor care permit protejarea pe principiul "apărării în adâncime" a informațiilor și a sistemelor informatice care asigură depozitarea informațiilor, accesul și transportul acestora. Soluția tehnică se bazează pe un set de echipamente ce pot avea producători diferiți, dar care sunt aliniate standardelor internaționale de interoperabilitate și vor putea fi integrate cu ușurință în cadrul unei rețele informatice existente. Sunt avute în vedere soluții ce permit analiza în profunzime a amenințărilor din mediul on-line (web, email), precum și soluții de securitate dedicate stațiilor de lucru. Se va realiza upgradarea și/sau redimensionarea soluțiilor pentru a fi asigurată menținerea nivelului de protecție împotriva noilor amenințări de securitate, având în vedere, atât creșterea nivelelor de trafic generate în cadrul IVC, cât și capacitatea producătorilor de a menține soluțiile la un standard înalt de securitate pentru o perioadă cât mai mare de timp.

3.2 Obiectivul general al proiectului

Actualizarea sistemului informatic existent şi includerea în acest sistem de noi infrastructuri IT&C cu valenţe critice pentru securitatea naţională în scopul sporirii capabilităţilor de identificare a atacurilor cibernetice, precum şi a creşterii nivelului de securitate cibernetică naţională reprezintă obiectivul general al proiectului „Actualizarea şi dezvoltarea sistemului naţional de protecţie a infrastructurilor IT&C cu valenţe critice pentru securitatea naţională împotriva ameninţărilor provenite din spaţiul cibernetic”, co-finanţat prin Fondul European de Dezvoltare Regională prin Programul Operaţional Competitivitate 2014-2020, subsumat unei abordări comune a UE în materie de securitate cibernetică.

Astfel, proiectul vizează modernizarea sistemelor de securitate deja implementate în cadrul autorităţilor/instituţiilor publice, precum şi interoperabilitatea sistemelor de securitate ce urmează a fi implementate şi integrate, cu sistemulinformatic deja existent, în privinţa coroborării de informaţii, colaborării, analizei şi reacţiei prin mecanismul informatic de alertare rapidă şi diseminare a informaţiilor în timp real.

Totodată se va îndeplini şi obiectivul de asigurare acontinuităţii serviciilor furnizate de către statul român pentru cetăţenii proprii sau ai Uniunii Europene.

3.3 Obiectivul specific la care contribuie furnizarea produselor

Soluția propusă, prin arhitectura și tehnologiile ce vor fi implementate, va

răspunde următoarelor cerințe:

asigurarea pentru rețelele informatice protejate din cadrul IVC a unui nivel de securitate cibernetică superior celui existent în prezent;

oferirea posibilităților de identificare a metodelor de compromitere cunoscute în prezent, dar și existența unor capabilități de identificare a atacurilor noi, de tipul "zero-day";

automatizarea proceselor, a notificărilor și a reacțiilor la o scară cât mai larg posibilă;

prevenirea atacurilor prin identificarea breșelor de securitate înainte de a fi exploatate sau combaterea acestora din fazele incipiente.

3.4 Produsele solicitate şi operaţiunile cu titlu accesoriu necesar a fi realizate

3.4.1 Produsele solicitate

Denumire produs	Cant.	U.M.	Preț unitar fără TVA lei	Valoare totală fără TVA lei	Locul de livrare	Durata minimă garanţie
0	1	2	3	4	5	6
LOT I						
Soluție tip UTM/NGFW	1	pachet	11.270.557,00	11.270.557,00	București Timiș	Conform anexei nr. 1
Soluție Email Gateway	1	pachet	5.386.052,00	5.386.052,00	București Constanța Sibiu Timiș	Conform anexei nr. 2
Soluție Web Gateway	1	pachet	5.270.780,50	5.270.780,50	București Constanța Timiș	Conform anexei nr. 3
Soluție SIEM	1	pachet	15.680.610,00	15.680.610,00	București Constanța Sibiu Timiș	Conform anexei nr. 4
Soluție APT 1	1	pachet	27.298.517,00	27.298.517,00	București Constanța Sibiu Timiș	Conform anexei nr. 5
Soluție EndPoint Security (AV, HIPS)	1	pachet	5.374.172,70	5.374.172,70	București	Conform anexei nr. 6
Firewall pentru rețea cooperare	19	Buc.	4.751,70	90.282,30	București Constanța Sibiu Timiș	Conform anexei nr. 7
Soluție APT 2	1	pachet	12.972.141,00	12.972.141,00	București Constanța Sibiu Timiș Argeș	Conform anexei nr. 8
Soluție APT 3	1	Buc.	7.127.550,00	7.127.550,00	Sibiu	Conform anexei nr. 9
Switch pentru rețea cooperare	17	Buc.	2.613,44	44.428,48	București Constanța Sibiu	Conform anexei nr. 10

					Timiș	
Stații de lucru cooperare	17	Buc.	2.613,44	44.428,48	București Constanța Sibiu Timiș	Conform anexei nr. 11
Soluție de tip High Power Computing	1	pachet	3.682.567,50	3.682.567,50	București	Conform anexei nr. 12
Soluție analiză trafic brut	1	pachet	294.605,40	294.605,40	București	Conform anexei nr. 13
Soluție Threat Intelligence	1	Buc.	4.751.700,00	4.751.700,00	București	Conform anexei nr. 14
Set diagnosticare și verificare parametrii rețea	1	pachet	47.517,00	47.517,00	București	Conform anexei nr. 15
Soluție sandbox	1	pachet	902.823,00	902.823,00	București	Conform anexei nr. 16
Software analiză malware	1	Buc.	142.551,00	142.551,00	București	Conform anexei nr. 17
Soluție detecție IoC	1	pachet	2.138.265,00	2.138.265,00	București Constanța Sibiu	Conform anexei nr. 18
Soluție de retenție a evenimentelor de securitate	1	pachet	285.102,00	285.102,00	București	Conform anexei nr. 19
Kit Forensics LAB	1	pachet	1.655.017,10	1.655.017,10	București	Conform anexei nr. 20
Kit Incident Response	1	pachet	2.138.265,00	2.138.265,00	București	Conform anexei nr. 21
Sistem destinat evaluării de securitate cibernetică	1	pachet	528.626,63	528.626,63	București	Conform anexei nr. 22
Sistem avansat de investigații în mediul OSINT	1	Buc.	3.326.190,00	3.326.190,00	București	Conform anexei nr. 23
Extensie CyberExtPol	1	pachet	1.900.680,00	1.900.680,00	București	Conform anexei nr. 24
Echipament tip server	12	Buc.	47.517,00	570.204,00	București	Conform anexei nr. 25
Echipament tip switch	10	Buc.	28.510,20	285.102,00	București	Conform anexei nr. 26
Soluție de securitate și control al utilizatorilor	1	Buc.	332.619,00	332.619,00	București	Conform anexei nr. 27
Laborator mobil pentru intervenție rapidă	4	pachet	415.773,75	1.663.095,00	București	Conform anexei nr. 28
Soluție centru comunicație de rezervă (backup)	1	pachet	8.655.221,60	8.655.221,60	București	Conform anexei nr. 29
Platformă analiză malware	1	pachet	4.084.086,20	4.084.086,20	București	Conform anexei nr. 30

Cerinţele tehnice minime obligatorii se regăsesc în anexele prezentului caiet de sarcini.

3.5. Extensibilitate/Modernizare

3.5.1 Garanţie

Toate produsele trebuie să fie acoperite de garanţie pentru cel puţin perioada solicitată de autoritatea contractantă, conform cerinţelor din anexele caietului de sarcini.

Garanția trebuie să acopere toate costurile rezultate din remedierea defectelor în perioada de garanție, inclusiv, dar fără a se limita la:

demontare, inclusiv închirierea de unelte speciale necesare pe durata intervenţiei;

ambalaje, inclusiv furnizarea de material protector pentru transport (carton,

cutii, lăzi etc.);

repararea tuturor componentelor defecte sau furnizarea unor noi componente;

înlocuirea părților defecte;

despachetarea, inclusiv curățarea spațiilor unde se efectuează intervenția;

instalarea în starea inițială;

testarea pentru a asigura funcționarea corectă;

repunerea în funcțiune.

Soluţiile vor fi oferite sub forma unor echipamente hardware de ultimă generație, iar ofertantul va pune la dispoziție toate componentele hardware şi licenţele software necesare menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice protejate prin prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora.

Furnizorul trebuie să asigure funcționarea produselor software de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

3.5.2 Livrare, ambalare, etichetare, transport şi asigurare pe durata transportului

Produsele vor fi livrate cantitativ şi calitativ în locaţia indicată de către autoritatea contractantă. Fiecare produs va fi însoţit de toate subansamblele/părţile componente necesare punerii şi menţinerii în funcţiune.

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

Ambalajul produselor trebuie să reziste manipulării accidentale, expunerii la temperaturi extreme şi precipitaţiilor din timpul transportului şi 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 echipamentelor cu excepția acelor ambalaje care sunt necesare a fi prezentate în vederea acordării garanției.

Transportul şi toate costurile asociate sunt în sarcina exclusivă a furnizorului. Produsele vor fi asigurate împotriva pierderii sau deteriorării intervenite pe parcursul transportului şi cauzate de orice factor extern.

Destinația de livrare este municipiul București şi localităţi din ţară, urmând ca locațiile să fie comunicate furnizorului declarat câștigător. Livrările și instalările echipamentelor hardware şi software vor fi efectuate eşalonat per instituție beneficiară – IVC. Întreaga durată de implementare la toate IVC-urile nu poate

depăși durata contractului, respectiv 12 luni. Verificarea îndeplinirii obligaţiilor contractuale de către autoritatea contractantă şi evaluarea stadiului activităţilor, în sensul respectării termenelor stabilite pentru livrarea produselor care fac obiectul contractului, se face prin raportare la conţinutul graficului de livrare acceptat. În cazul în care, pe parcursul duratei contractului, autoritatea contractantă constată că livrarea produselor nu respectă eşalonarea astfel cum este stabilită prin graficul de livrare, autoritatea contractantă are obligaţia de a solicita furnizorului să prezinte graficul actualizat, iar furnizorul are obligaţia 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.

3.5.3. Operaţiuni cu titlu accesoriu necesar a fi realizate produselor solicitate

3.5.3.1. Instalare, punere în funcţiune, testare

Furnizorul va implementa proiectul prin amplasarea, instalarea, punerea în funcțiune, configurarea și testarea produselor achiziționate, în locațiile comunicate la încheierea contractului, astfel:

furnizorul va instalatoate produsele în mod corespunzător asigurându-se că spaţiile unde s-a realizat instalarea rămân curate. După livrarea şi instalarea produselor, furnizorul va elimina toate deşeurile rezultate şi va lua măsurile adecvate pentru a aduna toate ambalajele de la locul de instalare;

furnizorul va realiza integrarea/conectarea la infrastructura existentă și apoi toate configurările/setările necesare pentru a pune produsele în funcțiune,odată ce produsele sunt asamblate;

punerea în funcțiune include, de asemenea, toate ajustările și setările necesare pentru a asigura instalarea corespunzătoare, în ceea ce privește performanța și calitatea, cu toate configurațiile necesare pentru o funcționare optimă;

furnizorul va efectua pe cheltuiala sa și fără nici un fel de costuri din partea autorității contractante toate testele pentru a asigurafuncționareaprodusului la parametriagreați;

furnizorul rămâne responsabil pentru protejarea produselor luând toate măsurile adecvate pentru a preveni lovituri, zgârieturi și alte deteriorări, până la acceptarea de către autoritatea contractantă.

3.5.3.2. Instruirea personalului pentru utilizare

Cerinţele minime obligatorii se regăsesc în anexele prezentului caiet de sarcini.

3.5.3.3. Mentenanța preventivă în perioada de garanție

Mentenanța Preventivă a produselor achiziționate implică operațiuni de întreținere planificată și reparații în perioada de garanție tehnică și acoperă toate costurile aferente intervenției, piesele de schimb, materialele, consumabilele și alte asemenea și forța de muncă, după caz. Astfel, Mentenanța Preventivă se va efectua în conformitate cu procedurile și termenele producătorului produselor, depuse de către furnizor prin ofertă.

3.5.3.5. Suport tehnic

Furnizorul va asigura suportul tehnic conform cerinţelor incluse în anexele la 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 din cadrul IVC 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 din cadrul IVC achiziționate prin proiect.

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, aplicaţiile sau tehnologiile folosite necesită corectarea unui bug şi/sau construcţia unui patch de la producător, timpul de remediere se va modifica cu timpul necesar producătorului să construiască patch-ul şi/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 soluţiei finale.

Remediere provizorie/temporară: o modificare în cadrul procedurilor sau datelor care permite desfăşurarea activităţii utilizatorului, ca soluţie care evită temporar manifestarea defectului reclamat.

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

Triajul incidentelor se va face în funcţie de gradul de urgenţă a acestora:

Denumire	Descriere
Urgent	Impact Major asupra funcţionării sistemului. Incidentul împiedică desfăşurarea activităţii instituţiei, care este serios afectată, pierderea funcţionalităţilor devenind critică.
Critic	Impact Semnificativ asupra funcţionării sistemului. Incidentul împiedică desfăşurarea în condiţii normale a activităţii. Nu sunt disponibile solutii alternative pentru functionalitatea in cauza, dar activitatea utilizatorilor poate continua, fiind limitata la componentele neafectate ale sistemului.
Major	Impact Mediu asupra functionarii sistemului. Incidentul afectează minor funcţionalităţile sistemului. Impactul asupra utilizatorilor reprezintă un inconvenient care se poate rezolva temporar prin soluţii alternative ocolitoare, pentru continuarea funcţionalităţilor.
Minor	Impact Minim asupra funcţionării sistemului. Incidentul nu afecteaza funcţionarea sistemului, putând fi tratat ca o eroare minoră care nu împiedică desfăşurarea în bune condiţii a activităţii.

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

3.6 Atribuțiile și responsabilitățile autorității contractante

Autoritatea contractantă este responsabilă pentru monitorizarea execuției contractului, efectuarea plăților către ofertant și desemnarea unor responsabili de contract. Rolul acestora va fi de a asigura comunicarea permanentă cu echipa ofertantului, evidența tuturor documentelor referitoare la derularea contractului, monitorizarea permanentă și evaluarea periodică a gradului de îndeplinire a obiectivelor contractului.

Autoritatea contractantă va furniza ofertantului capacitatea managerială și

de expertiză necesară pentru buna derulare și implementare a contractului, constând în:
- sprijin prin contribuția specialiștilor proprii la realizarea obiectivelor propuse prin prezentul contract;
- sprijin în asigurarea unei comunicări eficiente cu toate părțile implicate, în vederea implementării cu succes a activităților proiectului;
- acces la sursele de informare disponibile.

4. Documentaţii ce trebuie furnizate autorităţii contractante în legătură cu produsele

Documentaţiile pe care furnizorul trebuie să le livreze autorităţii contractante în cadrul contractului sunt menţionateîn anexele caietului de sarcini.

5. Recepţia produselor

Recepţia cantitativă şi calitativă a produselor se va efectua după livrarea/ prestarea serviciilor la destinaţia finală/locaţiile comunicate de către achizitorconform graficului de livrare/prestare. Recepția produselor se va realiza în mai multe etape, respectiv:

- recepția cantitativă se va realiza în 48 de ore de la livrarea produselor și a documentațiilor corespunzătoare, în cantitatea solicitată, la locația indicată de autoritatea contractantă,când se va semna un proces verbal de recepţie cantitativă;
- recepția calitativă se va realiza în 45 de zile de la instalarea şi configurarea produselor și, după caz, când toate defectele au fost remediate,când se va semna un proces verbal de recepţie calitativă, pe baza testelor aferente punerii în funcţiune a echipamentelor.

Recepţia produselor se face la sediul fiecărui beneficiar, în prezenţa delegatului furnizorului, în uma căreia se vor încheia procese verbale de recepţie parţiale. Pentru fiecare beneficiar se va încheia un protocol de acceptanţă parţială care va cuprinde procesele verbale de recepţie a produselor.

Beneficiarul (prin comisia de recepţie) are obligaţia de a inspecta/testa produsele pentru a verifica conformitatea lor cu specificaţiile tehnice stabilite în propunerea tehnică.

Dacă, în urma inspecţiilor şi testelor, bunurile corespund specificaţiilor din propunerea tehnică, se vor încheia documentele de recepţie cantitativă şi calitativă. Acceptanţa parţială/finală se va realiza în baza unui protocol de acceptanţă semnat atât de către furnizor cât şi de către achizitor, respectiv beneficiar la finalizarea livrării, instalării, configurării tuturor componentelor ce fac obiectul contractului. Protocolul de acceptanţă va fi semnat după ce procesele verbale de recepție parţială aferente livrării produselor, serviciilor de instalare şi configurare, vor fi semnate.

Acceptața finală se consideră încheiată după momentul în care s-a

finalizat procesul de instalare și punerea în funcțiune al tuturor echipamentelor sau produselor software din prezentul caiet de sarcini, respectiv după finalizarea serviciilor de instruire.

Dacă vreunul din bunurile inspectate sau testate nu corespunde specificaţiilor din propunerea tehnică, pe baza procesului-verbal de reclamaţie, achizitorul are dreptul să îl respingă, iar furnizorul are obligaţia ca în termenul de livrare şi fără a modifica preţul contractului:

a) de a înlocui bunurile refuzate, sau

b) de a face toate modificările necesare pentru ca bunurile să corespundă specificaţiilor lor tehnice.

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

6. Modalităţi şi condiţii de plată

Furnizorul va emite factura pentru produsele livrate şi o va transmite la adresa specificată de autoritatea contractantă.

Factura va fi emisă după semnarea de către autoritatea contractantă a procesului verbal de recepţie calitativă, acceptat, prin care se confirmă livrarea, instalarea/montarea, recepția şi acceptarea sistemului (punerea în funcţiune şi remedierea eventualelor defecte constatate, după caz) .

Achizitorul se obligă să plătească preţul bunurilor către furnizor, prin mijloace de plată admise de lege, în termen de 30 zile de la data emiterii documentelor de acceptanţă pentru fiecare beneficiar, pe baza următoarelor documente, după caz:

a) factură fiscală;

b) documente de recepţie cantitativă şi calitativă;

c) protocol de acceptanţă parţială/finală;

d) certificat de calitate şi conformitate;

e) certificat de garanţie.

7. Cadrul legal care guvernează relaţia dintre autoritatea contractantă şi furnizor

Furnizorul are obligaţia de a respecta în executarea contractului, obligaţiile aplicabile în domeniul mediului, social şi al muncii instituite prin dreptul Uniunii, prin dreptul naţional, prin acorduri colective sau prin dispoziţiile internaţionale de drept în domeniul mediului, social şi al muncii enumerate în anexa X la Directiva 2014/24. Alte acte normative care guvernează relaţia dintre furnizor şi autoritatea contractantă sunt:

Legea nr. 98/2016 privind achiziţiile publice, cu modificările şi completările ulterioare;

H.G. nr. 395/2016,cu modificările şi completările ulterioare;

Legea nr. 101/2016,cu modificările şi completările ulterioare;

Ordinul ANAP nr. 1068/2018 privind ghidul achiziţiilor 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.

8. Managementul / Gestionarea contractului și activități de raportare în cadrul contractului

Furnizorul are obligaţia de a întreprinde toate măsurile şi acţiunile necesare pentru realizarea performanţelor contractuale. Pentru monitorizarea performanţelor contractuale furnizorul va prezenta informaţii referitoare la rezervele de timp/alte resurse (inclusiv, modalitatea de implicare a personalului suport) avute în vedere să fie implicate pentru:

- măsuri asociate riscurilor identificate;
- modalitatea de soluţionare a eventualelor neconformităţi notificate de furnizor achizitorului sau de către achizitor furnizorului, conform condiţiilor din contract.

Se va realiza, astfel o planificare a activităților**,** cu indicarea tuturor fazelor/etapelor de realizare a acestora, în ordinea și succesiunea logică a evenimentelor (cu duratele de timp necesare pe activități și poziționarea în timp a acestora, precum și cu evidențierea punctelor de control/jaloanelor relevante pentru urmărirea realizărilor, respectiv intervalele de raportare aplicabile), împreună cu alocarea resurselor umane pe parcursul furnizării produselor/instalării echipamentelor ofertate (în funcție de responsabilitățile/atribuțiile deținute pentru realizarea fiecărei activități în parte), informații care vor trebui să probeze transpunerea prevederilor caietului de sarcini într-un plan de implementare fezabil.

8.1 Gestionarea relației dintre furnizor și autoritatea contractantă

Pe parcursul derulării contractului, autoritatea contractantă verifică dacă toate activitățile planificate au fost realizate, livrate și acceptate conform cerințelor caietului de sarcini. Graficul de livrare/prestare acceptat de părți, respectiv cantitățile de produse, se regăsesc în anexele la contract.

9. Riscuri aferente implementării contractului şi măsuri de gestionare a acestora

Nr. crt.	Denumire risc	Partea contractantă căreia i se alocă riscul	Măsuri gestionare riscuri
1.	Furnizorul îşi asumă riscurile în cazul întârzierii nejustificate a livrării sau nelivrării produselor din culpa lui	Furnizor	Achizitorul va aplica penalităţi sau va rezilia contractul de furnizare, fără ca acesta să plătească furnizorului plata de daune interese prevăzute în contractul de furnizare
2.	Necompletarea corectă sau lipsa	Furnizor	Se vor reface sau se vor completa

	unor documente de recepţie	Achizitor	documentele de recepţie în conformitate cu prevederile contractuale în baza reglementărilor legale, furnizorul având obligaţia de a transmite achizitorului toate documentele de recepţie
3.	Lipsa monitorizării efective din punct de vedere cost-calitate şi a modului de derulare a contractului	Furnizor Achizitor	Autoritatea contractantă va realiza analiza continuă a modului de derulare a contractului astfel încât să fie evaluată în permanenţă îndeplinirea obiectivelor achiziţiei, respectiv furnizarea produselor în locaţiile prevăzute în contract, fără disfuncţionalităţi şi la valoarea contractată
4.	Schimbări substanţiale în condiţiile contractuale pentru a permite prelungirea duratei contractului şi preţuri mai mari pentru furnizor	Furnizor	Autoritatea contractantă nu va accepta modificarea duratei contractului şi nu va accepta modificarea preţului contractului, decât în condiţiile din documentaţia de atribuire. În cazuri excepţionale, eventualele modificări vor fi temeinic fundamentate şi justificate
5.	Acceptarea schimbării specificaţiilor contractuale sub nivelul standardelor impuse prin documentaţie	Furnizor	Autoritatea contractantă nu va accepta modificări la contract în acest sens

Anexa 1 la caietul de sarcini

SOLUȚIE DE TIP UNIFIED THREAT MANAGEMENT / NEXT GENERATION FIREWALL

1. **Descrierea situatiei actuale**

La momentul actual 33 de instituții cu valențe critice (IVC) dețin o soluție UTM (Fortinet Fortigate) implementată.

2. **Descriere generică a tehnologiei**

Soluția de tip UTM/NGFW reprezintă o soluție hardware integrată de protecție a rețelelor cibernetice cu capabilităţi de: rutare, firewall, scanare antivirus, IPS, filtrare URL, control al aplicațiilor şi VPN, destinat folosirii ca o soluţie de securitate unificată.

3. **Caracteristici tehnice minimale**

Cerințe generale:

În cazul în care soluția ofertată pentru UTM /NGFW tip 1, tip 2 și tip 3 este diferită de soluția existentă (Fortinet Fortigate) ofertantul are obligația: I. de a importa în echipamentele noi toate configurațiile vechi, inclusiv modificările aduse de Centrul Național Cyberint (scripturi, configurări, export de date, etc.); II. de a efectua o sesiune de instruire de minim 5 zile, pentru 5 persoane ce trebuie să prezinte noțiuni specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului ofertat**,** incluzând, dar fară a se limita la următoarele informaţii: Bune practici privind instalarea, configurarea şi administrarea soluţiei; Prezentarea interfeţelor de administrare (web, CLI) şi a principalelor acţiuni ce pot fi întreprinse prin intermediul acestora; Configurare reguli de acces, politici de rutare şi politici de filtrare prin intermediul *whitelists / blacklists,* adrese IP,protocol de transportşi informaţii despre reputaţie; Noţiuni privind detecţia şi remedierea defecţiunilor tehnice (*troubleshooting*); Configurare serviciu de logare pentru transmitere evenimente prin intermediul protocolului *syslog;* Configurare VLAN, domenii virtuale, High Availability, NAT, IPSec VPN, Single Sign On, QoS, server DHCP şi a politicilor de prevenire a pierderilor de date (*Data Loss Prevention*); Configurare serviciu actualizare automată a semnăturilor şi a informaţiilor despre reputaţia adreselor IP; Generare evenimente de tip "*Netflow*"; Configurare protocoale de rutare dinamice: BGP şi OSPF. Cursul va fi de tip "*hands-on*", cu activități practice în care cursanții utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului. Cursul se va desfășura în limba română, într-o locație pusă la dispoziție de furnizor, în municipiul București. Instructorul trebuie să fie acreditat de producătorul soluției. Pentru demonstrarea pregătirii instructorului se vor prezenta certificate/autorizări/acreditări, sau alte documente emise de către producătorul soluției, sau de organisme abilitate în acest sens. Ofertantul va asigura servicii de catering pe perioada cursului, respectiv o masă de prânz şi un coffee-break pe zi(cafea, apă, ceai, produse de patiserie şi fructe, la discreţie)**.**
Pentru asigurarea redundanței, la nivelul IVC soluția va fi implementată în mod High-Availability
Soluția va conține următoarele tipuri de echipamente: Soluție UTM /NGFW tip 1 – 58 bucăți Soluție de tip UTM /NGFW tip 2 – 20 bucăți Soluție de tip UTM / NGFW tip 3 – 6 bucăți Soluție de tip UTM / NGFW tip 4 – 2 bucăți

3.1 Soluție UTM / NGFW tip 1

3.1.1 Specificații hardware	3.1.1.1. Minim 18 interfeţe de retea astfel: minim 8 interfete 10/100/1000 Ethernet RJ45, minim 2 interfeţe 10 GbE SFP+ (echipate cu module 10GBase-SR) si minim 8 interfeţe SFP GbE 3.1.1.2. Minim 1 port consolă. 3.1.1.3. Minim 1 port USB. 3.1.1.4. Port dedicat pentru HA 3.1.1.5. Capacitate hdd local: minim 480 GB 3.1.1.6. Sursă redundantă de putere.
3.1.2 Caracteristici	3.1.2.1. Firewall Throughput: minim 20 Gbps 3.1.2.2. IPS Throughput: minim 6 Gbps 3.1.2.3. NGFW Throughput: minim 5 Gbps 3.1.2.4. Threat Protection/Prevention Throughput: minim 4 Gbps 3.1.2.5. IPSec VPN Throughput: minim 10 Gbps 3.1.2.6. Număr sesiuni concurente: minim 8.000.000 3.1.2.7. Număr sesiuni noi pe secundă: minim 185.000 3.1.2.8. Număr de instanțe virtuale: minim 10
3.1.3 Funcționalități generale	3.1.3.1. Echipament integrat de securitate cu cel puțin următoarele funcţionalități simultane: Firewall de tip stateful; Router cu suport pentru protocoale de rutare dinamice; Posibilitate de grupare a interfetelor în mod bridge; Protecţie Antivirus; Criptare de date: IPSec VPN şi SSL VPN; Suport pentru QoS şi Traffic Shaping; Detecţia şi prevenirea intruziunilor – IDS/IPS; Filtrare URL; DLP Blocarea şi controlul traficului din reţea generat de aplicaţii; Update-uri automate; 3.1.3.2. Toate funcţionalităţile de securitate (antivirus, IPS, filtrare URL, etc), precum şi sistemul de operare aparțin aceluiași producător
3.1.4 Funcționalități securitate	
3.1.4.1. Funcționalități firewall	3.1.4.1.1. Funcţionalităţi NAT şi Transparent Bridge 3.1.4.1.2. Opțiune de a aplica NAT per politică 3.1.4.1.3. Suport VLAN Tagging 802.1q 3.1.4.1.4. Autentificarea utilizatorilor pe grupuri

	3.1.4.1.5. Suport VoIP SIP/H.323/SCCP şi Transversal NAT 3.1.4.1.6. Suport IPv6 3.1.4.1.7. Creare politici de securitate bazate pe identitatea utilizatorului/servicii folosite 3.1.4.1.8. Opţiune “Scheduling” pentru politicile de firewall
3.1.4.2. Funcţionalităţi VPN	3.1.4.2.1. Suport IPSec și SSL-VPN 3.1.4.2.2. Criptare DES, 3DES, AES 128, AES 256 3.1.4.2.3. Autentificare minim MD5/SHA-1/SHA-256 3.1.4.2.4. Funcţionalitate “Hub and Spoke” VPN 3.1.4.2.5. Suport protocol IKE 3.1.4.2.6. Suport IPSec NAT Transversal 3.1.4.2.7. Funcţionalitate Two-Factor Authentication pentru SSL-VPN 3.1.4.2.8. Suport pentru autentificare de grupuri de utilizatori prin LDAP (SSL-VPN) 3.1.4.2.9. Funcţionalităţi monitorizare tunele VPN 3.1.4.2.10. Producătorul are în portofoliu client de VPN IPSec şi SSL propriu
3.1.4.3. Funcţionalităţi Antivirus	3.1.4.3.1. Protecţie anti-malware 3.1.4.3.2. Protocoale suportate minim următoarele: HTTP/HTTPS, SMTP, POP3, FTP 3.1.4.3.3. Protecţie pe bază de reputaţie a adreselor IP şi URL-urilor 3.1.4.3.4. Update-uri automate ale semnăturilor
3.1.4.4. Funcţionalităţi sistem de control al aplicaţiilor	3.1.4.4.1. Identificarea şi controlul a peste 3000 de aplicaţii 3.1.4.4.2. Limitare de bandă per aplicaţie 3.1.4.4.3. Monitorizarea aplicaţiilor cu rata cea mai mare de consum de bandă 3.1.4.4.4. Monitorizarea aplicaţiilor pe baza IP/Utilizator
3.1.4.5. Funcţionalităţi sistem de prevenire a intruziunilor/ atacurilor (IPS)	3.1.4.5.1. Protecţie bazata pe semnături predefinite dar şi suport pentru semnături custom 3.1.4.5.2. Detectarea anomaliilor de protocol 3.1.4.5.3. Protecţie împotriva atacurilor de tip DoS 3.1.4.5.4. Update-uri automate ale semnăturilor
3.1.4.6. Funcționalități Data Loss Prevention	3.1.4.6.1. Permite definirea de reguli bazate pe: tip de fişier (fără a ţine cont de extensia fişierului), expresii regulate 3.1.4.6.2. Permite inspecţia fişierelor arhivate 3.1.4.6.3. Suport pentru document fingerprinting şi documente cu watermark 3.1.4.6.4. Permite inspecţia/logarea protocoalelor SMTP, HTTP/HTTPS şi FTP

3.1.5 Funcţionalităţi reţea	
3.1.5.1. Funcţionalităţi reţelistică şi rutare	3.1.5.1.1. Suport PPPoE şi DHCP Client/Server 3.1.5.1.2. Funcționalitate declarare rute statice 3.1.5.1.3. Rutare dinamică IPv4: RIP, OSPF, BGP, Multicast 3.1.5.1.4. Rutare dinamică Ipv6 3.1.5.1.5. Policy-based routing 3.1.5.1.6. Suport VRRP/ Link Failure Control 3.1.5.1.7. Rutare între VLAN-uri 3.1.5.1.8. Suport One-to-One NAT 3.1.5.1.9. Suport NAT64
3.1.5.2. Funcţionalităţi Traffic Shaping	3.1.5.2.1. Limitare/garantare a benzii de trafic prin politici până la nivel de aplicaţie 3.1.5.2.2. Suport pentru Differentiated Services (DiffServ)
3.1.5.3. Suport instanţe virtuale	3.1.5.3.1. Fiecare echipament suporta domenii /instante virtuale cu aceleaşi funcţionalităţi de securitate precum echipamentul standard
3.1.5.4. Suport pentru centre de date	3.1.5.4.1. Balansare de trafic pentru servere 3.1.5.4.2. Balansare de trafic prin metode de tip: round-robin, least RTT 3.1.5.4.3. Persistența sesiunilor
3.1.5.5. Funcţionalităţi High Availability – HA	3.1.5.5.1. Funcţionare Activ-Activ, Activ-Pasiv 3.1.5.5.2. Funcţionalitate Session Failover 3.1.5.5.3. Detectare şi notificare pentru echipament nefuncțional 3.1.5.5.4. Funcționalitate Link Failover
3.1.6 Funcţionalități de administrare, jurnalizare și autentificare a utilizatorilor	
3.1.6.1. Funcţionalităţi de administrare	3.1.6.1.1. Administrare prin WEB UI , Secure Command Shell (SSH) şi Command Line Interface (CLI) 3.1.6.1.2. Utilizatori/Administratori cu drepturi configurabile 3.1.6.1.3. Funcţionalitate de export/import a configuraţiei 3.1.6.1.4. Politică de control a parolelor
3.1.6.2. Funcţionalităţi de jurnalizare şi monitorizare	3.1.6.2.1. Monitorizare grafică în timp real şi istorică 3.1.6.2.2. Functionalitate export Netflow minim v5 3.1.6.2.3. Funcționalitate export loguri în format syslog 3.1.6.2.4. Suport SNMP 3.1.6.2.5. Notificare alerte prin email
3.1.6.3. Funcţionalităţi de autentificare a utilizatorilor	3.1.6.3.1. Definire locală a utilizatorilor 3.1.6.3.2. Integrare cu Windows Active Directory (AD) pentru Single Sign On 3.1.6.3.3. Integrare cu RADIUS/LDAP/TACACS+ 3.1.6.3.4. Suport pentru autentificarea grupurilor de utilizatori prin LDAP 3.1.6.3.5. Suport pentru autentificare prin certificate digitale PKI

	X.509
3.1.6.4. Condiţii de alimentare	3.1.6.4.1. Alimentare curent alternativ 100-240V, 50-60 Hz. 3.1.6.4.2. Două surse de alimentare redundante Hot-swappable incluse
3.1.6.5. Suport/licenţe/ software	3.1.6.5.1. Licenţă pentru minim 10 utilizatori SSL-VPN. 3.3.6.5.1. Se va asigura licențierea soluției pentru cel puțin următoarele funcționalități: controlul aplicațiilor, protecție Antivirus, IPS, filtrare URL, protecție Antispam
3.1.6.6. Accesorii	3.1.6.6.1. Set cabluri de alimentare cu conector C14-tată, set cabluri de alimentare cu conector CEE 7/7 tată, set/kit montaj rack
3.1.6.7. Dimensiuni de gabarit	3.1.6.7.1. Rackabil 1U, 19"

3.2 Soluție UTM / NGFW tip 2

3.2.1 Specificații hardware	3.2.1.1. Minim 16 interfete de retea astfel: minim 10 interfeţe 10/100/1000 Ethernet RJ45 si minim 6 interfeţe 10 GbE SFP+ (echipate cu module 10GBase-SR) 3.2.1.2. Minim 1 port consolă. 3.2.1.3. Minim 1 port USB. 3.2.1.4. Port pentru HA 3.2.1.5. Capacitate stocare locală: minim 480 GB 3.2.1.6. Sursă redundantă de putere.
3.2.2 Caracteristici	3.2.2.1. Firewall Throughput: minim 50 Gbps 3.2.2.2. IPS Throughput: minim 8 Gbps 3.2.2.3. NGFW Throughput: minim 7 Gbps 3.2.2.4. Threat Protection/Prevention Throughput: minim 5 Gbps 3.2.2.5. IPSec VPN Throughput: minim 10.5 Gbps 3.2.2.6. Număr sesiuni concurente: minim 12.000.000 3.2.2.7. Număr sesiuni noi pe secundă: minim 200.000 3.2.2.8. Număr de instanțe virtuale: minim 10
3.2.3 Funcționalități generale	3.2.3.1. Echipament integrat de securitate cu cel puțin următoarele funcţionalități simultane: Firewall de tip stateful; Router cu suport pentru protocoale de rutare dinamice; Posibilitate de grupare a interfetelor în mod bridge; Protecţie Antivirus; Criptare de date: IPSec VPN şi SSL VPN; Suport pentru QoS şi Traffic Shaping; Detecţia şi prevenirea intruziunilor – IDS/IPS; Filtrare URL; DLP

	Blocarea şi controlul traficului din reţea generat de aplicaţii; Update-uri automate; 3.2.3.2. Toate funcţionalităţile de securitate (antivirus, IPS, filtrare URL, etc), precum şi sistemul de operare aparțin aceluiași producător
3.2.4 Funcționalități securitate	
3.2.4.1. Funcționalități firewall	3.2.4.1.1. Funcţionalităţi NAT şi Transparent Bridge 3.2.4.1.2. Opțiune de a aplica NAT per politică 3.2.4.1.3. Suport VLAN Tagging 802.1q 3.2.4.1.4. Autentificarea utilizatorilor pe grupuri 3.2.4.1.5. Suport VoIP SIP/H.323/SCCP şi Transversal NAT 3.2.4.1.6. Suport IPv6 3.2.4.1.7. Creare politici de securitate bazate pe identitatea utilizatorului/servicii folosite 3.2.4.1.8. Opţiune “Scheduling” pentru politicile de firewall
3.2.4.2. Funcţionalităţi VPN	3.2.4.2.1. Suport IPSec și SSL-VPN 3.2.4.2.2. Criptare DES, 3DES, AES 128, AES 256 3.2.4.2.3. Autentificare minim MD5/SHA-1/SHA-256 3.2.4.2.4. Funcţionalitate “Hub and Spoke” VPN 3.2.4.2.5. Suport protocol IKE 3.2.4.2.6. Suport IPSec NAT Transversal 3.2.4.2.7. Funcţionalitate Two-Factor Authentication pentru SSL-VPN 3.2.4.2.8. Suport pentru autentificare de grupuri de utilizatori prin LDAP (SSL-VPN) 3.2.4.2.9. Funcţionalităţi monitorizare tunele VPN 3.2.4.2.10. Producătorul are în portofoliu client de VPN IPSec şi SSL propriu
3.2.4.3. Funcţionalităţi Antivirus	3.2.4.3.1. Protecţie anti-malware 3.2.4.3.2. Protocoale suportate minim următoarele: HTTP/HTTPS, SMTP, POP3, FTP 3.2.4.3.3. Protecţie pe bază de reputaţie a adreselor IP şi URL-urilor 3.2.4.3.4. Update-uri automate ale semnăturilor
3.2.4.4. Funcţionalităţi sistem de control al aplicaţiilor	3.2.4.4.1. Identificarea şi controlul a peste 3000 de aplicaţii 3.2.4.4.2. Limitare de bandă per aplicaţie 3.2.4.4.3. Monitorizarea aplicaţiilor cu rata cea mai mare de consum de bandă 3.2.4.4.4. Monitorizarea aplicaţiilor pe baza IP/Utilizator

3.2.4.5. Funcţionalităţi sistem de prevenire a intruziunilor/ atacurilor (IPS)	3.2.4.5.1. Protecţie bazata pe semnături predefinite dar şi suport pentru semnături custom 3.2.4.5.2. Detectarea anomaliilor de protocol 3.2.4.5.3. Protecţie împotriva atacurilor de tip DoS 3.2.4.5.4. Update-uri automate ale semnăturilor
3.2.4.6. Funcționalități Data Loss Prevention	3.2.4.6.1. Permite definirea de reguli bazate pe: tip de fişier (fără a ţine cont de extensia fişierului), expresii regulate 3.2.4.6.2. Permite inspecţia fişierelor arhivate 3.2.4.6.3. Suport pentru document fingerprinting şi documente cu watermark 3.2.4.6.4. Permite inspecţia/logarea protocoalelor SMTP, HTTP/HTTPS şi FTP
3.2.5 Funcţionalităţi rețea	
3.2.5.1. Funcţionalităţi reţelistică şi rutare	3.2.5.1.1. Suport PPPoE şi DHCP Client/Server 3.2.5.1.2. Funcționalitate declarare rute statice 3.2.5.1.3. Rutare dinamică IPv4: RIP, OSPF, BGP, Multicast 3.2.5.1.4. Rutare dinamică Ipv6 3.2.5.1.5. Policy-based routing 3.2.5.1.6. Suport VRRP/Link Failure Control 3.2.5.1.7. Rutare între VLAN-uri 3.2.5.1.8. Suport One-to-One NAT 3.2.5.1.9. Suport NAT64
3.2.5.2. Funcţionalităţi Traffic Shaping	3.2.5.2.1. Limitare/garantare a benzii de trafic prin politici până la nivel de aplicaţie 3.2.5.2.2. Suport pentru Differentiated Services (DiffServ)
3.2.5.3. Suport instanţe virtuale	3.2.5.3.1. Fiecare echipament suporta domenii /instante virtuale cu aceleaşi funcţionalităţi de securitate precum echipamentul standard
3.2.5.4. Suport pentru centre de date – data center	3.2.5.4.1. Balansare de trafic pentru servere 3.2.5.4.2. Balansare de trafic prin metode de tip: round-robin, least RTT 3.2.5.4.3. Persistența sesiunilor
3.2.5.5. Funcţionalităţi High Availability – HA	3.2.5.5.1. Funcţionare Activ-Activ, Activ-Pasiv 3.2.5.5.2. Funcţionalitate Session Failover 3.2.5.5.3. Detectare şi notificare pentru echipament nefuncțional 3.2.5.5.4. Funcționalitate Link Failover
3.2.6 Funcţionalităţi de administrare, jurnalizare și autentificare a utilizatorilor	
3.2.6.1. Funcţionalităţi de administrare	3.2.6.1.1. Administrare prin WEB UI , Secure Command Shell (SSH) şi Command Line Interface (CLI) 3.2.6.1.2. Utilizatori/Administratori cu drepturi configurabile 3.2.6.1.3. Funcţionalitate de export/import a configuraţiei

	3.2.6.1.4. Politică de control a parolelor
3.2.6.2. Funcţionalităţi de jurnalizare şi monitorizare	3.2.6.2.1. Monitorizare grafică în timp real şi istorică 3.2.6.2.2. Functionalitate export Netflow minim v5 3.2.6.2.3. Funcționalitate export loguri în format syslog 3.2.6.2.4. Suport SNMP 3.2.6.2.5. Notificare alerte prin email
3.2.6.3. Funcţionalităţi de autentificare a utilizatorilor	3.2.6.3.1. Definire locală a utilizatorilor 3.2.6.3.2. Integrare cu Windows Active Directory (AD) pentru Single Sign On 3.2.6.3.3. Integrare cu RADIUS/LDAP/TACACS+ 3.2.6.3.4. Suport pentru autentificarea grupurilor de utilizatori prin LDAP 3.2.6.3.5. Suport pentru autentificare prin certificate digitale PKI X.509
3.2.6.4. Condiţii de alimentare	3.2.6.4.1. Alimentare curent alternativ 100-240V, 50-60 Hz. 3.2.6.4.2. Două surse de alimentare redundante Hot-swappable incluse
3.2.6.5. Suport/licenţe/ software	3.2.6.5.1. Licenţă pentru minim 10 utilizatori SSL-VPN. 3.2.6.5.2. Se va asigura licențierea soluției pentru cel puțin următoarele funcționalități: controlul aplicațiilor, protecție Antivirus, IPS, filtrare URL, protecție Antispam
3.2.6.6. Accesorii	3.2.6.6.1. Set cabluri de alimentare cu conector C14-tată, set cabluri de alimentare cu conector CEE 7/7 tată, set/kit montaj rack
3.2.6.7. Dimensiuni de gabarit	3.2.6.7.1. Rackabil 2U, 19"

3.3 Soluție UTM / NGFW tip 3

3.3.1 Specificații hardware	3.3.1.1. Minim 22 interfete de retea astfel: minim 16 interfeţe 10/100/1000 Ethernet RJ45 si minim 6 interfeţe 10 GbE SFP+ (echipate cu module 10GBase-SR) 3.3.1.2. Minim 1 port consolă. 3.3.1.3. Minim 1 port USB. 3.3.1.4. Port pentru HA 3.3.1.5. Capacitate stocare locală: minim 480 GB 3.3.1.6. Sursă redundantă de putere.
3.3.2 Caracteristici	3.3.2.1. Firewall Throughput: minim 60 Gbps 3.3.2.2. IPS Throughput: minim 11.5 Gbps 3.3.2.3. NGFW Throughput: minim 9 Gbps 3.3.2.4. Threat Protection/Prevention Throughput: minim 5.2 Gbps 3.3.2.5. IPSec VPN Throughput: minim 15 Gbps

	3.3.2.6. Număr sesiuni concurente: minim 20.000.000 3.3.2.7. Număr sesiuni noi pe secundă: minim 300.000 3.3.2.8. Număr de instanțe virtuale: minim 10
3.3.3 Funcționalități generale	3.3.3.1. Echipament integrat de securitate cu cel puțin următoarele funcţionalități simultane: Firewall de tip stateful; Router cu suport pentru protocoale de rutare dinamice; Posibilitate de grupare a interfetelor în mod bridge; Protecţie Antivirus; Criptare de date: IPSec VPN şi SSL VPN; Suport pentru QoS şi Traffic Shaping; Detecţia şi prevenirea intruziunilor – IDS/IPS; Filtrare URL; DLP Blocarea şi controlul traficului din reţea generat de aplicaţii; Update-uri automate; 3.3.3.2. Toate funcţionalităţile de securitate (antivirus, IPS, filtrare URL, etc), precum şi sistemul de operare aparțin aceluiași producător
3.3.4 Funcționalități securitate	
3.3.4.1. Funcționalități firewall	3.3.4.1.1. Funcţionalităţi NAT şi Transparent Bridge 3.3.4.1.2. Opțiune de a aplica NAT per politică 3.3.4.1.3. Suport VLAN Tagging 802.1q 3.3.4.1.4. Autentificarea utilizatorilor pe grupuri 3.3.4.1.5. Suport VoIP SIP/H.323/SCCP şi Transversal NAT 3.3.4.1.6. Suport IPv6 3.3.4.1.7. Creare politici de securitate bazate pe identitatea utilizatorului/servicii folosite 3.3.4.1.8. Opţiune “Scheduling” pentru politicile de firewall
3.3.4.2. Funcţionalităţi VPN	3.3.4.2.1. Suport IPSec și SSL-VPN 3.3.4.2.2. Criptare DES, 3DES, AES 128, AES 256 3.3.4.2.3. Autentificare minim MD5/SHA-1/SHA-256 3.3.4.2.4. Funcţionalitate “Hub and Spoke” VPN 3.3.4.2.5. Suport protocol IKE 3.3.4.2.6. Suport IPSec NAT Transversal 3.3.4.2.7. Funcţionalitate Two-Factor Authentication pentru SSL-VPN 3.3.4.2.8. Suport pentru autentificare de grupuri de utilizatori prin LDAP (SSL-VPN) 3.3.4.2.9. Funcţionalităţi monitorizare tunele VPN

	3.3.4.2.10. Producătorul are în portofoliu client de VPN IPSec şi SSL propriu
3.3.4.3. Funcţionalităţi Antivirus	3.3.4.3.1. Protecţie anti-malware 3.3.4.3.2. Protocoale suportate minim următoarele: HTTP/HTTPS, SMTP, POP3, FTP 3.3.4.3.3. Protecţie pe bază de reputaţie a adreselor IP şi URL-urilor 3.3.4.3.4. Update-uri automate ale semnăturilor
3.3.4.4. Funcţionalităţi sistem de control al aplicaţiilor	3.3.4.4.1. Identificarea şi controlul a peste 3000 de aplicaţii 3.3.4.4.2. Limitare de bandă per aplicaţie 3.3.4.4.3. Monitorizarea aplicaţiilor cu rata cea mai mare de consum de bandă 3.3.4.4.4. Monitorizarea aplicaţiilor pe baza IP/Utilizator
3.3.4.5. Funcţionalităţi sistem de prevenire a intruziunilor/ atacurilor (IPS)	3.3.4.5.1. Protecţie bazata pe semnături predefinite dar şi suport pentru semnături custom 3.3.4.5.2. Detectarea anomaliilor de protocol 3.3.4.5.3. Protecţie împotriva atacurilor de tip DoS 3.3.4.5.4. Update-uri automate ale semnăturilor
3.3.4.6. Funcționalități Data Loss Prevention	3.3.4.6.1. Permite definirea de reguli bazate pe: tip de fişier (fără a ţine cont de extensia fişierului), expresii regulate 3.3.4.6.2. Permite inspecţia fişierelor arhivate 3.3.4.6.3. Suport pentru document fingerprinting şi documente cu watermark 3.3.4.6.4. Permite inspecţia/logarea protocoalelor SMTP, HTTP/HTTPS şi FTP
3.3.5 Funcţionalităţi rețea	
3.3.5.1. Funcţionalităţi reţelistică şi rutare	3.3.5.1.1. Suport PPPoE şi DHCP Client/Server 3.3.5.1.2. Funcționalitate declarare rute statice 3.3.5.1.3. Rutare dinamică IPv4: RIP, OSPF, BGP, Multicast 3.3.5.1.4. Rutare dinamică Ipv6 3.3.5.1.5. Policy-based routing 3.3.5.1.6. Suport VRRP/ Link Failure Control 3.3.5.1.7. Rutare între VLAN-uri 3.3.5.1.8. Suport One-to-One NAT 3.3.5.1.9. Suport NAT64
3.3.5.2. Funcţionalităţi Traffic Shaping	3.3.5.2.1. Limitare/garantare a benzii de trafic prin politici până la nivel de aplicaţie 3.3.5.2.2. Suport pentru Differentiated Services (DiffServ)
3.3.5.3. Suport instanţe virtuale	3.3.5.3.1. Fiecare echipament suporta domenii /instante virtuale cu aceleaşi funcţionalităţi de securitate precum echipamentul standard

3.3.5.4. Suport pentru centre de date – data center	3.3.5.4.1. Balansare de trafic pentru servere 3.3.5.4.2. Balansare de trafic prin metode de tip: round-robin, least RTT 3.3.5.4.3. Persistența sesiunilor
3.3.5.5. Funcţionalităţi High Availability – HA	3.3.5.5.1. Funcţionare Activ-Activ, Activ-Pasiv 3.3.5.5.2. Funcţionalitate Session Failover 3.3.5.5.3. Detectare şi notificare pentru echipament nefuncțional 3.3.5.5.4. Funcționalitate Link Failover
3.3.6 Funcţionalități de administrare, jurnalizare și autentificare a utilizatorilor	
3.3.6.1. Funcţionalităţi de administrare	3.3.6.1.1. Administrare prin WEB UI , Secure Command Shell (SSH) şi Command Line Interface (CLI) 3.3.6.1.2. Utilizatori/Administratori cu drepturi configurabile 3.3.6.1.3. Funcţionalitate de export/import a configuraţiei 3.3.6.1.4. Politică de control a parolelor
3.3.6.2. Funcţionalităţi de jurnalizare şi monitorizare	3.3.6.2.1. Monitorizare grafică în timp real şi istorică 3.3.6.2.2. Functionalitate export Netflow minim v5 3.3.6.2.3. Funcționalitate export loguri în format syslog 3.3.6.2.4. Suport SNMP 3.3.6.2.5. Notificare alerte prin email
3.3.6.3. Funcţionalităţi de autentificare a utilizatorilor	3.3.6.3.1. Definire locală a utilizatorilor 3.3.6.3.2. Integrare cu Windows Active Directory (AD) pentru Single Sign On 3.3.6.3.3. Integrare cu RADIUS/LDAP/TACACS+ 3.3.6.3.4. Suport pentru autentificarea grupurilor de utilizatori prin LDAP 3.3.6.3.5. Suport pentru autentificare prin certificate digitale PKI X.509
3.3.6.4. Condiţii de alimentare	3.3.6.4.1. Alimentare curent alternativ 100-240V, 50-60 Hz. 3.3.6.4.2. Două surse de alimentare redundante Hot-swappable incluse
3.3.6.5. Suport/licenţe/ software	3.3.6.5.2. Licenţă pentru minim 10 utilizatori SSL-VPN. 3.3.6.5.3. Se va asigura licențierea soluției pentru cel puțin următoarele funcționalități: controlul aplicațiilor, protecție Antivirus, IPS, filtrare URL, protecție Antispam
3.3.6.6. Accesorii	3.3.6.6.1. Set cabluri de alimentare cu conector C14-tată, set cabluri de alimentare cu conector CEE 7/7 tată, set/kit montaj rack
3.3.6.7. Dimensiuni de gabarit	3.3.6.7.1. Rackabil 2U, 19"

3.4 Soluție UTM / NGFW tip 4

3.4.1. Specificații hardware	3.4.1.1. Suportă instalarea a minim 48 de interfete de 1 GbE RJ45 Cu (minim 16 porturi Cu instalate cu conector RJ45) 3.4.1.2. Minim 60 de interfete de 10 GbE SFP+ (minim 4 porturi optice instalate SR cu conector dual LC) 3.4.1.3. Minim 12 interfete 40 GbE QSFP+ (minim 2 porturi optice instalate SR cu conector dual LC) 3.4.1.4. Minim o interfata de management dedicata 3.4.1.5. Alimentare curent alternativ 100-240V, 50-60 Hz. 3.4.1.6. Două surse de alimentare redundante Hot-swappable incluse. 3.4.1.7. MTBF minim 100.000 ore.
3.4.2. Caracteristici	3.4.2.1. Firewall throughput: minim 300 Gbps 3.4.2.2. Threat inspection throughput: minim 50Gbps (folosind ca incarcare pachete HTTP de 64KB sau pachete UDP de 1518 byte) 3.4.2.3. IPSec VPN Throughput: minim 150 Gbps 3.4.2.4. Minim 60.000 tuneluri IPSec concurente 3.4.2.5. Minim 192M conexiuni concurente 3.4.2.6. Minim 2M conexiuni TCP noi pe secunda
3.4.3. Funcționalități generale	3.4.3.1. Solutia trebuie să suporte automatizarea utilizând REST API 3.4.3.2. Soluția trebuie să întrunească cel puţin 96% Security Effectivness în raportul NSS Labs pentru NGFW/NGIPS din anul 2019 3.4.3.3. Licente activate: IDS/IPS cu posibilitate de decriptare trafic, SD-WAN, Threat prevention (antivirus, anti-spyware si protectie vulnerabilitati), URL Filtering, Contexte virtuale: minim 50 de contexte virtuale licentiate, Licente clienti VPN (minim 8000 de clienti), Analiza grafica jurnale, Platforma management
3.4.4. Funcționalități securitate	3.4.4.1. Soluţia trebuie să valideze politicile inainte de aplicarea lor pe echipamente 3.4.4.2. Soluţia trebuie să ofere o analiză detaliată a evenimentelor 3.4.4.3. Soluţia trebuie să poată prezenta rapoarte de trafic detaliate şi personalizabile precum şi activităţile rău intenţionate 3.4.4.4. Soluţia trebuie să ofere capabilităţi avansate de detectare şi analiză a malware-ului printr-o soluţie de tip sandbox on-premises produsă de acelaşi producător cu

	următoarele caracterisitici (capacitate de stocare minim 7000 de fişiere pe zi, dimensiune maximă 2U, capacitate de stocare minim 1.2 TB, minim 128GB memorie RAM, fişiere suportate minim: PDF, executabile Windows, Documente Office, zip, jar) 3.4.4.5. Soluţia trebuie să ofere client VPN IPSec sau SSL pentru Microsoft Windows si Android 3.4.4.6. Soluţia trebuie să ofere o protecţie completă NGIPS cu posibilitatea de a decripta traficul 3.4.4.7. Soluţia trebuie să poată monitoriza şi controla traficul per utilizator, adresa, aplicaţie utilizată sau adresa/categorie URL 3.4.4.8. Soluţia trebuie să poată filtra/monitoriza traficul şi logurile dupa locaţia geografică sau ţară 3.4.4.9. Soluţia trebuie să ofere protecţie anti-bot şi anti-malware 3.4.4.10. Soluția trebuie să poată filtra adresele URL (URL filtering) folosind cel puţin 60 de categorii URL în peste 40 de limbi de circulaţie internaţională 3.4.4.11. Soluția trebuie să ofere funcţii de securitate avansate cum ar fi semnături de aplicații, IPS integrat şi capacitatea de a detecta şi proteja împotriva atacurilor avansate (“evasion techniques”)
3.4.5. Funcţionalităţi rețea	3.4.5.1. Solutia oferita trebuie sa suporte o redundanta de tip activ-activ (2 echipamente) intr-o locatie centrala 3.4.5.2. Solutia trebuie sa suporte agregarea legaturilor (802.3ad) si optimizarea multi-link 3.4.5.3. Solutia trebuie sa ofere suport pentru protocoale de rutare dinamica 3.4.5.4. Solutia trebuie sa aiba capabilitati IPv6 cum ar fi dual-stack IPv4/IPv6, ICMPv6, DNSv2 si NAT 3.4.5.5. Solutia trebuie sa suporte VLAN tagging 3.4.5.6. Solutia trebuie sa oferte funcționalitatea de proxy pentru traficul SSH, HTTP, HTTPS, FTP, DNS 3.4.5.7. Solutia trebuie sa poata utiliza mai multe linkuri ISP. 3.4.5.8. Funcţionalități de administrare, jurnalizare si autentificare a utilizatorilor 3.4.5.9. Soluția trebuie să ofere un management centralizat care să suporte pana la 2000 echipamente 3.4.5.10. Platforma de management trebuie sa poata fi accesata printr-un client local sau prin interfata web (minim

	Mozilla Firefox si Google Chrome) 3.4.5.11. Platforma de management trebuie sa suporte mai multe conturi de administrator 3.4.5.12. Platforma de management trebuie sa poata fi integrata cu Active Directory sau similar prin LDAP securizat 3.4.5.13. Platforma de management trebuie sa poata administra toate echipamentele NGFW/NGIPS inclusiv actualizarea, configurarea, monitorizarea si raportarea intregului mediu NGFW/NGIPS implementat 3.4.5.14. Platforma de management trebuie sa ofere automatizarea activitatii si validarea configuratiei in momentul in care aceasta este trimisa catre echipamente 3.4.5.15. Solutia trebuie sa poata utiliza informatii din baze de date de utilizatori cum ar fi LDAP, Active Directory, RADIUS, TACACS+ 3.4.5.16. Soluția trebuie să fie capabila de stocarea a logurilor de trafic şi a tuturor setărilor ce ţin de configurațiile întregii platforme

4 Livrabile:

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de tip Unified Threat Management / NexT Generation Firewall.

5 Implementare

5.1 Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip Unified Threat Management/NexT Generation Firewallse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractuluişi va includecel puțin

următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- crearea/migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la momentul livrării,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- configurarea soluției pentru jurnalizarea evenimentelor la nivelul soluției SIEM,
- asigurarea de sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

5.2 Garanţie şi suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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

instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Starea actuală a soluției UTM la IVC

Nr. crt.	***Soluție existenta***	***Nr. buc.***
	FG800C	21
2.	FG200D	25
3.	FG200C	1

Distribuția soluției UTM/NGFW necesar a fi instalată

Nr. crt.	*Tip soluție*	*Nr. total buc.*	*Livrare*
1.	Tip 1	58	56 (București) 2 (Timiș)
2.	Tip 2	20	20 (București)
3.	Tip 3	6	6 (București)
4.	Tip 4	2	2 (București)

Anexa 2 la caietul de sarcini

SOLUȚIE DE TIP EMAIL GATEWAY

1. Descrierea situației actuale

La momentul actual există 26 de instituții cu valențe critice (IVC) care dețin soluție de tip Email Gateway(Cisco Email Security Appliance).

2. Caracteristici tehnice minimale:

2.1	Soluție de tip Email Gateway ce va conține 19 instanțe hardware și instanțe virtuale ce vor fi folosite în cadrul IVC-urilor în functie de necesitățile autorității contractante. Soluția va conține o licență care să protejeze concomitent cel puțin 25.000 de utilizatori simultani prin intermediul tuturor instanțelor din cadrul soluției. Soluția trebuie să asigure protecția utilizatorilor având capabilități de a carantina sau bloca mesajele de tip e-mail care conțin malware, spam, phishing sau alt tip de conținut cu comportament malițios.
2.2	Se va asigura licențierea soluției pentru cel puțin următoarele funcționalități: antivirus, antispam, filtrare dupa reputatie, criptare și DLP.
2.3	În cazul în care soluția ofertată este diferită de soluția existentă (Cisco Email Security Appliance) ofertantul are obligația: I. de a importa în echipamentele noi toate configurațiile vechi, inclusiv modificările aduse de Centrul Național Cyberint (scripturi, configurări, export de date, etc.); II. de a efectua o sesiune de instruire de minim 5 zile, pentru 5 persoane ce trebuie să prezinte noțiuni specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului ofertat**,** incluzând, dar fară a se limita la următoarele informaţii: Bune practici privind instalarea, configurarea şi administrarea soluţiei,

	Prezentarea interfeţelor de administrare (CLI, web) şi a principalelor acţiuni ce pot fi întreprinse prin intermediul acestora, Politici de filtrare email-uri, anti-malware şi anti-spam, inclusiv prin intermediul whitelists / blacklists şi reputaţie, Noţiuni privind detecţia şi remedierea defecţiunilor tehnice (troubleshooting), Politici de prevenire a exfiltrarilor de date accidentale (Data Loss Prevention), Configurare două echipamente similare în mod redundant (High Availability), Configurare serviciu de logare pentru transmitere evenimente prin unul din protocoalele syslog /syslog CEF, ftp, scp. Cursul va fi de tip "*hands-on*", cu activități practice în care cursanții utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului. Cursul se va desfășura în limba română, într-o locație pusă la dispoziție de furnizor, în municipiul București. Instructorul trebuie să fie acreditat de producătorul soluției. Pentru demonstrarea pregătirii instructorului se vor prezenta certificate/autorizări/acreditări, sau alte documente emise de către producătorul soluției, sau de organisme abilitate în acest sens. Ofertantul va asigura servicii de catering pe perioada cursului, respectiv o masă de prânz şi un coffee-break pe zi(cafea, apă, ceai, produse de patiserie şi fructe, la discreţie).
2.4	Asigură implementarea în cadrul infrastructurii beneficiarului în mod proxy "Mail Relay".
2.5	Deține certificare de tipul FIPS 140-2.
2.6	Echipamentul trebuie dimensionat astfel încât să poată asigura securitarea corespondenței de email pentru un număr de minim 10000 de utilizatori.
2.7	Oferă protecţie anti-malware şi anti-spam.
2.8	Suportă protocoalele SMTP şi SMTPS.
2.9	Asigură crearea rolurilor de administrare şi crearea unor spaţii de lucru specifice rolului şi drepturilor acestuia.
2.10	Oferă facilitatea aplicării politicilor de securitate prin modificarea regulilor predefinte sau prin adăugarea unor noi reguli, în funcţie de necesităţi.
2.11	Asigură actualizarea periodică, în mod automat a semnăturilor anti-malware şi anti-spam prin interconectare în mediul Internet.
2.12	Oferă posibilitatea salvării configuraţiei pentru realizarea unei copii de siguranţă.
2.13	Dispune de capabilităţi de identificare şi blocare a exfiltrărilor de date tip „*DLP*" prin analiza conţinutului email-urilor şi a ataşamentelor.
2.14	Asigură scanarea fişierelor comprimate/arhivate.

2.15	Asigură cel puțin următoarele capabilităţi anti-malware: •Detecţia şi blocarea aplicaţiilor maliţioase regăsite în ataşamentele mesajelor pe bază de semnături și tehnici euristice. •Mutarea în carantină a fişierelor infectate.
2.16	Asigură cel puțin următoarele capabilităţi anti-spam: •Carantină şi prezintă capabilităţi de identificare a spam-ului ce includ următoarele metode: „*bayesian*”, pe baza reputaţiei expeditorilor, RBL; •filtrarea email-urilor după: „*whitelists*”, „*blacklists*” şi scanare URL-uri existente în corpul mesajelor.
2.17	Oferă posibilitatea creării politicilor de filtrare a ataşamentelor.
2.18	Oferă protecţie împotriva atacurilor de tip „*directory harvest*”, „*phishing*” şi „*misdirected bounce”.*
2.19	Oferă un mecanism de management al mesajelor de tip ”bulk mail”.
2.20	Oferă posibilitatea de integrare cu servere LDAP pentru extragerea informaţiilor despre utilizatori, crearea grupurilor şi folosirea acestora în dezvoltarea politicilor.
2.21	Asigură facilitățile DKIM și SPF de validare a mesajelor.
2.22	Asigură crearea unor politici de redirecţionare a mesajelor email.
2.23	Asigură posibilitatea utilizării a cel puţin unui motor de scanare antivirus pentru identificarea aplicaţiilor maliţioase.
2.24	Oferă posibilitatea activării unei soluții de tip Advanced Malware Protection ce poate asigura următoarele facilități: - posibilitatea acordării de scoruri sau reputație și blocare - sandboxing
2.25	Asigură administrarea de la distanţă prin CLI sau interfaţă Web.
2.26	Dispune de capabilităţi de raportare prin intermediul unor grafice de funcţionare şi încărcare pe intervale de timp şi asigură generarea de statistici privind activitatea anti-spam, anti-virus şi a mesajelor prelucrate.
2.27	Oferă elaborarea de rapoarte complexe pe bază de şabloane predefinite ce cuprind cel puţin următoarele elemente: Tipuri de aplicaţii malware; Statusul de livrare al mesajelor email; adrese de email destinaţie/sursă; Politici de filtrare a conţinutului mesajelor electronice.
2.28	Asigură exportul rapoartelor cel puţin în format csv sau pdf.
2.29	Asigură auditul interacțiunii cu interfața WEB a utilizatorilor.
2.30	Log-urile generate sunt stocate local, iar utilizatorul are posibilitatea de a le exporta către un echipament extern cel puțin prin unul din protocoalele syslog /syslog CEF, ftp, scp.
2.31	Dimensiuni de gabarit: 19”, rackabil, maxim 2U.

3. Livrabile:

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de tipEmail Gateway**.**

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip Email Gatewayse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- crearea/migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la momentul livrării,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,

- configurarea soluției pentru jurnalizarea evenimentelor la nivelul soluției SIEM existente la fiecare beneficiar,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

4.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Distribuția soluției *Email Gateway* necesar a fi instalată

Nr. crt.	***Tip soluție***	***Nr. total buc.***	***Livrare***
	Email Gateway	19	București -15 buc Constanța - 2 buc Sibiu - 1 buc Timiș - 1 buc

Anexa 3 la caietul de sarcini

SOLUȚIE DE TIP WEB GATEWAY

1. Descrierea situației actuale

Soluția de tip Web Gateway reprezintă o soluție hardware integrată de protecție a utilizatorilor dintr-o rețea cibernetică cu capabilităţi de analiză a traficului web, protecție anti-malware și filtrare URL - Uniform Resource Locator.

La momentul actual există 34 de instituții cu valențe critice (IVC) care dețin soluțietip Web Gateway(Cisco Web Security Appliance).

Soluția solicitată va fi compusă din:

soluție Web Gateway tip 1 – 17 bucăți;

soluție Web Gateway tip 2 – 2 bucăți;

2. Caracteristici tehnice minimale:

2.1 Soluție Web Gateway tip 1

2.1.1	Soluție de tip Web Gateway ce va conține 17 instanțe hardware și instanțe virtuale ce vor fi folosite în cadrul IVC-urilor în funcție de necesitățile autorității contractante. Soluția va conține o licență care să protejeze cel puțin 25.000 de utilizatori simultan, și care va fi implementată pe toate instanțele din cadrul soluției.
2.1.2	Se va asigura licențierea soluției pentru cel puțin următoarele funcționalități: antivirus, filtrare după categorii URL, monitorizare trafic (layer 4) și controlul traficului la nivel de aplicație;
2.1.3	În cazul în care soluția ofertată este diferită de soluția existentă (Cisco Web Security Appliance) ofertantul are obligația: I. de a importa în echipamentele noi toate configurațiile vechi, inclusiv modificările aduse de Centrul Național Cyberint (scripturi, configurări, export de date, etc.); II. de a efectua o sesiune de instruire de minim 5 zile, pentru 5 persoane, ce trebuie să prezinte noțiuni specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului ofertat**,** incluzând, dar fară a se limita la, următoarele informaţii: Bune practici privind instalarea, configurarea şi administrarea soluţiei, Prezentarea interfeţelor de administrare (CLI, web) şi a principalelor acţiuni ce pot fi întreprinse prin intermediul acestora, Politici de filtrare URL şi anti-malware, inclusiv prin intermediul whitelists / blacklists, reputaţie şi categorii URL, Noţiuni privind detecţia şi remedierea defecţiunilor tehnice (troubleshooting), Configurarea serviciilor proxy HTTP, HTTPS şi FTP Prezentarea modului de realizare a rapoartelor şi de rulare a acestora,

	Configurare serviciu de logare pentru transmitere evenimente prin unul din protocoalele syslog/syslog CEF, ftp, scp. Cursul va fi de tip "*hands-on*", cu activități practice în care cursanții utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului. Cursul se va desfășura în limba română, într-o locație pusă la dispoziție de furnizor, în municipiul București. Instructorul trebuie să fie acreditat de producătorul soluției. Pentru demonstrarea pregătirii instructorului se vor prezenta certificate/autorizări/acreditări, sau alte documente emise de către producătorul soluției, sau de organisme abilitate în acest sens. Ofertantul va asigura servicii de catering pe perioada cursului, respectiv o masă de prânz şi un coffee-break pe zi(cafea, apă, ceai, produse de patiserie şi fructe, la discreţie).
2.1.4	Asigură implementarea în cadrul unei infrastructuri de reţea cel puţin a următoarelor configuraţii: •Proxy explicit; •Transparent.
2.1.5	Deține certificare de tipul FIPS 140-2.
2.1.6	Asigură crearea rolurilor de administrare (RBAC) şi crearea unor spaţii de lucru specifice rolului şi drepturilor acestora.
2.1.7	Echipamentul trebuie dimensionat astfel încât să poată asigura securitatea pentru minim 10000 de utilizatori conectați simultan.
2.1.8	Suportă funcţionarea în mod High-Availability.
2.1.9	Asigură aplicarea politicilor de securitate pe utilizatori/ grupuri de utilizatori ce vor fi preluaţi dintr-un server LDAP și Secure LDAP.
2.1.10	Asigură conectarea la o bază de date cu informaţii/cunoştinţe creată şi menţinută de producător, în vederea recepţionării informaţiilor despre noi categorii web şi reputaţia unor site-uri web, necesare pentru protecţia utilizatorilor.
2.1.11	Asigură actualizarea zilnică, în mod automat, a semnăturilor anti-malware prin interconectare în mediul Internet.
2.1.12	Actualizările sistemului de operare pot fi realizate din interfaţa grafică.
2.1.13	Asigură salvarea configurației pentru realizarea unei copii de siguranță.
2.1.14	Asigură integrarea cu soluții dedicate de tipul DLP prin intermediul protocolului ICAP.
2.1.15	Asigură decriptarea sesiunilor SSL prin tehnici precum „*man-in-the-middle*" compatibile cu TLS1.1, TLS1.2, TLS1.3.
2.1.16	Asigură detecţia/blocarea aplicaţiilor malware în traficul inspectat.
2.1.17	Asigură controlul traficului după categorii de aplicaţii, cel puţin pentru: •Servicii de evitare a filtrelor/de anonimizare, •Mesagerie Instantă și chat; •"Blogging";

	•Actualizări software; •Web-based email; •Jocuri online; •Social networking; •Site-uri pentru transfer „peer-to-peer”; •Partajare de fișiere.
2.1.18	Oferă opţiuni de limitare/blocare a traficului per aplicație.
2.1.19	Asigură controlul site-urilor WEB 2.0. care își modifică conținutul în mod dinamic.
2.1.20	Dispune cel puţin de următoarele capabilităţi de filtrare URL: •filtrarea după categorii URL predefinite (Ex.: pornografie, socializare, servicii de e-mail prin portal web, anonimizare, jocuri de noroc, „web chat”, „peer-to-peer”); •crearea de noi categorii URL, modificarea listelor categoriilor predefinite, dar şi eliminarea unui site web încadrat greşit în cele predefinite; •filtrarea accesului după categoriile definite; •contorizarea şi limitarea timpului de acces pentru fiecare categorie în parte după utilizator/grup de utilizatori; •blocarea manuală a unor URL-uri prin cuvinte cheie sau prin construirea expresiilor regulate tip „regex”.
2.1.21	Oferă posibilitatea creării unor pagini web specifice ce vor fi prezentate utilizatorilor în cazul violării unei politici de securitate, precum şi afişarea unui mesaj pentru aducerea la cunoştinţă a politicii de securitate a beneficiarului.
2.1.22	Oferă posibilitatea creării de politici prin care poate fi blocată descărcarea unor fişiere în funcţie de tipul acestora.
2.1.23	Asigură posibilitatea utilizării a cel puţin unui motor de scanare antivirus pentru identificarea aplicaţiilor maliţioase.
2.1.24	Oferă posibilitatea activării unei soluții de tip Advanced Malware Protection ce poate asigura următoarele facilități: - posibilitatea acordării de scoruri sau reputație și blocare - sandboxing
2.1.25	Asigură administrarea de la distanţă prin CLI (prin protocolul SSH) şi prin intermediul interfeţei Web (prin protocoalele HTTP/ HTTPS), de asemenea oferă posibilitatea realizării configurărilor de reţea prin intermediul intefeţei web.
2.1.26	Asigură realizarea de raportări complexe prin intermediul unor şabloane predefinite
2.1.27	Fișierele jurnal (logurile) generate sunt stocate local şi transmise către un echipament extern folosind cel puțin unul dintre protocoalele syslog/syslog CEF, ftp, scp, pentru colectare centralizată într-o soluţie de tip SIEM.

2.2 Soluție Web Gateway tip 2

2.2.1	Soluţia oferită trebuie să suporte implementări de tip local (on-premises), hybrid

	sau cloud fără a necesita licenţe suplimentare.
2.2.2	Soluţia oferită trebuie să suporte URL Filtering. Filtrarea URL se va face pe bază de categorii. De asemenea filtrarea se va face pe baza reputației fiecarui site în parte. Actualizarea atât a categoriilor cât și a reputației curente a fiecărui site intra în responsabilitatea furnizorului de produs, acestea trebuind a fi făcute automat și fără intervenția unui administrator.
2.2.3	Soluția oferită trebuie aibă capabilități de protecție antivirus şi antimalware.
2.2.4	Soluţia oferită trebuie să suporte clasificarea şi analizarea paginilor web în timp real din punct de vedere al securităţii. Clasificarea va fi realizată pe bază de conţinut.
2.2.5	Soluția oferită trebuie sa ofere posibilitatea de a crea categorie proprie în care se pot adaugă IP-uri sau domenii pentru cazuri specifice.
2.2.6	Soluția oferită trebuie să permită crearea unor politici granulare pentru controlul aplicaţiilor web. De exemplu, politica soluţiei oferite va putea permite accesul la Facebook, dar nu şi la Facebook Chat.
2.2.7	Soluția oferită trebuie să poată monitoriza, analiza sau aplica politici pentru traficul criptat HTTPS folosind certificat intern sau oferit de organizaţie.
2.2.8	Soluţia oferită va permite crearea de politici diferențiate bazate pe tip de protocol sau categorie web, cărora să li se poată asocia o bandă disponibilă.
2.2.9	Soluția oferită trebuie să suporte proxy explicit (adăugând adresa/FQDN în browser sau fișier PAC) sau proxy transparent (WCCP).
2.2.10	Soluţia va asigura aplicarea politicilor de securitate pe utilizatori/grupuri de utilizatori ce vor fi preluaţi dintr-un server LDAP.
2.2.11	Soluția oferită trebuie să poată aplica politici de acces ce pot fi setate cu parametri precum ora și data.
2.2.12	Soluția oferită trebuie să poată aplica politici bazate pe cote de utilizare. De exemplu, accesul la Facebook este permis în timpul orelor de program, dar cu o limită de maximum 1 oră.
2.2.13	Soluția oferită trebuie să poată fi administrată centralizat, folosind o interfață de management web.
2.2.14	Soluția oferită trebuie să permită autentificarea administratorilor folosind conturi locale sau conturi de domeniu.
2.2.15	Soluția oferită permite integrarea nativă cu o tehnologie de tip “data loss prevention (DLP)”.
2.2.16	Soluția oferită va permite integrarea nativă cu o tehnologie de tip “sandbox”, care să permită executarea şi analizarea fişierelor rămase suspecte după ce acestea au fost scanate şi analizate de către Proxy.
2.2.17	Soluția oferită trebuie să poată analiza site-urile Web 2.0, care îşi modifică conținutul în mod dinamic.
2.2.18	Soluția oferită trebuie să poată monitoriza şi bloca aplicații de cloud de tip “Shadow IT”, în special pe cele cu risc mare.
2.2.19	Soluția oferită trebuie să aibă capabilităţi de integrare nativă cu soluții de tip CASB, de preferat de la același producător pentru a filtra şi proteja traficul către

	aplicații de tip cloud contractate de către organizație (ex.: Office 365, G Suite etc.).
2.2.20	Soluția oferită trebuie să poată pune la dispoziție atât echipamente fizice (tip “appliance”) cât şi variante virtualizate (tip „virtual appliance”) cu funcții identice, folosind aceleași licențe, configurabile și administrabile din managementul centralizat. Variantele virtualizate trebuie sa suporte cel puțin unul din următoarele hypervizoare: VMware ESXi şi Microsoft Hyper-V.
2.2.21	Soluţia oferită trebuie să suporte clustering şi Virtual IP (VIP).
2.2.22	Soluția oferită trebuie să suporte protecția dispozitivelor mobile, în special laptopuri şi atunci când acestea sunt în afara reţelei organizaţiei.
2.2.23	Prin intermediul interfeței de management, soluția oferită trebuie să poată administra echipamentele fizice sau virtuale.
2.2.24	Soluția oferita trebuie să poată raporta problemele apărute prin intermediul email-ului sau prin SNMP.
2.2.25	Soluţia oferită trebuie să fie livrată cu suport de la furnizor pentru orice hardware/software/add-on (WEB Security Mobile, URL Filtering, Web Security DLP, Web Security, Protecţie antivirus şi antimalware) pentru 8000 utilizatori.

3. Livrabile:

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de tip Web Gateway.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip Web Gatewayse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractuluişi va include cel puțin următoarele servicii:

- montarea în rack,

- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- crearea/migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la momentul livrării,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- configurarea soluției pentru jurnalizarea evenimentelor la nivelul soluției SIEM existente la fiecare beneficiar,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

4.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Distribuția soluției *Web Gateway* necesar a fi instalată

Nr. crt.	***Tip soluție***	***Nr. total buc.***	***Livrare***
	Web Gateway tip 1	17	București - 15 buc Constanța - 1 buc Timiș - 1 buc
2.	Web Gateway tip 2	2	București - 2 buc

Anexa 4 la caietul de sarcini

SOLUȚIE DE TIP SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

1. Descriere situației actuale

La momentul actual, instituțiile cu valențe critice (IVC) care dețin soluții de tip SIEM este următoarea:

37 IVC-uri dețin soluția ArcSight Express Appliance cu licență de 500 EPS;

1 IVC deține soluția ArcSight Express cu licență de 1000 EPS;

În cadrul Centrului Național Cyberint există o licență de Arcsight ESM nelimitată ca număr de EPS cu SAID 107475297562.

În cadrul a 18 IVC-uri nu există nicio soluție de tip SIEM.

2.Caracteristici tehnice minimale:

2.1	Soluțiela cheie de tip SIEM, ce va conține toate componentele hardware/software necesare bunei funcționări a acesteia. Soluția va fi distribuită în cadrul a 56 de IVC-uri și o componentă la nivelul Centrului Național Cyberint care să centralizeze alertele de securitate colectate în cadrul tuturor IVC-urilor. Soluția trebuie să asigure preluarea evenimentelor de securitate de la toate sursele generatoare de evenimente din cadrul IVC-urilor, transmiterea acestora către componenta SIEM ce trebuie instalată în cadrul Centrului Cyberint și configurarea acestei componente, în conformitate cu cele mai bune practici în domeniu, pentru a genera conținut relevant din punct de vedere al securității cibernetice.
2.2	În cazul în care soluția ofertată este diferită de soluția existentă (ArcSight Express și Arcsight ESM) ofertantul trebuie să asigure cel puțin următoarele: - migrarea tuturor resurselor (asseturi, reguli de corelare, liste, active channels, dashboard-uri, query, query viewer, rapoarte, etc.) din soluția aflată în exploatare și crearea de conținut nou la solicitarea expresă din partea beneficiarului - migrarea tuturor evenimentelor stocate în cadrul soluției existente; - sesiune de instruire formată din două etape de minim 5 zile fiecare, pentru 12 persoane ce trebuie să prezinte noțiuni specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului ofertat**,** incluzând, dar fară a se limita la următoarele informaţii: Prezentarea modului de instalare a tuturor componentelor soluției, Prezentarea funcționalităților componentelor soluției, Prezentarea interfeţei de administrare şi a principalelor acţiuni ce pot fi întreprinse prin intermediul acesteia, Prezentarea modului de preluare (standard sau custom) a evenimentelor de securitate de la echipamente și aplicații, Principii colectare evenimente de securitate nestandardizate prin intermediul

	regex, Prezentarea tuturor resurselor implementate în cadrul soluției, Prezentarea modalităților de monitorizare în timp real a evenimentelor de securitate şi filtrare a evenimentelor după: timp, adresă IP sursă/destinaţie, nume sau tip, Principii, definire şi particularizare a modelelor de reţea, Prezentarea modului de creare a regulilor de corelare, Prezentarea modului de creare a rapoartelor particularizate şi rularea acestora în mod automat la intervale de timp prestabilite, Principii de creare şi personalizare a *dashboards*. Bune practici pentru a eficientiza activitatea de identificare a amenințărilor cibernetice Cursul va fi de tip "*hands-on*", cu activități practice în care cursanții utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului. Cursul se va desfășura în limba română,în două etape, prima într-o locație pusă la dispoziție de furnizor, în municipiul București, iar a doua la sediul beneficiarului, chiar pe infrastructura instalată. Instructorul trebuie să fie acreditat de producătorul soluției. Pentru demonstrarea pregătirii instructorului se vor prezenta certificate/autorizări/acreditări, sau alte documente emise de către producătorul soluției, sau de organisme abilitate în acest sens. Ofertantul va asigura servicii de catering pe perioada cursului, respectiv o masă de prânz şi un coffee-break pe zi(cafea, apă, ceai, produse de patiserie şi fructe, la discreţie).
2.3	Ofertantul va asigura maparea reţelei informatice existente în cadrul fiecărei IVC în soluţia SIEM prin definirea zonelor de reţea şi a asset-urilor existente, integrarea tuturor surselor generatoare de date existente în cadrul fiecărei IVC, surse menţionate la momentul instalării, și transmiterea automată către soluţia SIEM din cadrul Centrului Naţional Cyberint a alertelor de securitate în conformitate cu cerințele beneficiarului în momentul instalării.
2.4	Soluția trebuie să asigure pentru fiecare IVC capacitatea de procesare specificată în anexa A. Pentru infrastructurile care dețin soluția SIEM, se acceptă upgrade funcțional din punct de vedere al puterii de procesare al soluției actuale cu asigurarea continuității suportului (înlocuirea echipamentului hardware în caz de defectare a acestuia) sau înlocuirea acesteia cu o soluție de la alt producător. Upgrade-ul funcțional trebuie să mențină funcționalitățile soluției SIEM cel puțin la același nivel cu cel oferit de soluția aflată în exploatare conform fișei tehnice date de producător. Toate produsele SIEM din cadrul soluției trebuie să fie dezvoltate de același producător.

2.5	În cadrul Centrului Național Cyberint ofertantul va asigura instalarea componentei SIEM, pe suportul hardware din cadrul soluției High Power Computing (anexa 12 din prezentul caiet de sarcini).
2.6	Soluția trebuie să asigure în mod implicit colectarea şi interpretarea evenimentelor de la cel puțin următoarele echipamente de securitate IT, aplicaţii informatice sau sisteme de operare: MicrosoftWindows 10, Microsoft Server 2008, Microsoft Server 2012, Microsoft Server 2016, Sistem de operare IBM AIX, Sistem de operare UNIX/LINUX, Sistem de operare Solaris, Sistem de operare HP UX, Kaspersky Antivirus, McAfee VirusScan (sau McAfee ePolicy Orchestrator), Symantec EndPoint Protection, TrendMicro (Office Scan. Control Manager), IBM WebSphere, Oracle Weblogic, Sistem de virtualizare: VMWare ESX/ESXi şi vCenter, Microsoft Exchange, IBM Domino, Cisco Router, Juniper Router, Cisco Catalyst Switch, HP Switch, Nortel Contivity Switch, Cisco PIX Firewall, Cisco ASA Firewall, Checkpoint Firewall, Juniper Firewall, Fortinet Fortigate, Palo Alto Networks Firewall, SonicWALL Firewall, Snort IDS/IPS, Sourcefire IDS/IPS, Trend Micro TippingPoint IDS/IPS, Cisco IPS, McAfee Host Intrusion Prevention(sau McAfee ePolicy Orchestrator), Radware Defense Pro, IBM IDS/IPS, Top Layer IPS,

	Cisco IronPort Web Security Appliance, Squid Web Proxy, McAfee Web Security Appliance (sau McAfee ePolicy Orchestrator), BlueCoat Proxy SG, Imperva SecureSphere, Barracuda Web Application Firewall, F5 BIG-IP AFM, Oracle AuditVault, IBM InfoSphere Guardium, Microsoft SQL, Sybase Adaptive Server Enterprise, Cisco VPN Concentrator, Juniper VPN, Nortel VPN, CheckPoint VPN, Apache Server, Microsoft IIS, QualysGuard, Rapid7 NeXpose, eEye Retina, Saint Vulnerability Scanner, Cisco ACS, Microsoft Active Directory, Microsoft IAS Server, IBM Security Access Manager, Juniper SBR, RSA Authentication Manager, CA SiteMinder, Lieberman Random Password Manager, CA Top Secret, Fidelis Cybersecurity XPS, McAfee Data Loss Prevention (sau McAfee ePolicy Orchestrator), FireEye NX, EX, HX,CM,AX,FX,MPS, Damballa Failsafe, ForeScout CounterACT, Cisco Wireless LAN Controllers, Aruba Mobility Controller, Bit9 + Carbon Black Security, McAfee Application Control, CyberArk Privileged Threat Analytics, Arbor Networks Peakflow,

	Evenimente tip NetFlow.
2.7	Soluția trebuie să furnizeze un mecanism fiabil şi securizat de comunicaţii pentru transportul datelor, conform standardului FIPS 140-2.
2.8	Soluția trebuie să asigure instalarea în mod distribuit (pe noduri) a componentelor sale.
2.9	Soluția trebuie să ofere capacitatea de a mări performanța de corelare prin adăugarea unor instanțe (noduri) suplimentare
2.10	Soluția trebuie să ofere facilităţi de normalizare a datelor obţinute de la surse diferite de evenimente.
2.11	Soluția trebuie să asigure stocarea evenimentelor colectate și în format brut.
2.12	Soluția trebuie să asigure colectarea evenimentelor prin intermediul unei componente disponibile sub formă de agenţi/produs de colectare software. Această componentă trebuie să îndeplinească şi rolul de normalizare jurnale şi evenimente.
2.13	Componentele de tip agenţi de colectare trebuie să poată fi instalate atât local, centralizat pe o singură platformă de gestiune, cât şi la distanţă în locaţii dispersate din punct de vedere geografic.
2.14	Componentele de tip agenţi de colectare vor normaliza şi cataloga evenimentele întrun format comun, folosind o taxonomie cu cel puţin 50 de câmpuri predefinite.
2.15	Soluția trebuie să asigure mecanisme de protecţie a integrităţii datelor stocate prin intermediul semnăturilor de tip *hash*.
2.16	Soluția trebuie să dețină, la punctul de colectare, un mecanism de stocare temporară de tip „*cache*”. Acest mecanism va asigura retransmiterea ulterioară a datelor pentru a evita supraîncărcarea reţelei.
2.17	Soluția trebuie să asigure exportarea evenimentelor colectate în format CSV.
2.18	Soluția trebuie să asigure filtrarea opţională a evenimentelor la nivelul agentului de colectare.
2.19	Soluția trebuie să deţină un mecanism integrat de agregare a evenimentelor de securitate colectate.
2.20	Soluția trebuie să ofere un mecanism integrat de compresie a datelor stocate și permite definirea unor politici diferite de retenție a evenimentelor colectate.
2.21	Soluția trebuie să asigure corelarea evenimentelor colectate din surse de log-uri diferite.
2.22	Soluţia trebuie să dispună de obiecte predefinite specifice sistemului de colectare, corelare şi raportare, pentru o punere iniţială în funcţiune cât mai rapidă şi mai facilă (filtre, reguli de corelare, alerte, rapoarte etc.) dar să ofere şi posibilitatea de a defini propriile obiecte fără niciun fel de limitări sau restricţii funcţionale sau de licenţiere.
2.23	Soluția trebuie să asigure execuţia de corelări bazate pe reguli şi să ofere posibilitatea definirii unor acţiuni de răspuns ce includ cel puțin: - crearea unui eveniment, - notificare în interfaţa grafică - execuţia automată a unor comenzi configurabile cel puţin la nivelul soluţiei de analiză şi la nivelul agenţilor de colectare - transmiterea unui email.

2.24	Soluția trebuie să asigure corelarea în cadrul uneireguli în momentul detecției unui număr predefinit de evenimente similare.
2.25	Soluția trebuie să asigure crearea de către utilizator a regulilor de corelare şi să ofere un mecanism pentru testarea acestora. Pentru crearea regulilor, soluţia trebuie să permită utilizarea operatorilor booleeni (OR şi AND).
2.26	Toate obiectele şi resursele definite la nivelul soluţiei de către utilizatori trebuie să poată fi salvate pentru a fi reutilizate ulterior.
2.27	Rezultatele regulilor de corelare trebuie să poată fi utilizate secvenţial şi automat în cadrul altor reguli de corelare.
2.28	Soluţia trebuie să asigure definirea de liste de câmpuri (din cele incluse în taxonomia implicită) astfel încât ele să poată fi aplicate la nivelul obiectelor specifice soluţiei.
2.29	Soluţia trebuie să asigure definirea de filtre de evenimente şi salvarea acestora astfel încât ele să poată fi utilizate ulterior la nivelul celorlalte obiecte specifice soluţiei.
2.30	Soluția trebuie să asigure integrarea informațiilor de la produse de analiză a vulnerabilităţilor de rețea şi utilizarea acestor informaţii în procesul de corelare.
2.31	Soluția trebuie să asigure crearea unor liste de asseturi/ adrese IP pentru monitorizare şi notificarea automată în cazul identificării acestora în fluxul traficului de reţea.
2.32	Soluția trebuie să integreze informaţii de geolocaţie pentru adresele IP identificate în trafic.
2.33	Soluția trebuie să asigure colectarea evenimentelor de securitate generate din mai multe locaţii geografice.
2.34	Soluția trebuie să asigure monitorizarea în timp real prin afişarea în consola de management dedicată sau într-o interfață web a rezultatelor operaţiei de corelare a evenimentelor de securitate.
2.35	Soluția trebuie să asigure monitorizarea centralizată a stării agenţilor de colectare şi a celorlalte componente ale soluţiei.
2.36	Consola de management poate fi instalată în retele/locații diferite față de unde este instalată soluția.
2.37	Soluția trebuie să ofere posibilitatea de notificare a utilizatorilor sau grupurilor de utilizatori în funcţie de anumiți parametri configurabili.
2.38	Soluţia trebuie să asigure rularea unor comenzi direct la nivelul evenimentelor de interes, astfel încât să poată fi obţinute informaţii suplimentare (de exemplu: ping, traceroute, whois, nslookup, informaţii despre port).
2.39	Soluția trebuie să deţină capabilităţi de auto-descoperire a infrastructurii existente.
2.40	Soluția trebuie să asigure vizualizarea evenimentelor colectate în format brut și normalizat.
2.41	Soluția trebuie să ofere posbilitatea de clasificare și prioritizare a evenimentelor în funcție de criticitatea acestora.
2.42	Soluția trebuie să asigure investigarea incidentelor de securitate pornind de la evenimentul corelat până la identificarea evenimentelor primare ce au generat

	alerta.
2.43	Soluția trebuie să aibă o componentă de raportare care trebuie să fie parte integrată a soluţiei.
2.44	Formatul raportului trebuie să poată fi personalizat atât la nivel de informaţii fixe/template cât şi la nivel de conţinut, precum şi modul de prezentare al acestuia (informaţii în mod text, afişări vizuale diverse precum tabele sau chart-uri).
2.45	Rapoartele trebuie să poată fi configurate să ruleze pe un set predefinit de date apărute într-o perioadă de timp configurabilă, inclusiv pe date istorice (evenimente colectate în trecut).
2.46	Soluţia trebuie să includă posibilitatea integrării mai multor interogări de evenimente sau categorii de evenimente în cadrul aceluiaşi raport.
2.47	Soluţia trebuie să asigure funcţionalităţi de arhivare/backup pentru rapoartele generate.
2.48	Soluția trebuie să ofere rapoarte predefinite și să permită utilizatorilor crearea altor tipuri de rapoarte sau particularizarea celor predefinite.
2.49	Soluția trebuie să asigure exportarea rapoartelor cel puțin în următoarele formate: PDF și XLS.
2.50	Soluția trebuie să asigure rularea în mod programat şi manual a proceselor de generare a rapoartelor.
2.51	Soluția trebuie să asigure transmiterea rapoartelor programate prin email în mod automat.
2.52	Soluția trebuie să asigure definirea asset-urilor din rețea și popularea cu cel puțin următoarele informații: - nume, - nivel de criticitate, - adresă/adrese IP, - adresă/adrese MAC, - zonă de rețea, - vulnerabilități identificate.
2.53	Soluția trebuie să ofere un mecanism integrat de management al incidentelor de securitate ce permite: - Transmiterea alertei pe e-mail şi/sau afişarea ei în sistemul de management al soluţiei - Definirea de grupuri de destinatari organizaţi pe mai multe nivele -Escaladări automate către urmatoarele nivele în cadrul unui grup de destinatari -Personalizarea conţinutului mesajului de alertă pe baza informaţiilor din evenimentele ce au generat alerta.
2.54	Soluția trebuie să asigure definirea rolurilor de administrare “role-based”.
2.55	Soluția trebuie să asigure crearea unor spații de lucru diferite utilizatorilor, în funcție de rolul acestora.
2.56	Autentificarea utilizatorilor pentru acces la administrarea soluţiei trebuie să se poata realiza pe baza de conturi de utilizatori definiţi local, integrare cu sisteme terţe

	precum Microsoft Active Directory, RADIUS sau LDAP.
2.57	Soluția trebuie să asigure accesul securizat la interfața grafică, prin intermediul protocolului SSL.
2.58	Soluţia trebuie să asigure configurarea personalizată de panouri de monitorizare pe bază de grafice şi tabele şi posibilitatea accesării fluxului de evenimente/graficului de evenimente specific unei anumite înregistrări direct din aceste panouri;
2.59	Soluția trebuie să asigure salvarea configurației din interfața grafică, configurație ce include cel puțin următoarele resurse: - reguli, - surse de evenimente, - informații despre vulnerabilități, - rapoarte, - utilizatori, - grupuri de utilizatori. Configurația salvată poate fi importată în instanța soluției SIEM din care a fost creată.
2.60	Soluţia trebuie să includă un sistem integrat pentru stocarea evenimentelor, tip bază de date.
2.61	Soluţia trebuie să ofere mecanisme proprii de colectare, agregare și parsare pentru evenimentele provenite de la soluțiile care nu se regasesc într-o listă predefinită.
2.62	Soluţia trebuie să asigure transmiterea evenimentelor și alertelor către o soluție terță pentru stocarea acestora pe termen îndelungat.
2.63	Solutia trebuie sa ofere functionalitati de auditare și log-uri a sistemului.
2.64	Licenţiere: licenţa soluţiei va fi de tip perpetuă și va susține nivelele de EPS prezentate în anexa A din prezentul capitol al caietului de sarcini
2.65	Pentru componentele hardware, acestea trebuie sa fie dimensionate corespunzător pentru a asigura capacitatea de procesare specifică fiecărui IVC, conform recomandărilor furnizate de producător.

3. Livrabile:

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Proceduri de lucru pentru gestionarea alertelor de securitate în cadrul unui Security Operational Center (SOC). Aceste proceduri trebuie realizate pentru un SOC structurat pe mai multe nivele de analişti care gestionează

totalitatea alertelor colectate din cadrul sistemelor şi echipamentelor de securitate implementate la nivelul IVC prin acest proiect.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de tip SIEM**.**

4. Implementare

Ofertantul asigură maparea reţelei informatice existente în cadrul fiecărui IVC în soluţia SIEM prin definirea zonelor de reţea şi a asset-urilor existente, integrarea tuturor surselor generatoare de date existente în cadrul fiecărei IVC, surse menţionate la momentul instalării, și transmiterea automată către soluţia SIEM din cadrul Centrului Naţional Cyberint a alertelor de securitate, şi să ofere suport tehnic în vederea integrării şi interpretării acestor informaţii, precum şi realizarea altor configurări necesare pentru integrarea echipamentului livrat în rețeaua de destinație, în conformitate cu specificațiile tehnice oferite de Autoritatea contractantă la momentul livrării.

4.1 Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip SIEM se va implementa cu amplasare, instalare, punere în funcțiune, configurare și testarea acesteia, în locațiile comunicate la încheierea contractului, ce includ cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- crearea/migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la momentul livrării,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- implementarea şi punerea la dispoziţia Centrului Naţional Cyberint a unui mecanism de gestionare, pe mai multe nivele de analiză, a alertelor de securitate

preluate din cadrul tuturor IVC-urilor beneficiare, în conformitate cu procedurile de lucru pentru gestionarea alertelor livrate de furnizor,

- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- preluarea și parsarea corectă în soluția SIEM din cadrul IVC a logurilor de pe toate echipamentele din cadrul infrastructurii și asigurarea transmiterii acestora către Centrul Național Cyberint,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

4.2 Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Anexa A - Modul de distribuție a echipamentelor la IVC

Nr. crt.	Necesitate	Capacitate soluție existentă	Capacitate soluție solicitată	Număr IVC	Livrare
1.	Creștere capacitate procesare	500 EPS	1000 EPS	12	12 (București)
2.	Creștere capacitate procesare	500 EPS	1500 EPS	11	11 (București)
3.	Creștere capacitate procesare	500 EPS	2000 EPS	3	3 (București)
4.	Creștere capacitate procesare	500 EPS	2500 EPS	1	1 (Bucuresti)
5.	Creștere capacitate procesare	1000 EPS	2500 EPS	1	1 (Bucuresti)
6.	Implementare nouă		500 EPS	3	1 (Constanta) 2 (Bucuresti)
7.	Implementare nouă		1000 EPS	6	1 (Timiș) 5 (București)
8.	Implementare nouă		1500 EPS	7	1 (Constanța) 6 (București)
9.	Implementare nouă		2000 EPS	3	2 (Sibiu) 1 (Constanța)
10.	Asigurarea continuității suportului pentru soluția existentă sau înlocuirea acesteia cu o soluție de la alt producător.	500 EPS	500 EPS	10	10 (București)
11.	Soluție CNC		Un numar de EPS suficient	1 în cadrul	

			de mare pentru a putea procesa evenimentele din cadrul tuturor IVC	Centrului Național Cyberint	

Anexa 5 la caietul de sarcini

SOLUȚIE DE DETECȚIE TIP APT 1 (ADVANCED PERSISTENT THREAT)

1. Descriere situației actuale

La momentul actual, infrastructura este formată din următoarele echipamente:

46 de IVC-uri dețin senzori de detecție și analiză dinamică a traficului web de tip FireEye NX (13 buc. NX1400, 13 buc. NX2400, 17 buc. NX4400, 3 buc. NX7400);

33 de IVC-uri dețin senzori de detecție și analiză dinamică a traficului de email de tip FireEye EX (31 buc. EX3400 și 2 buc. EX8400);

În cadrul Centrului Național Cyberint există o platformă de management centralizat FireEye CM 9400 și un senzor de tip sandbox FireEye AX 5400;

În cadrul a 16 IVC-uri nu există soluții de tip FireEye.

2.Caracteristici generale ale soluției

2.1	Soluție la cheie care va fi reprezentată sub forma unui sistem integrat de analiză și investigații agresiuni cibernetice cu scopul de a detecta, analiza și răspunde la atacurile cu grad ridicat de risc, care utilizează aplicații direcționate, camuflate sau ascunse de tip *zero-day.*
2.2	Soluția va fi formată din **subsisteme tip appliance dedicate** (senzori) și o **platformă tip appliance de management centralizat** care să asigure coroborarea de informații între diversele subsisteme. Platforma și subsistemele din cadrul soluției trebuie să fie fabricate de către același producător, astfel încât să se asigure compatibilitatea și omogenitatea componentelor soluției.
2.3	Subsistemele soluției vor asigura analiza comportamentală la nivelul traficului de web și email, la nivelul stațiilor de lucru și vor asigura extragerea, la cerere, a artefactelor și componentelor executabile, verificarea acestora pe baza informațiilor de threat intelligence și analiza dinamică a acestora într-un mediu controlat.
2.4	Soluția va conține următorii senzori de tip appliance care vor fi distribuiți astfel: Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficul web (senzor de detecție APT-web tip 1 – 18 buc., tip 2 – 21 buc., tip 3 – 12 buc., tip 4 – 7 buc., și tip 5 – 3 buc.). Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficul de email (senzor de detecție APT-email tip 1 – 47 buc. și tip 2 – 1 buc.) Senzor de detecție a agresiunilor cibernetice pentru stațiile de lucru (senzor EDR tip 1 – 23 buc. și tip 2 – 1 buc.) senzor de analiză dinamică a fișierelor și URL-urilor considerate cu

	potențial malware într-un mediu virtualizat si protejat (senzor sandbox - 1 buc.)
2.5	Platforma de management centralizat va fi instalată *on-premise* la Centrul Național Cyberint și va asigura: corelarea alertelor între senzorii de detecție APT-web și email, senzorii EDR și senzorul de analiză dinamică a fișierelor si URL-urilor; distribuția de actualizări - update-uri, informații de tip threat intelligence și indicatori de compromitere obținuți local cu ajutorul celorlalte subsisteme, informații primite din rețeaua globală de inteligență, sau din surse externe (third party); raportarea detaliată, inclusiv tablouri de bord - dashboard-uri - unificate pentru grupurile de subsisteme administrate; centralizarea gestionării subsistemelor componente printr-o consolă unică; gestionarea actualizărilor de software și threat intelligence în modul offline, fără a fi necesară conectivitate la internet; administrarea integrată și unitară a subsistemelor componente, în timp real, prin folosirea unei interfețe grafice; generarea, stocarea și transmiterea de jurnalizări – log-uri - către un echipament extern de tip SIEM (cel puțin prin protocolul SYSLOG);
2.6	Platforma de tip appliance de management centralizat trebuie să fie dimensionată astfel încât să poată gestiona toți senzorii din prezentul caiet de sarcini.
2.7	Sistemul distribuit de senzori împreună cu platforma de gestiune centralizată a acestora se vor instala într-o rețea izolată, fără conexiune la Internet, transferul datelor din Internet (update-uri de semnături și sisteme de operare) și implicit din comunitățile de tip colaborativ în interiorul platformei se realizează printr-un echipament de tip diodă de date existent în infrastructura beneficiarului, conform procedurii următoare: În prima etapă, datele de interes sunt aduse pe serverul conectat la Internet, parte componentă a diodei de date, folosind scripturi puse la dispoziție de ofertant În a doua etapă datele sunt transferate pe serverul conectat în rețeaua internă în mod automat, cu ajutorul unor scripturi puse la dispoziție de autoritatea contractantă ca parte integrantă din funcționalitatea diodei de date; În a treia etapă informația transferată pe serverul conectat la rețeaua internă va fi integrată în sistemul de management al senzorilor prin intermediul scripturilor puse la dispoziție de ofertant.
2.8	Atât pentru componentele din soluția ofertată, care sunt diferite de cele existente în infrastructura actuală (FireEye NX, EX, AX și CMS), cât și pentru senzorul de detecție a agresiunilor cibernetice pentru stațiile de lucru, ofertantul va asigura o

	sesiune de instruire de minim 5 zile pentru fiecare subsistem, pentru 10 persoane în care vor fi prezentate noțiuni specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului ofertat, incluzând, dar fără a se limita la, următoarele informații: Prezentarea modului de instalare a tuturor componentelor soluției Prezentarea funcționalităților componentelor soluției Prezentarea interfeței de administrare şi a principalelor acțiuni ce pot fi întreprinse prin intermediul acesteia Prezentarea modului de preluare a fluxurilor specifice de trafic Prezentarea tuturor resurselor implementate în cadrul soluției Prezentarea modalităților de monitorizare în timp real a alertelor de securitate Prezentarea modului de creare a rapoartelor particularizate Bune practici pentru a eficientiza activitatea de identificare a amenințărilor cibernetice Sesiunile de instruire vor fi de tip “hands-on”, cu activități practice în care cursanții utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului. Acestea se vor desfășura în limba română, într-o locație pusă la dispoziție de furnizor, în municipiul București. Instructorul trebuie să fie acreditat de producătorul soluției. Pentru demonstrarea pregătirii instructorului se vor prezenta certificate/autorizări/acreditări, sau alte documente emise de către producătorul soluției, sau de organisme abilitate în acest sens. Ofertantul va asigura servicii de catering pe perioada cursului, respectiv o masă de prânz şi un coffee-break pe zi(cafea, apă, ceai, produse de patiserie şi fructe, la discreţie).
2.9	Ofertantul va oferi suport premium ce implică: acces direct la un specialist avansat de nivel superior; alocarea unui specialist/inginer dedicat care să asigure suport cel puțin pentru: probleme tehnice, cazuri de suport, update-uri despre escaladarea cazurilor la ingineri avansați sau management-ul produsului, întreținerea și update-ul echipamentelor; suport anual on-site ce implică atât verificări de performanță și funcționare ale echipamentelor, cât și asistență tehnică (dacă specialistul dedicat consideră că este necesară); recomandări privind detecția eficientă a atacurilor și caracteristici noi ale produselor; număr nelimitat de contacte de suport pentru portalul de acces si cazurile de suport deschise prin intermediul mai multor canale de comunicație.

2.1. Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficul web

2.1.1 Specificații hardware	Minim 4 interfeţe de monitorizare de 1 GbE Minim 1 interfaţă management de 1 GbE Minim 2 porturi USB Rackabil maxim 2U, 19"
2.1.2 Funcționalități generale	2.1.2.1 Soluția ofertată trebuie să realizeze inspecţia şi blocarea traficului web din cadrul unei reţele
	2.1.2.2 Soluția ofertata trebuie să asigure aplicarea de reguli predefinite pentru identificarea acţiunilor malware și să ofere posibilitatea actualizării acestora prin intermediul informaţiilor de tip “threat intelligence”
5.3.1.1.	2.1.2.3 Soluția trebuie să suporte configurarea în modul in-line și out-of-band
5.3.1.1.	2.1.2.4 Soluția trebuie sa poată funcționa ca ICAP server pentru a asigura primirea datelor prin protocolul ICAP pentru analiză
5.3.1.1.	2.1.2.5 Soluția trebuie să detecteze cel puțin următoarele faze ale atacurilor de tip Web: exploit-ul inițial, descărcare de cod binar malware, funcții de tip call-back sau conexiuni către centre de comanda si control (C2)
5.3.1.1.	2.1.2.6 Soluția ofertată trebuie să asigure suport pentru inspecţia cel puțin a următoarelor protocoale: HTTP, HTTPS, FTP, SMB;
5.3.1.1.	2.1.2.7 Soluția ofertata trebuie să poată detecta răspândirea laterală a atacului prin analiza traficului de tip SMB
5.3.1.1.	2.1.2.8 Soluția efectuează analiza dinamică a unor porțiuni de cod necunoscut, sau a obiectelor suspecte (identificate în traficul de la nivelul reţelei) într-un sistem de tip hypervisor
5.3.1.1.	2.1.2.9 Sistemul hypervisor trebuie să conțină cel puțin o mașină virtuală de tip sandbox pentru analiză malware, cu sistem de operare pre-instalat Microsoft Windows 10 cu diferite versiuni de aplicații si plugin-uri uzuale
5.3.1.1.	2.1.2.10 Soluția ofertată trebuie să fie de tip appliance hardware, iar furnizorul este responsabil de licențierea completă a software-ului utilizat de aceasta pentru analiza dinamică a malware-ului, a sistemelor de operare și a aplicațiilor folosite în mașinile virtuale de analiză.
5.3.1.1.	2.1.2.11 Soluția trebuie să asigure detecția atacurilor de tip Web Shell
5.3.1.1.	2.1.2.12 Soluția trebuie să asigure inspecția traficului HTTPS cu suport pentru protocoalele SSL/TLS, inclusiv amprentare

	JA3, whitelisting și URL Categorization
5.3.1.1.	2.1.2.13 Soluția trebuie să asigure analiza cel puțin a următoarelor tipuri de fișiere: msi, exe, dll, pdf, doc, jar, docx, xls, xlsx, gif, jpeg, png, tiff, eml, html, url, ppt, pptx, rtf, zip
5.3.1.1.	2.1.2.14 Soluția trebuie să asigure evidențierea URL-urilor suspecte din cadrul unei alerte și descărcarea capturilor de trafic asociate
5.3.1.1.	2.1.2.15 Soluția trebuie să asigure analiza dinamică a malware-ului în modul offline, fără a fi necesară conectivitate la Internet
5.3.1.1.	2.1.2.16 Soluția trebuie să asigure gestionarea actualizărilor de software si threat intelligence în modul offline
	2.1.2.17 Soluția trebuie să poată genera alerte retroactiv
	2.1.2.18 La finalul analizei unui fișier malware extras din traficul monitorizat, soluția trebuie să prezinte un raport complet care să conțină informații precum: -Tipul fișierului analizat; -Numele fișierului analizat; -Copie a fișierului malware; -Sumele de control (de exemplu în format MD5, SHA1/256/512) ale fișierelor; -Clasificarea în funcție de familia de malware; -Tipul de exploit folosit; -URL-uri; -Date de identificare ale sistemului compromis (IP, MAC); -Modificări aduse la nivelul sistemului de operare; -Aplicațiile targetate; -Modificări asupra sistemului de fișiere; -Modificări aduse asupra bazei de date Windows Registry; -Librării DLL încărcate; -Funcțiile Windows API apelate, în ordine cronologică; -Informaţii despre procesele create/modificate/oprite; -Detalii despre comportamentul la nivel de reţea format grafic (Conexiuni de reţea create şi protocoalele de transport folosite, porturi utilizate, interogări şi răspunsuri DNS, pachete http); -Adrese IP contactate;
5.3.1.1.	2.1.2.19 Soluția trebuie să asigure identificarea atacurilor malware pe baza regulilor de tip YARA
5.3.1.1.	2.1.2.20 Soluția trebuie să asigure administrarea prin conexiune securizată atât din linie de comanda (CLI) cât și

	printr-o interfață grafică web
5.3.1.1.	2.1.2.21 Soluția trebuie să ofere posibilitatea configurării de profile și privilegii utilizator pentru diverse roluri: (Ex. administrator, operator, auditor/viewer, etc.)
5.3.1.1.	2.1.2.22 Soluția trebuie să aibă capabilități de clasificare a detecției malware (ex.: Backdoor, Trojan, Exploit etc.) .
5.3.1.1.	2.1.2.23 Soluția trebuie sa fie capabilă să verifice dacă au apărut actualizări de sistem. Actualizările trebuie să poată fi realizate din interfața de administrare Web
5.3.1.1.	2.1.2.24 Soluția trebuie să ofere într-o interfață GUI posibilitatea verificării stării de funcționare a sistemului
5.3.1.1.	2.1.2.25 Soluția trebuie să poată identifica traficul filtrat de un echipament tip proxy Web.
5.3.1.1.	2.1.2.26 Soluția trebuie să permită whitelistarea unor clase de adrese IP
5.3.1.1.	2.1.2.27 Soluția trebuie să asigure autentificarea în consola prin utilizarea serviciilor de autentificare precum RADIUS, TACACS+, LDAP
5.3.1.1.	2.1.2.28 Soluția trebuie să poată utiliza anteturile XFF pentru a identifica mașina client care generează alertele atunci când este implementată în spatele unui server proxy
5.3.1.1.	2.1.2.29 Soluția trebuie să asigure exportul de rapoarte și alerte referitoare la malware în format PDF
5.3.1.1.	2.1.2.30 Soluția trebuie să indice severitatea incidentului analizat
5.3.1.1.	2.1.2.31 Soluția trebuie să asigure clasificarea alertelor bazată pe fazele ciclului de viață al infecției
5.3.1.1.	2.1.2.32 Soluția trebuie să asigure notificarea alertelor prin intermediul protocoalelor SNMP, Syslog sau SMTP
2.1.3 Accesorii	Set cabluri de alimentare cu conector C14-tată, set cabluri de alimentare cu conector CEE 7/7 tată, set/kit montaj rack.
2.1.4 Specificații de performanță (trafic web analizat)	2.1.4.1 Senzor tip 1 : minim 90 Mbps
	2.1.4.2 Senzor tip 2 : minim 200 Mbps
	2.1.4.3 Senzor tip 3 : minim 450 Mbps
	2.1.4.4 Senzor tip 4 : minim 0.9 Gbps
	2.1.4.5 Senzor tip 5 : minim 2.4 Gbps

2.2. Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficulde email

2.2.1 Specificații hardware	2.2.1.1 Minim 2 interfeţe de monitorizare de 1 GbE 2.2.1.2 Minim 1 interfață management de 1 GbE

	2.2.1.3 Capacitate de stocare de minim 240 GB și configurație hard-disk de minim RAID1 2.2.1.4 Minim 2 porturi USB 2.2.1.5 Sursă redundantă de alimentare 2.2.1.6 Rackabil maxim 2U, 19"
2.2.2 Funcționalități generale	2.2.2.1 Soluția trebuie să identifice aplicații malware la nivelul fluxului de email, folosind tehnici de detecție care nu se bazează exclusiv pe analiză statică (semnături, liste și reguli statice ce necesită actualizări constante), ci folosește inclusiv algoritmi de tip machine learning, cât și metode dinamice de tip sandboxing.
	2.2.2.2 Soluția trebuie să identifice atacuri de tip phishing și spear-phishing. Aceasta trebuie să analizeze atașamente și URL-uri pentru a identifica tentativele de compromitere a sistemelor informatice.
	2.2.2.3 Soluția trebuie să identifice atacuri de tip impersonare (email spoofing).
5.3.2.1.	2.2.2.4 Soluția trebuie să aibă capabilitatea de a scana atașametele email de tip arhivă.
5.3.2.1.	2.2.2.5 Soluția trebuie să poată alerta și carantina automat email-uri cu caracteristici sau atașamente malware, care conțin URL-uri (inclusiv cele obfuscate, scurtate sau de tip redirect), documente MS Office, PDF-uri, arhive, fișiere HTML, ș.a..
5.3.2.1.	2.2.2.6 Soluția trebuie să identifice amenințările prin analiza locală, fără să trimită fișierele în afara organizației, sau către servicii de analiză malware de tip cloud.
5.3.2.1.	2.2.2.7 Soluția trebuie să asigure analiza a cel puțin următoarelor tipuri de fișiere: exe, dll, pdf, swf/java class/jar, doc/docx, ppt/pptx, xls/xlsx, zip/rar, html, URL, msi, jpeg, eml, rtf
5.3.2.1.	2.2.2.8 Soluția trebuie să poată analiza fișierele încorporate în documente PDF, RTF sau MS Office.
5.3.2.1.	2.2.2.9 Pentru mesajele care conțin URL-uri de tip download de fișiere, soluția trebuie să poată descarcă fișierul indicat de URL, să îl analizeze și să blocheze mesajul în cazul în care fișierul este malware.
5.3.2.1.	2.2.2.10 Soluția trebuie să ofere posibilitatea de a alerta sau

	carantina mesaje care conțin fișiere jar atașate sau URL-uri către fișiere de tip jar.
5.3.2.1.	2.2.2.11 Soluția trebuie să fie capabilă să extragă și să analizeze URL-urile din conținutul mesajului și din atașemente de tip PDF, MS Office și fișiere arhivate.
5.3.2.1.	2.2.2.12 Soluția trebuie să fie capabilă să detecteze următoarele tehnici folosite de atacatori pentru a convinge utilizatorii să acceseze URL-uri: înlocuirea unui caracter cu unul asemănător (typosquatting) și adresa URL-ului diferită față de URL-ul afișat (URL overlay).
5.3.2.1.	2.2.2.13 Soluția trebuie să poată analiza URL-uri de tip FTP, HTTP și HTTPS.
5.3.2.1.	2.2.2.14 Soluția trebuie să poată analiza mesajele email transmise prin canale criptate.
5.3.2.1.	2.2.2.15 Soluția trebuie să fie capabilă să analizeze documentele și arhivele protejate cu parolă.
5.3.2.1.	2.2.2.16 Soluția trebuie să ofere detecție pentru ransomware.
5.3.2.1.	2.2.2.17 Soluția trebuie să poată genera alerte retroactiv.
5.3.2.1.	2.2.2.18 Soluția trebuie să asigure gruparea și filtrarea alertelor cel puțin după următoarele criterii: expeditor email, destinatar email, tip atașament, tip malware.
5.3.2.1.	2.2.2.19 Soluția trebuie să ofere informații investigative referitoare la mesajele email care au generat alerte. Informațiile furnizate trebuie să includă hash-uri ale fișierelor atașate/descărcate, link-uri web ce au fost implicate în atac, sau informații referitoare descărcarea de cod suplimentar.
5.3.2.1.	2.2.2.20 Soluția trebuie să ofere informații investigative în privința fișierelor analizate dinamic printr-o reprezentare grafică care prezinte detalii despre procese, accesarea memoriei, modificări de fișiere, regiștri, încărcare dll-uri, activități de tip code injection.
5.3.2.1.	2.2.2.21 În cazul în care atașamentul analizat generează conexiuni externe, soluția trebuie să le raporteze în cadrul alertei. Soluția trebuie să detecteze și să raporteze tentativele de comunicație la internet detectate în timpul analizei în sandbox.
5.3.2.1.	2.2.2.22 Soluția trebuie să fie capabilă să detecteze când

	funcțiile de sleep ale sistemului sunt folosite de malware pentru a evita analiza și trebuie să fie capabilă să accelereze timpul pentru a forța malware-ul să fie rulat.
5.3.2.1.	2.2.2.23 Soluția trebuie să poată analiza malware care implementează strategii de eludare a sandboxului (sandbox evasion techniques), precum execuția întârziată, diagnostic de mediu, verificarea interacțiunii umane, verificarea de domeniu, etc.
5.3.2.1.	2.2.2.24 Soluția trebuie să poată analiza dinamic fișierele în mașinile virtuale atât în mod izolat (fără să necesite conectivitate la internet), cât și în mod live prin analiza conexiunilor la rețea pentru o imagine completă a malware-ului (de ex. descărcare de module adiționale).
5.3.2.1.	2.2.2.25 Solutia trebuie sa asigure configurarea intervalului de timp permis pentru analiza mesajelor suspecte, înainte ca acestea să fie distribuite către destinatar.
5.3.2.1.	2.2.2.26 Soluția trebuie să asigure utilizarea de reguli YARA.
5.3.2.1.	2.2.2.27 Soluția trebuie să detecteze tipul de fișier ce va fi analizat, indiferent de extensia acestuia.
5.3.2.1.	2.2.2.28 Soluția trebuie să se poată instala *Inline,* pentru a analiza traficul de producție, sau *Out-Of-Band,* pentru a analiza o copie a poștei electronice.
5.3.2.1.	2.2.2.29 Soluția trebuie să poată fi instalată *on-premise* și să asigure gestionarea actualizărilor de software și threat intelligence în modul offline (air-gap mode)
5.3.2.1.	2.2.2.30 Soluția trebuie să poată transmite notificări automat prin Syslog, SNMP și SMTP.
5.3.2.1.	2.2.2.31 Soluția trebuie să poată utiliza TLS pentru a asigura confidențialitatea poștei electronice.
5.3.2.1.	2.2.2.32 Soluția trebuie să poată transmite automat notificări în cazul în care carantinează sau blochează mesaje email.
5.3.2.1.	2.2.2.33 Soluția trebuie să trimită alerte în cazul în care se depășește un anumit procent din spațiul de stocare aferent mesajelor carantinate.
5.3.2.1.	2.2.2.34 Soluția trebuie să ofere o consolă de management de tip web-based care nu necesită instalarea de software adițional pentru a putea fi accesată.

5.3.2.1.	2.2.2.35 Soluția trebuie să utilizeze un canal de comunicație criptat între administratori și consola de administrare.
5.3.2.1.	2.2.2.36 Soluția trebuie să asigure configurarea manuală a timpului local sau sincronizarea cu un server NTP.
5.3.2.1.	2.2.2.37 Soluția trebuie să asigure crearea de utilizatori cu roluri și drepturi diferite (de ex. Administrator sistem, utilizator pentru monitorizare alerte).
5.3.2.1.	2.2.2.38 Soluția trebuie să asigure autentificarea la consola de management prin RADIUS, TACACS+ și LDAP.
5.3.2.1.	2.2.2.39 Soluția trebuie să genereze rapoarte în format PDF sau CSV în funcție de natura informațiilor, care să conțină: alerte și detalii despre incident, sumar executiv, etc..
2.2.3 Specificații de performanță	2.2.3.1 Senzor tip 1 : analizează minim 600 atașamente unice pe oră.
	2.2.3.2 Senzor tip 2 : analizează minim 2600 atașamente unice pe oră.
2.2.4 Specificații de licențiere	Soluția trebuie să asigure analiza concomitentă a cel puțin 90.000 de căsuțe de email gestionate prin intermediul celor 47 echipamente incluse în soluție.

2.3. Senzor de detecție a agresiunilor cibernetice pentru stațiile de lucru

2.3.1 Funcționalități generale	2.3.1.1 Soluția ofertata trebuie sa fie o soluție completă de securitate pentru sisteme de calcul, care acoperă atât funcționalități de detecție și prevenție, cât și de investigare sau remediere (în funcție de modalitatea de implementare) pentru sisteme de operare Microsoft Windows, MAC OS X și Linux
	2.3.1.2 Soluția ofertată va include un controller central, sub formă de echipament hardware, cu rol de administrare a agenților instalați pe sistemele de calcul. Soluția asigura monitorizarea stațiilor de lucru și identificarea activităților malware.
	2.3.1.3 Agentul de colectare si analiză malware trebuie să asigure detecția, analiza, sau izolarea atacurilor cibernetice pentru sistemele de calcul din rețea.
	2.3.1.4 Comunicația intre agenții software și consola centrală se realizează în mod securizat.
	2.3.1.5 Agentul de endpoint trebuie să aibă impact minim asupra performațelor sistemelor de calcul.

	2.3.1.6 Soluția trebuie să asigure distribuirea indicatorilor de compromitere dinspre consola de management centralizat către agenții locali de la nivelul stațiilor de lucru.
	2.3.1.7 Soluția trebuie să asigure detecția și blocarea exploit-urilor folosind algoritmi ce analizează comportamentul aplicațiilor. Soluția asigură detectia atacurilor tip ROP (Return Oriented Programming), revershe shell, SEHOP corruption, exploit-uri Java
	2.3.1.8 Soluția trebuie să asigure detecția fișierelor malware in timp real
	2.3.1.9 Soluția trebuie să asigure scanarea fișierelor folosind metode de tip antivirus pe baza de semnături și euristic.
	2.3.1.10 Soluția trebuie să asigure scanarea fișierelor executabile folosind algoritmi de tip machine learning.
	2.3.1.11 Soluția trebuie să asigure generarea automată a unui timeline al evenimentelor care au dus la compromiterea stației.
	2.3.1.12 Soluția trebuie să ofere posibilitatea căutării după anumite metadate, sau cuvinte cheie.
	2.3.1.13 Funcția de căutare a soluției trebuie să fie disponibilă și printr-un API.
	2.3.1.14 Soluția trebuie să poată apela funcția de achiziție de fișiere atât din interfața grafică, cât și printr-un API.
	2.3.1.15 Soluția trebuie să asigure analiza/investigarea alertelor oferind informații despre: memorie / sistem / procese / fișiere / regiștri / tabela de rutare / conturi utilizatori, etc.
	2.3.1.16 Soluția trebuie sa asigure achiziția informaţiilor investigative precum întregul disk, întreaga memorie, și fișiere specificate.
	2.3.1.17 Soluția trebuie să primească indicatori de compromitere de la producător și de la celelalte subsisteme instalate în cadrul *Soluției detecție tip APT*, și să asigure crearea unor indicatori de compromitere personalizați și integrarea cu surse externe de indicatori.
	2.3.1.18 Soluția trebuie să asigure monitorizarea stațiilor de lucru, detecția de viruși, troieni, viermi informatici, spyware, adware, keyloggers, rootkits și exploit-urilor ce apar la utilizarea aplicațiilor de tip Adobe Reader, Adobe Flash, Internet Explorer, Firefox, Google Chrome, Java, Microsoft Outlook, Microsoft Word, Microsoft Excel și Microsoft PowerPoint, inclusiv blocarea și terminarea aplicațiilor afectate de exploit.

	2.3.1.19 Soluția trebuie să asigure trimiterea fișierelor pentru analiza suplimentară către o soluție de tip sandbox instalată in infrastructura beneficiarului (on premise)
	2.3.1.20 Soluția trebuie sa asigure integrarea cu soluții de tip SIEM în vederea colectarii metadatelor alertelor
	2.3.1.21 Analiza alertelor si managementul soluției trebuie să se realizeze on-premise, fără a trimite eșantioanele spre analiza către servicii de tip cloud.
	2.3.1.22 Soluția trebuie sa fie capabila sa actualizeze agenții în mod centralizat.
	2.3.1.23 Soluția trebuie sa asigure masuri de protecție împotriva opririi, sau restartării agentului instalat.
	2.3.1.24 Soluția trebuie sa asigure masuri de protecție împotriva dezinstalării prin configurarea unei parole.
	2.3.1.25 Soluția trebuie sa ofere un API pentru integrarea cu diferite soluții de securitate
	2.3.1.26 Soluția trebuie sa asigure administrarea printr-o consola/interfața web.
	2.3.1.27 Soluția trebuie sa permită excluderea de la scanare/blocare a agenților altor soluții instalați pe stații.
2.3.2 Specificații de performanță	2.3.2.1 Senzor tip 1: să permită gestionarea a minim 14.000 agenți endpoint 2.3.2.2 Senzor tip 2: să permită gestionarea a minim 50.000 agenți endpoint
2.3.3 Specificații de licențiere	Soluția trebuie sa asigure analiza concomitenta a cel puțin 53.000 de endpoint-uri gestionate prin intermediul celor 24 controllere incluse in soluție

2.4. Senzor de analiză dinamică a fișierelor și URL-urilor considerate cu potențial malware într-un mediu virtualizat si protejat

2.4.1 Specificații hardware	2.4.1.1 Minim 1 interfață de monitorizare 1 GbE 2.4.1.2 Minim 1 interfață management 1 GbE 2.4.1.3 Hard disk de capacitate minim 3 TB si minim RAID1 2.4.1.4 Sursă redundantă de putere 2.4.1.5 Rackabil maxim 1U, 19"
2.4.2 Funcționalități generale	2.4.2.1 Soluția trebuie să conțină cel puțin o mașină virtuală de tip sandbox pentru analiză malware cu sistem de operare pre-instalat Microsoft Windows 10.
	2.4.2.2 Sandbox-urile de analiză pre-configurate vor avea instalate cele mai comune aplicații de tip browser, plugin-uri și alte aplicații terțe (cel puțin Adobe Acrobat Reader, Microsoft Office Word, Excel, PowerPoint)
	2.4.2.3 Licențierea sistemelor de operare Microsoft Windows şi a

	aplicațiilor comerciale din cadrul sandbox-urilor de analiză preinstalate / pre-configurate va fi asigurată de către furnizorul sistemului de analiză.
	2.4.2.4 Soluția trebuie sa ofere restaurarea automată a sandbox-urilor de analiză la un baseline pre-configurat, imediat ce s-a finalizat analiza unui sample de malware.
	2.4.2.5 Soluția trebuie să analizeze cele mai comune tipuri de fișiere cunoscute ca fiind folosite pentru distribuirea sau găzduirea de aplicații malware (fișiere executabile PE, documente Microsoft Office, documente PDF, fișiere flash, sau fișiere de tip imagine).
	2.4.2.6 Soluția trebuie să suporte analiza obiectelor indicate prin URL.
	2.4.2.7 Soluția trebuie sa analizeze întregul ciclu de desfășurare a unui atac cibernetic, începând cu exploit-ul inițial, contactarea serverelor de comandă şi control şi descărcări ulterioare de alte module malware
	2.4.2.8 Soluția trebuie să ofere capacitatea de a identifica aplicații malware care detectează medii virtualizate / emulate și să dețină modalități de evitare a acestor tehnici anti-analiză
	2.4.2.9 Soluția trebuie să ofere jurnalizarea apelurilor de funcții Windows native și din interfața Windows API relevante în depistarea comportamentului cu caracter malware.
	2.4.2.10 Soluția trebuie sa ofere simularea acțiunilor unui utilizator real în cadrul sandbox-ului, astfel încât să fie analizate cu succes aplicațiile malware care îşi manifestă comportamentul doar după ce au observat prezența utilizatorului (prin apelarea unor funcții Windows native sau din interfața Windows API).
	2.4.2.11 Soluția trebuie să creeze rapoarte tehnice ce vor cuprinde informaţii despre fișierele analizate, precum: 1. Informații analiză statică, privind cel puțin următoarele aspecte de interes: a. Tipul fișierului analizat; b. Sumele de control (MD5 , SHA) ale fișierelor analizate / create pe sandbox-ul de analiză; c. Informaţii extrase din header-ul fișierelor executabile; d. Librăriile DLL, respectiv funcțiile folosite de malware, extrase din tabela de importuri (IAT); e. Secțiunile fișierelor exe/dll; 2. Informații analiză dinamică, privind cel puțin următoarele aspecte de interes:

	a. Modificări aduse la nivelul sistemului de operare; b. Modificări aduse la nivelul aplicaţiilor instalate pe sistemul de analiză; c. Modificări asupra sistemului de fișiere; d. Modificări aduse asupra bazei de date Windows Registry; e. Librării DLL încărcate; f. Funcțiile Windows API apelate; g. Informaţii despre procesele create/modificate/oprite; h. Obiecte de tip Mutex; i. Conexiuni de reţea create şi protocoalele de transport folosite; j. Captură trafic de rețea (fișier PCAP) generat de sistemul de analiză; k. Interogări DNS; l. URL-uri accesate; m. Adrese IP contactate şi porturile folosite;
	2.4.2.12 La finalul analizei malware soluţia trebuie sa furnizeze rezultatele într-un raport PDF, HTML, sau JSON.
	2.4.2.13 Soluția trebuie să ruleze aplicaţiile malware atât în modul sandbox (execuţia sample-urilor malware este efectuată într-un mediu izolat - fără conexiune la rețeaua Internet, dar având posibilitatea de a folosi servicii Internet emulate), cât şi în modul analiză live (conexiune reală la reţeaua Internet) pentru a analiza toate etapele unui atac cibernetic (exploatare vulnerabilitate, contactare domenii de comandă şi control, descărcare de alte module malware, ș.a.).
	2.4.2.14 Soluția trebuie sa ofere identificarea comportamentului generic al malware-ului şi încadrarea aplicaţiilor malware într-o anumită categorie (keylogger, rootkit, RAT, etc.) în baza unor şabloane de comportament.
	2.4.2.15 Soluția trebuie să fie instalată on-premise
	2.4.2.16 Soluția trebuie să analizeze cel puțin 8000 de fișiere pe zi

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de tip APT 1.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția APT1se va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractuluişi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- crearea / migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la momentul livrării,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- configurarea soluției pentru jurnalizarea evenimentelor la nivelul soluției SIEM existente la fiecare beneficiar,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

4.2. Garantie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Distribuția soluției APT 1 necesar a fi instalată

Nr. crt.	Tip soluție	Nr. total buc.	Livrare
1	Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficul web tip 1	18	București - 17 Constanța - 1
2. 2	Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficul web tip 2	21	București - 20 Constanța - 1
3. 3	Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficul web tip 3	12	București - 10 Sibiu - 1 Constanța - 1
4. 4	Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficul web tip 4	6	București - 5 Sibiu - 1
5. 5	Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficul web tip 5	3	București - 2 Constanța - 1
6. 6	Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficul de email tip 1	47	București - 42 Sibiu - 2 Constanța - 2 Timiș - 1
7. 7	Senzor de detecție și analiză dinamică a agresiunilor cibernetice pentru traficul de email tip 2	1	București
8. 8	Senzor de detecție a agresiunilor cibernetice pentru stațiile de lucru tip 1	23	București - 20 Constanța - 2 Sibiu - 1
9. 9	Senzor de detecție a agresiunilor cibernetice pentru stațiile de lucru tip 2	1	București
10. 10	Senzor de analiză dinamică a fișierelor și URL-urilor considerate cu potențial malware într-un mediu virtualizat si protejat	1	București

Anexa 6 la caietul de sarcini

SOLUȚIE DE TIP ENDPOINT PROTECTION

1. Descrierea situației actuale

La momentul actual, situația este următoarea:

21 IVC-uri deţin soluţia BitDefender GravityZone, existând în total un număr de 29032 licenţe;

4 IVC-uri nu dețin nicio soluție de tip Endpoint Security;

Sunt necesare 26656 licenţe adiţionale, însumând un număr total de 55688 licenţe, distribuite la 25 IVC-uri.

2. Caracteristici tehnice

Soluția oferită trebuie să îndeplinească următoarele caracteristici tehnice minimale:

2.1	Soluție de tip Endpoint Protection pentru 55.688 sisteme informatice indiferent de natura acestora (posturi de lucru fizice/virtuale de tip desktop, laptop).
2.2	În cazul în care soluția ofertată este diferită de cea operațională în momentul actual, ofertantul are obligația: I. de a importa în echipamentele noi toate configurațiile vechi, inclusiv modificările

	aduse de Centrul Național Cyberint (scripturi, configurări, export de date, etc.); II. de a asigura reprezentaților IVC-urilor beneficiare (în limita a 1 persoană/IVC) cursuri de specializare pe o durată de minim 18 ore, distribuite pe parcursul a 3 zile, pentru utilizarea și exploatarea soluției software propuse. Astfel, ofertantul va efectua o sesiune de instruire ce trebuie să prezinte noțiuni specifice privind integrarea software, configurarea, administrarea şi exploatarea produsului ofertat, incluzând, dar fară a se limita la, următoarele informaţii: • Prezentarea modului de instalare a tuturor componentelor soluției; • Prezentarea funcționalităților componentelor soluției; • Prezentarea interfeţei de administrare şi a principalelor acţiuni ce pot fi întreprinse prin intermediul acesteia; • Prezentarea modalităților de monitorizare a evenimentelor de securitate şi filtrarea acestora; • Prezentarea modului de creare a rapoartelor particularizate; • Prezentarea modului de realizare a actualizării soluţiei (online/offline); • Bune practici pentru crearea politicilor de securitate; Cursul va fi de tip "*hands-on*", cu activități practice în care cursanții utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului. Cursul se va desfășura în limba română, într-o locație pusă la dispoziție de furnizor, în municipiul București. Instructorul trebuie să fie acreditat de producătorul soluției. Pentru demonstrarea pregătirii instructorului se vor prezenta certificate/autorizări/acreditări, sau alte documente emise de către producătorul soluției, sau de organisme abilitate în acest sens. Ofertantul va asigura servicii de catering pe perioada cursului, respectiv o masă de prânz şi un coffee-break pe zi(cafea, apă, ceai, produse de patiserie şi fructe, la discreţie).
2.3	Soluția oferită include agenți software care pot fi instalați și pot rula în mod controlat pe nodurile (endpoint) protejate, respectiv pe stații de lucru, precum și o platformă de management centralizat a agenților.
2.4	Componentele centrale, de control, ale soluției oferite trebuie să poată fi instalate și să ruleze în mediu fizic sau în mediu virtual.
2.5	Agenții soluției oferite, care vor rula pe nodurile (endpoint) protejate, trebuie să ofere suport pentru instalarea pe cel puțin următoarele sisteme de operare: - Windows 7 - Windows 8 - Windows 8.1 - Windows 10 - Windows Server 2016, Windows Server 2012, Windows Server 2008, - Ubuntu 14.04, Ubuntu 16.04, CentOS 6, CentOS 7, macOS 10.13, macOS

	10.12.
2.6	Identificarea și inventarierea aplicațiilor disponibile pe stațiile de lucru.
2.7	Administrarea centralizată a politicilor de securitate aplicabile utilizării dispozitivelor amovibile (de tip USB , CD etc.) de stocare a datelor folosind tehnici de tip permis/respins
2.8	Soluția trebuie să permită controlul dispozitivelor amovibile în funcție de portul folosit de acestea (USB, FireWire, Card SD, etc.)
2.9	Soluția asigură posibilitatea de jurnalizare șic raportare asupra activităților ce implică folosirea dispozitivelor externe atașate la stațiile de lucru.
2.10	În soluția oferită, catalogarea dispozitivelor trebuie să poată fi făcută luând în considerare o serie de parametri unici de identificare a fiecărui dispozitiv.
2.11	Soluția va permite configurarea setărilor clientului de pe endpoint prin intermediul uneia sau mai multor politici.
2.12	Politicile astfel definite să poată fi aplicate la nivel de stații de lucru sau la nivel de grup de stații de lucru.
2.13	Soluția trebuie să utilizeze în procesul de scanare metode euristice pentru a detecta aplicații malware și alte potențiale amenințări în timp real.
2.14	Soluția să folosească în mod implicit tehnici de învățare automată (machine learning) pentru a crește capabilitățile acesteia de a detecta atacurile cibernetice avansate.
2.15	Soluția identifică cel puțin următoarele tipuri de atacuri: - APT (Andvanced Persistent Threat) - Zero-day - Atacuri fără fișiere (Fileless attacks) - Ransomware
2.16	Soluția trebuie să monitorizeze în mod continuu procesele ce rulează pe stațiile de lucru.
2.17	Soluția permite cel puțin următoarele tipuri de scanare: - Scanarea tuturor fișierelor - Scanarea memoriei RAM - Scanare după rootkit - Scanarea elementelor partajate în rețea;
2.18	Soluția verifică versiunile actualizărilor software atât pentru sistemul de operare cât și pentru setul de aplicații;
2.19	Soluția trebuie să permită trimiterea log-urilor (în format .CEF) către servere ce analizează date de tip Syslog.
2.20	Pentru agenții instalați pe stațiile de lucru, platforma trebuie să permită procese de actualizare, instalare și dezinstalare de la distanță.
2.21	Soluția trebuie să se integreze cu servere de tip LDAP sau AD.
2.22	Permite crearea rolurilor de administrare (RBAC) și crearea unor spații de lucru, pentru acces administrativ, respectiv specifice rolului și drepturilor acestora.
2.23	Soluția oferă protecție împotriva dezactivării neautorizate a agenților săi de către utilizatorii ce nu au acest drept.

2.24	Comunicația între platforma de management și agenții instalați pe stațiile de lucru se va face criptat (funcționalitatea trebuie să facă parte din platforma de management).
2.25	Soluția trebuie să permită generarea de rapoarte care să cuprindă informații despre stațiile de lucru (de exemplu activitate malware, stații protejate, activitate control dispozitive, etc.).
2.26	Rapoartele trebuie să fie exportabile cel puțin în format PDF și/sau CSV.

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de tip Endpoint Protection.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip Endpoint Protectionse va implementa cu instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice;
- realizarea tuturor configurărilor la nivelul sistemului de operare;
- configurarea pachetelor software;
- configurarea conexiunilor de reţea;
- crearea / migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la momentul livrării;
- realizarea altor configurări necesare pentru integrarea soluției în reţeaua de destinaţie;
- configurarea soluției pentru jurnalizarea evenimentelor la nivelul soluției

SIEM existente la fiecare beneficiar;

- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

4.2. Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Anexa 7 la caietul de sarcini

SOLUȚIE DE TIP FIREWALL

1. Descrierea tehnologiei

Soluția de tip Firewall reprezintă o soluție hardware integrată de protecție a rețelelor de comunicații cu capabilităţi de: rutare, firewall, control al listelor de acces şi VPN, destinat folosirii ca o soluţie de interconectare și control al traficului în funcție de un set de regului stabilite.

Pentru creșterea nivelului de securitate în cadrul rețelelor de comunicații, soluția va asigura separarea la nivelul hardware a nivelului de comunicații și a celui de control, iar implementarea unor politici de acces se va realiza prin intermediul unor interfețe dedicate de management.

De asemenea, pentru centralizarea log-urilor de securitate, soluția va asigura exportarea acestora într-o soluție de tip SIEM.

2. Caracteristici tehniceminimale ale soluției

2.1 Specificații hardware	2.1.1 Interfeţe intrare/ieşire (I/O): minim 8 x 10BASE-T/100BASE-TX/1000BASE-T 2.1.2 Minim 1 port consolă. 2.1.3 Minim 1 port USB. 2.1.4 Leduri indicare stare. 2.1.5 Montabil în rack (kit de instalare inclus).
2.2 Caracteristici	2.2.1 Firewall Throughput: minim 4 Gbps 2.2.2 IPSec VPN Throughput: minim 1 Gbps 2.2.3 Număr sesiuni concurente: minim 1.300.000 2.2.4 Număr sesiuni noi pe secundă: minim 30.000 2.2.5 Număr tunele VPN : 200
2.3 Funcționalități generale	Echipament integrat de securitate cu cel puțin următoarele funcţionalități simultane: •Firewall de tip stateful;

	•Router cu suport pentru protocoale de rutare dinamice; •Posibilitate de instalare în mod bridge Ethernet; •Criptare de date: IPSec VPN şi SSL VPN; •Suport pentru QoS şi Traffic Shaping;
Funcționalități securitate	
2.4 Funcționalități firewall	2.4.1 Funcţionalităţi NAT, PAT şi Transparent Bridge 2.4.2 Opțiune de a aplica NAT per politică 2.4.3 Suport VLAN Tagging 802.1q 2.4.4 Autentificarea utilizatorilor pe grupuri 2.4.5 Suport IPv6 2.4.6 Creare politici de securitate bazate pe identitatea utilizatorului/serviciilor folosit(e) 2.4.7 Opţiune “Scheduling” pentru politicile de firewall
Funcţionalităţi rețea	
2.5 Funcţionalităţi reţelistică şi rutare	2.5.1 Suport PPPoE şi DHCP Client/Server 2.5.2 Funcționalitate declarare rute statice 2.5.3 Rutare dinamică IPv4: RIP, OSPF, BGP, Multicast 2.5.4 Rutare dinamică Ipv6 2.5.5 Policy-based routing 2.5.6 Rutare între VLAN-uri 2.5.7 Suport One-to-One NAT
Funcţionalități de administrare, jurnalizare și autentificare a utilizatorilor	
2.6 Funcţionalităţi de administrare	2.6.1 Administrare prin WEB UI , Secure Command Shell (SSH) şi Command Line Interface (CLI) 2.6.2 Utilizatori/Administratori cu drepturi configurabile 2.6.3 Funcţionalitate de export/import a configuraţiei 2.6.4 Politică de control a parolelor
2.7 Funcţionalităţi de jurnalizare şi monitorizare	2.7.1 Monitorizare grafică în timp real şi istorică 2.7.2 Functionalitate export Netflow v5 2.7.3 Funcționalitate export loguri în format syslog 2.7.4 Suport SNMP 2.7.5 Notificare alerte prin email
2.8 Condiţii de alimentare	Alimentare curent alternativ 100-240V, 50-60 Hz
2.9 Accesorii	Set/kit montaj rack
2.10 Dimensiuni de gabarit	Rackabil, 19"

3. **Livrabile**

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de tip Firewall.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția Firewallse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- crearea / migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la momentul livrării,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- configurarea soluției pentru jurnalizarea evenimentelor la nivelul soluției SIEM existente la fiecare beneficiar,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

4.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim

3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice

acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Distribuția soluției *Firewall* necesar a fi instalată

Nr. crt.	***Tip soluție***	***Nr. total buc.***	***Livrare***
	Firewall	19	București - 13 Constanța - 3 Sibiu - 2 Timiș - 1

Anexa 8 la caietul de sarcini

SOLUȚIE DETECȚIE APT - TIP 2

1. Descriere generică a tehnologiei

Soluția reprezintă o platformă de securitate cibernetică care utilizează algoritmi specializați de învățare automată nesupravegheată și analiză comportamentală sau mecanisme complexe de inteligență artificială pentru a monitoriza traficul de date din cadrul unei infrastructuri IT&C. Aceasta este capabilă să analizeze și să detecteze atacurile cibernetice avansate (Advanced Persistent Threat) și atacurile cibernetice necunoscute (zero-day).

Platforma este formată din senzori specializați (echipamente de tip server), fiecare senzor fiind format din componente hardware și software, care analizează traficul intern și extern existent într-o rețea informatică.

Componenta hardware este reprezentată de serverele fizice care asigură resursele necesare funcționării în parametri optimi a componentei software.

Componenta software este cea care conține algoritmii proprietari, mecanismele de învățare automată și analiză comportamentală.

Platforma dispune de o componentă de management centralizat prin care se asigură unificarea informațiilor provenite de la toți senzorii asigurând o monitorizare și vizibilitate globală asupra alertelor. Componenta de management va fi asigurată printr-un echipament fizic, suplimentar față de echipamentele menționate în tabelul de la capitolul 4 și va fi instalată la sediul CNC.

Soluția trebuie să dispună de mecanisme de actualizare în mod offline, fără conexiune la Internet.

2. Caracteristici tehnice ale soluției

Soluția va conține următoarele tipuri de echipamente hardware:

9 echipamente hardware tip 1
14 echipamente hardware tip 2
3 echipamente hardware tip 3

Caracteristici componentă hardware:

2.1.Caracteristici	TIP 1	TIP 2	TIP 3
2.1.1.Dimensiune maximă, rackabil 19”	2U	2U	2U
2.1.2. Interfețe administrare	Minim 1 x 10/100/1000 BASE-T	Minim 1 x 10/100/1000 BASE-T	Minim 1 x 10/100/1000 BASE-T
2.1.3. Interfețe pentru	Minim 2 x 10/100/1000	Minim	Minim

analiză/monitorizare (minim)	BASE-T	2 x 10/100/1000 BASE-T 2 x 1Gbe/10Gbe SFP+	1 x 10/100/1000 BASE-T 2 x 1Gbe/10Gbe SFP+
2.1.4.Cantitate trafic de date analizat (minim)	270 Mbps	1.8 Gbps	4.8 Gbps
2.1.5. Nr. dispozitive informatice analizate (minim)	900	7.500	35.000
2.1.6.Sursă de alimentare	100 - 240 V	Dublă, 100-240 V	Dublă , 100-240V
2.1.7. Accesorii:	Ofertantul trebuie să asigure toate echipamentele și accesoriile necesare pentru instalarea echipamentelor fizice ale soluției ofertate în infrastructura beneficiarilor (ex: tap, switch, cabluri alimentare, adaptoare de rețea, cabluri rețea cupru/fibră optică).		
2.1.8. Capacitate stocare	Echipamentul trebuie dimensionat astfel încât să asigure retenția alertelor pe o durată de minim 6 luni de zile.		

Caracteristici componentă software:

2.2. Funcționalități generale	2.2.1. Sistemul trebuie să aibă capacitatea de a analiza o rețea informatică, învățând comportamentul rețelei și generând un model de comportament pentru fiecare dispozitiv și utilizator din rețea, astfel având posibilitatea de a detecta activitățile anormale.
	2.2.2. Sistemul monitorizează și analizează: - Traficul de rețea direct către Internet (inbound/outbound); - Traficul de rețea către Internet (inbound/outbound) care trece prin noduri de rețea intermediare de tip servere Proxy; - Traficul de rețea asociat protocolului DNS; - Traficul de rețea asociat protocolului DHCP; - Traficul de rețea din rețeaua LAN internă generat la accesarea unor aplicații sau servicii; - Traficul de rețea din rețeaua LAN internă generat în procesul de autentificare a stațiilor de lucru/serverelor la serverul de domeniu (Domain Controller); - Orice alt trafic de rețea generat între oricare dispozitive din rețeaua LAN internă.
	2.2.3. Echipamentul primește/procesează/analizează trafic de rețea folosind metoda SPAN sau prin folosirea unor dispozitive de tip Network TAP.
	2.2.4. Când soluția detectează anomalii și generează alerte,

	aceasta trebuie să aibă capabilitatea de a salva și de a exporta traficul de rețea asociat alertelor respective.
	2.2.5. Sistemul folosește algoritmi de învățare automată nesupravegheată (unsupervised machine learning). Sistemul nu are nevoie de seturi de date, reguli predefinite pentru detecția anomaliilor.
	2.2.6. Soluția identifică atacuri cibernetice necunoscute. Metodele avansate de învățare automată corelează modelele comportamentele obținute pentru a detecta amenințări cibernetice necunoscute.
	2.2.7. Modelele comportamentale obținute permit detectarea unor activități anormale, deviații de la comportamentul normal al rețelei, detectând astfel amenințările și atacurile cibernetice în timp real.
	2.2.8. Utilizând algoritmii de analiză comportamentală, soluția poate identifica aplicații malware care existau in rețea anterior instalării acesteia.
	2.2.9. Sistemul clasifică amenințările identificate în funcție de importanța acestora.
	2.2.10. Detectează comunicațiile dintre dispozitivele victimă din cadrul rețelei și serverele de Comandă și Control.
	2.2.11. Sistemul are opțiunea de a șterge datele colectate, fără a afecta funcționalitatea internă a echipamentului.
	2.2.12. Asigura efectuarea de backup/restore a configurațiilor generale.
	2.2.13. Sistemul permite integrarea cu servere de tip LDAP.
	2.2.14. Sistemul transmite notificări prin E-mail despre alertele identificate. Adresa de e-mail poate fi configurată de către administrator.
	2.2.15. Sistemul trebuie să asigure crearea unor conturi cât și tipuri de acces diferite pentru utilizatorii sistemului. Astfel se pot crea conturi pentru utilizator cu anumite drepturi de vizualizare în interfața grafică.
	2.2.16. Sistemul dispune de o interfață grafică interactivă prin care utilizatorul poate vizualiza activitatea de analiză și monitorizare.
	2.2.17. Accesarea interfeței grafice se poate realiza dintr-un browser web, folosind o conexiune criptată bazată pe certificat digital.
	2.2.18. Pentru conexiunea la interfața grafică este

	necesară autentificarea utilizatorului pe baza unui nume de utilizator și a unei parole.
	2.2.19. Interfața grafică dispune de un meniu principal cu diverse opțiuni disponibile unui utilizator în funcție de permisiunile acestuia.
	2.2.20. Descoperă/identifică subrețelele și dispozitivele din cadrul acestora din rețeaua analizată.
	2.2.21. Echipamentul furnizează, în funcție de traficul analizat, informații despre dispozitivele identificate.
	2.2.22. Soluția facilitează vizualizarea istoricului de alerte pentru un dispozitiv informatic.
	2.2.23. Pentru fiecare dispozitiv se poate selecta un interval de timp pentru a vedea istoricul conexiunilor.
	2.2.24. Soluția asigură gruparea dispozitivelor informatice în baza unor activități similare (ex: conexiuni către aceeași destinație).
	2.2.25. Din interfața grafică utilizatorul poate efectua căutări după cuvinte cheie (Ex: adrese IP, hostname, nume de domeniu, etc.).
	2.2.26. Pentru fiecare domeniu sau adresă IP ale unui server de comandă și control accesate din interiorul rețelei se pot extrage/vizualiza dispozitivele interne care au efectuat conexiuni către acesta.
	2.2.27. Utilizatorul poate modifica intervalul de timp pentru care se dorește vizualizarea alertelor.
	2.2.28. Alertele identificate sunt afișate în interfața grafică în funcție de nivelul de severitate atribuit de către echipament. De asemenea se poate alege un interval de timp pentru vizualizare.
	2.2.29. Pentru fiecare alertă soluția va furniza detalii suplimentare precum: data și ora, cine a generat alerta (adresă IP, hostname, etc.).
	2.2.30. Utilizatorul are opțiunea de a eticheta un dispozitiv informatic identificat în cadrul unui tip de comportament ca fiind legitim (similar cu procesul de whitelist).
	2.2.31. Utilizatorul poate să filtreze afișarea dispozitivelor în funcție de un tip de comportament / categorie de detecție.
	2.2.32. Pentru fiecare dispozitiv soluția generează și stochează informații despre comportamentul dispozitivului sub forma unui istoric al conexiunilor realizate. Asupra acestui

	istoric de conexiuni utilizatorul poate aplica opțiuni de filtrare. De asemenea utilizatorul poate descărca conexiunile sub forma unui fișier .pcap.
	2.2.33. Soluția trebuie să poată genera rapoarte automate despre întreaga rețea și incidentele detectate. Rapoartele pot fi descărcate pentru vizualizarea într-o aplicație externă.
	2.2.34. Utilizatorul poate eticheta (poate adăuga tag-uri) anumite incidente, dispozitive sau utilizatori din rețea.
	2.2.35. Soluția dispune de un modul ce asigură o căutare avansată în datele colectate din trafic. Căutarea poate fi realizată în funcție de anumite valori, folosind parametri specifici, expresii regulate sau operatori logici.
	2.2.36. Platforma trebuie să poată fi integrată cu sisteme de tip SIEM.
	2.2.37. Sistemul trebuie să asigure actualizarea software-ului în mod offline (nefiind conectat la Internet).
	2.2.38. Sistemul trebuie să asigure managementul centralizat al tuturor senzorilor instalați în diverse locații.
	2.2.39. Sistemul trebuie să faciliteze comunicarea criptată dintre serverul de management si senzori.
	2.2.40. Soluția trebuie să poată detecta următoarele tipuri de activități și comportamente, prin mecanisme specifice (machine learning, analiză comportamentală) : • Conexiuni interne și externe • Transfer de date intern și extern • Dispozitive conectate din rețeaua internă • Dispozitive conectate din exterior • Conexiuni active din rețeaua internă • Conexiuni active din exterior • Comportament/activitate anormală a unui dispozitiv • Cereri DNS reușite/nereușite • Autentificări Kerberos (reușite/nereușite) • Conexiuni suspicioase de la un dispozitiv către mai multe destinații • Conexiuni SMB nereușite/reușite • Scanarea adreselor din rețea (Address scans on the network) • Activitate minare criptomonede • Metode folosite de aplicațiile malware pentru mișcarea laterală • Sistemul de operare al dispozitivelor

	• Identificare servere de tip Proxy • Transfer de fișiere EXE • Transfer de fișiere RAR • Transfer de fișiere cu format necunoscut/payload • Atacuri de tip Bruteforce • Atacuri de tip Heartbleed • Aplicații specifice atacurilor de tip Advanced Persistent Threat (APT) • Detecția anomaliilor în utilizarea credențialelor • Comunicații cu rețeaua TOR • Scanare de porturi • Conectarea pe porturi non-standard sau compromiterea unui port legitim / port hijacking • Monitorizare trafic SMTP • Anomalii în traficul serverelor DNS (Traffic changes to DNS servers) • Cereri DNS de tip DynDNS (DynDNS DNS requests) • Pierdere excesivă a conexiunilor sau a pachetelor • Certificate SSL invalide

2.3. Cerințe generale

2.3.1.	Tehnologia trebuie să fie 100% „on premise”, fără a fi necesară conectarea în Internet pentru orice fel de motiv cu privire la funcționalitatea produsului. Orice tip de date sau informații culese de la client nu se trimit în extern, sau la producător, fără acordul clientului. Toate actualizările software trebuie efectuate offline, în mod centralizat și automat. Componenta software trebuie să se afle in întregime pe servere fizice, complet sub controlul clientului și în interiorul rețelei sale.
2.3.2.	Senzorii din cadrul platformei vor fi instalați și configurați în locații fizice diferite, astfel se va asigura comunicarea și partajarea în mod securizat a datelor între aceștia. Senzorii se pot administra la nivel local. Instalarea va cuprinde integrarea și unificarea tuturor senzorilor în cadrul componentei de management centralizat verificând astfel vizibilitatea totală la nivelul platformei. Componenta de management are interfață grafică web în care se va verifica că se primesc date de la toți senzorii.
2.3.3.	Ofertantul trebuie să asigure o sesiune de instruire de minim 5 zile, pentru 12 persoane, ce trebuie să prezintenoțiuni specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului ofertat, incluzând, dar fară a se limita la următoarele informaţii: Prezentarea funcționalităților componentelor soluției Prezentarea modului de instalare a tuturor componentelor soluției Prezentarea configurațiilor și politicilor implementate în cadrul soluției furnizate Prezentarea interfeţei de administrare şi a principalelor acţiuni ce pot fi întreprinse prin intermediul acesteia

Bune practici pentru instalarea echipamentului cu scopul de a colecta și monitoriza traficul de rețea în funcție de tipologia rețelelor

Modalități pentru actualizarea offline a componentei software

Prezentarea modului de verificare a instalării soluției, validarea că traficul de rețea ce se dorește monitorizat este primit și analizat de soluție

Prezentarea tuturor resurselor implementate în cadrul soluției

Prezentarea modalităților de monitorizare în timp real a alertelor, eliminare "false-positive", filtrare alerte, corelare evenimente, etc.

Prezentarea modului de investigare al unei alerte/atac cibernetic (Ex: vector de infecție, mișcare laterală, server de comandă și control, sisteme informatice infectate, moduri de comunicare, etc.)

Prezentarea modului de creare a rapoartelor

Bune practici pentru a eficientiza activitatea de identificare a atacurilor cibernetice

Ofertantul va pune la dispoziția beneficiarului un back-up al configurației soluției livrate.

Cursul va fi de tip "*hands-on*", cu activități practice în care cursanții utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului.

Cursul se va desfășura în limba română, într-o locație pusă la dispoziție de furnizor, în municipiul București. Instructorul trebuie să fie acreditat de producătorul soluției. Pentru demonstrarea pregătirii instructorului se vor prezenta certificate/autorizări/acreditări, sau alte documente emise de către producătorul soluției, sau de organisme abilitate în acest sens.

Ofertantul va asigura servicii de catering pe perioada cursului, respectiv o masă de prânz şi un coffee-break pe zi(cafea, apă, ceai, produse de patiserie şi fructe, la discreţie).

3. **Livrabile**

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză,

necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de tip detecție APT tip 2.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de detecție APT tip 2se va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- crearea / migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la momentul livrării,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- configurarea soluției pentru jurnalizarea evenimentelor la nivelul soluției SIEM existente la fiecare beneficiar,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate,
- implementarea unui flux automat de preluare a actualizarilor în mod offline, fără conexiune la Internet.

4.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.
- suport pentru fluxul automat de preluare a actualizarilor în mod offline, fără conexiune la Internet.

Distribuția soluției APT2 necesar a fi instalată

Nr. crt.	***Tip soluție APT2***	***Nr. total buc.***	***Livrare***
	Tip 1	9	București - 9
2.	Tip 2	14	București - 10 Sibiu - 2 Constanța - 1 Argeș - 1
3.	Tip 3	3	București - 3

Anexa 9 la caietul de sarcini

SOLUȚIE DETECȚIE APT - TIP 3

1. Descriere generică a tehnologiei

Platformă de securitate cibernetică ce utilizează algoritmi specializați de învățare automată și analiză comportamentală sau mecanisme complexe de inteligență artificială pentru a monitoriza traficul de date din cadrul unei infrastructuri de control industrial (ICS/SCADA). Aceasta este capabilă să analizeze și să detecteze atacurile cibernetice avansate (Advanced Threat) și atacurile cibernetice necunoscute (zero-day).

Platforma este formată din senzori specializați (componentă hardware și software) care captează, monitorizează și analizează traficul existent într-o rețea OT, respectiv asigură coroborarea de informații între diverse subsisteme, utilizând o platformă de management centralizat.

Componenta hardware este compusă din servere fizice care asigură resursele necesare funcționării în parametri optimi a componentei software.

Componenta software este cea care conține algoritmii proprietari, mecanismele de învățare automată și analiză comportamentală.

Soluția va fi instalată în cadrul unui singur IVC, în județul Sibiu.

2. Caracteristici tehnice ale soluției

2.1 Caracteristici echipament hardware:

2.1.1	Dimensiune maxima, rackabil 19”	2U
2.1.2	Interfețe administrare	Minim 1 x 10/100/1000 BASE-T
2.1.3	Interfețe pentru analiză/monitorizare	Minim 3 x 10/100/1000 BASE-T
2.1.4	Sursă de alimentare	Dublă, 100 - 240 V
2.1.5	Accesorii:	Ofertantul trebuie să asigure toate accesoriile necesare pentru instalarea echipamentelor fizice ale soluției ofertate în infrastructura beneficiarului (ex: cabluri alimentare, adaptoare de rețea, cabluri rețea cupru/fibra optica).
2.1.6	Capacitate stocare	Echipamentul trebuie să asigure retenția alertelor pe o durată de minim 3 luni de zile.

2.2 Caracteristici componentă software:

2.2.1	Sistemul trebuie să aibă capacitatea de a analiza o rețea operațională (OT Network), învățând comportamentul rețelei (utilizând algoritmi avansați de învățare/ machine learning/ inteligență artificială) și generând

	un model de comportament/ baseline pentru traficul din rețeaua OT, astfel având posibilitatea de a detecta activitățile anormale.
2.2.2	Echipamentul primește/ interpretează trafic de rețea folosind metoda SPAN (VLAN mirroring, Port mirroring)
2.2.3	Soluția trebuie să dispună de o interfață grafică accesibilă din browser care permite vizualizarea unor detalii despre alerte precum: cronologia alertelor, anvergura, dovezile colectate și sugestii de remediere.
2.2.4	Soluția trebuie să ofere informații valorificabile în scopul remedierii unor incidente curente ce includ informații despre adrese IP, nivelul de risc, tip și producător dispozitiv ICS, etc.
2.2.5	Soluția va oferi o listă cu incidente/alerte care au avut loc la nivelul rețelei. Aceasta trebuie să dispună de mecanisme de filtrare sau sortare a incidentelor.
2.2.6	Soluția trebuie să ofere o interfață grafică în scopul administrării echipamentului.
2.2.7	Soluția trebuie să includă o componentă de gestionare a indicatorilor de compromitere - IoC
2.2.8	Soluția trebuie să ofere funcționalitatea de a realiza capturi de trafic într-un format standard (cel puțin formatul PCAP) și analiză de trafic a acestora.
2.2.9	Datele înregistrate de către soluție trebuie să fie indexate, iar index-ul să conțină cel puțin tipul de protocol și adresele IP (sursă și destinație).
2.2.10	Soluția trebuie să permită retenția alertelor/ incidentelor cel puțin 90 de zile.
2.2.11	Soluția trebuie să ofere un scor alertelor pe baza anumitor indicatori pentru a prioritiza alertele cu grad ridicat de risc
2.2.12	Soluția asigură detecția atacurilor/incidentelor prezente în rețea încă de la momentul instalării.
2.2.13	Sistemul trebuie să fie scalabil și să asigure monitorizarea dispozitivelor din locații multiple pentru agregarea datelor.
2.2.14	Soluția trebuie să identifice modificările aduse controlerelor/ dispozitivelor din rețeaua OT.
2.2.15	Soluția trebuie să identifice toate modificările aduse controlerelor/ dispozitivelor din rețeaua OT.
2.2.16	Soluția trebuie să detecteze, să raporteze vulnerabilitățile specifice OT și să ofere detalii CVE/CVSSv3 (Common Vulnerabilities and Exposures/ Common Vulnerability Scoring System version 3).
2.2.17	Soluția trebuie să identifice configurațiile necorespunzătoare din punct de vedere al securității cibernetice la nivelul dispozitivelor ICS (ex. parole implicite sau slabe, conflicte de adrese IP, etc.)
2.2.18	Soluția trebuie să asigure o vedere centralizată a tuturor vulnerabilităților identificate în rețea. Din interfața grafică de management (Dashboard), administratorul trebuie să vizualizeze detalii cum ar fi: identificarea și

	vizualizarea alertelor, a evenimentelor de securitate, vizualizarea datelor la nivel de sistem informatic, etc..
2.2.19	Soluția trebuie să asigure generarea de rapoarte.
2.2.20	Soluția trebuie să asigure definirea politicilor de control al accesului bazat pe roluri pentru a restricționa accesul specific pentru utilizatori și/sau grupuri la anumite informații.
2.2.21	Capacitatea traficului suportat de către soluție trebuie să fie de cel puțin 1 Gbps.
2.2.22	Arhitectura soluţiei trebuie să permită monitorizarea a minim 10000 de dispozitive OT/IoT.
2.2.23	Soluția trebuie să trimită alerte și loguri către diferite soluții de SIEM.
2.2.24	Soluția trebuie să asigure integrarea cu echipamente de tipul Firewall.
2.2.25	Implementarea soluţiei nu trebuie să implice întreruperea rețelei OT.
2.2.26	Soluţia trebuie să inventariezeîn mod automat echipamentele observate din reţea şi să includă informaţii detaliate despre acestea (de exemplu IP, protocolul utilizat, stare, etc.).
2.2.27	Soluţia trebuie să aibă capabilitatea de a clasifica echipamentele pe baza tipului OT (de exemplu PLC, HMI, etc.).
2.2.28	Soluţia trebuie să identifice firmware, model, producător și alte informații despre dispozitivele din rețea.
2.2.29	Soluţia trebuie să asigure o vedere grafică, o diagramă cu topologia reţelei OT/IoT, arătând dispozitivele şi cum comunică acestea. Harta trebuie să permită afişarea detaliilor per componentă.
2.2.30	Soluția trebuie să suporte, minim, următoarele protocoale IT: • SNMP • SSH • HTTP / HTTPS • Telnet • FTP • DNS • ICMP • Browser • CDP • LLDP • DHCP V4/V6 • ARP • VNC • NTP • SMB
2.2.31	Soluţia trebuie să suporte, minim, următoarele protocoale specifice rețelelor industriale: • Modbus (extensia pentru Schneider inclusă)

	• Siemens S7/S7-Plus • EtherNet/IP • PCCC • GE SRTP • VNet/IP • Emerson DeltaV • Melsec/Melsoft • OPC UA • IEC104 • DNP3 • Profinet-DCP
2.2.32	Soluţia trebuie să suporte, minim, dispozitive de la următorii producători ICS: • Siemens • Rockwell • Schneider • Emerson • GE • ABB • Yokogawa • Mitsubishi • Honeywell
2.2.33	Pentru protocoalele ICS, solutia trebuie să permită monitorizare la nivelul comenzilor de protocol.
2.2.34	Soluția oferă vizualizări ce pot fi personalizate și care pot fi reprezentate sub formă de hartă a rețelei.
2.2.35	Soluția asigură filtrarea dispozitivelor din rețea după adresa IP pentru a vizualiza informații despre acestea.
2.2.36	Soluția asigură capacitatea de a vizualiza evenimentele în timp real.
2.2.37	Soluția trebuie să permită gruparea alertelor legate de aceeași investigație.
2.2.38	Trebuie să utilizeze metode de detecție a anomaliilor pentru a identifica atacuri cum ar fi exploatări ale vulnerabilităților zero-day, atacuri man in the middle (MITM), mișcare laterală, scanare de porturi, utilizarea nerecorespunzătoare sau configurarea greșită a dispozitivelor ICS.
2.2.39	Soluţia trebuie să suporte scanare folosind semnături cunoscute (ex: reguli YARA);
2.2.40	Soluția trebuie să asigure actualizări produsului în modul offline (soluția nefiind conectată la Internet).

2.3 Cerințe generale

2.3.1	Tehnologia trebuie să fie 100% „on premise”, fără a fi necesară conectarea în

Internet pentru orice fel de motiv cu privire la funcționalitatea produsului. Orice tip de date sau informații culese de la client nu se trimit în extern, sau la producător, fără acordul clientului. Toate actualizările software trebuie efectuate offline, în mod centralizat și automat. Componenta software trebuie să se afle in întregime pe servere fizice, complet sub controlul clientului și în interiorul rețelei sale.

2.3.2 Ofertantul va crea mecanismele necesare transmiterii logurilor generate de platforma catre componenta SIEM din cadrul Centrului National Cyberint.

2.3.3 Soluția și subsistemele acesteia se vor instala într-o rețea izolată, fără conexiune la Internet, transferul datelor din Internet (actualizări, informații de tip threat intelligence și alte pachete care asigură funcționalitatea în parametri optimi) se va realiza printr-un echipament de stocare extern (de exemplu: stick USB, HDD/SSD extern) sau de tip diodă de date, puse la dispoziție de ofertant.

2.3.4 Ofertantul trebuie să asigure o sesiune de instruire de minim 5 zile, pentru 8 persoane, ce trebuie să prezintenoțiuni specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului ofertat, incluzând, dar fară a se limita la următoarele informaţii:

- Prezentarea funcționalităților componentelor soluției
- Prezentarea modului de instalare a tuturor componentelor soluției
- Prezentarea configurațiilor și politicilor implementate în cadrul soluției furnizate
- Prezentarea interfeţei de administrare şi a principalelor acţiuni ce pot fi întreprinse prin intermediul acesteia
- Bune practici pentru instalarea echipamentului cu scopul de a colecta și monitoriza traficul de rețea în funcție de tipologia rețelelor
- Modalități pentru actualizarea offline a componentei software
- Prezentarea modului de verificare a instalării soluției, validarea că traficul de rețea ce se dorește monitorizat este primit și analizat de soluție
- Prezentarea tuturor resurselor implementate în cadrul soluției
- Prezentarea modalităților de monitorizare în timp real a alertelor, eliminare “false-positive”, filtrare alerte, corelare evenimente, etc.
- Prezentarea modului de investigare al unei alerte/atac cibernetic (Ex: vector de infecție, mișcare laterală, server de comandă și control, sisteme informatice infectate, moduri de comunicare, etc.)
- Prezentarea modului de creare a rapoartelor
- Bune practici pentru a eficientiza activitatea de identificare a atacurilor cibernetice
- Ofertantul va pune la dispoziția beneficiarului un back-up al configurației soluției livrate.

Cursul va fi de tip “hands-on”, cu activități practice în care cursanții utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului.

Cursul se va desfășura în limba română, într-o locație pusă la dispoziție de

furnizor, în municipiul București. Instructorul trebuie să fie acreditat de producătorul soluției. Pentru demonstrarea pregătirii instructorului se vor prezenta certificate/autorizări/acreditări, sau alte documente emise de către producătorul soluției, sau de organisme abilitate în acest sens.

Ofertantul va asigura servicii de catering pe perioada cursului, respectiv o masă de prânz şi un coffee-break pe zi(cafea, apă, ceai, produse de patiserie şi fructe, la discreţie).

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de detecție APT tip 3.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de detecție APT tip 3se va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- crearea / migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la

momentul livrării,

- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- configurarea soluției pentru jurnalizarea evenimentelor la nivelul soluției SIEM existente la fiecare beneficiar,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate,
- implementarea unui flux automat de preluare a actualizarilor în mod offline, fără conexiune la Internet.

4.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.
- suport pentru fluxul automat de preluare a actualizarilor în mod offline, fără conexiune la Internet.

Anexa 10 la caietul de sarcini

SWITCH CU 12 PORTURI 10/100/1000 ETHERNET

Este necesar a fi livrate 17 bucăți cu următoarele caracteristici.

1. **Caracteristici tehnice**

1. Caracteristici generale	Interfeţe 10/100/1000 Ethernet RJ45: minim 12 UPlink 1 Gb SFP : minim 2 Capacitate de switching: minim 32 Gbps; MTU configurabil la minim 9000 bytes; VLAN-ID: minim 4000
2. Caracteristici minimale incluse	IGMP snooping RSPAN sau Mirroring Tx/Rx/Both Auto-MDIX Servicii QoS Suport DHCP Permite rutare inter-vlan la nivelul switch-ului Autentificare RADIUS și TACACS+ SNMPv3 Voice VLAN Private VLAN Port-based ACL NTP server/client Proxy ARP DHCP snooping Dynamic ARP Inspection IP Source Guard
3. Standarde	IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS Prioritization IEEE 802.1Q VLAN IEEE 802.1s IEEE 802.1w IEEE 802.1X IEEE 802.1ab (LLDP) IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX şi 1000BASE-T IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T

		RMON I SNMP v1, v2c, and v3
4.	Management	Configurare CLI, interfață Web, SSH, consolă.
5.	Alimentare cu energie electrică	Sursă de alimentare instalată intern cu suport pentru standardele româneşti: 220 VAC / 50 Hz.
6.	Dimensiuni de gabarit	rackabil 19”, 1U.
7.	Accesorii	1 X cablu consolă; Set cabluri de alimentare cu conector C14-tată, set cabluri de alimentare cu conector CEE 7/7 tată; 1 X kit de instalare în rack 19"

2. Implementare

2.1 Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip Switchse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- crearea / migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la momentul livrării,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- configurarea soluției pentru jurnalizarea evenimentelor la nivelul soluției SIEM existente la fiecare beneficiar,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

2.2 Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data

instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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.

Distribuția soluției *Switch* necesar a fi instalată

Nr. crt.	***Tip soluție***	***Nr. total buc.***	***Livrare***
	Switch	17	București - 11

			Constanța - 3 Sibiu - 2 Timiș - 1

Anexa 11 la caietul de sarcini

STAȚII DE LUCRU REȚEA COOPERARE

Descriere generică

Este necesar a fi livrate 17 bucăți.

2. Caracteristici tehnice minimale

Caracteristică	**Cerință**
Procesor	Intel Core i5-9400 sau echivalent Frecvență: minim 2.9 GHz Frecvență turbo: minim 3.9 GHz Număr core-uri minim: 6 L3 cache minim: 9 MB
Placă de bază	Sloturi memorie: minim 2 tip DIMM LAN: Inclus pe placa de baza, suporta 10/100/1000 Mbps Porturi USB: minim 2 Porturi SATA III: minim 2
Memorie	DDR4: minim 16GB, 2x8GB
Hard Disk	Capacitate minim 1 TB 7200 rpm SATA III Buffer: minim 64 MB
Periferice	Kit tastatură-mouse cu interfață USB
Monitor	Tip: LED Diagonală: minim 23 inch Wide; Rezoluție: 1920x1080; Interfețe video minim: HDMI; Cabluri: HDMI;
Sistem de operare	Va fi instalat și licențiat sistemul de operare Microsoft Windows 10 Professional, 64 bit.
Accesorii	Set cabluri de alimentare
Performanţă energetică	Produsele trebuie să respecte cele mai recente standarde ENERGY STAR în materie de performanţă energetică. Cerinţa va fi considerată îndeplinită prin prezentarea unei etichete ecologice relevante de tip I sau altor mijloace doveditoare adecvate (ex: dosar tehnic al producătorului sau un raport de încercare din partea unui organism recunoscut care să demonstreze respectarea cerinţelor).
Folosirea substanţelor periculoase	În cazul în care produsul ofertat conţine substanţe înscrise pe lista REACH a substanţelor cu o concentraţie mai mare de 0,1% (procent de masă) în

	întregul produs şi/sau subansamblurile produsului, se va prezenta o declaraţie care să indice substanţele specifice prezente.
Gestiunea scoaterii din uz: reciclarea părţilor componente şi marcarea carcaselor, a suporturilor şi a ramelor din plastic	Se vor prezenta documente sau declarații din care să reiasă greutatea, compoziţia polimetrică, precum şi marcajele ISO 11469 şi ISO 1043 ale părţilor din plastic cu greutatea mai mare de 100 grame şi suprafaţa mai mare de 50 cm^2.

3. Implementare

3.1. Instalare și/sau integrare în cadrul infrastructurilor

Stațiile de lucruse vor implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie.

3.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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.).

Distribuția soluției *Switch* necesar a fi instalată

Nr. crt.	***Tip soluție***	***Nr. total buc.***	***Livrare***
3.	Switch	17	București - 11 Constanța - 3 Sibiu - 2 Timiș - 1

Anexa 12 la caietul de sarcini

SISTEM HIGH POWER COMPUTING HPC

1.Ofertantul va furniza o soluție de tip HPC a cărui structură de bază este formată din minim:
15 sisteme informatice de tip server;
5 sisteme informatice de tip storage;
2 switch-uri de tip Ethernet;
2 switch-uri de tip FC.

2. Caracteristici tehnice minimale ale soluției

Cerințe minimale generale	2.1.1. Serverele și storage-ul trebuie sa conțina o interfață hardware de management dedicată (cu port Ethernet dedicat), care sa asigure administrarea acestora prin intermediul unui browser web.
	2.1.2. Ofertantul trebuie să asigure interconectarea echipamentelor cu cabluri de fibră optică, cabluri UTP, cabluri Ethernet care sa asigure viteze de 10 Gbps şi cabluri de alimentare electrică pentru realizarea unui sistem tolerant la defecţiuni. Pentru fiecare echipament se va asigura bezel-kitul, sistemul de montare in rack (slide rails), managementul pentru cabluri, precum și cabluri de alimentare conector de tipul C14-tată C13-mamă cu lungimea de 2 m.
	2.1.3. Serverele, switch-urile Ethernet, switch-urile FC și echipamentele de tip storage, prevăzute în prezentul caiet de sarcini, trebuie să fie interoperabile.
	2.1.4. Solutia de tip HPC va conține o platformă de virtualizare comercială (Vmware vSphere sau Microsoft HyperV sau echivalent) care va include atât setul de produse de virtualizare a serverelor

	(hypervizor) din prezentul caiet de sarcini, cât si componenta de management centralizat a acestora.
Cerințe minimale pentru 1 (unu) sistem informatic de tip server (se aplică pentru fiecare dintre sistemele informatice de tip server solicitate)	**2.2.1.** Tip procesor: Intel Xeon Platinum 8200-Series sau echivalent, arhitectură pe 64 de biți, cu minim 24 core per procesor.
	2.2.2. Număr procesoare instalate: minim 2.
	2.2.3. Memorie RAM: minim 512GB DDR4, minim 2933 MT/s.
	2.2.4. HDD: minim 2 x 960GB SAS-SSD.
	2.2.5. Controller RAID integrat cu minim 2 GB cache care să suporte RAID 0,1 hardware.
	2.2.6. Controllerul RAID instalat pe sistem trebuie sa suporte criptarea datelor (data at rest) / SED.
	2.2.7. Controllerul RAID instalat trebuie sa suporte următoarele sisteme de operare/platforme de virtualizare: Microsoft Windows Server VMware SUSE Linux Enterprise Server Red Hat Enterprise Linux
	2.2.8. Minim 2 port-uri Base-T 1 Gbps Ethernet și 2 porturi 10 Gbps Ethernet SFP+ cu transceivere de 10Gbps Ethernet incluse.
	2.2.9. Minim 2 porturi FC de minim 16 Gbps, echipate cu modulele de tip SFP+ aferente.
	2.2.10. Sistemul trebuie sa fie echipat cu minim 6 sloturi PCI-Express 3.0 din care cel putin doua sa fie de tip x16 PCIe.
	2.2.11. Ventilatoare: minim 6 ventilatoare redundante hot-swap.
	2.2.12. Sistemul trebuie sa acopere cel puțin următoarele cerințe de securitate: sistemul trebuie să aibă capabilitati de recuperare a firmware-ului in cazul in care s-a detectat o compromitere a acestuia. sistemul trebuie sa aiba capabilitati de rollback la nivel de firmware. Rollback-ul trebuie sa se poata face la nivelul setarilor din fabrica si “last known good state”. sistemul trebuie sa aiba capabilitati de tip “Chassis Intrusion Detection” si sa detecteze deschideri ale carcasei sistemul trebuie sa aiba capabilitati de tip “UEFI Secure Boot”. sistemul trebuie sa aiba capabilitati de criptare a datelor (Data at rest) atat pe storage-ul intern. sistemul ofertat trebuie sa suporte TPM 1.2 si 2.0.
	2.2.13. Managementul de sistem trebuie să acopere cel puțin

	următoarele aspecte de interes: port de rețea dedicat; sistem încorporat de monitorizare a ventilatoarelor, surselor de alimentare, temperaturii, memorii, procesoare, disk-uri; suport instalat și activat pentru managementul serverului de la distanță (redirectare interfață grafică inclusiv în BIOS, tastatură și mouse, posibilitate de pornire/oprire de la distanță, suport SSL, SNMP, suport pentru remote virtual media) sistemul trebuie sa fie capabil sa ofere facilitati de tip upgrade de software si patch-uri sistemul de management de la distanta trebuie sa fie de tip agentless sistemul trebuie sa monitorizeze si sa inregistreze schimbarile care au avut loc in configuratia hardware a serverului sau in configurarea sistemului.
	2.2.14. Echipamentul trebuie să suporte integrarea cu o soluţie de management proprietară producătorului, prin intermediul căreia se vor putea administra în mod centralizat toate echipamentele de tip server cerute prin prezentul document.
	2.2.15. Echipamentul ofertat va respecta urmatoarele standarde pentru siguranta in exploatare si compatibilitate electromagnetica si se va face dovada faptului ca acestea au fost verificate de catre producator: Cerințe privind siguranta in exploatare: EN 60950-1:2006 +A2:2013 Cerințe de compatibilitate electromagnetica: EN 55024:2010, EN 55032:2012 Class A, EN 61000-3-2:2014
	2.2.16. Alimentare: hot-plug, redundantă, dimensionată corespunzător de către producătorul soluţiei pentru a susţine funcționarea serverului la încărcarea maximă
	2.2.17. Dimensiuni de gabarit: 19”, rackabil, kit de montare pe rack sliding rails cu management pentru cabluri inclus.
Cerințe minimale pentru sistemul informatic de tip storage	**2.3.1.** Storage-ul va fi de tip SAN compatibil cu serverele şi cu sistemele de tip switch, prevăzute în prezentul document
	2.3.2. Sistemul va conține un număr de sloturi de 2.5” pentru SSD-uri cu interfață SAS, suficient pentru a asigura capacitatea de stocare prevăzută în prezentul document
	2.3.3. Sistemul va fi livrat cu o capacitate de stocare brută de minim 60 TB formată exclusiv din dispozitive SSD
	2.3.4. În situaţia defectării unui dispozitiv SSD, în vederea înlocuirii se vor returna toate părţile componente din dispozitivul defect mai puţin partea de memorie.
	2.3.5. Sistemul informatic de tip *storage*trebuie să îndeplinească

	următorii indici de performanță: IOPS: minim 200K
	2.3.6. Sistemul informatic de tip *storage*va fi echipat cu SSD-uri având capacitatea de minim 1.6TB
	2.3.7. Sistemul va conține minim 2 controlere SAN
	2.3.8. Soluţia va asigura redundanţă la nivel de controller pentru administrarea dispozitivelor de stocare.
	2.3.9. Conectivitatea echipamentului trebuie să fie asigurată prin Fiber Channel: minim 4 port-uri FC (per controller) cu viteză de cel puţin 16 Gbps, cu transceivere aferente.
	2.3.10. Soluţia suportă administrarea de la distanţă prin interfaţă grafică (Web browser sau aplicaţie de management).
	2.3.11. Soluţia suportă separarea discurilor în unităţi logice separate (LUN)
	2.3.12. Soluţia suportă cel puțin următoarele configurații pentru HDD: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, prin intermediul unui controller RAID integrat.
	2.3.13. Soluția oferă scalabilitate prin posibilitatea de adăugare a unor module adiţionale.
	2.3.14. Alimentare: 2 surse de alimentare hot-plug/hot-swap, redundante cu cabluri de alimentare incluse
	2.3.15. Se vor oferi cabluri de fibră optică de lungime corespunzătoare la momentul instalării, pentru asigurarea interconectării cu fiecare echipament de tip switch Fiber Channel, din prezentul caiet de sarcini.
	2.3.16. Dimensiunea de gabarit a întregului sistem: rackabil 19”, kit de montare pe rack inclus.
Cerințe minimale pentru switch-ul de tip FC	**2.4.1.** Deţine minim 24 porturi tip SFP+ ce asigură conexiuni la viteze de transfer de cel puțin 16 Gbps.
	2.4.2. Minim 24 de module SFP+ compatibile cu switch-urile FC, precum și 24 de licențe pentru activarea acestora
	2.4.3. Soluţia este compatibilă cu celelalte echipamente din prezentul caiet de sarcini (servere, storage)
	2.4.4. Soluția include instrumente pentru management de trafic, diagnoză și rezolvarea de probleme
	2.4.5. Soluția oferă acces pentru management prin următoarele protocoale: SFTP, SSHv2, SNMPv3.
	2.4.6. Alimentare: 2 surse de alimentare redundante, hot-plug, intrare 220 VAC / 50 Hz.
	2.4.7. Echipamentul va fi instalat în cadrul unui rack de 19”, prin intermediul unui kit de instalare inclus.
	2.4.8. Se vor livra toate cablurile necesare pentru interconectarea redundantă a switch-urilor FC cu serverele și storage-ul.
Cerințe minimale pentru switch-ul de tip Ethernet	**2.5.1.** Switch-urile trebuie să fie compatibile cu serverele din cadrul caietului de sarcini.

	2.5.2. Switch-ul trebuie sa aibă minim 24 de porturi 10 Gbps SFP+
	2.5.3. Ofertantul trebuie să asigure cabluri şi transceivere de 10Gbps Ethernet incluse, de lungime corespunzătoare la momentul instalării, necesare pentru interconectarea redundantă a switch-urilor Ethernet cu serverele.
	2.5.4. Specificaţii hardware Minim 24 porturi 10Gbps SFP+ 1 port RJ45 console/management 1 port USB sursă de alimentare redundantă
	2.5.5. Dimensiuni de gabarit: rackabil, 1U, cu kit de instalare inclus.
	2.5.6. Performanţa sistemului (valori minime) •Switching capacity – 480 Gbps •Throughput – 250 Mbps •VLANs supported – 4000 •QOS •Acces Control Lists pe port şi VLAN •Private VLAN •Standarde •IEEE 802.3 •IEEE 802.3ae 10 Gigabit Ethernet •IEEE 802.3ad – LACP •IEEE 802.1d – Spanning Tree Protocol •IEEE 802.1w – Rapid Reconfiguration of Spanning Tree •IEEE 802.1s – Multiple VLAN Instances of Spanning Tree •IEEE 802.1p – CoS Prioritization •IEEE 802.1q – VLAN •IEEE 802.1x – User Authentication

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției HPC.

4. Implementare

4.1 Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip High Power Computingse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

montarea în rack,
conectarea la rețeaua informatică,
instalarea de firmware și drivere,
configurarea conexiunilor de alimentare cu energie electrică,
securizarea sistemului de operare și serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
realizarea tuturor configurărilor la nivelul sistemului de operare,
configurarea pachetelor software,
configurarea conexiunilor de reţea,
configurarea tabelelor de acces,
realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie
instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi
asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate

4.2 Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Anexa 13 la caietul de sarcini

SOLUȚIE ANALIZĂ TRAFIC BRUT

1.Descrierea generală a tehnologiei solicitate

Soluție la cheie, dedicată analizei de trafic, ce va conține toate componentele hardware/software necesare bunei funcționări a acesteia.

Soluția de analiză a traficului brut de date poate fi livrată sub formă de virtual appliance (mașină virtuală)on-premise.

2. Caracteristici tehnice ale soluției

Ofertantul va furniza o "Soluție analiză trafic brut" cu următoarele caracteristici tehnice minimale:

	Soluția trebuie să permită importul/ încărcarea fișierelor de trafic brut de date în format .pcap și analiza individuală sau simultană a acestora.
2.	Soluția trebuie să suporte importul/ încărcarea fișierelor .pcap cu dimensiuni de minim 2 GB per fișier.
3.	Trebuie să suporte analiza/indexarea unui volum de date de minim 2 TB per caz în lucru.
4.	Trebuie să poziționeze grafic, pe harta globului, adresele IP existente în cadrul sesiunilor TCP/UDP (geolocalizarea evenimentelor).
5.	Produsul ofertat trebuie să ofere informații de geolocație a adreselor IP identificate în cadrul traficului, în mod independent, fără accesarea Internetului sau altor resurse externe. De asemenea, este necesar ca produsul să suporte actualizarea fără conexiune la Internet a datelor referitoare la interogările de tip whois.
6.	Trebuie să ofere posibilitatea aplicării de filtre în vederea clasificării şi analizei diverselor servicii sau protocoale.
7.	Trebuie să dispună de capabilități similare unui sistem IDS ce detectează evenimente de securitate cibernetică pe baza regulilor prestabilite de către producător. Totodată, soluția oferă posibilitatea dezvoltării de reguli proprii pentru generarea alertelor pe bază de adrese IP, domenii, porturi, hashuri introduse de către utilizatori.
8.	Trebuie să permită actualizarea offline a sistemului (cu ajutorul unui suport de memorie extern), de către beneficiar, prin descărcarea update-urilor de la o resursă pusă la dispoziție de către producător.
9.	Trebuie să dispună de capabilităţi DPI (Deep Packet Inspection) sau similare.
10.	Trebuie să permită extragerea fișierelor/artefactelor reconstituite din trafic.
11.	Trebuie să permită filtrarea capturilor de trafic într-un mod vizual după cel puțin următoarele criterii: •Interval de timp;

	•Adresă IP sursă și destinație; •Port sursă și destinație; •Adresa MAC sursă și destinație; •Hostname; •Nume utilizator/ conturi asociate cu diverse platforme; •Adresă de email; •Protocol/ serviciu; •Domain Name System (DNS); •Țară origine/ destinație IP;
12.	Trebuie să permită crearea unor criterii de filtrare a traficului şi exportarea pachetelor în fişiere ”.pcap” după filtrare.
13.	Trebuie să permită efectuarea de căutări după cuvinte cheie (keywords/ strings).
14.	Trebuie să permită afişarea unor statistici ale traficului analizat.
15.	Trebuie să suporte **cel puţin** detecția/ identificarea/ interpretarea următoarelor protocoale: IPv4, IPv6, TCP, UDP, SSL/TLS, RDP, IMAP, RTP, TELNET, SSH, SMB, SIP, HTTP, SMTP, POP3, FTP, DNS.
16.	Exploatarea soluţiei este realizată prin intermediul unei interfeţe web ce structurează informația în dashboard-uri populate cu panouri grafice și tabele.
17.	Trebuie să permită realizarea și exportarea de rapoarte (în format PDF/CSV/HTML) pe baza rezultatelor obţinute în urma unor filtrări ale evenimentelor, pentru orice perioadă de timp definită de utilizator.
18.	Trebuie să permită afișarea unui timeline al evenimentelor prezente, pentru tot traficul brut de date încărcat în soluție sau conform unui interval de timp selectat.
19.	Virtual appliance, va fi configurat astfel încât să suporte următoarele cerințe hardware minimale asigurate de beneficiar: - Compatibil minim ESXi 6.0; - RAM: 64 GB per Virtual Appliance; - Storage: 10TB;

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de analiză trafic brut.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de de analiză trafic brutse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locația comunicată la încheierea contractului şi va include cel puțin următoarele servicii:

- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

4.2. Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Anexa 14 la caietul de sarcini

SOLUȚIE THREAT INTELLIGENCE

1.Descriere generică a tehnologiei

Ofertantul va furniza o soluţie de tip pachet softwareși hardware on-premise, care va integra fluxurile de informații referitoare la amenințări cibernetice (threat intelligence feeds), atât open-source cât și comerciale, solicitate de beneficiar. Soluția va permite integrarea bidirecțională cu soluția SIEM aflată în exploatare și instalată în rețeaua internă a Beneficiarului, iar informațiile vor fi partajate între soluții pe baza criteriilor stabilite de autoritatea

contractantă.

2. Caracteristici tehnice ale soluției

Soluția oferită trebuie să îndeplinească următoarele caracteristici tehnice minimale:

	Soluția trebuie să integreze într-o singură platformă de management toate sursele de informații solicitate de beneficiar referitoare la amenințări și atacuri cibernetice.
	Soluția trebuie să includă o componentă SaaS, disponibilă beneficiarului sub forma unei aplicatii sau portal web, care să administreze și să gestioneze toate operațiunile de colectare, agregare și procesare de informații provenite din OSINT și solutii de securitate terțe, fără un efort de management semnificativ de gestionare din partea beneficiarului.
	Soluția trebuie să includă 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, fără conexiune la internet.
	Soluția trebuie să prezinte prin intermediul unui singur panou de afișare (dashboard) toate informațiile cunoscute și relevante în jurul unui Indicator de compromitere (IoC), inclusiv scorul asociat, etichete, sursele în care este referențiat, URL-uri de referință, buletine de tip threat intelligence, utilizatori ce contribuie la investigație, campanii și alte IoC-uri asociate.
	Soluția trebuie să includă un mecanism de sincronizare, care să asigure operarea în medii de tip air-gapped (neconectate la Internet), pentru a transfera datele în mod automat și securizat.
	Soluția trebuie să permită corelarea între fluxurile de date relevante, cum ar fi IoC-uri, campanii, actori și TTP-uri.
	Soluția trebuie să furnizeze automat un scor de încredere pentru IoC-uri noi fără a fi necesară o configurare manuală.
	Soluția trebuie să ofere 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.
	Soluția trebuie să seteze în mod automat o durată de viață pentru indicatori.
	Soluția trebuie să ofere capacitatea de a importa informații/date în sistem din interfața grafică, în cel puțin următoarele formate: CSV, JSON, XML.
	Soluția trebuie să ofere capacitatea de a importa informații/date în sistem printr-un API, în format JSON.
	Soluția trebuie să poată parsa informațiile dintr-o formă nestructurată a datelor provenite dintr-o altă sursă. Soluția trebuie să normalizeze datele de intrare într-un format structurat.
	Soluția trebuie să suporte parsarea informațiilor din rapoarte nestructurate trimise prin email către o căsuță de email dedicată la care soluția are acces.
	Soluția trebuie să ofere posibilitatea de a parsa automat indicatori de compromitere dintr-un e-mail de tip phishing trimis la o adresa de email dedicata.
	Soluția trebuie să ofere STIX / TAXII pentru interacțiunea cu alte soluții de TI.
	Soluția trebuie să permita deduplicarea datelor.
	Soluția trebuie 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).
	Soluția trebuie să permită crearea de integrări personalizate pentru fluxuri și contextualizare a datelor prin intermediul unor SDK/API-uri documentate.
	Soluția trebuie să permită beneficiarului utilizarea unui API pentru folosirea de scripturi și / sau alte depozite de date pentru automatizarea procesării acestora.
	Soluția trebuie să ofere o gamă largă de fluxuri OSINT fără costuri suplimentare și fără să fie nevoie de personalizare sau configurare. Soluția trebuie să includă o gamă largă de furnizori comerciali de CTI, de la care să fie preluate IoC-uri, buletine de atacuri cibernetice și orice altă informație despre amenințari cibernetice oferite de fiecare furnizor comercial. Soluția va include toate feed-urile comerciale de threat intelligence furnizate de cel puțin următoarele companii: Crowd Strike, Intel471.
	Soluția trebuie să ofere 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.
	Soluția trebuie să permită analistului inserarea de comentarii pe marginea amenintarilor, a indicatorilor sau a buletinelor de amenințare în scopul întregirii informațiilor disponibile.
	Soluția trebuie să permită crearea de legaturi dintre un indicator și alte date specifice, precum threat actor sau informații referitoare la campanie.
	Soluția trebuie să poată exporta orice buletin de amenințări (threat bulletin) sau orice alt produs de threat intelligence creat de platformă în format PDF.
	Soluția trebuie să suporte exportul de IoC-uri în format CSV.
	Soluția trebuie să suporte crearea de etichete (tag-uri) pentru informațiile publice sau private care sunt vizibile numai pentru beneficiar, pentru a permite etichetarea informațiilor private astfel încât acestea să nu poată fi distribuite în afara organizației.
	Soluția trebuie să includă o integrare bidirecțională cu sistemul de tip SIEM aflat în exploatare la nivelul beneficiarului, inclusiv să fie pus la dispoziție un pachet de conținut out of the box care să fie integrat în SIEM. Pachetul de conținut trebuie să suporte actualizări, iar furnizorul soluției trebuie să ofere aceste actualizări periodic.
	Soluția trebuie să permită analistului să scrie filtre pe baza unor parametri multipli (ex: scor de încredere, sursă, interval de timp etc.) pentru a determina ce informație este sincronizată cu sistemul de securitate de tip SIEM.
	Soluția trebuie să aibă capabilitatea de a primi alerte de corelare (matches) pentru IoC-urile monitorizate raportate de SIEM și să furnizeze statistici și analize ale acestor alerte în interfața de utilizare a soluției.
	Soluția trebuie sa ofere un REST API.
	Soluția trebuie să permită crearea de whitelists (liste de valori permise) cu domenii cunoscute.
	Soluția trebuie să identifice și să coreleze documentele de referință și informațiile

	despre amenințări în cazul oricărui indicator de compromitere (IoC).
	Soluția trebuie să poată afișa toate sursele de raportare pentru orice IoC dat, împreună cu orice context pe care îl oferă, cum ar fi etichete, scoruri de risc și alte date disponibile.
	Soluția trebuie să permită adăugarea oricărei etichete (tag) la un indicator în timpul analizei.
	Soluția trebuie să ofere posibilitatea de a face căutari în toate datele deținute de platformă printr-o singură interogare formată dintr-un șir de caractere.
	Soluția trebuie să permită efectuarea de căutări pe baza etichetelor (tag-urile) atribuite.
	Soluția trebuie să permită căutări parțiale ale indicatorului / căutări wildcard.
	Soluția trebuie să permită filtrarea rezultatelor căutării după tipul de entitate.
	Soluția trebuie să permită importul de indicatori de compromitere custom, care să fie stocați local și privat, fără nici o stocare în cloud sau orice sistem extern.
	Soluția trebuie să permită crearea buletinelor, campaniilor sau ale altor entități referitoare la amenințări (threats) în mod privat, astfel încât acestea să fie stocate local, în infrastructura beneficiarului și care să nu fie vizibile pentru nicio platformă SaaS sau pentru alți utilizatori externi.
	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.
	Componentele sistemului trebuie să fie furnizate ca mașini virtuale sau echipamente (appliance) hardware în locația beneficiarului.
	Furnizorul trebuie să poată implementa/ să pună la dispoziție un mecanism de sincronizare unidirecțional, astfel încât datele să poată fi transferate în condiții de siguranță între două instanțe aflate în rețele cu nivele de securizare diferite.
	Platforma trebuie să poată corela în mod automat jurnalele istorice (log-uri) de la soluția SIEM, ce captează evenimente cu o capacitate de 5000 EPS (evenimente pe secunda), cu IoC-urile din platforma de threat intelligence.
	Soluția trebuie să permită recepționarea în flux continuu a noilor feed-uri de informații cu privire la amenințări și analiza automată a jurnalelor (log-uri) captate de soluția SIEM cu o vechime de cel puțin 3 luni în urmă de la momentul primirii IoC, pentru a detecta indicatorii de compromitere în cadrul logurilor.

Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea Soluției Threat Intelligence.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția Threat Intelligencese va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locația comunicată la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- configurarea tabelelor de acces,
- crearea / migrarea politicilor de securitate existente în funcție de arhitectura și specificațiile tehnice oferite de către autoritatea contractantă la momentul livrării
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie
- asigurarea integrării cu soluția SIEM
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate

4.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care

un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date cu cunoștințe a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”;
- Suport pentru mecanismul de sincronizare a datelor din rețeaua Internet în rețeaua privată a beneficiarului.

Anexa 15 la caietul de sarcini

SET DIAGNOSTICARE SI VERIFICARE PARAMETRI REȚEA

1.Descrierea generală a tehnologiei

Setul de diagnosticare și verificare parametri rețea va cuprinde echipamente portabile, pentru analiza și diagnoza rețelelor, a cablărilor și a echipamentelor conectate, pe interfețe din cupru și fibră optică, în vederea identificării defectelor în cablările pasive și active, precum și la verificarea și monitorizarea parametrilor de funcționare a rețelelor (inclusiv Wi-Fi).

2. Caracteristici tehnice ale soluției

Ofertantul va furniza un "*Set diagnosticare și verificare parametrii rețea*" cu următoarele caracteristici tehnice minimale:

1	Conectorii prevăzuți trebuie să asigure condiții adecvate pentru a permite conectarea directă la următoarele topologii Ethernet: • 10Mbps/100Mbps/1Gbps, cel puțin 1 port RJ-45 • 1Gbps, cel puțin 1 port SFP
2	Analizorul trebuie să permită testarea VLAN-urilor configurate în rețea.
3	Analizorul trebuie să permită folosirea funcției Ping pentru dispozitivele selectate.
4	Analizorul trebuie să fie capabil de a identifica parametrii unui dispozitiv compatibil Ethernet conectat (cel puțin adresa IP).
5	Testează conectivitatea clienților Wi-Fi și identifică numele AP, canalul și nivelul de securitate și monitorizează parametri de rețea (rate de transfer, pierderi de pachete, latență).
6	Analizorul va permite generarea în mod automat de teste de performanță și alte rapoarte și va emite rezultatele în format PDF și/sau XML, ce vor putea fi descărcate

	prin USB și/sau SD card
7	Analizorul trebuie să fie capabil de a captura trafic între două dispozitive de rețea conectate la rețea în porturile de testare A și B (RJ45) la 1 Gbps, (in-line tap), nefiind necesar niciun echipament suplimentar.
8	Analizorul trebuie să fie capabil de a analiza calitatea apelului într-o conversație Voice over IP (VoIP).
9	Analizorul, atunci când este conectat la o rețea de cupru, trebuie să poată efectua un test de cablu, să emită rapoarte specifice (împerechere, continuitate, polaritate, lungime cablu, distanța pînă la defect) și să afișeze grafic pe display datele obținute.
10	Analizorul trebuie să fie capabil de a testa funcționarea unui traseu de fibră optică.
11	Analizorul va avea în dotare echipamentele necesare (terminatori/identificatori/reflectori etc.) pentru efectuarea de teste punct la punct sau loopback în rețea
12	Analizorul poate să fie construit fizic, ca o singură sau mai multe entități ce trebuie să funcționeze cu baterii reîncărcabile iar când acestea sunt descărcate, prin intermediul unui adaptor de la surse externe de 100-240 volți c.a. (+ / - 10%). Adaptorul trebuie să fie capabil sa încarce bateriile fără a fi nevoie de a scoate bateria din echipament.
13	Analizorul trebuie să fie capabil de minim 2 ore de funcționare continuă pe baterie.
14	Echipamentul trebuie să fie portabil cu o greutate nu mai mare de 2 kg.
15	Echipamentul trebuie să funcționeze la caracteristicile de performanță specificate într-un mediu de temperatură și umiditate de 10 ° C până la 40 ° C.
16	Echipamentul trebuie să reziste la un mediu de depozitare de la -20 ° C până la +50 ° C.
17	Are predefinite profile de test pentru parametri de rețea
18	Furnizează informații necesare pentru a rezolva probleme legate de PoE
19	Identifică cabluri atunci când sunt folosite la capăt terminale cu ID
20	Induce ton in cabluri pentru a putea facilita localizarea acestora
21	Permite identificarea portului în care este conectat un cablu de test
22	Echipamentul trebuie să dispună de display grafic color, minim 3,5 inch cu touch screen
23	Setul va include minim: • echipament/echipamente dedicate analizei şi diagnosticarea reţelelor de calculatoare; • modul SFP 1Gbps (multimode) • modul SFP 1Gbps (single mode) • patch cablu minim CAT5e STP • echipament ce detectează frecvența de ton pe cablurile telefonice/ethernet • terminatori identificatori care pot fi folosiţi pentru identificarea cablurilor și pentru verificarea sertizării cablurilor • antena WIFI externă • acumulator/acumulatori pentru echipamentele furnizate • încărcător pentru echipamentele furnizate • geantă/genți pentru transport

3. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi a software-ul de bază vor fi disponibile pentru descărcare prin Internet din momentul publicării acestora pe site-ul web oficial al producătorului.

Anexa 16 la caietul de sarcini

SOLUTIE SANDBOX PENTRU ANALIZA AUTOMATĂ A APLICAŢIILOR MALWARE

1. Descriere generică a tehnologiei

Ofertantul va furniza o soluţie de tip pachet software on-premise, pentru analiza automată a fişierelor din punct de vedere al potențialului malware. De asemenea, ofertantul se va ocupa de instalarea mașinilor virtuale de analiză folosite de sandbox, precum și de configurarea acestora în diferite rețele (online/offline).

2. Caracteristici tehnice ale soluției

Soluția oferită trebuie să îndeplinească următoarele caracteristici tehnice minimale:

	Soluția va fi instalată on-premise.
	Soluția asigură analiza diferitelor fișiere pe mașini virtuale de analiză malware, cu versiuni ale sistemului de operare Microsoft Windows (cel puțin Windows 7 32 și 64 bits și Windows 10) și Linux.
	Furnizorul asigură instalarea și configurarea soluției cu o serie de mașini virtuale de analiză malware, cu versiuni ale sistemului de operare Microsoft Windows (cel puțin Windows 7 32 și 64 bits și Windows 10) și Linux.
	Furnizorul instalează și configurează două medii de analiză: un mediu de tip sandbox (execuţia sample-urilor malware este efectuată într-un mediu izolat - fără conexiune la rețeaua Internet, dar având posibilitatea de a folosi servicii Internet simulate), şi un mediu de analiză live (conexiune reală la reţeaua Internet). Cele două medii de lucru (sandbox și live) dispun de aceleași mașini virtuale de analiză malware (duplicate). Instalarea acestora este realizată de furnizor.
	Soluția permite construirea și adăugarea unor mașini virtuale de analiză malware personalizate, în vederea simulării mediului de lucru din cadrul unei organizații.
	Mașinile virtuale de analiză, cu sistemul de operare Microsoft Windows, vor avea instalate aplicaţii de tip browser (Internet Explorer, Mozilla Firefox, Google Chrome), plugin-uri (cel puțin Adobe Flash) şi alte terţe aplicaţii (cel puţin Adobe Acrobat Reader, JRE, Microsoft Office Word, Excel, Powerpoint).
	Mașinile virtuale de analiză, cu sistemul de operare Linux/Unix, vor avea instalate aplicaţii de tip browser, precum și aplicații terțe (cel puțin Python, Perl).
	Soluția este compatibilă cu mediul de virtualizare VMWare, și permite managementul mașinilor virtuale de analiză prin intermediul VMWare.
	Licenţierea sistemelor de operare Microsoft Windows şi a aplicaţiilor comerciale din cadrul mașinilor virtuale de analiză preinstalate / pre-configurate va fi asigurată de către furnizorul sistemului de analiză.
	Soluția asigură restaurarea automată a mașinilor virtuale de analiză, imediat ce se

	termină fiecare proces de analiză.
	Asigură analiza celor mai comune tipuri de fişiere cunoscute ca fiind folosite pentru distribuirea sau găzduirea de aplicaţii malware (fişiere executabile – EXE, DLL, documente Microsoft Office – DOC, DOCX, XLS, XLSX, PPT, PPTX, documente PDF, fişiere JAR, și fișiere powershell PS1).
	Asigură analiza obiectelor care se regăsesc la o adresă URL.
	Asigură analiza întregului ciclu de desfăşurare a unui atac cibernetic, începând cu rularea aplicației malware, urmată de monitorizarea tuturor acțiunilor ulterioare generate de acesta (ex: contactarea serverului de comandă şi control, descărcări ulterioare ale altor module malware, scrierea pe disk a altor fișiere, rularea de comenzi, etc.).
	Asigură analiza și rularea aplicaţiilor malware ce au capabilitatea de a identifica medii virtualizate / emulate.
	Asigură jurnalizarea apelurilor de funcţii Windows native și din interfața Windows API, relevante în depistarea comportamentului cu caracter malware.
	Asigură simularea prezenței utilizatorului în mașinile virtuale de analiză, astfel încât să asigure rularea cu succes a aplicaţiile malware care îşi manifestă comportamentul doar după ce au observat (prin metode specifice) prezenţa utilizatorului.
	Soluția asigură, în cadrul mașinilor de analiză, simularea interacţiunii utilizatorului cu aplicaţiile care au interfaţă grafică şi care necesită furnizarea unui răspuns la ferestre dialog sau parcurgerea unor paşi de instalare.
	Asigură inspecția HTTPS și analiza traficului de rețea criptat
	Asigură crearea de rapoarte tehnice ce vor cuprinde informaţii despre fişierele analizate precum: •Informații analiză statică, privind cel puțin următoarele aspecte de interes: •Tipul fişierului analizat; •Sumele de control (cel puțin SHA256) ale fişierelor analizate / create pe mașinile virtuale de analiză; •În cazul executabilelor se va indica eventuala folosire de aplicaţii de tip packer şi tipul acestora; •Informaţii extrase din header-ul fişierelor executabile: •Librăriile DLL, respectiv funcţiile folosite de malware, extrase din tabela de importuri (IAT); •Numărul şi caracteristicile secţiunilor componente; •Informații analiză dinamică, privind cel puțin următoarele aspecte de interes: •Modificări aduse la nivelul sistemului de operare; •Modificări asupra sistemului de fişiere; •Modificări aduse asupra bazei de date Windows Registry; •Librării DLL încărcate la *run time*; •Informaţii despre procesele create/modificate/oprite; •Informaţii despre serviciile Windows create/modificate/oprite; •Obiecte de tip Mutex create; •Eventuale *Hook*-uri; •Conexiuni de reţea create; •Detalii despre protocoale de comunicaţii folosite de malware;

	•Interogări DNS; •URL-uri accesate; •Adrese IP contactate şi porturile logice folosite; •Capturi de ecran efectuate pe parcursul analizei aplicaţiilor malware.
	La finalul analizei malware soluţia furnizează rezultatele într-un raport PDF şi/sau HTML, XML, JSON.
	Asigură identificarea comportamentului malware generic şi încadrarea aplicaţiilor malware într-o anumită familie (keylogger, rootkit, infostealer, etc.) în baza unor şabloane de comportament.
	Asigură definirea şi importarea de semnături personalizate în formatul YARA pentru analizarea tuturor artefactelor generate în urma unei analize sandbox.
	Asigură interacțiunea utilizatorului cu mașina virtuală de analiză pentru a detona cu succes aplicațiile malware complexe, precum și tentativele de phishing avansate. Interacțiunea cu mașina de analiză se va efectua direct din interfața web.

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea Soluției Sandbox pentru Analiza Automată a Aplicaţiilor Malware.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția Sandbox pentru analiza automata a aplicațiilor malwarese va implementa cu instalare, punere în funcțiune, configurare și testare, în locația comunicată la încheierea contractului şi va include cel puțin următoarele servicii:

- securizarea sistemului de operare și serviciilor active pentru a asigura protecția împotriva atacurilor informatice
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software
- instalarea și configurarea soluției ofertate într-un mediu de virtualizare

VMWare

- crearea arhitecturii folosite de către produsul de tip sandbox (instalarea și configurarea mașinilor virtuale de analiză)
- configurarea rețelelor de analiză în modurile sandbox (cu internet simulat) și live (acces direct către mediul Internet)
- licenţierea sistemelor de operare Microsoft Windows şi a aplicaţiilor comerciale din cadrul mașinilor virtuale de analiză

realizarea altor configurări necesare pentru integrarea soluției software livrată in reteaua de destinatie, în conformitate cu specificațiile tehnice oferite de autoritatea contractantă la momentul livrarii.

Echipamentul hardware pe care va fi instalată soluția software on-premise este asigurat de către beneficiar.

4.2. Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea,

detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Anexa 17 la caietul de sarcini

SOFTWARE ANALIZA MALWARE PENTRU DEZASAMBLARE/DEBUGGING/DECOMPILARE EXECUTABILE WINDOWS/LINUX/MAC OS X

1. Descriere generică a tehnologiei solicitate

Ofertantul va furniza o aplicație pentru dezasamblare / debugging / decompilare executabile Windows/Linux/Mac OS X.

2. Caracteristici tehnice ale soluției

Soluția oferită trebuie să îndeplinească următoarele caracteristici tehnice minimale:

2.1	Aplicaţia poate fi instalată pe sistemul de operare Microsoft Windows.

2.2	Asigură debugging pe executabile specifice sistemelor de operare Windows, Linux şi Mac OS X.
2.3	Aplicația suportă Cross-Platform Debugging: Din cadrul sistemului de operare Microsoft Windows, unde se instalează aplicația, se vor putea derula sesiuni de remote debugging pe executabile ce rulează pe sisteme de operare Linux și Mac OS X cu arhitectură pe 32 sau 64 de biți;
2.4	Permite dezasamblarea cel puțin a următoarelor tipuri de fişiere: Portable Executable (PE) (x86, x64, ARM); Common Object File Format (COFF); Mach-O pentru OS X ELF; Raw Binary; Object Module Format (OMF); Dalvik Executable (DEX); Windows CE PE (ARM, SH-3, SH-4, MIPS); EPOC (Symbian OS executable); Windows Crash Dump (DMP);
2.5	Modulul pentru dezasamblare suportă cel puţin următoarele familii de procesoare: ARM (32 bit și 64 bit); Intel x86 și x64; Intel Pentium; Intel IA-64; AMD64; Thumb2; PowerPC; MIPS; 6502; Dalvik (Android bytecode, DEX); Hewlett-Packard HP-PA; PIC24;
2.6	Permite recunoașterea funcțiilor din librăriile standard compilate cu compilatoarele GNU și Microsoft Visual Studio.
2.7	Permite generarea de pseudocode (de preferat scris in limbajul C).
2.8	Permite vizualizarea codului dezasamblat sub forma unui graf.
2.9	Permite inserarea de comentarii în dreptul instrucțiunilor de cod dezasamblate.
2.10	Permite extinderea capabilităţilor sale prin dezvoltarea de plugin-uri şi scripturi cel puțin în limbajele de programare C și Python.

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea Soluției Software Analiza Malware pentru dezasamblare/debugging/decompilare executabile windows/linux/mac os x.

4. Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora.

Anexa 18 la caietul de sarcini

SOLUȚIE DETECȚIE IOC

1. Descriere generică a tehnologiei

Soluția solicitată reprezintă un sistem appliance de tip IDS distribuit care trebuie să asigure gestionarea unui număr mare de Indicatori de Compromitere (IoC) și detecția acestor indicatori în timp real în traficul de rețea procesat la nivelul echipamentelor.

Soluția va fi compusă din 25 echipamente hardware (senzori) ce vor fi integrate în cadrul IVC și o componentă de management centralizat, instalată în cadrul CNC, care va asigura gestionarea tuturor senzorilor și va permite distribuirea în mod unitar și concomitent a unor seturi de indicatori de compromitere.

În cadrul IVC soluția va fi implementată în mod offline, traficul fiind transmis în mod TAP.

Soluția nu va necesita conexiune la mediul Internet.

Indicatorii de compromitere gestionați vor fi de tip adresă IP, domeniu web și URL.

2. Caracteristici tehnice minimale ale soluției

2.1 Descriere generală	Sistem appliance de tip IDS distribuit care generează alerte atunci când IoC-urile încărcate în acesta sunt regăsite în trafic. Sistemul trebuie să permită încarcărea și procesarea concomitentă a unui număr de minim 1.000.000 IoC, transmiterea acestora către unul sau mai mulți senzori în conformitate cu selecția utilizatorului și să asigure afișarea rezultatelor cu privire la detecția acestora în traficul procesat într-un interval de timp de maxim 5 minute; Durata de încărcare a unui număr de 1.000.000 IoC să nu depășească 2 ore; Indicatorii de compromitere gestionați vor fi de tip adresă IP, domeniu web și URL;

2.2 Componente	Soluția va fi alcătuită dintr-o componentă de management centralizat și un număr de minim 25 senzori ce se vor instala la instituții separate; Soluția trebuie să fie scalabilă, oferind posibilitatea de adăugare ulterioară de noi senzori;
2.3 Componenta de management centralizat	Trebuie să poată realiza managementul tuturor sistemelor IDS; Trebuie să permită adăugarea de noi senzori; Trebuie să ruleze pe un sistem dedicat, accesibil de la distanță și simultan de către minim 10 utilizatori; Trebuie să ofere posibilitatea de accesare atât prin intermediul interfeței web cât și prin protocolul ssh; Autentificarea se va realiza pe baza unui nume de utilizator și a unei parole; Canalul de comunicatii de la server către sistemele IDS să fie protejat (printr-un protocol de criptare cunoscut sau prin algoritm proprietar); Trebuie să realizeze centralizarea alertelor generate de sistemele IDS și să ofere posibilitatea de a le transmite către o soluție SIEM; Trebuie să ofere posibilitatea de a grupa mai multe sisteme IDS în functie de anumite criterii; Trebuie să ofere posibilitatea de vizualizare a stării de funcționare a sistemelor IDS și de a semnala cantitatea de trafic procesat de aceste sisteme; Trebuie să aibă posibilitatea de adăugare/ștergere IoC pe/de pe un sistem sau un grup de sisteme; Trebuie să aibă posibilitatea de a efectua căutări de IoC-uri pe un sistem sau un grup de sisteme; Trebuie să aibă posibilitatea de adăugare/ștergere/căutare a unor liste de IoC; Trebuie să permită auditarea activității utilizatorilor și stocarea jurnalelor pe o perioadă de 6 luni; Această componentă poate fi oferită sub formă de server fizic

2.4 Caracteristici minimale incluse ale senzorului IDS	Appliance cu minim 3 porturi ethernet de 1Gbps (un port management care să asigure conexiunea cu sistemul centralizat, 2 porturi procesare trafic); Să asigure capacitate de procesare a traficului fără pierderi de pachete pentru un flux de 2 x 1Gbps; Alertele detectate să fie transmise într-un interval de maxim 5 minute către componenta de management centralizat; Alerta generată să conțină date relevante despre traficul detectat (minim: timestamp, adresa IP sursa, adresa IP destinație, protocol, port sursa, port destinație, nume domeniu, url accesat, ioc accesat); Alerta generată să conțină informații ce permit identificarea senzorului (sursei) care a generat alerta; Să asigure optiunea „back to factory defaults”, astfel încât să fie posibilă mutarea facilă a echipamentului dintr-o rețea în alta.
2.5 Dimensiuni de gabarit IDS	rackabil 19”, maxim 2U.
2.6 Dimensiuni de gabarit a componentei de management centralizat	rackabil 19”, maxim 1U dacă se livrează un server fizic.
2.7 Accesorii	Set cabluri de alimentare; Ofertantul trebuie să asigure toate echipamentele ce vor permite integrarea senzorilor în rețelele beneficiarului pentru 2 fluxuri de 1gbps (tap, switch, kit rack, etc)
2.8 Licențe	Ofertantul va pune la dispoziție, dacă este cazul, toate licențele software necesare funcționării soluției.

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea Soluției

Detecție IOC.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip Detecție IOC se va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractuluişi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie
- configurarea soluției pentru jurnalizarea evenimentelor la nivelul soluției SIEM existente la fiecare beneficiar
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate

4.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Distribuția senzorilor hardware necesar a fi instalată

Nr. crt.	***Tip soluție***	***Nr. total buc.***	***Livrare***
	Senzor IDS	25	București (22) Sibiu (2) Constanța (1)

Anexa 19 la caietul de sarcini

SOLUȚIE DE RETENȚIE A EVENIMENTELOR DE SECURITATE

1. Descriere generică a tehnologiei

Ofertantul va furniza o soluţie de tip pachet software on-premise, care va asigura colectarea și stocarea jurnalelor și evenimentelor de securitate furnizate de toate componentele infrastructurii IT solicitate de beneficiar, administrarea și managementul centralizat al agenților de colectare precum și distribuirea jurnalelor și evenimentelor de securitate către alte soluții de analiză și monitorizare solicitate de beneficiar.

2. Caracteristici tehnice ale soluției

Soluția oferită trebuie să îndeplinească următoarele caracteristici tehnice minimale:

2.1	Soluţia furnizată trebuie să fie un produs de tip comercial dedicat managementului jurnalelor şi evenimentelor de securitate generate de componentele infrastructurii IT, având capabilităţi de colectare, administrare şi raportare.
2.2	Soluţia trebuie să colecteze într-o modalitate securizată (canal de comunicare criptat) şi centralizată jurnalele şi evenimentele raportate de diverse componente ale infrastructurii IT.
2.3	Soluţia trebuie să permită prelucrarea log-urilor şi evenimentelor de la sisteme ce nu se regăsesc într-o listă predefinită: log-uri personalizate (custom).
2.4	Soluţia trebuie să asigure mecanisme de stocare a evenimentelor şi jurnalelor într-o zonă de memorie din care acestea pot fi accesate şi prelucrate în timp real, dar şi mecanisme de arhivare a evenimentelor.
2.5	Soluţia trebuie să permită colectarea evenimentelor şi jurnalelor de securitate atât local (din locaţia în care soluţia este instalată), cât şi de pe sisteme aflate în zone geografice diferite. Colectarea poate fi realizată și prin intermediul unor componente software de tip agenţi de colectare.

2.6	Soluţia trebuie să pună la dispoziţie o interfaţă grafică pentru vizualizarea şi căutarea evenimentelor, precum şi pentru raportare.
2.7	Agenţii de colectare trebuie sa permită instalarea cel puțin pe sisteme Windows.
2.8	Printre sistemele predefinite pentru care soluţia poate colecta şi interpreta jurnale şi evenimente în mod implicit (fără a necesita configurări personalizate) trebuie să se numere minim: - Soluţii de tip anti-virus; - Echipamente de reţelistică precum routere, switch-uri; - Soluţii de tip firewall; - Soluţii de tip IDS/IPS; - Servere aplicaţii web; - Soluții DLP - Soluţii de scanare şi testare de vulnerabilităţi; - Sisteme de operare; - Servere de mesagerie electronică; - Informaţii provenite prin protocoale de tip Syslog şi NetFlow.
2.9	Soluţia trebuie sa permită implementarea la nivelul agenţilor de colectare a funcţionalităţii de filtrare a evenimentelor, configurabilă selectiv de către administrator.
2.10	Agenţii de colectare trebuie să suporte transmisia automată a fluxului de date colectate către cel puțin o destinație.
2.11	Soluția trebuie să permită executarea mai multor căutări concurente într-o singură sesiune a unui utilizator unic.
2.12	Soluţia trebuie să permită rularea de căutări cu ferestre de timp personalizabile.
2.13	Soluţia trebuie să implementeze un mecanism de căutare intuitiv care să aibă la bază o logică de tip boolean, în care operanzii să poată fi reprezentaţi de cuvinte cheie sau câmpuri de interes, iar operatorii să includă pe lângă operaţiile logice (AND, OR, NOT) şi operatori specifici prin intermediul cărora să poată fi create în mod automat reprezentări grafice ale rezultatelor.
2.14	Soluţia trebuie să permită salvarea unei interogări pentru a fi utilizată în viitor.
2.15	Soluţia trebuie să permită exportul local al rezultatelor căutărilor.
2.16	Soluţia trebuie să permită definirea de rapoarte bazate pe parametri configurabili, la nivel de conţinut.
2.17	Soluţia trebuie să permită crearea de rapoarte care să ruleze la intervale de timp predefinite (scheduled), precum şi rapoarte care să fie rulate la momentul lansării cererii.
2.18	Soluţia trebuie să permită transmiterea alertelor sau rapoartelor prin intermediul email.
2.19	Soluţia trebuie să permită reprezentarea grafică, prin intermediul panourilor de bord (dashboards), a rezultatelor interogărilor personalizate, definite de utilizator.
2.20	Soluţia trebuie să poată genera alerte în timp real care să urmărească elemente definite în baza unui filtru de căutare. Alertele trebuie să poată fi transmise ca notificări prin intermediul emailului.
2.21	Soluţia trebuie să pună la dispoziţie o interfaţă grafică intuitivă, pentru administrare şi utilizare.
2.22	Soluţia trebuie să implementeze un mecanism de autentificare al utilizatorilor care să permită:

	- Autentificarea utilizatorilor definiţi local în cadrul soluției; - Integrare cu sisteme LDAP.
2.23	Soluţia trebuie să permită definirea de grupuri de utilizatori, fiecare grup cu drepturi specifice, granulare, configurabile de către administrator.
2.24	Soluția trebuie să fie capabilă să trimită date cel puțin către o soluție de tip SIEM.
2.25	Soluţia trebuie să permită configurarea de către administrator a zonelor de stocare a datelor.
2.26	Soluţia trebuie să permită configurarea numărului maxim de zile de stocare pentru retenție.
2.27	Soluția trebuie să ofere posibilitatea de a cripta câmpurile de date în timpul colectării evenimentelor şi să ofere capacitatea de a decripta atunci cand este necesar (în rezultatele căutării sau rapoarte).
2.28	Soluţia trebuie să asigure compresia evenimentelor stocate.
2.29	Soluţia trebuie să permită administrarea centralizată a modulelor acesteia. Această funcţionalitate poate fi îndeplintă şi prin intermediul unor module (software sau hardware) adiţionale.
2.30	Administrarea centralizată a soluţiei trebuie să permită îndeplinirea cel puţin a următoarelor funcţionalităţi: - Monitorizarea componentei de stocare din punct de vedere al parametrilor de funcţionare; - Administrarea unitară a parametrilor de configurare aplicați asupra componentelor şi/sau modulelor soluţiei; - Monitorizarea în mod automat a statusului curent pentru componentele hardware ale componentei centrale.
2.31	Licența și toate componentele software ale soluției ce vor fi instalate în locația beneficiarului vor trebui să asigure o capacitate de procesare a jurnalelor de securitate de minim 120 GB/zi.
2.32	Soluţia trebuie să permită creşterea puterii de stocare şi procesare evenimente printr-o simplă licenţiere. Soluţia trebuie să ofere scalabilitate de până la 500 GB/zi.

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea Soluției

de Retenție a Evenimentelor de Securitate.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de de Retenție a Evenimentelor de Securitatese va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- realizarea altor configurări necesare pentru integrarea soluției livrate în reţeaua de destinaţie,
- integrareacu soluția SIEM de la nivelul beneficiarului,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale.

4.2. Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Anexa 20 la caietul de sarcini

KIT FORENSICS LAB

1.Descriere generală:

Kit-ul Forensics LAB va permite investigarea modului de operare (modus-operandi) al actorilor cibernetici, prin identificarea și analiza tehnicilor, tacticilor și procedurilor utilizate în desfășurarea atacului cibernetic. Reconstituirea activităților întreprinse de atacator se realizează prin metode și instrumente specifice de tip computer forensics prin care se pot extrage informații din urmele sau artefactele create la nivelul sistemelor de operare, în urma acțiunilor derulate de atacatori: exploatare, intruziune, persistență, mișcare laterală, exfiltrare de date, alte acțiuni conform obiectivelor atacatorului etc. Astfel, vor fi dezvoltate capabilitățile laboratorului de analiză forensics prin instrumente software și hardware specializate, care vor oferi funcționalități de analiză a artefactelor la nivelul unei game largi de sisteme de operare (versiuni ale sistemelor de operare Microsoft Windows, Linux, Apple MacOs).

2. Definirea componentelor:

Kit Forensics Lab		
Nr.	**Denumiri componente**	**Număr componente**
2.1.	Echipamente tip server specializate pentru investigație computer forensics	5
2.2.	Software investigație computer forensics pentru sistemele de operare Microsoft Windows	9
2.3.	Software investigație computer forensics pentru sistemele de operare Linux	8
2.4.	Soluție de investigație computer forensics pentru sistemele de operare MacOS	3
2.5.	Stații de lucru	3
2.6.	Laptop	5
2.7.	Software recuperare date șterse	4
2.8.	Software antivirus	10
2.9.	Software investigare istoric navigare Internet	4
2.10.	Dispozitive de stocare tip HDD extern	6
2.11.	Software extragere și analiză date de pe dispozitivele mobile	1

2.1 Echipamente tip server specializate pentru investigație computer forensics

Reprezintă un sistem de calcul optimizat, creat special pentru colectarea, stocarea și analizarea probelor digitale.

Caracteristici tehnice minimale:

2.1.1	Placă de bază: Număr porturi USB 3.0: minim 4 Număr porturi USB 2.0: minim 2 Procesor x 2 bucăți: Număr nuclee: minim 14 Număr threaduri: minim 28 Frecventa de baza: minim 2.00 GHz Frecventa Max Turbo/Boost: minim 3.20 GHz Cache: minim 19 MB Memoria RAM: Capacitate: minim 256 GB Tip: minim DDR4 Frecventa: minim 2400 MHz Memoria Video: Tip: GDDR6 Capacitate: minim 11 GB Nuclee: minim 4200 Bus memorie: minim 352 bit Capacitate de stocare: 1 bay echipat cu Solid State Drive format M.2 NVMe PCIe sau SATA, capacitate minim 1 TB pentru sistemul de operare; 2 bay echipate cu Solid State Drive, capacitate minim 1 TB per bay; 1 bay echipat cu dispozitiv de citire și scriere BluRay DVD; Minim 1 bay Hot swap pentru HDD cu interfata SATA; Spațiu de stocare cu capacitatea totală utilizabilă minim 7 TB compus din Solid State Drives în configurație RAID 5 sau RAID 10. Conectori de rețea (NIC): 1 x port RJ45, viteză minimă 1 Gigabit Ethernet
2.1.2	Are încorporat un dispozitiv de copiere care suportă achiziția de date în mod forensics (blochează operațiile de scriere pe dispozitivul sursă și asigură doar operațiile de citire) pentru următoarele tipuri de interfețe: USB 3.0, FireWire, IDE, PCIe, SAS, SATA, interfață de alimentare pentru dispozitivele conectate.
2.1.3	Se va livra împreună cu tastatură wireless (format tastatură: US English sau echivalent), mouse wireless și monitor tip LED, cu diagonala minim 27” inch.
2.1.4	Furnizorul va pune la dispozitie un mediu de stocare (DVD sau Bluray sau Stick USB) cu imaginea sistemului de operare și alte configurări, drivere necesare pentru instalarea echipamentului.
2.1.5	Conține cabluri de alimentare la priză la 220Vac, cu ștecher tip schuko sau adaptor.
2.1.6	Sistem de operare cu licență, preinstalat: Windows 10 Professional, 64-bit.
2.1.7	Furnizorul va pune la dispozitie o trusă cu: Adaptoare sau cabluri de alimentare și date necesare pentru conectarea dispozitivelor de stocare la interfețele SATA, SAS, USB 3.0, PCIE, FireWire, IDE.

	Trusă de șurubelnițe

2.2 Software investigație computer forensics pentru sistemele de operare Microsoft Windows

Aplicație software pentru procesarea și investigarea probelor digitale utilizate în procesul de computer forensics pentru sistemele de operare Microsoft Windows.

Caracteristici tehnice minimale:

2.2.1	Soluția trebuie să ruleze pe sistemul de operare Windows 10.
2.2.2	Soluția trebuie să realizeze operațiile de colectare, importare și investigare a probelor digitale (imagini forensics, fișiere, etc.)
2.2.3	Soluția trebuie să dispună de o interfață grafică.
2.2.4	Pentru a reduce timpul de procesare al datelor, soluția utilizează mai multe threaduri separate pentru execuție.
2.2.5	Soluția trebuie să asigure crearea de cazuri separate pentru fiecare investigație, precum și crearea de utilizatori care pot investiga aceste cazuri.
2.2.6	Soluția trebuie să țină evidența cazurilor într-o bază de date.
2.2.7	Soluția trebuie să includă funcționalități de management al cazurilor, având posibilitatea de a salva un caz și a deschide un caz închis anterior.
2.2.8	Soluția trebuie să ofere utilizatorului posibilitatea de particularizare a procesului de investigare asupra anumitor operațiuni de procesare a datelor (Data Carving, Hashing, Indexare, etc.).
2.2.9	Soluția trebuie să asigure investigarea a cel puțin două tipuri de date: date statice (colectate anterior analizei) și date live (colectate de pe un sistem informatic pornit în momentul analizei).
2.2.10	Soluția trebuie să suporte analiza următoarelor formate ale imaginilor forensics: AFF, E01, DMG, AD1, L01, Lx01, Raw DD, ISO, Microsoft VHD, VMDK (VmWare).
2.2.11	Permite următoarele operațiuni asupra imaginilor forensics: - verificarea integrității unei imagini forensics; - montarea imaginilor probelor forensics ca discuri locale.
2.2.12	Identifică și analizează următoarele sisteme de fișiere: FAT 12, FAT 16, FAT32, Ext2, Ext3, Ext4, NTFS, HFS, HFS+, precum și suport pentru Apple File System (APFS).
2.2.13	Soluția recunoaște următoarele formate de diskuri criptate: BitLocker, FileVault2.
2.2.14	Soluția trebuie să ofere un set predefinit de filtre precum și opțiunea ca utilizatorul să își creeze un filtru personalizat. Permite operațiuni avansate de filtrare a datelor procesate.
2.2.15	Soluția dispune de interfață grafică pentru organizarea datelor pe diferite categorii. Interfața conține ferestre/taburi corespunzatoare unor categorii distincte: Imagini, Video, Sistemul de fisiere, vizualizare Text si Hex.
2.2.16	Soluția filtrează în mod automat fișierele în funcție de extensie, tipul fișierelor (fișiere șterse, recuperate/carved, etc.), semnături (imagini, email, etc.)
2.2.17	Soluția trebuie să dispună de un modul de analiză email pentru fișierele Microsoft Outlook *.pst. Soluția trebuie să asigure vizualizarea mesajelor individuale (destinatari, expeditori, conținut) și să asigure efectuarea de căutari în conținutul

	mesajelor.
2.2.18	Soluția permite căutari pe bază de expresii regulate sub forma de cuvinte cheie în datele analizate. Investigatorul poate importa o listă de cuvinte cheie într-un format specific soluției pentru efectuarea de căutari.
2.2.19	Permite căutarea pe bază de index (crează un index al stringurilor identificate în datele procesate pentru a asigura utilizatorului o modalitate de a căuta rapid cuvinte cheie), având un modul integrat de tip dtsearch sau similar.
2.2.20	Soluția poate identifica fișierele duplicate.
2.2.21	Permite analiza pe baza entropiei pentru a detecta fișierele arhivate sau criptate.
2.2.22	Permite dezarhivarea fisierelor compuse de tip container pentru alte fișiere sau date (arhive, fisiere OLE, Microsoft Office, etc.)
2.2.23	Permite indexarea datelor importate precum și aplicarea algoritmilor de tip hash (MD5, SHA-1, SHA-256) asupra fișierelor indexate. Deţine o bază de date cu fişierele cunoscute ce poate fi utilizată ca filtru de eliminare a fişierelor în procesul de investigare.
2.2.24	Din interfața grafică soluția trebuie să permită atât exportarea fișierelor în formatul nativ cât și exportarea informațiilor despre fișiere în format CSV.
2.2.25	Permite sortarea datelor și a fișierelor în funcție de metadate (denumire, metadate temporale, dimensiune, etc.)
2.2.26	Solutia conține un modul specializat care identifică imagini aparținând aceleași categorii (pornografie, arme, droguri, etc.). Identificarea este realizată prin folosirea unei baze de date cu semnături.
2.2.27	Soluția trebuie să permită etichetarea unui grup de fișiere, oferind astfel o metodă de organizare a datelor. Utilizatorul poate crea mai multe etichete personalizate.
2.2.28	Soluția trebuie să dețină capabilităţi de recuperare a datelor (data carving) din zona nealocată.
2.2.29	Soluția trebuie să permită exportarea metadatelor despre geolocație în format KML.
2.2.30	Soluția are un modul integrat pentru a detecta eventuale fișiere suspecte prin examinarea sau scanarea acestora după elemente malware cunoscute.
2.2.31	Soluția trebuie să includă facilități de vizualizare a continutului fișierelor fără instalarea de programe software adiționale.
2.2.32	Poate analiza artefacte asociate browserelor web: Chrome, Mozilla Firefox, Internet Explorer, Safari.
2.2.33	Permite analiza containerelor Volume Shadow Copies specifice Windows.
2.2.34	Soluția permite crearea unui raport cu informațiile relevante dintr-un caz. În conținutul raportului soluția trebuie să adauge și denumirile fișierelor etichetate de utilizator în timpul investigației. Raportul poate fi exportat cel puțin în format PDF.
2.2.35	Permite analiza artefactelor asociate aplicațiilor de tip social media: Skype, Viber, WeChat.
2.2.36	Soluția permite investigatorului să ruleze scripturi asupra datelor analizate.
2.2.37	Soluția ofertată trebuie să asigure funcționalitatea de a accesa și importa datele existente la sediul beneficiarului, rezultate în urma prelucrării cu aplicația software Forensic Toolkit produsă de Access Data.

2.3.Software investigație computer forensics pentru sistemele de operare Linux

Soluţie de tip software pentru efectuarea investigaţiilor de tip computer forensics pentru sistemele de operare Linux având funcționalități de a extrage, procesa și analiza datele digitale.

Caracteristici tehnice minimale:

2.3.1.	Asigură realizarea operațiilor de colectare, importare și investigare a probelor digitale.
2.3.2.	Asigură adăugarea mai multor imagini forensics în format E01 într-un singur caz.
2.3.3	Este oferită ultima versiune stabilă a producătorului.
2.3.4	Poate procesa date extrase de pe dispozitive mobile precum Android, iOS, Kindle Fire, HDD-uri, SSD-uri şi carduri SD.
2.3.5.	Poate extrage şi procesa date forensics localizate în cloud, asociate platformelor social media.
2.3.6	Utilizatorul poate configura procesul de investigare al datelor dintr-un caz prin selectarea sau deselectarea anumitor opțiuni de investigare.
2.3.7	Poate procesa următoarele formate ale imaginilor forensics: E01, Ex01, L01, Lx01, RAW.dd, .dmg, .vhd, VMDK, .ufd.
2.3.8	Asigură extragerea și analiza conținutului arhivelor 7zip,.zip, .rar
2.3.9	Exportă rapoarte în formate diferite precum XML, HTML, PDF.
2.3.10	Încearcă diverse metode de obţinere a permisiunilor de root pe dispozitivele Android şi raportează succesul sau insuccesul acestei operaţiuni.
2.3.11	Asigură încărcarea probelor (fișiere și directoare) specifice atât sistemelor de operare Linux cât și OS X.
2.3.12	Realizează procesarea datelor prin intermediul unei baze de date indexate care permite operații rapide de căutare.
2.3.13	Asigură filtrarea datelor analizate utilizând cuvinte cheie sau expresii regulate.
2.3.14	Efectuează căutări după cuvinte cheie sau expresii regulate inclusiv în spațiul nealocat.
2.3.15	Aplică algoritmi de tip hash (MD5 sau SHA-1) asupra fișierelor examinate. Poate compara valorile calculate prin aplicarea funcțiilor de hashing asupra fișierelor analizate cu un set de valori cunoscute asociate unor fișiere de încredere.
2.3.16	Asigură identificarea tipurilor de artefacte forensics, soluția având un set predefinit de filtre precum și opțiunea ca utilizatorul să își creeze un filtru personalizat.
2.3.17	Asigură segmentarea imaginilor forensics în părți de dimensiuni mai mici la momentul achiziției.
2.3.18	Poate calcula rezultatele aplicării funcțiilor hash MD5 și SHA-1 pentru întreaga imagine forensics, pe care le include într-un fișier text.
2.3.19	Permite compresia imaginilor în format E01 în momentul achiziției.
2.3.20	Poate identifica fișierele duplicate.
2.3.21	Dispune de o interfață grafică intuitivă.
2.3.22	Generează un grafic în funcție de timp în care este reprezentat numărul de

	artefacte generate la anumite moment de timp.
2.3.23	Are capacitatea de a previzualiza fișiere în formatul lor standard într-o fereastră integrată în interfața grafică până la exportarea acestora.
2.3.24	Permite vizualizarea în format hexadecimal a fișierelor.
2.3.25	Asigură previzualizarea bazelor de date în format SQLite, în mod implicit, într-o fereastră din interfața grafică.
2.3.26	Permite unui utilizator să eticheteze un grup de fișiere, oferind astfel o metodă de organizare a datelor.
2.3.27	Permite vizualizarea spațiului de memorie nealocat de pe sistemul analizat.
2.3.28	Detectează dacă dispozitivul analizat este criptat, iar în cazul în care dispune de parola de criptare poate decripta conținutul. Încearcă diverse parole cunoscute pentru a încerca decriptarea datelor.
2.3.29	Asigură analiza sistemelor de fișiere ext2, ext3, ext4, HFS+, FAT32, exFAT.
2.3.30	Extrage artefacte și configurări generate la conectarea sistemului de calcul într-o rețea.
2.3.31	Asigură vizualizarea artefactelor generate într-un interval de timp ales de investigator.
2.3.32	Pe lângă exportarea artefactelor, asigură și exportarea metadatelor asociate acestora.
2.3.33	Extrage artefacte generate de navigarea utilizatorilor pe Internet.
2.3.34	Permite exportarea artefactelor.
2.3.35	Recuperează fișiere din memoria nealocată.
2.3.36	În urma analizei poate extrage informații despre sistemul de operare
2.3.37	Asigură un management al cazurilor (exportare, mutare, importare).

2.4 Soluție de investigație computer forensics pentru sistemele de operare MacOS

Soluţia de tip software investigaţii computer forensics pentru MacOS reprezintă o soluţie formată din:

- 3 x licență aplicație software specializată în procesarea și analiza datelor de pe sisteme de calcul ce rulează un sistem de operare MacOS;
- 3 x dispozitiv mobil de calcul tip laptop;
- 3 x soluție hardware și software pentru realizarea imaginilor de tip forensic: dispozitiv extern tip SSD și aplicația software integrată, utilizată pentru procesul de colectare, extragere și triaj al datelor digitale de pe sistemele de operare MacOS.

Caracteristici tehnice minimale:

2.4.1 Aplicație software specializată în procesarea și analiza datele de pe sisteme de calcul ce rulează un sistem de operare MacOS.

2.4.1.1	Este compatibilă cu sistemele de operare macOS 10.13 sau mai noi.
2.4.1.2	Asigură realizarea operațiilor de importare și investigare a probelor digitale.
2.4.1.3	Este oferită ultima versiune stabilă a producătorului.
2.4.1.4	Asigură procesarea datelor extrase de pe dispozitive ce rulează sistemul de

	operare iOS (iPhone și iPad, iPod).
2.4.1.5	Dispune de interfață grafică.
2.4.1.6	Asigură managementul cazurilor, prin operațiuni de salvare a unui caz precum și restaurarea ulterioară.
2.4.1.7	Datele investigate pot fi de două tipuri: statice (colectate anterior, precum imaginile forensics RAW, E01) și live (colectate în momentul analizei, precum volume sau partiții montate, directoare).
2.4.1.8	Asigură procesarea cel puțin a următoarelor formate ale imaginilor forensics: E01, L01, EX01, Linux DD, DMG.
2.4.1.9	Identifică și analizează cel puțin următoarele sisteme de fișiere: FAT, NTFS, HFS+, APFS(Apple File System).
2.4.1.10	Asigură montarea și decriptarea datelor criptate folosind FileVault.
2.4.1.11	Utilizatorul poate configura procesul de investigare al datelor dintr-un caz prin selectarea sau deselectarea anumitor opțiuni de investigare.
2.4.1.12	Suportă parsarea fișierelor de înregistrare de tipul FileSystem events(.fseventsd).
2.4.1.13	Asigură operațiuni avansate de filtrare a datelor procesate, soluția având un set predefinit de filtre precum și opțiunea ca utilizatorul să își creeze un filtru personalizat.
2.4.1.14	Deţine o bază de date cu fişierele cunoscute ce poate fi utilizată ca filtru de eliminare a fişierelor în procesul de investigare.
2.4.1.15	Soluția asigură filtrarea fișierelor în funcție de extensie sau categorie (ex: documente)
2.4.1.16	Identifică fișiere grafice sau video de pe sistemele de operare macOSX.
2.4.1.17	Identifică fișiere audio de pe sistemele de operare macOSX.
2.4.1.18	Are capacitatea de a extrage fișierele noi sau fișierele ce au suferit modificări între un back-up al sistemului de fișiere și conținutul său actual la momentul realizării imaginii forensics (SnapShot pentru APFS).
2.4.1.19	Identifică şi analizează artefactele referitoare la conexiunile Wi-Fi.
2.4.1.20	Asigură indexarea datelor importate precum și aplicarea algoritmilor de tip hash (ex: MD5, SHA-1) asupra fișierelor indexate.
2.4.1.21	Căutarea permite utilizarea de expresii regulate și importarea unei liste de termeni.Oferă facilități de căutare pe bază de cuvinte cheie.
2.4.1.22	Din interfața grafică utilizatorul poate exporta rapoarte de analiză cel puțin în următoarele formate .pdf, .html, .csv.
2.4.1.23	Dispune de o funcție prin care un utilizator să eticheteze un grup de fișiere, oferind astfel o metodă de organizare a datelor.
2.4.1.24	Deține capabilităţi de recuperare a datelor și fișierelor (file/data carving), inclusiv din spațiul nealocat.
2.4.1.25	Asigură extragerea și analiza conținutul fișierelor de tip arhivă de pe sistemele de operare macOSX.
2.4.1.2	Include facilități de vizualizare internă a documentelor fără a avea instalate

6	programele software aferente tipurilor respective de fișiere.
2.4.1.27	Extrage și asigură vizualizarea mail-urilor de pe sistemul analizat.
2.4.1.28	Extrage artefacte generate de cel puțin următoarele tipuri de browsere web: Chrome, Firefox, Safari.
2.4.1.29	Analizează copiile de siguranță ale sistemului de operare macOS generate de Time Machine.
2.4.1.30	Asigură analiza memoriei volatile (RAM).
2.4.1.31	Soluția asigură exportarea fișierelor în formatul lor nativ.

2.4.2 Dispozitiv mobil de calcul tip laptop

2.4.2.1	Sistem de calcul mobil (tip laptop) destinat pentru achiziţia şi recuperarea probelor digitale.
2.4.2.2	Procesor: Intel Core i9 generaţia 9 sau echivalent Frecvenţa minim: 2.3 GHz
2.4.2.3	Video: Placă video AMD Radeon Pro 5500M sau echivalent Memorie: minim 4 GB
2.4.2.4	Display: Display Retina sau echivalent Diagonală: minim 16 inch
2.4.2.5	Memorie RAM: - capacitate: minim 32 GB - tip memorie: versiunea minimă DDR4 - frecvență: minim 2600 MHz
2.4.2.6	Stocare: - tip: SSD - capacitate minim 2 TB
2.4.2.7	Multimedia: - camera WEB: DA - difuzoare sunet integrate: DA, minim 2 - microfon integrat: DA
2.4.2.8	Porturi: - Thunderbolt v3: minim 4 porturi
2.4.2.9	Conectivitate: - Bluetooth: minim versiunea 5.0 - Wireless: IEEE 802.11ac Wi-Fi, compatibil cu IEEE 802.11a/b/g/n
2.4.2.10	Baterie: - tip: litiu-polimer - capacitate: minim 82 Wh
2.4.2.11	Adaptoare: - adaptor Thunderbolt 3 la USB 3.0

	- adaptor Thunderbolt 3 la HDMI - adaptor Thunderbolt 3 la Gigabit Ethernet Funcționalitățile pot fi comasate și într-un singur adaptor.
2.4.2.12	Cabluri: - cablu Thunderbolt 3 la Thunderbolt 3 de minim 0.5m lungime
2.4.2.13	Alte caracteristici: - format tastatură: US English sau echivalent; - culoare laptop: Space Gray sau echivalent; - sistem de operare inclus: macOS versiunea Mojave 10.14 sau mai nouă; - adaptor de alimentare și cablu de încărcare USB-C; - trackpad force touch sau echivalent; - touch ID sau echivalent; - touch bar; - Pachet software licențiat, compatibil cu sistemul de operare, ce permite operațiuni de citire/scriere asupra dispozitivelor de stocare externe ce utilizează sistemul de fișiere NTFS.
2.4.2.14	Ghiozdan sau rucsac compatibil cu laptopul solicitat, de culoare neagră.
2.4.2.15	**Performanţă energetică** Produsele trebuie să respecte cele mai recente standarde ENERGY STAR în materie de performanţă energetică. Cerinţa va fi considerată îndeplinită prin prezentarea unei etichete ecologice relevante de tip I sau altor mijloace doveditoare adecvate (ex: dosar tehnic al producătorului sau un raport de încercare din partea unui organism recunoscut care să demonstreze respectarea cerinţelor).
2.4.2.16	**Folosirea substanţelor periculoase** În cazul în care produsul ofertat conţine substanţe înscrise pe lista REACH a substanţelor cu o concentraţie mai mare de 0,1% (procent de masă) în întregul produs şi/sau subansamblurile produsului, se va prezenta o declaraţie care să indice substanţele specifice prezente.
2.4.2.17	**Gestiunea scoaterii din uz: reciclarea părţilor componente şi marcarea carcaselor, a suporturilor şi a ramelor din plastic** Se vor prezenta documente sau declarații din care să reiasă greutatea, compoziţia polimetrică, precum şi marcajele ISO 11469 şi ISO 1043 ale părţilor din plastic cu greutatea mai mare de 100 grame şi suprafaţa mai mare de 50 cm^2.

2.4.3 Soluție hardware și software pentru realizarea imaginilor de tip forensic

2.4.3.1	Este stocată pe un suport de memorie tip SSD cu o capacitate de minim 512 GB.
2.4.3.2	Dispune de propriul sistem de operare instalat pe suportul de memorie.
2.4.3.3	Generează valori hash folosind algoritmii Message Digest 5, Secure Hash Algorithm 1, Secure Hash Algorithm 256.
2.4.3.4	Are interfață grafică.
2.4.3.5	Este compatibilă cu sistemele de operare macOS 10.13(High Sierra) sau mai noi.
2.4.3.6	Permite realizarea imaginii forensic prin conectarea suportului de memorie la

	sistemul analizat.
2.4.3.7	Poate realizarea imaginea forensic prin intermediul metodei Target Disk Mode.
2.4.3.8	Suportă actualizări ale software-ului.
2.4.3.9	Asigură afișarea fusului orar pentru amprenta de timp a raportului de clonare.
2.4.3.10	Asigură colectarea selectivă a anumitor fișiere și directoare din sistemul suspect pentru triajul rapid al datelor.
2.4.3.11	În pasul de selecție pentru extragerea fișierelor, programul asigură clasificarea acestora pe categorii de artefacte.
2.4.3.12	Asigură posibilitatea de a utiliza un disk extern ca destinație a datelor extrase.
2.4.3.13	Datele extrase pot fi salvate fie într-un director sau într-un logical container.
2.4.3.14	Poate extrage memoria volatilă (RAM) de pe un sistem.
2.4.3.15	Realizează imagini forensics în format Raw, DMG, E01.
2.4.3.16	Asigură realizarea unei imagini forensics în mai multe segmente cu dimensiuni definite de utilizator.
2.4.3.17	La terminarea procesului de clonare, este creat un fișier de jurnalizare cu informații despre desfășurarea procesului.
2.4.3.18	Aplicatia detectează volumele criptate cu tehnologia FileVault. Aplicația asigură decriptarea datelor criptate cu FileVault dacă se furnizează credențialele folosite la criptare.
2.4.3.19	Semnalizează în interfața grafică ce partiții ale sistemului sunt criptate.
2.4.3.20	Asigura detecția si clonarea volumelor de tip Fusion Drive (volum logic format din mai multe hard diskuri fizice).
2.4.3.21	Identifică containerele de tip APFS.
2.4.3.22	Asigură clonarea containerelor de tip APFS.
2.4.3.23	Asigură clonarea containere de tip APFS Fusion.
2.4.3.24	Asigură clonarea volumelor de tip CoreStorage.
2.4.3.25	Asigură clonarea sistemelor informatice cu cipuri de securitate T2 și decriptarea datelor (dacă sunt furnizate credențialele necesare).
2.4.3.26	Dispune de opțiunea de montare în modul read-only sau read-write a diskurilor prezente pe sistemului informatic analizat.
2.4.3.27	Opțiune pentru formatarea diskurilor sistemului informatic analizat.
2.4.3.28	Asigură calcularea unei valori hash (MD5/SHA-1/SHA-256) pentru imaginile (E01, RAW, DMG) rezultate în urma procesului de clonare.

2.5 Stații de lucru

Caracteristici tehnice minimale:

	Caracteristică	**Cerință**
2.5.1	Procesor	Intel Core i7-8700, AMD Ryzen 3600 sau echivalent Frecvență: minim 3.2 GHz Număr core-uri minim: 6 Număr thread-uri minim: 12 Cache minim: 12 MB
2.5.2	Placă de bază	Soclu: compatibil cu procesorul Chipset: Intel B360/AMD B450 sau echivalent LAN: Inclus pe placa de baza, suporta 10/100/1000 Mbps Dual Bios sau echivalent

		SATA: minim 4 porturi
2.5.3.	Placa video	Chipset: AMD Radeon RX 560 sau echivalent Memorie: minim 4 Gb GDDR5 Interfață: PCIeX 16 Frecvență nucleu: minim 1200 MHz Interfață memorie: minim 128 bit Viteză memorie (Memory speed): minim 7 Gbps Cooler: activ Display Port: Da HDMI: Da Sa suporte vizualizarea simultană pe minim doua monitoare
2.5.4.	Memorie	DDR4: minim 32GB, Dual Channel Kit Frecvență: minim 2400 Mhz; Radiator: Da
2.5.5.	Hard Disk	Capacitate minim 2 TB 7200 rpm SATA III Buffer: 256 MB
2.5.6.	SSD	Capacitate minim 500 GB Suport NVMe: Da Interfata: M.2
2.5.7.	Unitate optica	CD/DVD-RW
2.5.8.	Placă de retea suplimentară	Interfață PCI-E, 1 x RJ-45 10/100/1000.
2.5.9.	Sursa	Minim 600 W PFC activ; Eficiență : minim 85%; Protecții, minim: SCP, OCP, OVP
2.5.10.	Standard I/O Ports, minim	1 x USB 3.1 2 x USB 3.x 2 x USB 2.0 1 x USB Type-C 1 x RJ-45 10/100/1000 1 x ieșire audio 1 x intrare audio 1 x DVI 1 x HDMI
2.5.11.	Tastatura	Interfață: USB Taste numerice: Da Format tastatură: US English sau echivalent
2.5.12.	Mouse	Interfață: USB Tehnologie: laser Rotita scroll: Da
2.5.13.	Căști	Cablu: minim 1.2m Conectivitate: 3.5mm jack Tip: over-head Microfon: nu/detașabil Active noise cancelling

2.5.14.	Monitor	Bucăți: 2 Tip: LED Diagonală: min 23.6 inch Wide; Rezoluție: 1920x1080; Posibilitate montare VESA: 100 x 100 mm Interfețe video minim: HDMI, DisplayPort; Cabluri: HDMI, DisplayPort, Alimentare
2.5.15.	Suport VESA pentru 2 monitoare	Tip: reglabil Compatibilitate: 100 x 100 mm Înălțime reglabilă Rotire: 360 grade; se poate învârti liber până la 90 grade Accesorii montare incluse
2.5.16.	Sistem de operare	Va fi instalat și licențiat sistemul de operare Microsoft Windows 10 Professional, 64 bit.
2.5.17.	Accesorii	Set cabluri de alimentare
2.5.18.	Performanţă energetică	Produsele trebuie să respecte cele mai recente standarde ENERGY STAR în materie de performanţă energetică. Cerinţa va fi considerată îndeplinită prin prezentarea unei etichete ecologice relevante de tip I sau altor mijloace doveditoare adecvate (ex: dosar tehnic al producătorului sau un raport de încercare din partea unui organism recunoscut care să demonstreze respectarea cerinţelor).
2.5.19.	Folosirea substanţelor periculoase	În cazul în care produsul ofertat conţine substanţe înscrise pe lista REACH a substanţelor cu o concentraţie mai mare de 0,1% (procent de masă) în întregul produs şi/sau subansamblurile produsului, se va prezenta o declaraţie care să indice substanţele specifice prezente.
2.5.20.	Gestiunea scoaterii din uz: reciclarea părţilor componente şi marcarea carcaselor, a suporturilor şi a ramelor din plastic	Se vor prezenta documente sau declarații din care să reiasă greutatea, compoziţia polimetrică, precum şi marcajele ISO 11469 şi ISO 1043 ale părţilor din plastic cu greutatea mai mare de 100 grame şi suprafaţa mai mare de 50 cm^2.

2.6 Laptop

Echipament hardware de tip laptop folosit în domeniul computer forensics pentru clonarea/copierea dispozitivelor de stocare în formate de tip forensics. Soluția este compusă dintr-un dispozitiv hardware și accesorii (cabluri, adaptoare, module hardware adiționale).

Caracteristici tehnice minimale:

2.6.1	Descriere	Este un sistem special construit şi destinat utilizării în activităţi de tip FORENSIC. Conţine un sistem de calcul mobil (laptop) destinat pentru achiziţia şi recuperarea probelor digitale.
2.6.2	Procesor	-număr nuclee: minim 8 -frecvență de bază: minim 3.5 GHz -frecvență Turbo: minim 4.8 GHz -memorie Cache: minim 12 MB
2.6.3	Display	-diagonală: minim 15 inch, maxim 16 inch
2.6.4	Memorie RAM	-capacitate: 64 GB sau mai mare -tip memorie: minim DDR4 -frecvență: 2400 MHz sau mai mare
2.6.5	Stocare	Minim 4 slot-uri pentru SSD, dintre care minim 2 pe interfață M.2 Cele 2 sloturi M.2 sunt echipate cu: - slot 1: SSD capacitate minim 1 TB - slot 2: SSD capacitate minim 2 TB
2.6.6	Funcționalități	-cititor de carduri integrat (SDHC/SDXC/SD/Mini-SD/MMC/RSMMC): DA - format tastatură US English sau echivalent, complet iluminată color și pad numeric integrate: DA - tastatură și mouse cu interfață USB/WiFi suplimentare (format tastatură: US English sau echivalent) -Touch Pad: DA - Porturi Audio: DA
2.6.7	Porturi	-USB 3.0: minim 3 -USB 3.1: minim 1 -Thunderbolt 3: minim 1 -HDMI sau Display Port: minim 1 -Mini DisplayPort 1.3: minim 2
2.6.8	Conectivitate	- port LAN 10/100/1000 Mbps -Bluetooth integrat -Wireless integrat
2.6.9	Baterie	-tip: smart lithium-ion
2.6.10	Alte caracteristici	-sistem de operare inclus: Microsoft Windows 10 Professional, 64-biți -alimentator cu ștecher tip F (Schuko) inclus -geantă de transport capitonată, rezistentă la şocuri şi intemperii, adecvată laptopului
2.6.11	Sisteme de siguranță	-cititor de amprentă integrat

2.6.12	Garanție	Minim 36 luni
2.6.13	Performanţă energetică	Produsele trebuie să respecte cele mai recente standarde ENERGY STAR în materie de performanţă energetică. Cerinţa va fi considerată îndeplinită prin prezentarea unei etichete ecologice relevante de tip I sau altor mijloace doveditoare adecvate (ex: dosar tehnic al producătorului sau un raport de încercare din partea unui organism recunoscut care să demonstreze respectarea cerinţelor).
2.6.14	Folosirea substanţelor periculoase	În cazul în care produsul ofertat conţine substanţe înscrise pe lista REACH a substanţelor cu o concentraţie mai mare de 0,1% (procent de masă) în întregul produs şi/sau subansamblurile produsului, se va prezenta o declaraţie care să indice substanţele specifice prezente.
2.6.15	Gestiunea scoaterii din uz: reciclarea părţilor componente şi marcarea carcaselor, a suporturilor şi a ramelor din plastic	Se vor prezenta documente sau declarații din care să reiasă greutatea, compoziţia polimetrică, precum şi marcajele ISO 11469 şi ISO 1043 ale părţilor din plastic cu greutatea mai mare de 100 grame şi suprafaţa mai mare de 50 cm^2.

2.7 Software recuperare date șterse

Aplicație software cu funcția de recuperare a datelor şterse sau deteriorate de pe multiple dispozitive de stocare a datelor în format digital.

Caracteristici tehnice minimale:

2.7.1	Recuperare din structura de fișiere (minim): FAT, exFAT, NTFS, HFS+.
2.7.2	Suportă: HDD ,SSD, memorii USB, carduri de memorie.
2.7.3	Recuperare documente Microsoft Office (doc, docx, ppt, pptx, odt, xlsx, xls) și fișiere pdf.
2.7.4	Recuperare fișiere audio, video, imagini (ex: avi, mp4, mov, mkv, mpg, mpeg, flv, swf, bmp, jpg, png, mp3).
2.7.5	Recuperare fișiere email (pst, msg).
2.7.6	Recuperare fișiere tip arhivă (7z, rar, tar, zip, bz2).
2.7.7	Recuperarea date de pe hard diskuri formatate.
2.7.8	Funcție de previzualizare a datelor.
2.7.9	Funcție de filtrare după fișiere șterse.

2.7.10	Detecția și recuperarea de date de pe partiții șterse.
2.7.11	Capabilitatea de funcționare pe sistemele de operare Microsoft Windows 7, 8, 10.

2.8 Software antivirus

Caracteristici tehnice minimale:

2.8.1	Posibilitate actualizare offline
2.8.2	Protecţie în timp real al datelor
2.8.3	Anti-phising/anti-spam/anti-ransomware
2.8.4	Securitate web
2.8.5	Protecție fișiere
2.8.6	Monitorizare comportamentală a aplicațiilor active în timp real
2.8.7	Protecţie cameră web
2.8.8	Firewall integrat
2.8.9	VPN (Virtual Private Network) integrat
2.8.10	Compatibil cu sistemul de operare Microsoft Windows 10
2.8.11	Scanarea și monitorizarea rețelelor wireless
2.8.12	Protecția parolelor
2.8.13	Update automat pentru aplicațiile vulnerabile
2.8.14	Data/file shredder (distrugere permanentă a fișierelor)

2.9 Software investigare istoric navigare Internet

Aplicație software cu funcția de extragere a datelor referitoare la activitatea pe Internet a utilizatorului sistemului de calcul analizat. Poate extrage informații de pe mai multe browsere WEB precum Google Chrome, Mozilla Firefox, Internet Explorer, etc.

Caracteristici tehnice minimale:

2.9.1	Extrage, analizează și generează rapoarte folosind informațiile generate de navigarea pe Internet pentru următoarele browsere WEB : Google Chrome, Mozilla Firefox, Internet Explorer 11, Edge
2.9.2	Identifică cele mai accesate siteuri sau creșterea activității utilizatorului la navigarea pe Internet.
2.9.3	Rezultatele se pot filtra după cuvinte cheie sau în intervale temporale.
2.9.4	Asigură recuperara fișierelor asociate istoricului din browserele WEB.
2.9.5	Extrage imaginile vizualizate de utilizatorul sistemului de calcul din fișierele cache ale browserului WEB.
2.9.6	Extrage paginile WEB vizualizate de utilizatorul sistemului de calcul din fișierele cache ale browserului WEB.
2.9.7	Poate extrage istoricul de căutări pe Internet ale utilizatorului de pe motoarele de căutare.
2.9.8	Permite exportarea unor rapoarte referitoare la datele descoperite după efectuarea

	investigației în format csv.
2.9.9	Asigură posibilitatea de a seta fusul orar după care sunt determinate metadatele temporale ale înregistrărilor din istoricul de navigare pe Internet.
2.9.10	Dispune de o interfață grafică intuitivă pentru vizualizarea și analizarea datelor prin care se asigură: - vizualizarea URL-urilor extrase; - opțiuni de filtrare; - data și ora când a fost vizitat un site web; -numărul de accesări pentru fiecare URL; -locația de unde au fost extrase datele (ex: fișiere cache, istoric, cookie)
2.9.11	Permite importarea manuală doar a anumitor fișiere ce se doresc analizate.

2.10 Dispozitive de stocare tip HDD extern

Caracteristici tehnice minimale:

Nr. Crt.	Caracteristici	Valori
2.10.1	Tip disc	HDD extern
2.10.2	Capacitate	Minim 4TB
2.10.3	Interfață	Minim USB 3.0
2.10.4	Format	2.5”
2.10.5	Tip produs	Portabil, alimentat prin USB, fără sursă externă de alimentare

2.11 Software extragere și analiză date de pe dispozitivele mobile

Soluţie software completă pentru investigaţii informatice pentru terminale mobile.

Caracteristici tehnice minimale:

2.11.1	Soluția asigură extragerea/ achiziţia de date informatice din telefoanele mobile (inclusiv telefoane produse de companii chinezești), cât şi din mediile de stocare de tip memory card;
2.11.2	Soluția conţine adaptor USB pentru conectarea la dispozitivele mobile;
2.11.3	Soluția conţine cabluri de date şi adaptoare specifice conectării la dispozitivele mobile;
2.11.4	Soluția asigură extragerea automată a informaţiilor despre echipament (model/ producător/ IMEI);
2.11.5	Soluția efectuează extracţii la nivel logic;
2.11.6	Soluția asigură fotografierea terminalului mobil cu o cameră video pentru adnotarea raportului cu elemente de identificare fizică ale terminalului;
2.11.7	Soluția asigură extracţia fişierelor din telefoanele mobile cu cel puţin următoarele sisteme de operare: Ios, Android, Windows mobile, Blackberry;
2.11.8	Soluția asigură extracţia fişierelor din telefoane mobile cu cel puţin următoarele

	chipset-uri: Mediatek, Qualcomm, Spreadtrum, Exynos şi Infineon;
2.11.9	Soluția asigură extracţia fizică de date (clona integrală a memoriei fizice) şi decodare a dispozitivelor mobile;
2.11.10	Soluția asigură extracţia sistemului de fişiere;
2.11.11	Soluția asigură funcția de deblocare parole/ ecran prin metode de bypass;
2.11.12	Soluția asigură copierea cartelelor SIM/ microsim/ nanosim;
2.11.13	Soluția realizează atât decodarea datelor extrase, cât şi analiza acestora prin categorisirea lor;
2.11.14	Soluția asigură sortarea şi filtrarea fişierelor în funcţie de categorie;
2.11.15	Soluția decodează şi analizează agenda telefonică, liste SMS/MMS, istoric apeluri, calendar aplicaţii instalate, istoric locaţii bazat pe GPS;
2.11.16	Soluția asigură extragerea datelor şterse;
2.11.17	Soluția colectează şi analizează date ale utilizatorilor conectaţi la reţelele de socializare, la servicii de stocare online şi la alte servicii de tip Cloud;
2.11.18	Soluția realizează automat legături şi evidenţiază relaţii între datele obţinute din diferite extracţii de pe telefoanele mobile;
2.11.19	Soluția generează rapoarte personalizate şi detaliate, prin exportarea datelor extrase cel puţin în fişiere format PDF şi DOC/DOCX;
2.11.20	Soluția va include: software de extragere a datelor din telefonul mobil; software de analiză a datelor extrase; software de extragere a datelor stocate în Cloud; software de analiză integrată a datelor provenite din surse multiple; set cabluri de conectare şi adaptoare pentru dispozitivele mobile (cu update pentru cele mai noi dispozitive); adaptor SIM/ MicroSIM/ NanoSIM; camera video/webcam USB pentru conectare la calculator cabluri Power-ON; cititor de carduri cu protecţie WRITE-Block;

3. Livrabile

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

Acolo unde există, documentația de administrare și operare.Acolo unde există, ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea

up-grade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

Acolo unde există, documentația de utilizare.Acolo unde există, ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de tip Kit Forensics Lab.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip Kit Forensics Lab se va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie.

4.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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.

Anexa 21 la caietul de sarcini

KIT INCIDENT RESPONSE

1. Descriere generală:

Kit-ul incident response este o soluție folosită la momentul intervenției în caz de incident la nivelul IVC pentru scanarea sistemelor informatice dintr-o rețea pe baza unor indicatori de compromitere cunoscuți coroborată cu o soluție de monitorizare și detecție a intruziunilor prin analiza traficului de rețea.

Activitățile desfășurate de echipele de reacție rapidă în cadrul procesului de intervenție la incidente de securitate cibernetică constau în identificarea rapidă a tuturor sistemelor infectate, izolarea acestora de restul infrastructurii IT&C, eradicarea infecției, restaurarea sistemelor și recuperarea funcționalităților afectate la starea inițială. Etapa de identificare a sistemelor infectate prezintă o importanță deosebită întrucât poate avea efecte înlănțuite în cadrul etapelor succesoare de izolare și eradicare. În situația în care nu au fost identificate corect toate sistemele compromise, atacul cibernetic nu a fost complet înlăturat. Se impune dezvoltarea capabilităților de reacție la incidente prin introducerea unei soluții specializate pentru scanarea sistemelor informatice dintr-o rețea pe baza unor indicatori de compromitere cunoscuți coroborată cu o soluție de monitorizare și detecție a intruziunilor în traficul de rețea.

Soluția de scanare a sistemelor informatice va include o bază de date compusă din indicatori de compromitere ale atacurilor cibernetice cunoscute prin care se pot detecta urme produse de atacator la nivelul sistemului de operare (la nivelul proceselor, sistemului de fișiere, regiștrilor, conturilor de utilizatori, serviciilor, autorun, conexiunilor de rețea, fișiere de jurnalizare, elemente interne ale funcționării sistemului de operare - mutexex, named pipes).

Din punct de vedere funcțional, soluția de monitorizare și detecție a intruziunilor se va compune dintr-un sistem de detecție pe bază de semnături tip IDS (Intrusion Detection System) și un sistem de detecție pe bază de comportament de tip Sandbox. Soluția va putea fi instalată în rețeaua informatică a beneficiarului și va fi capabilă să identifice aplicații malware avansate necunoscute, exploit-uri zeroday, atacuri WEB, spear phishing, exfiltrare de date, botnets, trojans, worms, ransomware, keyloggers, comunicații către servere de comandă și control și activități ale atacatorului ce nu pot fi identificate cu soluții de securitate standard.

2. Definirea componentelor:

Kit Incident Response		
Nr.	**Denumiri componente**	**Număr componente**
2.1	Soluție pentru scanarea sistemelor informatice dintr-o rețea pe baza unor indicatori de compromitere cunoscuți	5
2.2	Soluție pentru răspuns rapid la incidente de securitate cibernetică	1

2.1 Soluție pentru scanarea sistemelor informatice dintr-o rețea pe baza unor indicatori de compromitere cunoscuți

Ofertantul va furniza o soluţie software on-premise, care va permite scanarea sistemelor de fișiere ale sistemelor informatice pe baza unor indicatori de compromitere cunoscuți. Totodată, va permite și scanarea zonei nealocate de pe un disk pentru identificarea unui element malware folosit și șters de atacator.

Soluția include o bază de date compusă din indicatori de compromitere asociați atacurilor cibernetice cunoscute prin care se pot detecta urme produse de atacator la nivelul sistemului de operare (la nivelul proceselor, sistemului de fișiere, regiștrilor, conturilor de utilizatori, serviciilor, autorun, conexiunilor de rețea, fișiere de jurnalizare, elemente interne ale funcționării sistemului de operare - mutex, named pipes). În plus, baza de date se poate extinde prin indicatori privați, generați de beneficiar.

Caracteristici tehnice minimale:

2.1.1	Soluția trebuie să permită scanarea cu reguli Yara a unui sistem de fișiere sau a unei partiții.
2.1.2	Soluția trebuie să fie disponibilă on-premise.
2.1.3	Soluția trebuie să ruleze în linie de comandă.
2.1.4	Soluția trebuie să permită rularea simultană a mai multor instanțe pe același workstation.
2.1.5	Soluția trebuie să ruleze pe dispozitivele care au instalate ca sistem de operare Microsoft Windows sau o distribuție Linux.
2.1.6	Soluția trebuie să suporte formatul STIX (CybOX) pentru importul de IOC-uri private.
2.1.7	Soluția trebuie să dispună de o bază de date formată din: reguli Yara hash-uri MD5/SHA1/SHA256 caracteristici privind denumirea fișierelor malware informații asociate serverelor de comandă și control
2.1.8	Regulile Yara din baza de date a soluției trebuie să conțină denumiri speciale, în funcție de tipul de malware identificat (exemplu: APT, Generic, Supicious, etc.)
2.1.9	Regulile Yara din baza de date a soluției trebuie să conțină cel puțin următoarele metadate pentru fiecare detecție:

	Autor Descriere Data de creare a regulii Yara Scor Referință către o resursă online (opțional)
2.1.10	Soluția trebuie să permită adăugarea următoarelor tipuri de IOC-uri private/confidențiale: reguli Yara hash-uri MD5/SHA1/SHA256 caracteristici privind denumirea fișierelor informații asociate serverelor de comandă și control
2.1.11	Soluția trebuie să permită scanarea fișierelor adăugate într-un director partajat. Raportul de scanare al acestor fișiere trebuie să se salveze în cel puțin unul din următoarele formate: JSON/Syslog
2.1.12	Soluția trebuie să permită scanarea sistemului de fișiere asociat unei imagini forensic montate.
2.1.13	Soluția trebuie să permită analiza Windows Eventlogs în vederea detectării anomaliilor cauzate de utilitare publice folosite în activități de tip hacking (hacktools).
2.1.14	Soluția trebuie să permită analiza bazei de date Windows Registry în vederea detectării cheilor personalizate folosite de elementele malware.
2.1.15	Soluția trebuie să permită analiza infrastructurii interne WMI.
2.1.16	Soluția trebuie să permită parsarea bazei de date AppCompatCache/ShimCache registry în vederea analizei logurilor privind execuția fișierelor malware.
2.1.17	Soluția trebuie să permită parsarea cheilor Shellbags și identificarea fișierelor accesate de utilizator.
2.1.18	Soluția trebuie să verifice detecții suspicioase în intrările de tip Job sau taskuri programabile
2.1.19	Soluția trebuie să verifice analiza fișierelor WER și să genereze o alertă în cazul în care acestea au fost generate de exploatarea unui CVE.
2.1.20	Soluția trebuie să permită scanarea directorului Prefetch în vederea identificării fișierelor malware care au rulat pe sistemul de operare.
2.1.21	Soluția trebuie să verifice integritatea celor mai comune fișiere de sistem, prin folosirea de reguli Yara
2.1.22	Soluția trebuie să permită scanarea și identificarea de posibile elemente malware în spațiul nealocat.
2.1.23	Soluția trebuie să permită scanarea fișierelor dintr-o arhivă, prin decompresia și analiza acestora în RAM.
2.1.24	Soluția trebuie să identifice posibilele fișiere de tip log create de un fișier malware.

2.1.25	Soluția trebuie să identifice utilitarele publice folosite în activități de tip hacking (ex: Mimikatz).
2.1.26	Soluția trebuie să permită salvarea rapoartelor privind evenimentele identificate în fișiere Text, HTML și Syslog.
2.1.27	Soluția trebuie să permită salvarea logurilor în format CEF, pentru a se putea integra cu o soluție SIEM.
2.1.28	Soluția trebuie să permită afișarea rezultatelor scanării în consola de comandă, folosind un cod al culorilor.
2.1.29	Producătorul soluției trebuie să dispună de o interfață web asociată utilizatorului prin care se permite descărcarea de Update-uri ale aplicației și ale semnăturilor

2.2 Soluție pentru răspuns rapid la incidente de securitate cibernetică

Soluția este constituită din două componente. Soluția este utilizată în cadrul incidentelor cibernetice pentru a monitoriza și detecta urmele atacurilor cibernetice, cu scopul de a micșora intervalul de timp de la detecție până la mitigarea acestuia.

Caracteristici tehnice minimale:

2.2.1 Componenta 1 - Sistem care se integrează în cadrul unei rețele informatice pentru a monitoriza și analiza traficul intern și extern, cu scopul de a depista urme ale unui incident cibernetic.

Sistemul este alcătuit dintr-o componentă hardware și o componentă software integrată.

	2.2.1.1 Cerințe componentă software
	Trebuie să asigure inspectarea traficului de date din cadrul unei rețele(trafic intern și extern) și monitorizarea protocoalelor de comunicație uzuale și vizibilitate la nivel de aplicație.
2)	Soluția asigură transmiterea fișierelor către o soluție de tip sandbox.
3)	Detectează comunicațiile cu serverele de comandă și control, activități de mișcare și răspândire laterală, atacuri cibernetice targetate și complexe.
4)	Detectează atacuri avansate de tip zero-day, precum și comportamentul și activitățile atacatorului în diferite faze ale unui atac cibernetic.
5)	Detectează și asigură protecția împotriva atacurilor de tip ransomware.
6)	Detectează și asigură protecția împotriva atacurilor web.
7)	Detectează și asigură protecția împotriva atacurilor pe email (ex: phishing)
8)	Detectează și asigură protecția împotriva aplicațiilor malware de tip bot, troian, worm, backdoor.
9)	Detectează atacuri pe bază de reputație (la nivel de adresă IP, fișier) și analiză heuristică.
10)	Asigură o reprezentare grafică a atacului printr-o interfață grafică accesibilă utilizatorului.
11)	Soluția trebuie să asigure integrarea cu alte soluții de securitate din portofoliul producătorului sau al altor producători.
12)	Suport pentru flux de date minim 3GBps.

	2.2.1.2 Cerințe componentă hardware:
	Dimensiune: Montare Rack 19”
2)	Greutate: Maxim 35 kg
3)	Porturi pentru management: minim 1 x 10/100/1000 BASE-T RJ 45
4)	Porturi pentru date: 5 x 10/100/1000 BASE-T RJ 45 4 x 10Gb SFP+ (cu adaptoare LC incluse)
5)	Capacitate de stocare: Minim 4 HDD de 1 TB, configurate în RAID 10 sau SSD minim 160 GB
6)	Alimentare: 240 VAC
7)	Temperatură optimă de funcționare: 10 – 35 grade Celsius
8)	Minim 2 porturi USB
9)	Echipamentele livrate vor fi noi. Nu se acceptă echipamente remanufacturate şi/sau care au în componenţă elemente care au fost folosite anterior.

2.2.2 Componenta 2 - Sistem specializat de tip sandbox, pentru detecția fișierelor malware folosind mașini virtuale pentru detonare.

Sistemul este alcătuit dintr-o componentă hardware și o componentă software integrată.

	2.2.2.1 Cerințe componentă software:
	Server specializat pentru analiză de tip sandbox.
2)	Soluția permite analiza cel puțin a următoarelor tipuri de fișiere: chm, class, dll, doc, docx, exe, jar, js, jtd, lnk, pdf, ppt, pptx, ps1, rtf, swf, vbs, vbe, xls, xlsx, xml.
3)	Soluția are capacitatea de a utiliza in cadrul analizei următoarele sisteme de operare: Windows XP, Windows 7, Windows 8/8.1, Windows 10, Windows Server 2003, 2008/2008R2, 2012/2012R2, 2016.
4)	Suportă următoarele variante de Microsoft Office: 2003, 2007, 2010, 2013, 2016.
5)	Asigură detecția pe baza de reguli YARA precum și adăugare de reguli YARA proprii.
6)	Are integrată interfată grafică web pentru management .
7)	In interfața grafică se pot vizualiza toate detecțiile referitoare la fișierele trimise spre analiză.
8)	Pentru un fișier analizat în mediu sandbox se observă și se extrage comportamentul acestuia iar rezultatele sunt puse la dispoziția utilizatorului într-un raport de analiză.
9)	Efectuează o clasificare automată a fișierelor analizate în funcție de riscul acestora.
10)	Deține o fereastră dedicată pentru a monitoriza starea de funcționalitate a componentelor.

11)	Asigură tehnici de analiză statică și dinamică asupra fișierelor detonate.
12)	La finalul analizei, investigatorul: • poate vizualiza rezultatele în interfața grafică; • poate exporta un raport de analiză în format PDF, HTML, etc.
13)	Soluția are integrat un modul de tip whitelist prin care se pot încărca fișiere legitime.
14)	Utilizatorul poate administra masinile virtuale destinate pentru analiză din interfața grafică.
15)	Soluția asigură generarea de rapoarte pe intervale de timp cu activitatea de analiză efectuată de echipament.
16)	Soluția trebuie să asigure actualizări ale componentelor software offline, fără a necesita acces la Internet.
17)	Soluția trebuie să asigure integrarea cu alte soluții de securitate din portofoliul producătorului sau al altor producători.

	2.2.2.2 Caracteristici componentă hardware
	Capacitate: minim 40.000 sample-uri pe zi
2)	Număr mașini virtuale folosite pentru detonare: minim 55
3)	Dimensiune: Montabil Rack 19”
4)	Greutate: Maxim 35 kg
5)	Porturi pentru management: minim 1 x 10/100/1000 BASE-T RJ 45
6)	Porturi pentru date: 3 x 10/100/1000 BASE-T RJ 45
7)	Capacitate de stocare: minim 4 TB
8)	Alimentare: 240 VAC, AC redundant
9)	Temperatură optimă de funcționare: 10 – 35 grade Celsius
10)	Port pentru conectare monitor și minim 2 porturi USB
11)	Echipamentele livrate vor fi noi. Nu se acceptă echipamente remanufacturate şi/sau care au în componenţă elemente care au fost folosite anterior.

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză,

necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de tip Kit Incident Response.

4. Implementare

4.1 Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip **Kit Incident Response** se va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software.

4.2 Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Anexa 22 la caietul de sarcini

SISTEM DESTINAT EVALUĂRII DE SECURITATE CIBERNETICĂ

SISTEM DESTINAT EVALUĂRII DE SECURITATE CIBERNETICĂ		
Nr.	**Denumiri componente**	**Număr bucăţi**
1.	Soluţie pentru scanarea vulnerabilităţilor aplicaţiilor web tip 1	1
2.	Soluție pentru scanarea vulnerabilităților sistemelor informatice dintr-o rețea	2
3.	Sistem portabil de calcul, cu putere mare de procesare	2
4.	Sistem informatic mobil destinat evaluărilor de securitate cibernetică	7
5.	Soluție pentru scanarea vulnerabilităților aplicațiilor web tip 2	5

1. Soluţie pentru scanarea vulnerabilităţilor aplicaţiilor web tip 1

Ofertantul va furniza o soluţie software pentru identificarea automată a vulnerabilităţilor din cadrul aplicaţiilor web, cu următoarele caracteristici tehnice minimale:

1.1	1 (una) licență de utilizator,
1.2	Să furnizeze o soluţie, ce cuprinde o platformă integrată, pentru testarea automata a securității aplicațiilor web
1.3	Asigură verificarea/validarea automată a vulnerabilităților identificate în etapale de scanare prin: - Simularea activității unui pentester real - Exploatarea vulnerabilităților într-un mod sigur și care nu afectează sistemul scanat
1.4	Dispune de capabilităţi pentru testarea cel puțin a următoarelor tehnologii: HTML5 AJAX; JavaScript; Web 2.0; Single Page Applications (SPAs).
1.5	Asigură setarea credențialelor de autentificare în vederea testării secțiunilor protejate de autentificare de tipul:

	Form-based, Client Certificate NTLM/Kerberos
1.6	Asigură detectarea a peste 2000 de variante de vulnerabilități de securitate
1.7	Asigură testarea unui numar nelimitat de site-uri web.
1.8	Asigură descoperirea site-ului web şi oferă o expunere vizuală a structurii site-ului (sitemap/sitestructure).
1.9	Asigură realizarea unei scanări manuale de tip „*crawl*”.
1.10	Asigură testarea nivelului de complexitate al parolelor din paginile web (brute force authentication tester).
1.11	Asigură identificarea și restricționarea funcției de *logout* din cadrul aplicației web supusăscanării.
1.12	Asigură excluderea unor pagini și a unor parametri în cadrul procesului de scanare.
1.13	Asigură instalarea pe cel puțin următoarele sisteme de operare: Microsoft Windows 7, 8 și 10; Microsoft Windows Server 2008 R2, 2012 și 2016.
1.14	Asigură scanarea și identificarea vulnerabilităților specifice platformei Wordpress
1.15	Asigură rularea scanărilor prin programarea acestora la un interval de timp dorit.
1.16	Asigură elaborarea de rapoarte complexe pe baza unor şabloane predefinite şi exportarea acestora în format PDF şi HTML. De asemenea, asigură definirea şi rularea unor rapoarte personalizate.
1.17	Oferă informaţii suplimentare despre vulnerabilităţile identificate, ce vor include şi metode de remediere.
1.18	Asigură integrarea cu software de Issue Tracking
1.19	Asigură definirea unor profiluri/opţiuni de scanare
1.20	Asigură identificarea automată a unei pagini de eroare custom
1.21	Asigură cel puțin următoarele tipuri de mecanisme de autentificare: CAPTCHA One Time Tokens
1.22	Asigură actualizarea informaţiilor despre vulnerabilităţi în mod automat prin interconectare în mediul Internet.
1.23	Asigură clasificarea vulnerabilităţilor identificate după severitatea acestora şi după impactul ce îl pot aduce în cadrul organizaţiei.

2. Soluție pentru scanarea vulnerabilităților sistemelor informatice dintr-o rețea

Ofertantul va furniza o soluție pentru identificarea vulnerabilităților de rețea, cu următoarele caracteristici tehnice minimale:

2.1.	Solutia trebuie să asigure scanarea sistemelor informatice dintr-o rețea și să identifice vulnerabilitățile acestora
2.2.	Soluţia trebuie să fie de tip aplicaţie software care poate fi instalată pe cel puţin următoarele sisteme de operare: - Microsoft Windows 7, Windows 8/8.1, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016

	- RedHat Enterprise Linux Server 6 și Ubuntu Linux 16
2.3	Trebuie să asigure scanarea unui număr **nelimitat** de adrese IP.
2.4	Administrarea soluţiei trebuie sa fie realizată prin intermediul unei interfețe grafice (de tip web). Accesul la interfaţa grafică (de tip web) este realizat în mod securizat, prin procolul SSL.
2.5	Trebuie să asigure urmatoarele tipuri de scanări: Port Scanning Service Discovery Scanări Tehnologii SCADA Scanări Aplicații Web Scanări Sisteme Windows
2.6	Trebuie să ofere informaţii suplimentare despre vulnerabilităţile identificate: descriere, risc, identificator specific producătorului, metode pentru remediere.
2.7	Trebuie să asigure capabilităţi de notificare prin e-mail.
2.8	Trebuie să asigure funcționalitatea de raportare ce include: - existenţa unor şabloane predefinite - posibilitatea de a crea şabloane - crearea rapoartelor in formatele html, csv, xml
2.9	Trebuie să asigure rularea unor rapoarte diferenţiale folosind informațiile rezultate în urma unor scanări diferite pentru identificarea cu ușurință a diferențelor.
2.10	Trebuie să asigure rularea unor scanări de tip discovery pentru identificarea sistemelor existente din rețea.
2.11	Trebuie să asigure identificarea vulnerabilităţilor prin scanarea activă a reţelei şi nu necesită instalarea de agenţi software locali pe sistemele scanate.
2.12	Trebuie să asigure introducerea credenţialelor pentru inspecţie amănunţită.
2.13	Trebuie să asigure actualizarea informaţiilor despre vulnerabilităţi în mod automat prin conectare la mediul Internet.
2.14	Trebuie să asigure crearea unei scanări pentru rulare imediată sau programată la un interval de timp.
2.15	Trebuie să asigure scanarea sistemelor ce dețin adrese IPv4 şi IPv6.
2.16	Trebuie să pună la dispoziție un API ce permite utilizatorului interacțiunea cu soluția fără să acceseze interfața grafică.
2.17	Trebuie sa dețină certificare în conformitate cu standardul Common Criteria de nivel minim EAL2.
2.18	Trebuie să ofere informaţii despre progresul activităţilor de scanare aflate în derulare.
2.19	Trebuie să asigure scanarea unui segment de reţea.
2.20	Trebuie să asigure controlul accesului în aplicație multi-users sau bazat pe roluri de utilizatori
2.21	Trebuie să asigure vizualizarea rezultatelor într-un dashboard interactiv
2.22	Trebuie să asigure scanarea tehnologiilor de tip baze de date
2.23	Trebuie să asigure definirea unor șabloane de scanare
2.24	Trebuie să asigure scanarea după o serie de șabloane predefinite

3. Sistem portabil de calcul, cu putere mare de procesare – 2 bucăți

3.1 Descriere generică

Stații de lucru mobile, cu putere mare de procesare.

3.2 Caracteristici tehnice minimale:

Procesor	Intel Xeon E-2276M sau echivalent
	Frecvență bază: minim 2.7Ghz
	Frecvență maximă: minim 4.6Ghz
	Număr nuclee: minim 6
	Dimensiune Cache: minim 12MB
Video	Placă video NVIDIA Quadro RTX 5000 sau echivalent
	Dimensiune memorie video: minim 16GB
	Tip memorie video: minim GDDR6
Memorie	Tip: minim DDR4
	Capacitate: minim 128 GB
	Frecvenţă: minim 2666Mhz
Hard Disk	Tip: SSD, M.2 PCIe-NVMe
	Capacitate: minim 1 TB
Comunicaţii	Placă Reţea wireless 802.11 ax
	Bluetooth versiune minima 5.0
	NFC
Porturi/Sloturi	1 Audio Jack
	1 Port Ethernet RJ45
	2 Porturi USB 3.1
	1 Port USB-C / Thunderbolt 3
	1 Cititor Smart Card
	1 Cititor carduri media
	1 Port HDMI 2.0
Display	Diagonală: minim 17.3”
	Rezoluţie: 1920x1080
	Tip ecran: IPS, Anti-Glare
Baterie	Număr celule: minim 6
	Capacitate: minim 90Wh
Altele	TouchPad
	Pointing Stick (“Joystick”, denumit și “nub”, poziționat pe tastatură)
	Fingerprint Reader
	Tastatură Backlit cu format US
Adaptor	Alimentator cu ștecher tip F (Schuko) inclus
Ghiozdan	Compatibil cu stația de lucru mobilăsolicitată, culoare neagră/închisă
Switch	Viteză: Gigabit
	Interfață de Management: DA
	Funcționalitate de Port Mirroring: DA
	Numar minim porturi: 8 porturi
	Alimentator: inclus
Performanţă energetică	Produsele trebuie să respecte cele mai recente standarde ENERGY STAR în materie de performanţă energetică. Cerinţa va fi considerată îndeplinită prin prezentarea unei etichete ecologice relevante de tip I sau altor mijloace doveditoare adecvate (ex: dosar tehnic al producătorului sau un raport de încercare din partea unui organism

	recunoscut care să demonstreze respectarea cerinţelor).
Folosirea substanţelor periculoase	În cazul în care produsul ofertat conţine substanţe înscrise pe lista REACH a substanţelor cu o concentraţie mai mare de 0,1% (procent de masă) în întregul produs şi/sau subansamblurile produsului, se va prezenta o declaraţie care să indice substanţele specifice prezente.
Gestiunea scoaterii din uz: reciclarea părţilor componente şi marcarea carcaselor, a suporturilor şi a ramelor din plastic	Se vor prezenta documente sau declarații din care să reiasă greutatea, compoziţia polimetrică, precum şi marcajele ISO 11469 şi ISO 1043 ale părţilor din plastic cu greutatea mai mare de 100 grame şi suprafaţa mai mare de 50 cm^2.

4. **Sistem informatic mobil destinat evaluărilor de securitate cibernetică – 7 bucăți**

4.1 Descriere generică

Stații de lucru mobile, utilizate pentru testarea securității cibernetice.

4.2Caracteristici tehnice minimale:

Procesor	Model: Intel i9 Generația 9 sau echivalent
	Frecvență bază: minim 2.3Ghz
	Frecvență maxima: minim 4.8Ghz
	Număr nuclee: minim 8
	Dimensiune Cache: minim 16MB
Video	Placă video NVIDIA GeForce GTX 1650 Max-Q sau echivalent
	Dimensiune memorie video: minim 4 GB
	Tip memorie video: minim GDDR5
Memorie	Tip: minim DDR4
	Frecvență: minim 2666Mhz
	Capacitate: minim 32 GB
Hard Disk	Tip: SSD, M.2 PCIe-NVMe
	Capacitate: minim 512 GB
Comunicaţii	Placă Reţea wireless 802.11ax
	Bluetooth versiune minima 5.0
Porturi/Sloturi	1 Audio Jack
	1 Port Ethernet RJ45 sau Adaptor RJ45
	Minim 1 Port USB 3.1

	1 Port USB-C / Thunderbolt 3
	1 Cititor carduri media
	1 Port HDMI 2.0
Display	Diagonală: minim 14”
	Rezoluţie: 1920x1080
	Tip ecran: IPS, Anti-Glare
Baterie	Număr celule: minim 4
	Capacitate: minim 80Wh
Altele	TouchPad
	Pointing Stick (“Joystick”, denumit și “nub”, poziționat pe tastatură)
	Fingerprint Reader
	Cititor Smart Card
	Tastatură Backlit
Adaptor	Alimentator cu ștecher tip F (Schuko) inclus
Ghiozdan	Compatibil cu stația de lucru mobilă solicitată, culoare neagră/închisă
HDD Extern	Capacitate: 2TB, minim USB 3.0
Performanţă energetică	Produsele trebuie să respecte cele mai recente standarde ENERGY STAR în materie de performanţă energetică. Cerinţa va fi considerată îndeplinită prin prezentarea unei etichete ecologice relevante de tip I sau altor mijloace doveditoare adecvate (ex: dosar tehnic al producătorului sau un raport de încercare din partea unui organism recunoscut care să demonstreze respectarea cerinţelor).
Folosirea substanţelor periculoase	În cazul în care produsul ofertat conţine substanţe înscrise pe lista REACH a substanţelor cu o concentraţie mai mare de 0,1% (procent de masă) în întregul produs şi/sau subansamblurile produsului, se va prezenta o declaraţie care să indice substanţele specifice prezente.
Gestiunea scoaterii din uz: reciclarea părţilor componente şi marcarea carcaselor, a suporturilor şi a ramelor din plastic	Se vor prezenta documente sau declarații din care să reiasă greutatea, compoziţia polimetrică, precum şi marcajele ISO 11469 şi ISO 1043 ale părţilor din plastic cu greutatea mai mare de 100 grame şi suprafaţa mai mare de 50 cm^2.

5. Soluție pentru scanarea vulnerabilităților aplicațiilor web tip 2

Ofertantul va furniza licențele pentru aplicație/utilizatori sau echivalent, cu următoarele caracterisitici tehnice minimale:

Numărul şi tipul licenţelor	
1.	5 (cinci) licențe de utilizator
Cerință principală	
1.	Să furnizeze o soluţie, ce cuprinde o platformă integrată de tip Interceptor Proxy, pentru testarea securității aplicațiilor web
Cerințe tehnice	
1.	Asigură rularea în cadrul mai multor sisteme de operare (Windows, Linux, Mac OS);
2.	Combină atât tehnici manuale cât și automate pentru testarea securității aplicațiilor web;
3.	Conține următoarele module de tip: “Proxy” pentru interceptare, ce asigură inspectarea și modificarea cererilor și răspunsurilor dintre browser și aplicația web, precum și trimiterea cererilor către modulele de tip “Intruder” și “Repeter”; “Spider/Crawler”, ce asigură identificarea link-urilor și a conținutului din cadrul aplicațiilor web; “Scanner” avansat, ce asigură identificarea automată a principalelor tipuri de vulnerabilități din cadrul aplicației web; “Intruder”, ce asigură crearea unui atac customizat automat pentru identificarea unor vulnerabilități fără restricții privind frecvența cererilor HTTP transmise; “Repeater”, ce asigură manipularea unor cereri pentru a fi retransmise; “Sequencer”, ce asigură analiza parametrilor de sesiune; “Decoder/Encoder” ce asigură convertirea datelor între tipurile Plain text, URL, Base64, ASCII Hex, Hex, Octal și Binary; “Comparer” ce asigură compararea a cel putin 2 șiruri de caractere simultan.
4.	Asigură testarea simultană și independentă a mai multor ținte (targets) fără restricție privind numărul acestora;
5.	Asigură vizualizarea și editarea atât a conținutului cât și a header-ului din cadrul cererilor și răspunsurilor HTTP.
6.	Asigură testarea și identificarea a cel puțin 50 de vulnerabilități generice (cunoscute).
7.	Asigură vizualizarea istoricului de cereri și răspunsuri interceptate de proxy în timpul sesiunii curente;
8.	Asigură vizualizarea structurii aplicației (site map) pe baza cererilor și scanărilor efectuate în cadrul sesiunii curente;
9	Asigură adăugarea de extensii/plugin-uri;
10.	Oferă posibilitatea de a salva și a restabili sesiunea de lucru cu operațiunile efectuate în cadrul testărilor de securitate pentru aplicațiile web;
11.	Generează recomandări (cel puțin generale) pentru remedierea vulnerabilităților identificate automat;
12.	Asigură generarea unui raport (cel puțin în formatele *html* și *xml*) la sfârșitul operațiunii de scanare a aplicațiilor;

6. Livrabile

Documentațiile pe care ofertantul trebuie să le livreze autorității

contractante în cadrul contractului sunt cel puţin următoarele:

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției de Sistem Destinat Evaluării de Securitate Cibernetică.

7. Implementare

7.1 Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip Sistem Destinat Evaluării de Securitate Ciberneticăse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie.

7.2 Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care

un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Anexa 23 la caietul de sarcini

SOLUȚIE PENTRU INVESTIGAȚII ÎN MEDIUL OSINT

1. Descriere generică a tehnologiei

Soluție complexă utilizată pentru obținerea de date din mediul OSINT.

2. Caracteristici tehnice minimale ale soluției

Ofertantul va furniza o soluție software complexă pentru obținerea de date din mediul OSINT care să extragă informații semnificative și relevante pentru analizele operaționale într-un interval redus de timp pe baza unor algoritmi. Aceasta trebuie să permită corelarea identității, cercului relațional, apartenenței la anumite entități private sau guvernamentale, caracteristici legate de relațiile interpersonale și eventuale trăsături de comportament și structurarea acestor date într-un mod unitar și logic.
Ofertantul trebuie să asigure o sesiune de instruire de minim 10 ore, pentru 5 persoane, ce trebuie să prezintenoțiuni specifice privind integrarea, configurarea, administrarea şi exploatarea produsului ofertat. Cursul va fi de tip "*hands-on*", cu activități practice în care cursanții utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind configurarea, administrarea şi exploatarea produsului. Cursul se va desfășura în limba română,într-o locație pusă la dispoziție de furnizor,

în municipiul București. Instructorul trebuie să fie acreditat de producătorul soluției. Pentru demonstrarea pregătirii instructorului se vor prezenta certificate/autorizări/acreditări, sau alte documente emise de către producătorul soluției, sau de organisme abilitate în acest sens. Ofertantul va asigura servicii de catering pe perioada cursului, respectiv o masă de prânz şi un coffee-break pe zi(cafea, apă, ceai, produse de patiserie şi fructe, la discreţie).
Soluția tehnică asigură agregarea de informații din surse deschise disponibile în mediul online.
Soluția tehnică va stoca local informațiile colectate (în cadrul infrastructurii informatice ce va fi livrată clientului).
Soluția tehnică va permite filtrarea datelor colectate pentru a putea înlătura datele considerate irelevante.
Soluția tehnică va crea liste de utilizatori autorizați să acceseze informațiile deținute și va restricționa pe mai multe niveluri de autorizare anumite funcții avansate.
Soluția tehnică va realiza interogarea datelor pe baza unor cuvinte și expresii cheie simple sau complexe.
Soluția va permite actualizarea periodică a modulelor componente.
Interfața grafică va fi accesibilă utilizatorilor fără abilitați tehnice avansate și va oferi o serie de elemente vizuale intuitive pentru executarea comenzilor.
Solutia va oferi suport pentru cautarea si prelucrarea datelor solicitate independent de limba în care acestea sunt scrise.
Soluția oferă căutarea simultană de termeni și expresii prin mai multe surse, atât din colecții proprii, dar și de la terți, respectiv parteneri pe baza acordurilor sau a contractării unor servicii oferite de aceștia (api-uri, resurse de date sau informaționale)
Soluția va permite culegerea constantă de date de pe pagini web definite de utilizator (web spiders) și stocarea de date pentru minim 90 de zile și colectarea de date din feed-uri multiple, alături de colectarea și structurarea de date publice din platforme de Social Media principale, de pe minimum 5000 de pagini web.
Soluția tehnică oferă interfață grafică pentru crearea unor crawleri sau mecanisme de colectare customizate pentru extragerea de date.
Soluția permite extragerea și gruparea de date referitoare la entități, inclusiv a conexiunilor directe și indirecte dintre acestea.
Soluția tehnică oferă integrarea sau reprezentarea datelor colectate în funcție de repartizarea geografică.
Soluția tehnică oferă un modul de vizualizare a legăturilor dintre entități.
Soluția oferă posibilitatea culegerii de date folosind identități virtuale sau api-uri cu acces avansat în bazele de date ale unor platforme online.
Soluția permite exportarea datelor obținute într-un format compatibil cu mai multe sisteme de operare.
Soluția tehnică oferă instrumente de analiză comportamentală și de stare de spirit a unor entități de interes pe baza de algoritmi proprietari.
Soluția tehnică oferă algoritmi de detecție pentru persoane cu influență dintr-un grup structurat.
Ofertantul va asigura necesarul complet de echipamente hardware pentru a implementa soluția în mod optim pentru client, pentru un număr de 10 stații de lucru,

redundanță pentru asigurarea funcționării în cazuri de avarie și conectică aferentă.
Cerințele hardware minime pentru stațiile de lucru ale utilizatorilor sunt: sistem de operare Microsoft Windows 10 sau mai recent, memorie 8Gb RAM, procesor Intel i5 sau echivalent, conexiune rapidă la INTERNET.
Sistemul va permite procesarea datelor din surse deschise reușind să gestioneze un flux de minim 100 Mbit/s.
Soluția tehnică va fi livrată cu echipamente de securitate care să asigure integritatea, confidențialitatea și disponibilitatea datelor obținute.
Furnizorul soluției tehnice va pune la dispoziție o bibliotecă de resurse tehnice si cunoștințe care să poată fi accesate online permanent.
Ofertantul va livra toate licențele necesare pentru utilizarea sistemului de minim 10 utilizatori.

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea Soluției pentruInvestigații în Mediul OSINT.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip pentruInvestigații în Mediul OSINTse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,

- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

4.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- Acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.

Anexa 24 la caietul de sarcini

EXTENSIE A POLIGONULUI CIBERNETIC CYBEREXPOL

1. Descrierea situației existente

Centrul Național Cyberint dispune de o infrastructură de tip *poligon cibernetic* compusă din 16 noduri de procesare licențiate VMware (32 x VMware VCloud Suite Standard).

Infrastructura aflată în producție utilizează o suită de soluții și anume: soluție *de management al mediului virtualizat* (soluție custom bazată pe vRealize Orchestrator) precum și o soluție de deployment automat (VlabManager furnizată de ByteLife) care folosesc API-ul VMware și au ca scop crearea unor sisteme virtuale ce stau la baza dezvoltării exercițiilor din sfera securității cibernetice.

2. Ofertantul va furniza o soluție de tip *HPC* a cărui structură de bază este formată din:

8 (opt) sisteme informatice de tip server (*server de tip 1*);
1 (unu) sistem informatic de tip storage;
2 (două) switch-uri de tip Ethernet;
4 (patru) sisteme informatice de tip deep learning server (*server de tip 2*);
Licențele necesare integrării cu infrastructura deja existentă.

3. Caracteristici tehnice ale soluției

3.1 Cerințe minimale generale	**3.1.1**Ofertantul trebuie să asigure interconectarea echipamentelor cu cabluri de fibră optică, cabluri UTP şi cabluri de alimentare electrică. Pentru fiecare echipament se va asigura bezel-kitul, sistemul de montare în rack, managementul pentru cabluri, precum și cabluri de alimentare conector de tipul C14-tată C13-mamă.
	3.1.2 Serverele de tip 1, switch-urile Ethernet și echipamentul de tip storage, prevăzute în prezentul caiet de sarcini trebuie să fie interoperabile cu echipamentele existente în infrastructura beneficiarului (menționate la pct. 3.1.3 și 3.1.4).
	3.1.3 Soluția de tip HPC oferită va utiliza următoarele echipamente deja existente în infrastructura beneficiarului. : 2 switch-uri FC tip Cisco MDS 9148 FC; 2 switch-uri Ethernet CISCO Catalyst 4500X;
	3.1.4 Pentru a menține active toate funcționalitățile *infrastructurii deja existente* soluția de tip Extensie a poligonului cibernetic CyberExPol va conține: Reînnoirea serviciilor de tip Basic Suport pentru licentele de tip VMware VCloud Suite Standard ale celor 16 noduri deja existente; o licență VMware Vcenter Server 6 Standard cu Basic Suport; licențierea serverelor de tip 1 cu VMware VCloud Suite Standard cu Basic Suport.

3.2 Sistem informatic de tip server(*server de tip 1*)

Cerințe tehnice minimale (se aplică pentru fiecare dintre sistemele informatice de tip server solicitate):

Tip procesor: Intel Xeon Platinum 8268 sau echivalent; Număr procesoare: 2.
Memorie RAM: minim 1 TB DDR4; minim 2933 MT/s – RDIMM.
Stocare: minim 4 x 800 GB SFF 12G SAS SSD.
Controller RAID integrat cu minim 2 GB cache, care să suporte RAID 0,1 sau 5 hardware.
Minim 2 port-uri 1 GbE-BaseT (RJ45) și 2 porturi 10 Gb SFP+, cu 4 transceivere de 10 Gbps Ethernet cu conectori de tip duplex LC incluse: 2 transceivere necesare conexiunii cu switch-urile CISCO Catalyst 4500X, prezente în infrastructura beneficiarului; 2 transceivere pentru porturile serverului.
Minim 2 porturi FC ce asigură conectarea redundantă la o viteza de minimum 8 Gbps cu storage-ul solicitat la pct. *2.3,* prin intermediul switch-urilor de tip FC menționate la pct. *2.1.3*, cu 4 transceivere de 8 Gbps cu conectori de tip LC incluse: 2 transceivere necesare conexiunii cu switch-urile FC Cisco MDS 9148, prezente în infrastructura beneficiarului; 2 transceivere pentru porturile serverului.
Interfețe management: port dedicat de management RJ-45.
Ventilatoare: minim 7 ventilatoare hot-plug redundante.
Serverul trebuie să dispună de un panou frontal cu LED-uri sau ecran LCD pentru diagnosticarea rapidă a stării de funcționare a componentelor critice.
Managementul de sistem se va efectua printr-o interfaţă grafică web care va fi accesibilă prin portul dedicat de management și va satisface cel puțin următoarele cerințe: Two-factor authentication; SSH; Virtual sau Remote Console, inclusiv cu suport HTML5; Virtual Media; Monitorizare CPU, memorie RAM, spațiu de stocare, ventilatoare, surse alimentare; Redfish API.
Serverul trebuie să fie echipat cu modul TPM 2.0.
Serverul trebuie să aibă capabilități de tip “UEFI Secure Boot”.
Alimentare: minim 2 surse de alimentare hot-plug, dimensionată corespunzător de către producătorul soluţiei pentru a susţine funcționarea serverului la încărcarea maximă.

vor fi prevăzute cabluri de alimentare de tip C13-C14 pentru alimentarea serverelui de lungime corespunzătoare, la momentul instalării.
Dimensiuni de gabarit: rackabil, 1U.
Serverul trebuie să fie compatibil cu platforma VMware vSphere 6.x. Serverul trebuie să dispună de licențiere VMware pentru fiecare procesor fizic din componența sa (2 x VMware VCloud Suite Standard). Licențele trebuie să întrunească următoarele cerințe minime: nivel de suport BASIC (suport tehnic 12h/zi, 5 zile pe săptămână); perioadă de suport de 3 ani.

3.3 Sistem informatic de tip storage

Cerințe tehnice minimale:

3.3.1 Storage-ul va fi de tip SAN și va fi compatibil din punct de vedere funcţional cu sisteme de tip switch FC (de exemplu Cisco MDS 9148, existente în infrastructura beneficiarului).
3.3.2 Soluţia trebuie să ofere posibilităţi de stocare a datelor pe suport de tip SSD cu interfata SAS. Capacitatea soluției: soluțiava utiliza minim 24 de SSD-uri cu capacitatea de 1.92 TB SAS 12Gbps; minim 46 TB spațiu de stocare brut.
3.3.3 Soluția oferă scalabilitate prin posibilitatea de adăugare a unor module adiţionale.
3.3.4 Soluţia va avea în componență un dual storage controller SAN.
3.3.5 Conectivitatea echipamentului trebuie să fie asigurată prin Fiber Channel: minim 2 port-uri FC per controller cu viteză de cel puțin 8 Gbps, cu transceiverele tip LC incluse: 4 pentru switch-urile FC Cisco MDS 9148; 4 pentru interfețele storage controller-elor.
3.3.6 Interfețe management: 1 port dedicat de management RJ-45 per storage controller; port CLI mini-USB per storage controller.
3.3.7 Managementul de sistem se va efectua printr-o interfaţă grafică web, care va fi accesibilă prin porturile dedicate de management.
3.3.8 Soluţia oferă posibilitatea de separare a discurilor în unităţi logice separate (LUN), cu urmatoarele caracateristici: capacitate minimă LUN 128TiB (140 TB); număr minim volume 512; posibilitatea de efectuare de Snapshot-uri (minim 512).
3.3.9 Soluţia suportă cel puțin următoarele configurații pentru SSD: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10.
3.3.10 Alimentare: 2 surse de alimentare hot-plug, redundante.
3.3.11 Dimensiunea de gabarit a întregului sistem: rackabil 19”, maxim 2U.

3.3.12	Sisteme de operare suportate: Microsoft Windows Server 2019; Microsoft Windows Server 2016; Microsoft Windows Server 2012; Vmware ESXi; Red Hat Linux; SuSE Linux.
3.3.13	Sistemul suportă plug-in dedicat pentru managementul integrat al storage-ului prin intermediul VCenter Server.

3.4 Switch Ethernet

Cerințe tehnice minimale (se aplică pentru fiecare dintre switch-urile solicitate):

3.4.1 Switch-ul trebuie să dispună de un număr minim de 24 porturi RJ-45 10/100/1000 Mbps și minim 4 porturi 1GbE SFP, cu modulele SFP de tip LC aferente incluse.		
3.4.2 Switch capacity de minim 88 Gbps, throughput de minim 41,66 Mpps, memorie RAM mimim 2 GB și memorie Flash minim 2 GB.		
3.4.3	Suport Layer 2	Adrese MAC suportate: minim 16.000. Număr minim de VLAN-uri suportate: 4093. MTU configurabil la minim 9198 bytes (jumbo frames). IEEE 802.1D: Spanning Tree Protocol. IEEE 802.1Q: VLAN tagging. IEEE 802.1ab: Link Layer Discovery Protocol. IEEE 802.1p: CoS prioritization. IEEE 802.1s: Multiple Spanning Tree Protocol. IEEE 802.1w: Rapid Spanning Tree Protocol. IEEE 802.1x: Port Acces Control. IEEE 802.3 10BASE-T. IEEE 802.3ab 1000BASE-T. IEEE 802.3ad: Link Aggregation Control Protocol. IEEE 802.3u 100BASE-T. IEEE 802.3z 1000BASE-X.
3.4.4	Suport Layer 3	Să suporte protocoale de rutare: static IP routing, RIP v1/v2, OSPF v3, IGMP v1/v2/v3, RIPng, PIM.
3.4.5	Alte facilități suportate	Dynamic Host Configuration Protocol (DHCP server) QoS LLDP-MED TACACS+ și RADIUS Authentification DHCP Snooping Dynamic ARP Inspection (DAI) SSH
3.4.6	Facilități management	configurare CLI, web, telnet, consolă SSH suport rollback configurație
3.4.7	Alimentare	Sursă de alimentare instalată intern cu suport pentru standardele româneşti: 230V AC la 50 Hz.
3.4.8	Dimensiuni de gabarit	Rackabil 19”, 1U. Trebuie să includă un kit de instalare în rack de 19” cu toate accesoriile necesare.
3.4.9	Accesorii	1 X cablu consolă; Set cabluri de alimentare cu conector C14-tată, set cabluri de alimentare cu conector CEE 7/7 tată; 1 X kit de instalare 19" 1U cu toate cablurile de protecţie (împământare), şuruburile, cât şi alte accesorii necesare instalării şi punerii în funcţiune incluse.

3.5 Sistem informatic de tip server(*server de tip 2*)

Cerințe tehnice minimale (se aplică pentru fiecare dintre sistemele informatice de tip server 2 solicitate):

3.5.1. Tip procesor: Intel Xeon Gold 5218-Series sau echivalent; număr procesoare: 2.
3.5.2. Sistemul trebuie să fie echipat cu minim 8 sloturi PCI-Express Gen 3, de tip x16.
3.5.3. Placă video: Nvidia RTX 2080 Ti Turbo GDDR6 sau echivalent; număr plăci video/server: 8 GPU / Server. Plăcile trebuie să fie conectate la sloturile PCI Express Gen 3, de tip x16 menționate anterior.
3.5.4. Memorie RAM: minim 256 GB DDR4 cu frecvență minimă de 2933 MHz, ECC, RDIMM.
3.5.5. Specificații spațiu de stocare: minim 8 x 512 GB SSD, SFF, care să suporte configurații RAID 0,1,5,10 (Software RAID).
3.5.6. Specificații interfață rețea: minim un port dedicat de management 1 GbE RJ-45 și 2 porturi de minim 1 GbE pentru conexiunea LAN .
3.5.7. Serverul trebuie să conțină un controller BMC, care suportă iKVM.
3.5.8. Porturi disponibile: 2 x USB 3.0; 1 x port VGA;
3.5.9. Dimensiunea de gabarit a întregului sistem: rackabil 19”, maxim 4U.
3.5.10. Alimentare: 2+1 surse redundante, dimensionată corespunzător de către producătorul soluţiei pentru a susţine funcționarea serverului la încărcarea maximă.
3.5.11. Kit de instalare în rack, cu toate cablurile de protecţie (împământare), şuruburile, cât şi alte accesorii necesare instalării şi punerii în funcţiune incluse.

4. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției Extensie a Poligonului Cibernetic Cyberexpol.

5. Implementare

5.1 Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip Extensie a Poligonului Cibernetic Cyberexpolse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare,

în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate,
- instalarea și configurarea platformei Vmware ESXi 6.7 pusă la dispoziție de ofertant la momentul livrării, pentru toate serverele,
- configurarea tuturor conexiunilor de rețea între echipamentele mentionate: servere, switch-uri și storage-uri, precum şi realizarea altor configurări necesare pentru integrarea echipamentelor livrate în reţeaua de destinaţie, în conformitate cu specificațiile tehnice oferite de autoritatea contractantă la momentul livrării.

5.2 Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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.

Anexa 25 la caietul de sarcini

ECHIPAMENTE DE TIP SERVER

1. Caracteristici tehnice minimale:

Soluția oferită va conține 12 echipamente de tip server, identic configurate, care vor îndeplini următoarele cerințe minime obligatorii:

Cerință funcțională	
1.1	Șasiu: Maxim 2U Rackmount.
1.2	Platforma: Suport pentru minim două procesoare.
1.3	Procesor: 2 procesoare Intel Xeon Gold 2nd Generation, minim 20 core, frecvența nominală de minim 2.1 GHz.
1.4	Chipset: minim Intel C620.
1.5	Memorie: minim 384 GB Dual Rank, minim DDR4-2666; memorie instalată (12 module de 32GB). Sistemul trebuie să suporte minim 24 sloturi DIMM. Posibilitatea de a utiliza atât memorie RDIMM cât și LRDIMM. Sistemul trebuie să fie capabil să suporte memorie de tip Persistent Memory.
1.6	Răcire: Sistemul trebuie să suporte și să conțină minim 6 ventilatoare redundante, hot-plug.
1.7	Sloturi PCI: Sistemul trebuie să suporte 8 sloturi PCI-Express 3.0 din care cel puțin două să fie de tip x16 PCIe. Sistemul trebuie să fie echipat cu minim 6 sloturi PCI-Express 3.0 din care cel puțin două să fie de tip x16 PCIe. Sloturi PCI-Express libere: minim 2 sloturi PCI-Express 3.0.
1.8	Conectivitate/interfețe: Porturi disponibile: 4 x 1 GbE-BaseT (RJ45); 4 x 10 GbE-BaseT (RJ45); USB 3.0 (minim un port USB în partea frontală și minim 2 porturi pe spatele serverului); 1 x RJ45 management port dedicat; Un port serial; Un slot de tip Micro SD. Sistemul trebuie să suporte adaptoare de rețea cu viteze de 10/25 Gb.
1.9	Controller: Sistemul trebuie să includă controller SATA onboard cu RAID Software. Acesta trebuie să suporte HDD rotative, SSD și drive de tip M.2. Adițional, sistemul trebuie să suporte și să includă controllere care să lucreze în Single Mode, RAID sau HBA. Sistemul trebuie să permita și să includă controllere RAID de tip SAS 12 Gbps și PCIe 3.0 care să suporte următoarele tipuri de RAID: 0/1/10/5/50/6/60.

	Controllerele RAID instalate pe sistem trebuie să suporte criptarea datelor (data at rest). Controllerele RAID instalate trebuie să suporte atât HDD de 12G SAS cât și HDD de 6G SATA. Controllerele RAID ofertate trebuie să suporte cel puțin următoarele sisteme de operare: Microsoft Windows Server VMware SUSE Linux Enterprise Server Red Hat Enterprise Linux În sistem se vor instala două controllere: Primary Controller: La acest controller se vor conecta cele 24 de discuri menționate mai jos. Controllerul va avea minim 2 GB Cache. Secondary Controller: La acest controller se vor conecta cele 2 de discuri M.2 menționate mai jos.
1.10	Tipuri de stocare: Sistemul trebuie să suporte minim 26 X HDD/SSD de 2.5 inch. Sistemul trebuie să suporte unități de stocare de tip 2.5 inch HDD/SSD SAS și SATA. Sistemul trebuie să suporte inclusiv unități de stocare de tip NVMe.
1.11	Capacitatea de stocare instalată: Minim 24 x 480GB SSD SATA RI 2.5 inch Minim 2 x 240GB SATA SSD MU M.2
1.12	Surse de alimentare: Sistemul trebuie să suporte și să conțină minim două surse de tensiune de tip hot plug redundante cu minim 94% eficiență. Puterea instalată per sursă trebuie să fie minim 750W. Vor fi prevăzute cabluri de alimentare de tip C13-C14 cu lungimea de 2 m.
1.13	Sistemul va fi prevăzut cu toate kit-urile necesare pentru instalarea în rack și braț pentru managementul cablurilor.
1.14	Sistemul ofertat trebuie să suporte minim următoarele sisteme de operare: Microsoft Windows Server 2012 R2, 2016 și 2019 Red Hat Enterprise Linux 7.6 VMware 6.5 și 6.7 SUSE Linux Enterprise Server 12 și 15
1.15	Securitate: Sistemul trebuie să aibă capabilități de recuperare a firmware-ului în cazul în care s-a detectat o compromitere a acestuia. Sistemul trebuie să aibă capabilități de tip “Chassis Intrusion Detection” Sistemul trebuie să aiba capabilități de tip “UEFI Secure Boot”. Sistemul trebuie să aibă capabilități de criptare a datelor utilizând chei de criptare. Sistemul ofertat trebuie să suporte TPM 1.2 și 2.0. Secure erase.

1.16	Sistemul trebuie să suporte acceleratoare și plăci grafice de tip NVIDIA/MATROX.
1.17	Sistemul ofertat trebuie să fie prevăzut cu un panou frontal cu LED-uri sau afișaj LCD care să ajute la identificarea ușoară a componentelor defecte (surse de tensiune, memorii, procesoare, sloturi PCI, ventilatoare).
1.18	Sistemul trebuie să suporte management de la distanță. Sistemul trebuie să aibă o interfață dedicată pentru managementul de la distanță. Sistemul trebuie să fie capabil să ofere facilități de tip upgrade de software, monitorizare și management.
1.19	Soluția pentru managementul infrastructurii serverelor ofertate trebuie să aibă capabilități de tip: Unified API ce vor permite implementarea unei infrastructuri programabile care să poată furniza facilități de tip IaaS (Infrastructure as a Service) în cadrul centrului de date. Să permită managementul serverelor. Automatizarea operațiunilor administratorilor Proactive health monitoring. Descoperire automată a serverelor, inițializarea infrastructurii de management, crearea profilurilor pentru servere împreună cu conexiunile de rețea, inclusiv posibilitatea de vizualizare a conexiunilor de rețea fizice și virtuale, oferind astfel administratorilor o singură interfață grafică pentru management și control. Verificarea stării de Health. Scripting tools. Alertare Soluția trebuie să suporte SNMP V3 Soluția de management trebuie să fie compliantă cu standardul FIPS (Federal Information Processing Strandard). Soluţia furnizată trebuie să fie licenţiată pentru toate sistemele ofertate.

2. Implementare

2.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip serverse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,

- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie.

2.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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.

Anexa 26 la caietul de sarcini

ECHIPAMENT TIP SWITCH

1. **Descriere generică a tehnologiei solicitate:**

Blocul funcțional „Switch 48 porturi 10Gbps” este format din 10 echipamente de tip switch, identic configurate.

2. **Caracteristici tehnice minimale** (se aplică pentru fiecare dintre switch-urile solicitate)**:**

2.1 Module de alimentare redundante instalate.
2.2 Module redundante de ventilație instalate.
2.3 Șasiu care să se poată instala într-un rack standard de 19 inch.
2.4 Să aibă instalat un sistem de răcire în care direcția de circulație a aerului să fie de tip faţă-spate.
2.5 Să ofere posibilitatea de actualizare a sistemului de operare în timpul funcționării sistemului fără a afecta traficul.
2.6 Să ofere funcții de control al traficului folosind liste de control al accesului pentru nivelele ISO OSI 2, 3 şi 4, atât pentru protocolul IPv4 cât şi pentru protocolul IPv6;
2.7Să suporte protocolul NetConf sau echivalent.
2.8Să permită configurarea a cel puțin 3900 VLAN-uri.
2.9Să ofere cel puțin 48 interfețe Ethernet 10Gbps de tip RJ45 care să suporte viteze de 100Mbps/1Gbps/10Gbps.
2.10Să ofere cel puțin 6 interfețe Ethernet 40/100Gbps de tip QSFP, capabile să suporte viteze de 10Gbps/40Gbps/100Gbps, echipate cu cel puțin 2 cabluri optice cu lungime minimă de 10 metri și conectori QSFP la ambele capete.
2.11Să ofere o capacitate de comutare de cel puțin 2 Tbps.
2.12Să aibă procesor de control multi-core și memorie de cel puțin 24 GB.
2.13Să suporte ultimele versiuni ale protocoalelor de rutare: OSPF, BGP.
2.14Să suporte protocolul LACP.
2.15Să suporte o tabelă de routare cu cel puțin 750.000 de intrări IPv4.
2.16Să ofere posibilitatea de monitorizare a traficului.

3. Implementare

3.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția de tip switchse va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,

- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie.

3.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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.

Anexa 27 la caietul de sarcini

SOLUȚIE DE SECURITATE ŞI CONTROL AL UTILIZATORILOR

1. Descriere generică a tehnologiei solicitate

Soluția de securitate şi control al utilizatorilor - PASM (Privileged Account and Session Management) este o soluție ce monitorizează și controlează accesul utilizatorilor privilegiați la echipamente de tip server din cadrul unei rețele și înregistrează toate sesiunile și activitățile acestora în timp real.

Soluția administrează accesul utilizatorilor la sisteme, creează și aplică o politică de parole pentru utilizatorii interni și externi și suportă crearea unor reguli de autorizare pentru acordarea sau interzicerea accesului la resurse.

De asemenea, transmite alerte la inițierea sesiunilor privilegiate, monitorizează sesiunile în timp real, înregistrează sesiunile și extrage metadatele pentru căutări ulterioare și auditarea activităților din fiecare sesiune.

În ceea ce privește protecția în timp real, soluția are capacitatea de a identifica și distinge între sesiunile legitime și cele suspecte, recunoaște automat utilizarea neconformă a aplicațiilor și a liniilor de comandă, alertează și încheie automat sesiunile considerate malițioase.

2. Caracteristici tehnice minimale ale soluției

Nr. Crt.	*Cerința*

1.	Soluția va fi de tip appliance virtual sau soluție software care va putea fi instalată pe mașină virtuală.
2.	Soluția trebuie să permită auditarea utilizatorilor pe minim 200 de echipamente/ servere.
3.	Soluția trebuie să permită definirea și urmărirea alocării drepturilor de acces, cât și auditarea accesului la diferitele resurse informatice aferente sistemelor de operare.
4.	Soluția trebuie să aibă posibilitatea de a oferi acces pe baza de roluri definite pentru a evita accesul neautorizat sau al unui utilizator cu rol diferit la serverele critice.
5.	Soluția trebuie să permită integrarea cu un server LDAP extern, unde sunt ținute profilurile utilizatorilor.
6.	Soluția trebuie să ofere posibilitatea de a oferi accesul la resurse pe baza unui program de timp care să poată fi definit.
7.	Soluția trebuie să ofere posibilitatea de a reduce controlat și granular privilegiile conturilor de tip „superuser” pentru administratorii de aplicații Microsoft și „root” pentru UNIX/Linux.
8.	Soluția trebuie să permită definirea de politici de acces la resurse pe baza criteriilor multiple: interval orar, metoda de acces, metoda de logare, porturi, adresă sursă, tipul conectării etc.
9.	Soluția trebuie să permită definirea de politici de acces individualizate pentru sisteme, în funcție de rolul acestora, indiferent de domeniul din care acestea fac parte.
10.	Soluția trebuie să ofere posibilitatea eliminării conturilor administrative comune, prin implementarea funcționalităților de delegare a sarcinilor administrative, administratorii având drepturi doar la componentele necesare îndeplinirii sarcinilor.
11.	Soluția trebuie să suporte criptarea datelor transmise prin rețea și a datelor aplicației.
12.	Soluția trebuie să aibă un modul prin care se pot face conexiuni către sistemele de tip UNIX, folosind ca autentificare conturi de Active Directory. În acest fel, va fi și un singur sistem central pentru stocarea datelor de acces al utilizatorilor.
13.	Soluția trebuie să ofere funcționalități de administrare a parolelor, a conturilor partajate și privilegiate.
14.	Soluția trebuie să permită accesul utilizatorilor la parolele conturilor privilegiate pe baza de reguli de acces. Regulile de acces trebuie să poată fi create și modificate de către administratorul soluției.
15.	Soluția trebuie să ofere un mecanism de auditare în timp real a activității utilizatorilor ce au acces la conturile privilegiate
16.	Soluția trebuie să poată genera rapoarte de activitate ale activităților aferente conturilor de utilizatori privilegiați.
17.	În cazul detecției unui comportament ce se abate de la tiparul comportamentului utilizatorului, soluția trebuie să poată termina forțat sesiunea.
18.	În funcție de gradul de risc, soluția trebuie să poată fi configurată să înregistreze activitatea desfășurată într-o sesiune
19.	Soluția trebuie să permită utilizatorilor folosirea conturilor înregistrate în sistem, fără ca aceștia să poată vedea parola prin folosirea unei metode de autentificare automate.

20.	Soluția trebuie să permită integrarea cu sisteme SIEM
21.	Soluția trebuie să permită vizualizarea datelor in timp real (dashboard-uri predefinite/ particularizate interactive)
22.	Soluția trebuie să permită căutări/filtrări complexe ale evenimentelor/ sesiunilor/ metadatelor (ex. căutări text in înregistrări video)
23.	Soluția trebuie să permită crearea de rapoarte personalizate pe lângă cele implicite, cu posibilitatea de programare a executării automate a acestora (scheduling).

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea Soluției de Securitate şi Control al Utilizatorilor.

4 Implementare

4.1 Instalare și/sau integrare în cadrul infrastructurilor

Soluția de Securitate şi Control al Utilizatorilorse va implementa cu instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie.

4.2 Suport software

Furnizorul trebuie să asigure funcționarea produselor software de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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.

Anexa 28 la caietul de sarcini

LABORATOR MOBIL PENTRU INTERVENȚIE RAPIDĂ

1. Descriere:

Procesul de intervenție rapidă este un element critic esențial pentru gestionarea incidentelor de securitate cibernetică, având scopul de a identifica și de a contracara activităților întreprinse de atacator. Activitățile desfășurate de echipele de intervenție constau în identificarea corectă a sistemelor infectate și limitarea zonei de propagare a infecției, având ca efecte reducerea pierderilor organizației, înlăturarea vulnerabilităților exploatate, restaurarea serviciilor și a proceselor, precum și reducerea riscurilor de a fi afectate de un atac similar în viitor. Investigarea unui atac cibernetic, la sediul instituției beneficiare, necesită utilizarea unor instrumente software și a unor echipamente hardware specializate, dimensionate în funcție de gravitatea atacului. Procesele de colectare a datelor și de transport ale acestora la un laborator amplasat într-o locație fixă, în vederea analizei, conduc la creșterea timpului necesar derulării investigației, respectiv restaurării funcționalităților rețelelor afectate.

Laboratorul mobil va fi compus din:

Sisteme de calcul portabile de tip laptop, cu capacitate ridicată de procesare și stocare, prevăzute cu porturi de intrare de viteză mare (Thunderbolt, USB3.1) specializate pentru activități specifice forensics de triaj, achiziție sau analiză de date. Sistemele vor include cutii sau carcase pentru transport și rezistență la șocuri.

Truse de dispozitive de tip write-block pentru accesarea în mod protejat, read-only, a probelor digitale de pe dispozitive de stocare variate precum harddisk-uri, stick-uri de memorie USB și carduri de memorie. Trusa trebuie să includă adaptoarele, sursele de alimentare, cablurile și accesoriile necesare pentru conectarea dispozitivelor de stocare care folosesc oricare dintre tehnologiile FireWire, SATA,SAS IDE, PCIE, M.2. Dispozitivele și accesoriile menționate vor fi livratecu o cutie sau carcasă pentru transport și rezistență la șocuri.

Echipamente dedicate pentru copierea dispozitivelor de stocare și realizarea imaginilor forensics bit cu bit în formate consacrate de tip E01 și raw DD. Permit copierea simultană de la minim 4 surse de date către 4 destinații. Produsul va fi livrat cu o cutie de transport pentru rezistența la șocuri.

Sisteme de calcul portabile de tip server cu putere de calcul și capacitate de stocare ridicate folosite pentru stocare de date, capturi de trafic de rețea și

analize forensics. Produsul va filivrat cu o cutie de transport pentru rezistența la șocuri.

Dispozitive de stocare tip SSD, cu viteză de citire și de scriere ridicate.

Autovehicule din clasa SUV cu capabilități de transport a sarcinilor ridicate, având spațiul de depozitare mare, adaptat și amenajat special pentru a asigura condiții de rezistență la șocuri mecanice pentru transportul în siguranță ale echipamentelor din dotare, inclusiv a Kit-uluiIncident Response. Autovehiculele trebuie să dispună de tracțiune integrală (4x4) și de o gardă la sol mărită pentru a permite condiții de disponibilitate permanentă în vederea deplasării echipelor de intervenție indiferent de împrejurările meteorologice sau de infrastructura rutieră. Autovehiculele trebuie să ofere posibilitatea de a alimenta cu energie electrică dispozitive electronice la o tensiune de 230v.

2. Definirea componentelor:

Laborator mobil pentru intervenție rapidă **Cantitatea solicitată: 4 laboratoare**		
Nr.	**Fiecare laborator cuprinde următoarele componente:**	**Cantitate**
2.1.	Autovehicul SUV 4x4	1
2.2.	Trusă dispozitive de tip write-block	2
2.3.	Laptop	2
2.4.	Server portabil forensics / captura trafic	1
2.5.	Echipamente pentru copiere dispozitive de stocare	1
2.6.	Dispozitive de stocare tip SSD capacitate 2TB	10
2.7.	Dispozitive de stocare tip SSD capacitate 4TB	10

2.1 Autovehicul SUV 4x4

Descriere:

Autovehicule special adaptate pentru a asigura condiții optime de funcționare pentru echipamentele specificate în Anexa 28 - Laborator mobil pentru intervenție rapidăși de transport în siguranță al echipamentelor specificate în Anexa 21 - Kit Incident Response și Anexa 28 - Laborator mobil pentru intervenție rapidă, indiferent de împrejurările meteorologice sau de infrastructura rutieră. Autovehiculele permit transportul resurselor și funcționarea tehnologiilor necesare derulării investigațiilor cibernetice și oferă echipelor de intervenție accesul rapid la informațiile critice pentru evaluarea incidentului de securitate cibernetică. Autovehiculele trebuie să ofere spațiu suficient pentru funcționarea și transportul echipamentelor menționate. Totodată, este necesară și fixarea echipamentelor pe durata deplasării. Autovehiculele trebuie să asigure alimentarea cu energie electrică timp de minim 6 ore, prin intermediul unui generator electric, a echipamentelor specificate în caracteristicile tehnice minimale.

Ofertantul trebuie să prezinte fişa tehnică a vehiculului în care sunt precizate emisiile de CO_2 şi faptul că sunt îndeplinite cerinţele normei de poluare Euro 6.

Caracteristici tehnice minimale

2.1.1	Autovehicul de tip SUV cu 4 uși laterale și hayon.
2.1.2	Garda la sol: minim 190 mm.
2.1.3	Lungime: minim 4800 mm.
2.1.4	Lățime (inclusiv oglinzi retrovizoare depliate): minim 2100 mm.
2.1.5	Înălțime: minim 1700 mm.
2.1.6	Volum portbagaj (având bancheta din spate nerabatată): minim 570 litri.
2.1.7	Dimensiuni jante: minim 19 inch.
2.1.8	Număr locuri pe scaune: minim 5 locuri.
2.1.9	Carburant: Benzină.
2.1.10	Capacitate cilindrică (cmc): minim 2900cmc
2.1.11	Cuplu motor (Nm): minim 400 Nm.
2.1.12	Putere nominală: minim 240 KW (322CP).
2.1.13	Tracțiune: 4x4 în mod permanent.
2.1.14	Selector moduri de deplasare (de exemplu eco, normal, comfort, dinamic).
2.1.15	Cutie de viteze automată.
2.1.16	Sistem antiblocare cu distribuție electronică a forței de frânare (ABS).
2.1.17	Sistem electronic de control al stabilității mașinii.
2.1.18	Frână de staționare electronică.
2.1.19	Airbag-uri frontale și laterale față, airbag genunchi sau torace pentru șofer, airbag tip cortină.
2.1.20	Senzori de parcare în faţă şi în spate.
2.1.21	Tetiere scaune (față și spate) pentru toate locurile.
2.1.22	Tapiţerie din piele sau piele ecologică.
2.1.23	Asistent pentru menținerea constantă și adaptarea vitezei de rulare în funcție de ceilalți participanți la trafic.
2.1.24	Centuri de siguranţă pentru toate scaunele.

2.1.25	Sistem de monitorizare a presiunii din pneuri.
2.1.26	Control electronic al aerului condiționat (climă) pe minim două zone.
2.1.27	Scaune față încălzite.
2.1.28	Volan încălzit.
2.1.29	Parbriz încălzit.
2.1.30	Geamuri laterale spate și lunetă cu protecție pentru a reduce vizibilitatea în mașină (privacy glass).
2.1.31	Set de jante din aliaj .
2.1.32	Computer de bord cu sistem de navigaţie și ecran color de minim 7 inch.
2.1.33	Sistem audio cu radio, bluetooth, mufă USB, minim 4 difuzoare.
2.1.34	Sistem de direcție servo-asistată.
2.1.35	Oglinzi retrovizoare exterioare cu reglaj electric şi degivrante.
2.1.36	Închidere centralizată cu telecomandă pe cheie sau sistem inteligent pentru închidere/deschidere (fără cheie).
2.1.37	Faruri cu tehnologie LED (fază scurtă și lungă).
2.1.38	Volan reglabil, poziționat pe partea stângă.

Dotări și condiții suplimentare pentru fiecare autovehicul asigurate de operatorul economic:

2.1.39	Autovehiculele trebuie să ofere spațiu suficient pentru funcționarea și transportul echipamentelor menționate. Totodată, este necesar și fixarea echipamentelor pe durata deplasării.
2.1.40	Generator curent electric portabil, alimentat cu benzină, ce asigură funcționarea simultană a echipamentelor ofertate la categoriile Laptop (2 bucăți), Trusă dispozitive de tip write-block (minim 2 dispozitive tip write-block din trusă), Server portabil forensics / captura trafic (1 bucată), Echipamente pentru copiere dispozitive de stocare (1 bucată). Generatorul trebuie să asigure: - o tensiune alternativă de 230 V; - modul AVR, undă sinusoidală pură; - o autonomie de funcționare în sarcină de minim 6 ore cu rezervor propriu sau prin suplimentarea cu una sau mai multe canistre, ce trebuie să poată fi inclusă/incluse în portbagaj, alături de celelalte echipamente. - zgomot redus.
2.1.41	Compresor auto pentru reglarea presiunii din pneuri, cu alimentare 12 V.
2.1.42	Podeaua compartimentului șoferului și pasagerului/pasagerilor va fi acoperită cu covor de cauciuc sau material plastic.

2.1.43	Triunghi reflectorizant - 2 buc., stingător de incendiu tip auto, trusă medicală tip auto, valabile începând cu anul 2020.
2.1.44	Automobilul se livrează cu jante echipate cu anvelope profil vară. Se va livra și un set de anvelope profil iarnă cu jante de aliaj incluse.

Cerințe privind calitatea:

2.1.45	Configurația mecanică va fi cea de fabrică (motor, transmisie, sistem frânare și sistem direcție).
2.1.46	Autovehiculele livrate vor fi noi, neexpuse în showroom, fabricate în anul semnării contractului, nu vor avea niciun defect ca urmare a proiectului, materialelor sau manoperei ori oricărei alte acțiuni sau omisiuni a producătorului/furnizorului și vor funcționa în condiții normale.

Cerinţele privind garanţia şi suportul

2.1.47	Operatorul economic va acorda o perioadă de garanţie de minim 36 luni sau 100000 km.
2.1.48	Piesele de schimb aflate în garanţie vor fi asigurate gratuit pe perioada garanţiei comerciale, cu respectarea condiţiilor impuse de producător la acordarea garanţiei.
2.1.49	Cheltuielile pentru remedierea defecţiunilor care fac obiectul garanţiei, apărute în perioada de garanţie vor fi suportate de furnizor.

Cerințe de livrare:

2.1.50	Autovehiculele achiziționate vor fi livrate în acelaşi timp pe raza municipiului București.
2.1.51	Furnizorul va livra autoturismul cu carnet de service, însoțit de lista operatorilor economici ce asigură, în România, service în perioadele de garanție. Se va pune la dispoziție graficul cu reviziile tehnice ce trebuie efectuate în perioada de garanţie acordată produselor. Se va prezenta în ce constau acestea și ce materiale şi piese de schimb sunt necesare la fiecare tip de revizie.
2.1.52	La livrare, furnizorul se obligă să pună la dispoziția beneficiarului documentația tehnică aferentă în limba română, pentru autovehicule.

Cerințe privind recepția autovehiculelor:

2.1.53	Recepția cantitativă și calitativă va fi efectuată în prezența reprezentanților furnizorului, ocazie cu care se vor preda beneficiarului: Cărțile de identitate ale autovehiculelor; Certificatele de garanție pentru autovehicule; Factura în original.

2.2. Trusă de dispozitive de tip write-block

Descriere:

Trusă de dispozitive de tip write-block (permite doar operațiile de citire și are protecție la operațiile de scriere) folosite în domeniul computer forensics

pentru copierea dispozitivelor de stocare, precum: HDD-uri, SDD-uri, memorii USB. Soluția este formată din 6 dispozitive hardware și accesoriile asociate acestora (cabluri, adaptoare, module hardware adiționale).

Caracteristici tehnice minimale:

Nr.	Caracteristici	Cerințe minimale
2.2.1	Componentele trusei	Echipament pentru copiere dispozitive de stocare cu protecție la scriere Dispozitiv tip write-block pentru interfața PCIe; Dispozitiv tip write-block pentru interfața SAS; Dispozitiv tip write-block pentru interfața SATA/IDE; Dispozitiv tip write-block pentru interfața USB; Dispozitiv tip write-block pentru interfața FireWire. Cutie de transport cu protecție la șocuri mecanice
2.2.2	Echipament pentru copiere dispozitive de stocare cu protecție la scriere	- Porturi sursă (citire) implicite sau folosind adaptoare: SATA/SAS (minim 2); USB versiunea minimă 3.0 sau mai nouă (minim 1); FireWire (minim 1); iSCSI (network share); PCIe (minim 1); IDE. - Porturi destinație (scriere) implicite sau folosind adaptoare: SATA/SAS (minim 2); USB 3.0 (minim 1); iSCSI si CIFS (network share); SATA (minim 2). - Rețea: RJ45 10 Gb/s (minim 1). - Moduri pentru copiere tip forensics: 1:1, 1:2, 2:2 -Tipul fișierelor rezultate: Raw/DD; .E01. -Tipul sistemelor de fișiere rezultate: FAT32; ExFAT; NTFS; HFS+; Ext4. -Funcționalități de bază: Copiază dispozitivele de stocare prin metode de tip write-block (permite doar operațiile de citire și are protecție la operațiile de scriere); Are opțiune de ștergere (wipe); Realizează o valoare hash a imaginii create folosind un algoritm de hash (ex: MD5 sau SHA1);

		Detectează și elimină HPA si DCO; Afișează informații despre dispozitivele de stocare; Salvează informații despre operațiunile efectuate în fișiere de jurnalizare (log-uri); -Interfața: Touchscreen sau cu butoane. -LED-uri: ON/OFF; Led de stare - alimentare cu curent continuu; Led de stare - statusul rețelei. -Adaptoare și module necesare: PCIe SSD Card; PCIe M.2 SSD; PCIe Apple SSD; PCIe IDE; -Cabluri: Toate cablurile necesare pentru conectarea corespunzătoare a adaptoarelor și dispozitivelor de stocare solicitate. - Sursă de alimentare, cablu de alimentare și stecher adaptat pentru priză Shucko.
2.2.3	Dispozitiv tip write-block pentru interfața PCIe	Interfață PCIe; Interfață USB versiunea minimă 3.0; Cabluri: USB versiunea minimă 3.0; PCIe; - Adaptor pentru PCIe SSD; - Adaptor pentru M.2 SSD; - Adaptor pentru Apple SSD; -Sursă de alimentare, cablu de alimentare și stecher adaptat pentru priză Shucko.
2.2.4	Dispozitiv tip write-block pentru interfața SAS	Interfață SAS; Interfață USB versiunea minimă 3.0; Cabluri: USB versiunea minimă 3.0 (minim 1); Semnal și alimentare SAS (minim 1); Sursă de alimentare, cablu de alimentare și ștecher adaptat pentru priza Shucko.
2.2.5	Dispozitiv tip write-block pentru interfața SATA/IDE	Interfață SATA 3; Interfață IDE; Interfață USB versiunea minimă 3.0; Cabluri: USB versiunea minimă 3.0; 3M la Molex; SATA la 3M; Semnal IDE

		Semnal SATA; Semnal ZIF. Adaptor HDD IDE 2.5”; Adaptor HDD IDE 1.8”; Adaptor HDD ZIF; Sursă de alimentare, cablu de alimentare și ștecher adaptat pentru priza Shucko.
2.2.6	Dispozitiv write-block pentru interfața USB	Interfață USB versiunea minimă 3.0 pentru conectarea dispozitivului de stocare; Interfață USB versiunea minimă 3.0 și cablu USB versiunea minimă 3.0 pentru conectarea dispozitivului write-block la PC; Sursă de alimentare, cablu de alimentare și ștecher adaptat pentru priza Shucko.
2.2.7	Dispozitiv write-block pentru interfața FireWire	Interfață Firewire 400 sau 800; Interfață mini USB sau USB versiunea minimă 2.0; Cabluri (minim): Mini USB sau USB versiunea minimă 2.0; FireWire semnal. Sursă de alimentare, cablu de alimentare și ștecher adaptat pentru priza Shucko.
2.2.8	Alte caracteristici generale	Echipamentele livrate vor fi noi. Nu se acceptă echipamente remanufacturate şi/sau care au în componenţă elemente care au fost folosite anterior.

2.3. Laptop

Descriere:

Echipament hardware de tip laptop folosit în domeniul computer forensics pentru clonarea/copierea dispozitivelor de stocare în formate de tip forensics. Soluția este compusă dintr-un dispozitiv hardware și accesorii (cabluri, adaptoare, module hardware adiționale).

Caracteristici tehnice minimale:

2.3.1	Descriere	Este un sistem special construit şi destinat utilizării în activităţi de tip FORENSIC. Conţine un sistem de calcul mobil (laptop) destinat pentru achiziţia şi recuperarea probelor digitale.
2.3.2	Procesor	-număr nuclee: minim 8 -frecvență de bază: minim 3.5 GHz -frecvență Turbo: minim 4.8 GHz -memorie Cache: minim 12 MB
2.3.3	Display	-diagonală: minim 15 inch, maxim 16 inch
2.3.4	Memorie RAM	-capacitate: 64 GB sau mai mare -tip memorie: minim DDR4 -frecvență: 2400 MHz sau mai mare

2.3.5	Stocare	Minim 4 slot-uri pentru SSD, dintre care minim 2 pe interfață M.2 Cele 2 sloturi M.2 sunt echipate cu: - slot 1: SSD capacitate minim 1 TB - slot 2: SSD capacitate minim 2 TB
2.3.6	Funcționalități	-cititor de carduri integrat (SDHC/SDXC/SD/Mini-SD/MMC/RSMMC): DA - format tastatură US English sau echivalent, complet iluminată color și pad numeric integrate: DA - tastatură și mouse cu interfață USB/WiFi suplimentare (format tastatură: US English sau echivalent) -Touch Pad: DA - Porturi Audio: DA
2.3.7	Porturi	-USB 3.0: minim 3 -USB 3.1: minim 1 -Thunderbolt 3: minim 1 -HDMI sau Display Port: minim 1 -Mini DisplayPort 1.3: minim 2
2.3.8	Conectivitate	- port LAN 10/100/1000 Mbps -Bluetooth integrat -Wireless integrat
2.3.9	Baterie	-tip: smart lithium-ion
2.3.10	Alte caracteristici	-sistem de operare inclus: Microsoft Windows 10 Professional, 64-biți -alimentator cu ștecher tip F (Schuko) inclus -geantă de transport capitonată, rezistentă la şocuri şi intemperii, adecvată laptopului
2.3.11	Sisteme de siguranță	-cititor de amprentă integrat
2.3.12	Performanţă energetică	Produsele trebuie să respecte cele mai recente standarde ENERGY STAR în materie de performanţă energetică. Cerinţa va fi considerată îndeplinită prin prezentarea unei etichete ecologice relevante de tip I sau altor mijloace doveditoare adecvate (ex: dosar tehnic al producătorului sau un raport de încercare din partea unui organism recunoscut care să demonstreze respectarea cerinţelor).
2.3.13	Folosirea substanţelor periculoase	În cazul în care produsul ofertat conţine substanţe înscrise pe lista REACH a substanţelor cu o concentraţie mai mare de 0,1% (procent de masă) în întregul produs şi/sau subansamblurile

		produsului, se va prezenta o declaraţie care să indice substanţele specifice prezente.
2.3.14	Gestiunea scoaterii din uz: reciclarea părţilor componente şi marcarea carcaselor, a suporturilor şi a ramelor din plastic	Se vor prezenta documente sau declarații din care să reiasă greutatea, compoziţia polimetrică, precum şi marcajele ISO 11469 şi ISO 1043 ale părţilor din plastic cu greutatea mai mare de 100 grame şi suprafaţa mai mare de 50 cm^2.

2.4. Server portabil forensics / captura trafic

Descriere:

Reprezintă un sistem de calcul optimizat, creat special pentru colectarea, stocarea și analizarea probelor digitale, dotat cu sistem de stocare de tip RAID și cu dispozitive interne de blocare a scrierii pentru suporții analizați.

Caracteristici tehnice minimale:

2.4.1	Procesor cu minim 6 nuclee de procesare
2.4.2	Frecvență de bază procesor de minimum 3.0 GHz
2.4.3	Frecvență Turbo procesor de minimum 4.5 GHz
2.4.4	Memorie Cache a procesorului de minim 12 MB
2.4.5	Minim 31 GB memorie RAM DDR4
2.4.6	Sistem de operare Microsoft Windows 10 Pro 64 bit
2.4.7	Dimensiuni reduse – maxim 18 inch x 11 inch x 10 inch
2.4.8	Geantă de transport rezistentă la şocuri, cu dimensiuni și compartimentare adecvată echipamentului
2.4.9	Monitor LCD de minim 15.6 inch compatibil cu echipamentul
2.4.10	Mouse și tastatură incluse (format tastatură: US English sau echivalent)
2.4.11	Dispozitiv de stocare intern tip SSD de minim 950 GB pe care va fi instalat sistemul de operare
2.4.12	Spațiu de stocare și procesarea datelor trebuie asigurate prin dispozitive tip SSD intern cu o capacitate totală de minim 6 TB
2.4.13	Modul integrat în carcasa sistemului de calcul utilizat la realizarea clonelor folosite în activitatea de digital forensics care să aibă minim următoarele capabilități: - un port PCIe pentru transfer de date - un port SAS/SATA(SAS gen.1, SATA gen.2) - un port USB minim versiunea 3.0 - un port IDE - un port SATA gen.3 - un port FireWire

	- un port de alimentare DC cu 4 pini pentru alimentarea dispozitivelor SAS, SATA, PCIe, IDE - dispune de indicatori tip LED pentru a semnaliza setarea de blocare a scrierii sau permiterea operațiunilor de citire, scriere pentru dispozitivele conectate. - este compatibil cu sistemul de operare Windows 10 - poate furniza o tensiune de 5V DC și un curent de 2A, precum și o tensiune 12V DC cu un curent 2A pentru alimentarea dispozitivelor de stocare conectate. - se conectează cu placa de bază a sistemului prin USB3.0
2.4.14	Minimum 4 porturi USB 3.0 (în plus față de cele din modulul forensics)
2.4.15	Minimum un port HDMI
2.4.16	Minimum 2 porturi USB 2.0
2.4.17	Minimum un port RJ45 Gigabit Ethernet
2.4.18	Sursă de alimentare inclusă prevăzută cu ștecher tip F (Schuko).
2.4.19	Ieșire audio.
2.4.20	Cabluri de alimentare și transmitere date pentru interfețe SAS
2.4.21	Cabluri de alimentare și transmitere date pentru interfețe SATA
2.4.22	Cabluri de transmitere date pentru interfețe IDE
2.4.23	Cabluri de alimentare și transmitere date pentru interfețe Firewire
2.4.24	Cablu de transmitere date PCIe
2.4.25	Cablu de alimentare de la 3M la Molex
2.4.26	Adaptor LIF la SATA
2.4.27	Adaptor ZIF la IDE
2.4.28	Adaptor PCIe pentru SSD cu interfață format (tip) Apple
2.4.29	Adaptor PCIe pentru SSD interfață M.2 NVME

2.5. Echipamente pentru copiere dispozitive de stocare

Descriere:

Echipament hardware folosit în domeniul computer forensics pentru clonarea/copierea dispozitivelor de stocare în formate de tip forensics. Soluția este compusă dintr-un dispozitiv hardware și accesorii (cabluri, adaptoare, module hardware adiționale).

Caracteristici tehnice minimale:

Nr.	Caracteristici	Cerințe minimale
2.5.1	Viteza de clonare/copiere minimă:	Viteză de 400 MB/s la clonarea dispozitivelor de stocare de tip SSD.
2.5.2	Formate de imagini	DD, E01, Ex01, DMG.
2.5.3	Verificarea procesului de clonare	Se folosesc algoritmi de hash precum

		MD5, SHA1 și SHA256. Verificarea unei imagini clonate se poate realiza și simultan cu procesul de clonare.
2.5.4	Porturi sursă	- 2 x SATA sau SAS; - 1 x USB 3.0; - 1 x PCIe. - adaptor sau modul suplimentar pentru interfețele Thunderbolt 2 sau 3 și USB-C.
2.5.5	Porturi destinație	-2 x SATA sau SAS; -2 x SATA; -1x USB 3.0;
2.5.6	Alti conectori	1 x 10 Gigabit Ethernet (conector de rețea);
2.5.7	Echipamentul va conține următoarele accesorii (conectori, cabluri, adaptoare):	- Sursă și cablu de alimentare la curent electric compatibile cu priză schuko; - Minim 4 x Cabluri SATA/SAS; - 1 x adaptor pentru interfata M.2 SATA; -1 x adaptor pentru interfața M.2 NVME -1 x adaptor mSATA la SATA; - 1 x adaptor IDE; - Manual de utilizare în format electronic
2.5.8	Dimensiuni maxime ale dispozitivului	30 cm x 10 cm x 20 cm
	Funcționalități:	
2.5.9	Detectează zone ascunse de pe dispozitivul de stocare sursă, precum: HPA (Host Protected Area), DCO (Device Configuration Overlay);	
2.5.10	Capacitatea de a continua operația de clonare sau citire în cazul unor dispozitive de stocare cu sectoare defecte.	
2.5.11	Conține o funcție dedicată pentru ștergerea datelor de pe dispozitivele de stocare atașate (funcție Wipe).	
2.5.12	Permite clonarea unei surse către mai multe destinații.	
2.5.13	Permite utilizatorului setarea unui set de operațiuni care să fie executate secvențial (copiere, hash, ștergere);	
2.5.14	Permite clonarea simultană a minim două medii de stocare sursă către minim 4 medii de stocare destinație	
2.5.15	Permite clonarea unei locații din rețea, precum și folosirea unei locații din rețea ca și destinație pentru operațiunea de clonare. (Folosind porturile 10 Gigabit Ethernet);	
2.5.16	Permite formatarea mediilor de stocare în sistemele de fișiere NTFS, exFAT, FAT32, EXT4;	
2.5.17	Verifică dacă un mediu de stocare este gol sau a fost șters;	

2.5.18	Sunt create fișiere de jurnalizare pentru operațiunilor efectuate. Acestea pot fi vizualizate pe echipament sau exportate;
2.5.19	Asigură restaurarea unei imagini de tip DD, E01, EX01, DMG pe un hard disk;
2.5.20	Deține funcția de previzualizare (browsing) pentru conținutul sistemului de fisiere al dispozitivului de stocare atașat.
2.5.21	Deține funcție pentru criptarea unui dispozitiv de stocare atașat.
2.5.22	Asigură detecția dispozitivelor de stocare criptate cu tehnologia BitLocker.
2.5.23	Permite clonarea sub formă de imagine logică, selectând anumite fișiere sau folosind funcția de căutare.
2.5.24	Dispozitivul dispune de un ecran tactil incorporat prin care se accesează interfața grafică cu toate operațiunile disponibile.

2.6. Dispozitive de stocare tip SSD capacitate 2TB
Descriere:
Dispozitive de stocare tip SSD, cu viteză de citire și scriere ridicate.
Caracteristici tehnice minimale:

2.6.1	Tip disc	SSD
2.6.2	Capacitate	Minim 2 TB
2.6.3	Interfață	SATA III 6Gb/s
2.6.4	Format	2.5 inch SATA III
2.6.5	Viteză de citire secvențială	Minim 540 MB/s
2.6.6	Viteză de scriere secvențială	Minim 510 MB/s
2.6.7	Viteză de citire aleatorie	Minim 95000 IOPS (4KB, QD32)
2.6.8	Viteză de scriere aleatorie	Minim 84000 IOPS (4KB, QD32)
2.6.9	MTBF	Minim 1400000 ore
2.6.10	Garanție	Minim 36 luni

2.7. Dispozitive de stocare tip SSD capacitate 4TB
Descriere:
Dispozitive de stocare tip SSD, cu viteză de citire și scriere ridicate.
Caracteristici tehnice minimale:

2.7.1	Tip disc	SSD
2.7.2	Capacitate	Minim 4TB
2.7.3	Interfață	SATA III 6Gb/s
2.7.4	Format	2.5 inch SATA III
2.7.5	Viteză de citire secvențială	Minim 540 MB/s
2.7.6	Viteză de scriere secvențială	Minim 510 MB/s
2.7.7	Viteză de citire aleatorie	Minim 95000 IOPS (4KB, QD32)
2.7.8	Viteză de scriere aleatorie	Minim 82000 IOPS (4KB, QD32)
2.7.9	MTBF	Minim 1400000 ore
2.7.10	Garanție	Minim 36 luni

3. Livrabile

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

Documentația de administrare și operare.

Dacă este cazul, ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-urilor și dezinstalarea/reinstalarea, intervenții în cazuri de forță majoră.

Documentația de utilizare.

Dacă este cazul, ofertantul va livra versiunea electronică a manualului de utilizare care va cuprinde pașii de urmat de către utilizatori în vederea exploatării produsului.

4. Implementare

4.1. Instalare și/sau integrare în cadrul infrastructurilor

Soluția Laborator Mobil pentru Intervenție Rapidă se va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

4.2. Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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.

Anexa 29 la caietul de sarcini

CENTRU COMUNICAȚIE DE REZERVĂ (BACKUP)

1. Descriere generală:

Ofertantul va furniza o soluție de implementare a unui centru de comunicație de rezervă, ce va îngloba toate produsele de la punctul 2 și va asigura compatibilitatea acestora.

2. Definirea componentelor:

Centru comunicație de rezervă (backup)		
Nr.	**Denumiri componente**	**Număr componente**
2.1.	Switch fibre channel	6
2.2.	Router	4
2.3.	Switch top of the rack (management)	10
2.4.	NGFW (Next Generation Firewall)	4
2.5.	Soluție pentru analiza fluxurilor (flow)	1
2.6.	Soluție de tip Application and Logs Management	1
2.7.	Soluție de tip server	8
2.8.	Soluție de tip sistem de stocare	1
2.9.	Soluție de tip mediu virtualizat	1
2.10	Soluție de suport fizic de tip rack	6
2.11	Stații de lucru pentru management	5
2.12	Soluție de tip sursă de alimentare continuă (UPS)	6
2.13	Soluție software pentru backup & restore	1
2.14	Soluție de tip Media Wall	1

2.1 Switch fibre channel

Caracteristici tehnice minimale:

2.1.1	Deţine minim 24 porturi tip SFP+ ce asigură conexiuni la viteze de transfer de cel puțin 16 Gbps Fibre Channel.

2.1.2	Minim 24 de module SFP+ compatibile cu switch-urile FC, precum și 24 de licențe pentru activarea acestora.
2.1.3	Soluţia este compatibilă cu celelalte echipamente din cadrul soluției (servere, storage)
2.1.4	Soluția include instrumente pentru management de trafic, diagnoză și rezolvarea de probleme.
2.1.5	Soluția oferă acces pentru management prin următoarele protocoale: SFTP, SSHv2, SNMPv3.
2.1.6	Alimentare: 2 surse de alimentare redundante, hot-plug, intrare 220 VAC / 50 Hz.
2.1.7	Echipamentul va fi instalat în cadrul unui rack de 19”, prin intermediul unui kit de instalare inclus.
2.1.8	Se vor livra toate cablurile necesare pentru interconectarea redundantă a switch-urilor FC cu serverele și storage-ul.

2.2 Router
Caracteristici tehnice minimale:

2.2.1	Tip echipament	Echipamentul oferă cel puțin capabilități de: Rutare a traficului între mai multe rețele VPN IPsec Compatibil SD-WAN
2.2.2	Performanțe	Rată de transfer minim. 300 Mbps Rată de transfer trafic criptat minim 300 Mbps Algoritmi criptare: DES, 3DES, AES-256, AES-GCM
2.2.3	Rutare și interfețe	Interfețe intrare/ieșire (I/O): Minim 1 port RJ-45 10/100/1000 Gigabit Ethernet Minim 2 porturi SFP echipate cu SFP 1G Interfață de management/Consolă: tip serial RJ-45 și mini USB Alte porturi: 1 x USB Suportă min. 2 sloturi de extindere Suport pentru SSD Protocoale LAN/WAN: RIPv1, RIPv2, OSPF, BGP, IS-IS, MPLS, VLAN, PIM, GRE, DHCP, DNS, QoS, HDLC, MACsec, 802.1 ag, 802.3 ah, BFD, PPP, MLPPP, MLFR, PPPoE, WRED.
2.2.4	Certificări de siguranță	IEC 60950-1, UL 60950-1, EN 60950-1, CAN/CSA-C22.2, EN 300 386, EN 55024, EN 55032, EN 61000, ICES-003, CISPR 24, CISPR32.

2.2.5	Configurație de bază	Memorie RAM minimum 4 GB Memorie FLASH minimum 8 GB Leduri indicare stare Minim 1 sursă de alimentare AC 100 – 240V 50/60Hz Consum maxim (AC): 250 W MTBF minim 200000 ore Temperatura de operare cel puțin între 0 și 40 grade C
2.2.6	Accesorii	Set cabluri de alimentare cu conector C14-tată, set cabluri de alimentare cu conector CEE 7/7 tată, set/kit montare in rack, set cabluri consolă
2.2.7	Dimensiuni de gabarit	Rackabil în rack standard EIA 19”, să ocupe maxim 1U

2.3 Switch top of the rack (management)

Caracteristici tehnice minimale:

2.3.1	Descriere generală	Minim 48 porturi 10/100/1000 Ethernet; Minim 2 porturi 1/10GB SFP/SFP+ echipate cu 2 x 10 GE SFP+ SR;
2.3.2	Performanţe	Capacitate de switching minim 176 Gbps; Throughput minim 130 Mpps MTU configurabil pana la 9000 bytes (jumbo frames); Minim 16000 adrese MAC.
2.3.3	Rute IPv4	Minim 512 rute IPv4
2.3.4	Rute IPv6	Produsul oferă implementare de rute IPv6.
2.3.5	Memorie	Memoria instalată trebuie să asigure simultan toate functionalităţile solicitate.
2.3.6	Sistem de operare şi caracteristici minimale incluse (cel puţin următoarele)	NetFlow sau sFlow sau jFlow Servicii QoS LACP min. 32 grupuri LACP min 8 porturi pe LAG Tehnologii interconectare min. 4 switchuri astfel încât să opere ca un singur switch. NTP sau SNTP Compatibil Spanning-Tree SNMP v1,v2 sau v2c,v3 RMON Voice VLAN Dynamic ARP inspection IGMP v1, v2, v3 Traffic Mirroring

		TFTP Server DHCP Autentificare TACACS+ şi RADIUS
2.3.7	Standarde (cel puţin următoarele)	IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS Prioritization IEEE 802.1Q VLAN IEEE 802.1s IEEE 802.1w IEEE 802.1X IEEE 802.1ab (LLDP) IEEE 802.3x IEEE 802.3u IEEE 802.3ab IEEE 802.3z IEEE 802.3ad (LACP)
2.3.8	Licenţe	licență 2 x 10GE suportă ACL layer 3/4 suportă minim 4090 Vlan-uri suportă minim 512 route IPv4
2.3.9	Management	Configurare CLI, web, telnet, SSH, consolă.
2.3.10	Alimentare cu energie electrică	Minim o sursă de alimentare instalată intern
2.3.11	Temperatură operare	0° la 40°C
2.3.12	Dimensiuni de gabarit	rackabil 19”, 1U
2.3.13	Accesorii	1 x cablu consolă; Set cabluri de alimentare cu conector C14-tată, set cabluri de alimentare cu conector CEE 7/7 tată; 1 x kit de instalare 19" 1U cu toate cablurile de protecţie (împământare), şuruburile, cât şi alte accesorii necesare instalării şi punerii în funcţiune incluse;

2.4 NGFW (Next Generation Firewall)

Caracteristici tehnice minimale:

2.4.1	Tip echipament	Echipamentul oferă cel puțin capabilități de: Control al aplicațiilor; Filtrare a traficului; VPN
2.4.2	Performanțe	Rată de transfer firewall (pachete mari) minim 3 Gbps Rată de transfer NGFW minim 1.5 Gbps

		Rată de transfer IPS minim 2.2 Gbps Rată de transfer VPN IPsec minim 800 Mbps Număr sesiuni concurente mininm 1 milion Număr conexiuni/secundă minim 18000 Număr VPN peers/tunnels minim 1500 High availability (HA) active/active și active/standby sau active/active și active/passive
2.4.3	Rutare și interfețe	Interfețe intrare/ieșire (I/O): Minim 12 x 10 /100/1000 RJ 45 Minim 4 x 1G Gigabit Ethernet SFP Minim 1 port de management Interfață de management/Consolă: da, tip RJ-45 Suport pentru management centralizat Alte porturi: 1 x USB Protocoale LAN/WAN : RIP, OSPF, BGP
2.4.4	Aplicații de securitate	filtrare URL Application Visibility and Control (AVC)
2.4.5	Configurație de bază	Procesor Intel Xeon sau echivalent RAM mnim 16GB FLASH minim 8GB SSD minim 100 GB Leduri indicare stare Minim o sursă de alimentare
2.4.6	Accesorii	Set cabluri de alimentare cu conector C14-tată, set cabluri de alimentare cu conector CEE 7/7 tată, set/kit montare in rack, set cabluri consolă
2.4.7	Dimensiuni de gabarit	Rackabil în rack standard EIA 19”, să ocupe maxim 1U

2.5 Soluție pentru analiza fluxurilor (flow)

Descriere generică a tehnologiei solicitate

Ofertantul va furniza o aplicație sau suită de aplicații ce permit obținerea vizibilității traficului în rețea, detecția și răspunsul la amenințările din rețea în timp real.

Caracteristici tehnice minimale:

2.5.1	Monitorizează fluxurile de date din mai multe segmente de rețea sau VLAN-uri
2.5.2	Permite stocarea și analiza traficului din rețele
2.5.3	Permite compresie sau agregare sau deduplicare a datelor
2.5.4	Detectează amenințările de securitate, anomaliile din cadrul rețelelor și oferă vizibilitate asupra acestora prin intermediul unui centru de control.

2.5.5	Utilizează fluxuri de date de tip NetFlow, IPFIX, sFlow sau jFlow
2.5.6	Oferă vizibilitate până la nivelul 7 OSI obținând informații despre aplicația ce rulează în rețea
2.5.7	Oferă informații despre RTT (Round Trip Time), SRT (Server Response Time) sau Retransmissions din rețelele monitorizate
2.5.8	Poate agrega informații din mai multe surse (ex. NetFlow, sFlow) și le poate retransmite către una sau mai multe destinații.
2.5.9	Soluția poate rula și în medii virtualizate putând fi integrată în rețelele protejate sub forma unor appliance-uri virtuale
2.5.10	Suportă analiza a minim 30000 fluxuri de date (flow) pe secundă
2.5.11	Soluția permite învățarea comportamentului rețelei pentru detecția anomaliilor
2.5.12	Permite integrarea cu sisteme de tip SIEM

2.6 Soluție de tip Application and Logs Management

Descriere generică a tehnologiei solicitate

Ofertantul va furniza o aplicație sau o suită de aplicații ce permite colectarea, indexarea, analizarea și corelarea logurilor din mai multe surse (ex: server de aplicații, web, mașini virtuale, echipamente de rețea, sisteme de operare, s.a.) ce are ca scop urmărirea, detecția și alertarea în cazul apariției unor posibile evenimente/amenințări de securitate.

Caracteristici tehnice minimale:

2.6.1	Asigură în mod implicit colectarea de date și evenimente de la cel puțin următoarele echipamente de securitate IT, aplicaţii informatice sau sisteme de operare: - Sisteme de operare Microsoft: Windows XP, 7, 8, Server 2000, Server 2003, Server 2008, Server 2012, - Sistem de operare IBM AIX, - Sistem de operare UNIX, - Sistem de operare Solaris, - Sistem de operare HP UX, - Kaspersky Antivirus, - McAfee VirusScan (sau McAfee ePolicy Orchestrator), - Symantec EndPoint Protection, - TrendMicro (Office Scan. Control Manager, VirusWall), - Microsoft Forefront (sau EndPoint Protection), - IBM WebSphere, - Oracle Weblogic, - Sistem de virtualizare: VMWare ESX/ESXi şi vCenter,

	- Microsoft Exchange, - IBM Lotus Domino, - Cisco Router, - Juniper Router, - Cisco Catalyst Switch, - HP ProCurve Ethernet Switch, - Nortel Contivity Switch, - Cisco PIX Firewall, - Cisco ASA Firewall, - Checkpoint Firewall-1, - Juniper SRX Firewall, - Fortinet Fortigate, - Palo Alto Networks Firewall, - SonicWALL Firewall, - CyberGuard Firewall, - Snort IDS/IPS, - Sourcefire IDS/IPS, - HP TippingPoint IDS/IPS, - Cisco IPS, - Juniper Networks IDP, - McAfee IntruShield (NSP), - Radware Defense Pro, - Enterasys Dragon, - IBM ISS Proventia, - Radware Defense Pro, - Top Layer IPS, - Cisco IronPort Web Security Appliance, - Squid Web Proxy, - McAfee Web Security Appliance (sau McAfee ePolicy Orchestrator), - Microsoft ISA Server, - BlueCoat Proxy SG, - Cisco IronPort Email Security Appliance, - McAfee Email Security Appliance (sau McAfee ePolicy Orchestrator), - Imperva SecureSphere, - Barracuda Web Application Firewall, - F5 BIG-IP ASM, - Oracle AuditVault, - IBM DB2, - Microsoft SQL, - Sybase Adaptive Server Enterprise, - Cisco VPN Concentrator, - Juniper VPN, - Nortel Contivity VPN, - CheckPoint VPN, - Apache HTTP Access şi Errors Logs, - Microsoft IIS,

	- Tenable Nessus, - Nmap, - nCircle IP360, - QualysGuard Vulnerability Manager, - McAfee Vulnerability Manager, - Rapid7 NeXpose, - eEye Retina, - Saint Vulnerability Scanner; - Cisco ACS, - Microsoft Active Directory, - Microsoft IAS Server, - IBM Tivoli Access Manager, - Juniper SBR, - RSA Authentication Manager, - CA SiteMinder, - Lieberman Random Password Manager, - CA Top Secret, - Fidelis XPS Data Loss Prevention, - Symantec Data Loss Prevention, - McAfee Data Loss Prevention (sau McAfee ePolicy Orchestrator), - Niksun network forensics, - FireEye, - Damballa Failsafe, - HBGary Active Defense, - ForeScout CounterACT, - Cisco Aironet, - Aruba Mobility Controller, - Bit9 Parity, - McAfee Application Control, - Cyber-Ark Vault, - Arbor Networks Peakflow, - Evenimente tip NetFlow.
2.6.2	Asigură amplasarea mai multor echipamente similare într-o arhitectură ierarhică și transmiterea alertelor corelate și a evenimentelor (în format brut și normalizat) către nivelul superior.
2.6.3	Oferă facilități de normalizare a datelor obținute de la surse diferite de evenimente.
2.6.4	Asigură stocarea evenimentelor colectate și în format brut.
2.6.5	Detectează amenințările de securitate din rețelele monitorizate oferind imaginea exactă asupra acestora prin intermediul unui centru de control
2.6.6	Asigură mecanisme de protecție a integrității datelor stocate prin intermediul algoritmilor de tip *hash*.
2.6.7	Asigură exportarea evenimentelor colectate în format CSV.

2.6.8	Asigură identificarea amenințărilor cibernetice în condiții cât mai apropiate de cele în timp real
2.6.9	Asigură corelarea evenimentelor colectate din surse de log-uri diferite.
2.6.10	Oferă un pachet predefinit de reguli de corelare şi alertare.
2.6.11	Asigură generarea automată a unui scor de severitate al evenimentelor
2.6.12	Asigură monitorizarea în timp real prin afișarea în consola grafică a rezultatelor operației de corelare a evenimentelor de securitate.
2.6.13	Asigură execuția de corelări bazate pe anumite conditii specifice și permite definirea unor acţiuni de răspuns (alerte) ce includ cel puțin: a) crearea unui eveniment, b) transmiterea unui email
2.6.14	Asigură definirea unei limite de evenimente similare identificate, în vederea generării unei alerte.
2.6.15	Asigură investigarea incidentelor de securitate pornind de la evenimentul corelat până la identificarea evenimentelor primare ce au generat alerta.
2.6.16	Posibilitatea utilizării expresiilor regulate, operatori booleani, expresii statistice în aplicația de căutare
2.6.17	Posibilitatea de generare rapoarte pe baza unor interogări
2.6.18	Posibilitate salvare rapoarte în format PDF
2.6.19	Posibilitate customizare Dashboard
2.6.20	Posibilitate geolocalizare adrese IP
2.6.21	Posibilitate integrare cu AD/LDAP
2.6.22	Asigură salvarea configurației din interfața grafică, configurație ce include cel puțin următoarele resurse: a) reguli, b) informații despre vulnerabilități, c) rapoarte
2.6.23	Asigură crearea unor spații de lucru diferite utilizatorilor, în funcție de rolul acestora.

2.6.24	EPS susținute: minim 5000, sau capacitate stocare evenimente: minim 100GB/zi.
2.6.25	Soluția poate rula și în medii virtualizate putând fi integrată în rețelele monitorizate sub forma unor appliance-uri virtuale

2.7 Soluție de tip server

Descriere generică a tehnologiei solicitate

Ofertantul va furniza un echipament de tip server, cu caracteristicile în parametrii definiți prin prezentul document.

Caracteristici tehnice minimale:

2.7.1	Produsul va fi rackabil, în rack standard de 19” și va avea înălțimea de 2U
2.7.2	Produsul va include toate accesoriile necesare montării în rack și realizării unei cablări ergonomice a conexiunilor electrice și de date.
2.7.3	**Procesor:** Minim Intel Xeon Gold 6248 (2.5GHz, 27.5MB Cache, 20 cores, DDR4-2933MHz, TDP 150W), High Performance heatsink, sau echivalent Produsul va fi echipat cu minim 2 procesoare
2.7.4	**Memorie RAM:** Produsul va suporta minim 24 module DIMM și o capacitate totală de memorie RAM de 3TB Produsul va fi echipat cu minim 512 GB DDR4-2933 MT/s, Registered DIMMs, distribuiți în module de capacități egale
2.7.5	**Unități de stocare:** Produsul va fi echipat cu un număr suficient de module (cage) pentru a suporta instalarea a minim 12 disk-uri SFF, interfață SAS, în partea frontală Produsul va fi echipat cu un controller dedicat de stocare ce permite configurarea de disk-uri SAS 12G în sistem RAID (RAID 0, 1, 1+0, 5, 5+0, 6, 6+0) Produsul va fi echipat cu minim 2 disk-uri SSD, format SFF 2.5” standard, interfață SAS 12G, capacitate minim 400GB, mixed-usage
2.7.6	**Securitate:** Produsul va veni echipat cu modul TPM minim versiunea 2.0 Produsul va suporta UEFI Secure Boot
2.7.7	**Interfaţă video:** Rezoluție max 1920x1200@60Hz-32 bpp, integrată pe placa de bază
2.7.8	**Panou monitorizare stare:** Panou frontal cu led-uri pentru monitorizarea stării serverului: sursă alimentare, stare generală server
2.7.9	**Interfeţe reţea:** Produsul va fi echipat cu placă de rețea (on-board sau distinctă) care oferă minim 2 conexiuni RJ45 ethernet la viteza de 10Gb/s fiecare Produsul va fi echipat cu placă de rețea (on-board sau distinctă) care oferă

	minim 2 conexiuni FO tip LC ethernet la viteza de 10Gb/s fiecare. Produsul va include interfețele de conectare (GBIC), în cazul în care acestea nu fac parte implicit din modulul FC Produsul va oferi o interfață de rețea RJ45 distinctă pentru management
2.7.10	**Fibre Channel:** Produsul va fi echipat cu minim un modul distinct care să ofere minim 2 porturi FC cu conectori LC, la viteza de minim 16Gb, compatibilitate Windows 2012R2/2016 Server, Linux Produsul va include interfețele de conectare (GBIC), în cazul în care acestea nu fac parte implicit din modulul FC
2.7.11	**Interfețe adiționale:** Minim 2xUSB 3.0 liber pe panoul din spate Minim 1xUSB 3.0 liber pe panoul frontal Minim 1 port video pe panoul frontal
2.7.12	**Management:** Produsul va permite monitorizarea şi managementul stării echipamentului prin interfaţă web, prin portul dedicat de management, ce va permite monitorizarea stării de funcţionare a disk-urilor, procesoarelor, ventilatoarelor etc., consolă virtuală, media virtual, pornire/oprire/reboot Produsul va veni cu licență perpetuă pentru funcționalitățile avansate ale interfeței de management
2.7.13	**Sursă de alimentare:** Produsul va fi echipat cu minim 2 surse de alimentare redundante, hot plug Putere minimă 800W per sursă Eficienţă min. 90%; Tensiune de alimentare 100 – 240 $V_{c.a}$; Frecvenţă curent de alimentare 50 – 60 Hz;
2.7.14	**Ventilatoare:** Produsul va include minim 6 ventilatoare cu viteză variabilă, în funcție de temperatura sistemului
2.7.15	**Altele:** În cazul defectării unui mediu de stocare persistent (HDD, SSD, M2, card SD etc.), acesta va fi înlocuit în baza garanției fără returnarea la producător a mediului defect Pentru toate porturile de interconectare RJ45 și FO cu care este dotat echipamentul vor fi incluse și cablurile aferente, de lungime minim 5m. În cazul cablurilor FO, unul din conectori va fi compatibil cu portul din server, iar celălalt va fi de tip LC.

2.8Soluție de tip sistem de stocare

Descriere generică a tehnologiei solicitate

Ofertantul va furniza un echipament de stocare, cu caracteristicile în parametrii definiți prin prezentul document.

Caracteristici tehnice minimale:

2.8.1	Unitatea/unitățile de control, precum și modulele de expansiune cu discuri vor avea dimensiuni standard ce permit montarea în rack și vor include toate

	elementele necesare montării în rack standard de 19”
2.8.2	Sistemul va conține cel puțin două unități de control (storage processors / controller nodes / service processors)
2.8.3	Fiecare unitate de control va fi echipată cu procesor de minim 1.8GHz, minim 6-core
2.8.4	Fiecare modul hardware al sistemului va fi echipat cu minim două surse de alimentare, în configurație redundantă
2.8.5	Administrarea sistemului se poate face de la distanță, prin interfață web
2.8.6	Alimentarea va fi cu curent alternativ, între 100-240V, 50-60Hz
2.8.7	Sistemul va fi livrat într-o configurație care să includă cel puțin diskuri SSD și SAS 10K, conform capacităților precizate în prezentul document
2.8.8	Sistemul va asigura configurarea de Fast/Flash Cache de minim 800 GB pe dispozitive de stocare tip SSD, separat de cele folosite pentru stocare propriu zisă.
2.8.9	Sistemul va permite o capacitate maximă de stocare (raw) de minim 2.4PB, în configurație complet echipată
2.8.10	Sistemul va permite adăugarea ulterioară de shelf-uri cu medii de stocare suplimentare și va include shelf-urile necesare pentru a suporta capacitatea de stocare solicitată. Sistemul va veni echipat cu următoarele capacități de stocare: - minim 8 TB capacitate raw pe discuri de tip SSD (fără diskurile de Fast Cache) - minim 18 TB capacitate raw pe discuri de tip SAS 10K - minim 108 TB capacitate totală pe discuri rotaționale (SAS și NL-SAS. Include capacitatea obligatorie pe discuri SAS)
2.8.11	Sistemul va include licențe perpetue pentru folosirea întregii capacități ofertate și a facilităților solicitate
2.8.12	Sistemul va permite nativ configurarea de volume virtuale Vmware (vVOL). Dacă este necesar, va fi inclusă licența aferentă.
2.8.13	Sistemul va permite configurarea de LUN-uri de tip Thin sau Thick. Dacă este necesar, va fi inclusă licența aferentă.
2.8.14	Sistemul va permite configurații RAID 1/0, 5, 6. Dacă este necesar, va fi inclusă licența aferentă.
2.8.15	Sistemul va permite deduplicare. Dacă este necesar, va fi inclusă licența aferentă.
2.8.16	Sistemul va suporta nativ tehnologiile de conectare iSCSI și Fibre **Channel**. Dacă este necesar, va fi inclusă licența aferentă.
2.8.17	Sistemul va veni echipat cu minim 4 porturi Fibre Channel per controller, viteză minimă 16GBps
2.8.18	Numărul maxim de porturi Fibre Channel 16GBps suportate de sistem în configurație maximală nu va fi mai mic de 16
2.8.19	Numărul maxim de inițiatori suportați de sistem nu va fi mai mic de 2048
2.8.20	Sistemul va veni echipat cu minim 4 porturi RJ45 10 Gbps per controller
2.8.21	Sistemul va permite criptarea datelor stocate. Dacă este necesar, va fi inclusă licența aferentă.
2.8.22	Sistemul va permite realizarea de snapshot-uri. Dacă este necesar, va fi

	inclusă licența aferentă.
2.8.23	Sistemul va permite replicarea datelor stocate. Dacă este necesar, va fi inclusă licența aferentă.
2.8.24	În cazul defectării unui mediu de stocare persistent (HDD, SSD, M2, card SD etc.), acesta va fi înlocuit în baza garanției fără returnarea la producător a mediului defect

2.9 Soluție de tip mediu virtualizat

Descriere generică a tehnologiei solicitate

Ofertantul va furniza o aplicație sau suită de aplicații ce permit rularea de mașini virtuale pe infrastructură fizică, cu o interfață unică de configurare.

Caracteristici tehnice minimale:

2.9.1	Permite crearea, importarea, rularea și administrarea de mașini virtuale
2.9.2	Soluția este instalată direct pe platforma hardware a unuia dintre sistemele informatice de tip *server* şi îndeplineşte rolul de *hypervisor tip1 (nativ)* pentru administrarea maşinilor virtuale.
2.9.3	Platforma permite configurarea maşinilor virtuale cu cel puţin următoarele sisteme de operare: Microsoft Windows: 7, 7 SP1, 8, 8.1, 10, Server 2012, Server 2012 R2, Server 2016, Server 2019; CentOS: 7; Red Hat Enterprise Linux: 7; SUSE Linux Enterprise: 12; Ubuntu;
2.9.4	Oferă o interfață unică de administrare a întregii infrastructuri virtualizate – mașini virtuale, noduri fizice, rețeaua virtuală, stocarea externă, librării software
2.9.5	Administrarea centralizată va permite efectuarea operațiunilor asupra sistemului prin intermediul unei interfețe web
2.9.6	Administrarea centralizată a sistemului va permite definirea de roluri de administrare, pentru a restricționa selectiv nivelul de acces al unor grupuri de utilizatori la funcționalitățile platformei de virtualizare
2.9.7	Soluţia trebuie să permită integrare cu Active Directory, în sensul autentificării utilizatorilor din domeniu la nivelul consolei de management a soluţiei de virtualizare
2.9.8	Soluția oferă posibilitatea de a crea și utiliza șabloane (templates) pentru implementarea rapidă de noi mașini virtuale ce include şi posibilitatea de personalizare.
2.9.9	Soluția trebuie să ofere un set de instrumente software care asigură integrarea acesteia în arhitectura de rețea (Virtual Switch)
2.9.10	Soluția permite controlul QoS pentru accesul maşinilor virtuale la resursele hardware ale sistemelor de stocare
2.9.11	Permite migrarea live a mașinilor virtuale, fără întreruperea funcționării serviciilor acestora și fără pierdere de date. Migrarea live permite mutarea uneia sau mai multor mașini virtuale de pe un server fizic pe altul (inclusiv între servere cu specificaţii hardware diferite), prin balansarea automată a

	resurselor
2.9.12	Asigură o funcționare în regim de high-availability integrat pentru anumite mașini virtuale, care presupune inclusiv disponibilitatea continuă a aplicațiilor şi relocarea acestora pe un alt server fizic fără pierderea datelor, în cazul defectării mașinilor fizice gazdă
2.9.13	Asigură disponibilitatea continuă a aplicațiilor şi mutarea automată a maşinilor virtuale pe alte servere fizice în condițiile desfășurării de operațiuni de mentenanță asupra serverului fizic care găzduiește mașina virtuală
2.9.14	Permite integrarea redundantă (SAN multipath) cu soluții de stocare externe, prin tehnologii de rețea Ethernet (iSCSI) și Fibre Channel
2.9.15	Soluția permite configurarea și accesarea simultană a unui spațiu de stocare extern de către toate nodurile fizice pe care este instalată soluția de virtualizare (Shared Storage)
2.9.16	Soluția oferă posibilitatea de replicare a maşinilor virtuale către un centru de date secundar pentru crearea unui proces de tip disaster recovery.
2.9.17	Soluția de virtualizare dispune de instrumente virtuale de securitate integrate.
2.9.18	Permite optimizarea alocării spaţiului pe disk-uri (thin disk provisioning).
2.9.19	Soluţia are implementat un mecanism care să permită administrarea ordinii de pornire a maşinilor virtuale prin impunerea unor timpi de întârziere într-un mod centralizat, prin intermediul platformei de management a platformei de virtualizare
2.9.20	Soluția propusă permite alocarea dinamică a resurselor hardware disponibile (spre exemplu CPU sau memorie RAM) prin subpartiţionarea resurselor hardware şi asocierea acestora unor grupuri de maşini virtuale
2.9.21	Permite balansarea manuală sau dinamică, pe baza unor politici prestabilite, a resurselor de procesare existente în platforma virtuală.
2.9.22	Permite crearea și administrarea de infrastructuri virtuale de rețea în cadrul sistemului
2.9.23	Asigură posibilitatea de creare și configurare de rețele virtuale (VLAN și PVLAN) prin integrarea directă cu echipamente active de rețea.
2.9.24	Asigură prioritizarea accesului la resursele de rețea prin monitorizarea permanentă a traficului de reţea şi gestionarea încărcării (network offload).
2.9.25	Asigură posibilitatea de administrare a resurselor de rețea ca resurse multiple, separate, și de organizare a acestora sub formă de clustere (NIC teaming) pentru balansarea încărcării la nivelul reţelei.
2.9.26	Soluția permite controlul QoS pentru conexiunile de rețea ale mașinilor virtuale.
2.9.27	Soluția ofertată asigură realizarea backup-ului datelor şi informaţiilor ce includ şi configurările maşinilor virtuale.
2.9.28	Soluția oferă interfețe API pentru automatizarea și integrarea funcționalităților cu terțe aplicații.
2.9.29	Oferă posibilitatea de actualizare a hypervisor-ului prin procesul de update și/sau patching, în vederea optimizării soluției și eliminării vulnerabilităților de securitate.
2.9.30	Conține licențierea necesară pentru integrarea inițială a 8 noduri fizice bi-procesor

2.9.31	Permite realizarea de snapshot-uri live ale mașinilor virtuale.
2.9.32	Permite gestionarea snapshot-urilor mașinilor virtuale și restaurarea acestora la orice versiune anterioară înregistrată.
2.9.33	Asigură alertarea proactivă cu privire la depășirea pragurilor de funcționare normală a parametrilor componentelor de procesare (memoria RAM, capacitatea CPU etc.).
2.9.34	Permite extinderea ulterioară a numărului de noduri ce alcătuiesc clusterul prin achiziționarea de licențe suplimentare, până la minim 64 noduri fizice
2.9.35	Permite rularea a minim 5000 mașini virtuale la nivelul întregului cluster
2.9.36	Permite minim 256 de nuclee de procesare logice pentru fiecare nod
2.9.37	Permite minim 6TB de memorie RAM pentru fiecare nod
2.9.38	Permite rularea a minim 512 de mașini virtuale pe fiecare nod
2.9.39	Permite alocarea a minim 64 de nuclee de procesare per mașină virtuală
2.9.40	Permite alocarea a minim 1TB de memorie RAM per mașină virtuală

2.10 Soluție de suport fizic de tip rack

Descriere generică a tehnologiei solicitate

Ofertantul va furniza un cabinet metalic de tip rack pentru echipamente IT, cu lățimea standard de 19”.

Caracteristici tehnice minimale:

2.10.1	Produsul va avea o capacitate de 42U de lățime standard de 19”
2.10.2	Produsul va veni echipat cu șinele verticale pe care se montează echipamentele și pereți metalici detașabili pe ambele laturi
2.10.3	Produsul va avea uși metalice perforate cu densitate între 30-80%, atât în față cât și în spate, sau care permit un flux de aer de minim 5000cm2
2.10.4	Lățime exterioară între 700 – 800 mm
2.10.5	Înălțime exterioară maxim 2000 mm (fără roți sau suporți)
2.10.6	Adâncime exterioară între 900 - 1200 mm
2.10.7	Greutate suportată: minim 800kg
2.10.8	Ușile frontale și posterioare vor avea o deschidere de minim 90 grade
2.10.9	Ușile frontale și posterioare vor fi detașabile
2.10.10	Produsul va avea lăcașe pentru introducerea cablurilor atât în partea de sus cât și jos
2.10.11	Produsul va avea roți pe partea posterioară pentru a facilita manevrarea
2.10.12	Culoare exterioară: negru
2.10.13	Produsul va avea lăcașe laterale pentru organizarea cablurilor, distribuite vertical pe toată înălțimea

2.11 Stații de lucru pentru management

Caracteristici tehnice minimale:

2.11.1	Procesor	Intel Core i7-8700, AMD Ryzen 3600 sau echivalent Frecvență: minim 3.2 GHz Număr core-uri minim: 6 Număr thread-uri minim: 12 Cache minim: 12 MB
2.11.2	Placă de bază	Soclu: compatibil cu procesorul Chipset: Intel B360/AMD B450 sau echivalent LAN: Inclus pe placa de baza, suporta 10/100/1000 Mbps Dual Bios sau echivalent SATA: minim 4 porturi
2.11.3	Placa video	Chipset: AMD Radeon RX 560 sau echivalent Memorie: minim 4 Gb GDDR5 Interfață: PCIeX 16 Frecvență nucleu: minim 1200 MHz Interfață memorie: minim 128 bit Viteză memorie (Memory speed): minim 7 Gbps Cooler: activ Display Port: Da HDMI: Da Sa suporte vizualizarea simultană pe minim doua monitoare
2.11.4	Memorie	DDR4: minim 32GB, Dual Channel Kit Frecvență: minim 2400 Mhz; Radiator: Da
2.11.5	Hard Disk	Capacitate minim 2 TB 7200 rpm SATA III Buffer: 256 MB
2.11.6	SSD	Capacitate minim 500 GB Suport NVMe: Da Interfata: M.2
2.11.7	Unitate optica	CD/DVD-RW
2.11.8	Placă de retea suplimentară	Interfață PCI-E, 1 x RJ-45 10/100/1000.
2.11.9	Sursa	Minim 600 W PFC activ; Eficiență : minim 85%; Protecții, minim: SCP, OCP, OVP
2.11.10	Standard I/O Ports, minim	1 x USB 3.1 2 x USB 3.x 2 x USB 2.0 1 x USB Type-C 1 x RJ-45 10/100/1000 1 x ieșire audio

		1 x intrare audio 1 x DVI 1 x HDMI
2.11.11	Tastatura	Interfață: USB Taste numerice: Da Format tastatură: US English sau echivalent
2.11.12	Mouse	Interfață: USB Tehnologie: laser Rotita scroll: Da
2.11.13	Căști	Cablu: minim 1.2m Conectivitate: 3.5mm jack Tip: over-head Microfon: nu/detașabil Active noise cancelling
2.11.14	Monitor	Bucăți: 2 Tip: LED Diagonală: min 23.6 inch Wide; Rezoluție: 1920x1080; Posibilitate montare VESA: 100 x 100 mm Interfețe video minim: HDMI, DisplayPort; Cabluri: HDMI, DisplayPort, Alimentare
2.11.15	Suport VESA pentru 2 monitoare	Tip: reglabil Compatibilitate: 100 x 100 mm Înălțime reglabilă Rotire: 360 grade; se poate învârti liber până la 90 grade Accesorii montare incluse
2.11.16	Sistem de operare	Va fi instalat și licențiat sistemul de operare Microsoft Windows 10 Professional, 64 bit.
2.11.17	Accesorii	Set cabluri de alimentare
2.11.18	Performanţă energetică	Produsele trebuie să respecte cele mai recente standarde ENERGY STAR în materie de performanţă energetică. Cerinţa va fi considerată îndeplinită prin prezentarea unei etichete ecologice relevante de tip I sau altor mijloace doveditoare adecvate (ex: dosar tehnic al producătorului sau un raport de încercare din partea unui organism recunoscut care să demonstreze respectarea cerinţelor).
2.11.19	Folosirea substanţelor periculoase	În cazul în care produsul ofertat conţine substanţe înscrise pe lista REACH a substanţelor cu o concentraţie mai mare de 0,1% (procent de masă) în întregul produs şi/sau

		subansamblurile produsului, se va prezenta o declaraţie care să indice substanţele specifice prezente.
2.11.20	Gestiunea scoaterii din uz: reciclarea părţilor componente şi marcarea carcaselor, a suporturilor şi a ramelor din plastic	Se vor prezenta documente sau declaraţii din care să reiasă greutatea, compoziţia polimetrică, precum şi marcajele ISO 11469 şi ISO 1043 ale părţilor din plastic cu greutatea mai mare de 100 grame şi suprafaţa mai mare de 50 cm^2.

2.12 Soluție de tip sursă de alimentare continuă (UPS)

Descriere generică a tehnologiei solicitate

Ofertantul va furniza o soluție de acces neîntreruptibil cu alimentare electrică de tip Smart UPS.

Caracteristici tehnice minimale:

2.12.1	Produsul va avea o tensiune nominală de intrare de 230V AC, frecvență 50/60Hz și o capacitate de minim 3000VA
2.12.2	Produsul va permite nativ montarea în rack standard de 19” și va conține toate elementele necesare montării în rack
2.12.3	Produsul va avea înălțime maximă 3U
2.12.4	Produsul va permite monitorizarea prin rețea ethernet prin protocoalele HTTP, HTTPS, IPv4, SNMP, TCP/IP;
2.12.5	Produsul va avea minim 8 ieșiri tip C13 de tensiune nominală 230V
2.12.6	Produsul va avea un randament la încărcare de minim 92%
2.12.7	Produsul va oferi protecție in-line (line-interactive) în cazul întreruperii alimentării cu energie electrică sau a devierii de la standard a parametrilor tensiunii de intrare
2.12.8	Sursa va permite configurarea tensiune de ieșire la 220, 230 sau 240V
2.12.9	Produsul va avea panou de control cu afișaj pentru următorii parametri: prezentă tensiune reţea; gradul de încărcare al bateriei; mod de lucru pe baterie; alertă pentru schimbarea acumulatorilor; alertă suprasarcină; - procent al sarcinii faţă de sarcina maximă
2.12.10	Produsul va avea alarmă sonoră pentru: •alarmă în mod de lucru pe baterie; •alarmă distinctă pentru acumulatori descărcaţi;
2.12.11	Produsul va include cabluri de alimentare: - 1 cablu alimentare reţea; - 8 cabluri IEC 320 C13 min. 10A

2.13 Soluție software pentru backup & restore

Descriere generică a tehnologiei solicitate

Ofertantul va furniza o aplicație sau suită de aplicații ce oferă funcții de backup și restore, cu o interfață unică de configurare.

Caracteristici tehnice minimale:

2.13.1	Soluția solicitată trebuie să includă toate licențele software necesare pentru a asigura protecția datelor și a aplicațiilor specificate, prin mecanisme de salvare și arhivare si să permită monitorizarea acestor procese.
2.13.2	Soluția trebuie să se integreze atât cu unități de stocare pe bandă, pentru a permite arhivare pe termen lung, cât și cu unități de backup dedicate, cu diskuri SSD sau/și rotaționale
2.13.3	Aplicația pentru asigurarea copiilor de siguranță, de salvare și restaurare a datelor, trebuie să ofere o interfață centrală de administrare și control
2.13.4	Soluția trebuie să includă o interfață unică de monitorizare pentru aplicația de salvare și restaurare a datelor cât și pentru echipamentul dedicat pentru păstrarea copiilor de siguranță
2.13.5	Soluția trebuie să permită configurarea politicilor de backup la nivel de fișier, director, a sistemului de operare, imaginii întregului sistem sau doar pentru o aplicație specifică
2.13.6	Soluția trebuie să permită integrarea cu Microsoft SQL, Microsoft Exchange, Microsoft SharePoint și asigurarea protecției acestora prin politici de backup la nivel de aplicație
2.13.7	Soluția trebuie să se poată integra cu hipervizorii Microsoft Hyper-V și/sau VmWare vSphere, oferind funcții specifice la nivel de cluster de mașini virtuale – backup și restore de mașini virtuale și fișiere ale acestora
2.13.8	Soluția va susține deduplicarea datelor la sursă sau destinație prin segmentare variabilă și compresie
2.13.9	Procesul de deduplicare trebuie să se desfășoare continuu, fără stocare temporară a datelor
2.13.10	Soluția trebuie să ofere posibilitatea ca agenții săi să comunice direct cu sistemul de deduplicare pentru păstrare a copiilor de siguranță
2.13.11	Soluția va permite definirea și rularea unor rutine ca parte a procesului de backup a unei aplicații, rutine ce vor rula înainte sau imediat după desfășurarea procesului de salvare a datelor în funcție de cerințele specifice aplicației din mediul de producție
2.13.12	Soluția va permite realizarea de backup a sistemelor Windows și Linux la nivel de blocuri de date fără necesitatea de analiză a sistemului de fișiere. De asemenea, recuperarea la nivelul unui fișier să poată fi realizată indiferent de politica de protecție aplicată
2.13.13	Transferul datelor de la sursă la destinație urmare a proceselor de backup trebuie să poată fi criptat, la fel și stocarea copiilor de siguranță, indiferent de politicile de retenție
2.13.14	Soluția trebuie să permită integrarea cu aplicații externe, de la alți producători, prin integrare cu interfețe standard, REST API.
2.13.15	Licențierea soluției să includă capacitatea totală a datelor protejate, minim 11TB, cu posibilitate de extindere ulterioară

2.14 Soluție de tip Media Wall

Descriere generică a tehnologiei solicitate

Obiectul achiziţiei îl reprezintă furnizarea unei soluţii complete pentru un sistem integrat de preluare, afişare şi gestionare a surselor video, conţinând atât aplicaţiile software şi echipamentele hardware necesare, precum şi toate licenţele aferente funcţionării sistemului la parametrii optimi impuşi de condiţiile şi cerinţele prezentului caiet de sarcini.

Caracteristici tehnice minimale:s

2.14.1	Soluția va fi alcătuită dintr-un panel de 9 monitoare dispuse într-o matrice de 3 coloane x 3 rânduri
2.14.2	Fiecare monitor ce alcătuiește soluția va fi din gama profesională, cu posibilitate funcţionare 24-7, o diagonala de minim 46” și rezoluție minim FullHD 1920x1080
2.14.3	Dimensiunea maximă a videowall-ului este de 3,7 x 2,1 metri
2.14.4	Interstiţiul maxim între două monitoare nu trebuie să depăşească 2 mm
2.14.5	Marginea carcasei unui monitor nu va fi mai groasă de 2.5mm pe niciuna din laturi
2.14.6	Rezoluţia totală reală a sistemului trebuie să fie de minim 5760 x 3240 pixeli
2.14.7	Monitoarele vor fi de tip panel LCD S-IPS cu iluminare LED directă sau cu panel de tip S-PVA cu iluminare directa.
2.14.8	Luminozitate minimă 600 cd/m2
2.14.9	Contrast minim 1100:1
2.14.10	Timp de răspuns maxim G2G 8 ms
2.14.11	Senzor de lumină destinat ajustării luminozităţii monitoarelor în funcţie de condiţiile camerei
2.14.12	Soluția va include suportul pe care se montează monitoarele componente
2.14.13	Soluția va include și o unitate de comandă care să integreze monitoarele individuale
2.14.14	Unitatea de comandă trebuie să poată primi semnal video, prin porturi DisplayPort, de la minim 4 surse individuale
2.14.15	Unitatea de comandă trebuie să permită afișarea simultană pe videowall a minim 4 surse de semnal, iar dimensiunile și poziția în care acestea sunt afișate în cadrul videowall-ului să poată fi ajustate

3. Cerințe privind necesar de instruire asupra tehnologiilor:

Pentru produsele de la punctele 2.4 (Next Generation Firewall), 2.5 (Soluție pentru analiza fluxurilor), 2.6 (Soluție de tip Application and Logs Management), 2.13 (Soluție software pentru backup și restore), ofertantul va efectua câte o sesiune de instruiredе 3 zile pentru 5 persoane, ce trebuie să prezinte noțiuni specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produselor ofertate**.**

Cursul va fi de tip “*hands-on*”, cu activități practice în care cursanții

utilizează, administrează și testează soluția ofertată, aplicând noțiunile specifice privind integrarea hardware, integrarea software, configurarea, administrarea şi exploatarea produsului.

Cursul se va desfășura în limba română, într-o locație pusă la dispoziție de furnizor, în municipiul București. Instructorul trebuie să fie acreditat de producătorul soluției. Pentru demonstrarea pregătirii instructorului se vor prezenta certificate / autorizări/acreditări, sau alte documente emise de către producătorul soluției, sau de organisme abilitate în acest sens.

Ofertantul va asigura servicii de catering pe perioada cursului, respectiv o masă de prânz şi un coffee-break pe zi(cafea, apă, ceai, produse de patiserie şi fructe, la discreţie).

4. Livrabile:

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentația de instruire

Ofertantul va livra în format fizic și electronic documentația de instruire.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției Centru Comunicație de Rezervă (Backup).

5. Implementare

5.1 Instalare și/sau integrare în cadrul infrastructurilor

Soluția Centru Comunicație de Rezervă (Backup)se va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,

- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

5.2 Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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.

Anexa 30 la caietul de sarcini

PLATFORMĂ ANALIZĂ MALWARE

1. Descriere generală:

Ofertantul va furniza o soluție de implementare a unei platforme de analiză malware.

2. Definirea componentelor:

Platformă analiză malware		
Nr.	**Denumiri componente**	**Număr componente**
2.1.	Soluție cu scanare antivirus cu motoare multiple	2
2.2.	Soluție clonat HDD	4
2.3.	Soluție clonat terminale mobile	1
2.4.	Soluție de tip server	8
2.5.	Soluție de tip sistem de stocare	1
2.6.	Soluție de tip mediu virtualizat	1
2.7.	Soluție de suport fizic pentru servere de tip Rack	2
2.8.	Stații de lucru pentru management	10
2.9.	Soluție de tip sursă de alimentare continuă (UPS)	4

2.1 Soluție cu scanare antivirus cu motoare multiple

Descriere:

Ofertantul va furniza o aplicație software ce realizează scanarea antivirus folosind motoare multiple. Aceasta va realiza scanarea fișierelor utilizând minim 22 motoare antivirus. Arhitectura aplicației va fi de tip client – server, ambele componente suportând instalarea pe sistemele de operare Microsoft Windows.

Caracteristici tehnice minimale:

2.1.1	Sistemul are o arhitectură de tip client – server.
2.1.2	Aplicația Server trebuie să poată fi instalată pe sistemul de operare Microsoft Windows 7, 8, 10 și pe Microsoft Server 2008, 2008R2, 2012, 2012R2, 2016.
2.1.3	Aplicația Client trebuie să permită instalarea pe versiunile 32 și 64 biți ale sistemelor de operare Microsoft Windows 7, Windows 8, Windows 8.1, Windwos 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012R2, Windows Server 2016.
2.1.4	Soluția realizează scanarea antivirus a fișierelor utilizând minim 22 motoare de scanare antivirus.
2.1.5	Soluția include în lista de motoare antivirus folosite cel puțin următoarele motoare proprietare: ESET, Bitdefender, Avira, McAfee, Kaspersky, Symantec, Trend Micro.
2.1.6	Permite scanarea fișierelor prin utilizarea în paralel a motoarelor de scanare antivirus.
2.1.7	Permite scanarea unui fișier la cerere prin intermediul unei interfețe web.
2.1.8	Soluția permite scanarea de fișiere, directoare, partiții, hard-disk-uri și procese active din memoria volatilă prin intermediul unei aplicații cu interfață grafică (client) ce se poate descărca din consola web (server).
2.1.9	Permite scanarea fișierelor de pe multiple sisteme dintr-o rețea și raportarea centralizată a rezultatelor către consola web de administrare.
2.1.10	Permite actualizarea offline a semnăturilor antivirus, în cazul în care soluția nu are acces Internet.
2.1.11	Permite scanarea cel puțin a următoarelor tipuri de fișiere: DOC, DOCX, PPT, PPTX, EPS, EXE, Font, GIF, GZIP, ICO, ISU, TNEF, TTF, CAB, JAR, JPEG, LHA, MDB, MP3, MPEG, HLP, WMF, XLS, XLSX, XML, XWS, ZIP, OBJ, PDF, PST, PIF, SFX, RAR, RIFF, TAR, TXT, TIFF, ZOO, ISO, NSI, MSI,EML, MSG, HTML, MHTML, BZ, SQL.
2.1.12	Permite configurare și administrare centralizată prin intermediul unei console web în care se pot executa cel puțin următoarele acțiuni: Căutarea în cadrul rezultatelor scanărilor după denumirea malware-ului și suma de control MD5, SHA1; Exportarea rapoartelor de scanare în formatul .CSV și .PDF; Listarea motoarelor antivirus active; Afișarea ultimelor actualizări ale semnăturilor pentru fiecare motor antivirus;
2.1.13	Consola web poate fi accesată prin cel puțin următoarele browsere: Google Chrome, Mozilla Firefox, Internet Explorer, Safari, Microsoft Edge
2.1.14	Permite transmiterea detecțiilor către un server syslog.

2.1.15	Oferă interfață de tip REST Web API pentru integrarea în arhitecturi existente.
2.1.16	Permite suplimentarea numărului de motoare antivirus existente în pachetele de bază.
2.1.17	Permite adăugarea de motoare de scanare externe.

2.2 Soluție clonat HDD

Descriere:

Echipament hardware folosit în domeniul computer forensics pentru clonarea/copierea dispozitivelor de stocare în formate de tip forensics. Soluția este compusă dintr-un dispozitiv hardware și accesorii (cabluri, adaptoare, module hardware adiționale).

Caracteristici tehnice minimale:

	Caracteristici	Cerințe minimale
2.2.1	Viteza de clonare/copiere minimă:	Viteză de 400 MB/s la clonarea dispozitivelor de stocare de tip SSD.
2.2.2	Formate de imagini	DD, E01, Ex01, DMG.
2.2.3	Verificarea procesului de clonare	Se folosesc algoritmi de hash precum MD5, SHA1 și SHA256. Verificarea unei imagini clonate se poate realiza și simultan cu procesul de clonare.
2.2.4	Porturi sursă	- 2 x SATA sau SAS; - 1 x USB 3.0; - 1 x PCIe. - adaptor sau modul suplimentar pentru interfețele Thunderbolt 2 sau 3 și USB-C.
2.2.5	Porturi destinație	-2 x SATA sau SAS; -2 x SATA; -1x USB 3.0;
2.2.6	Alti conectori	1 x 10 Gigabit Ethernet (conector de rețea);
2.2.7	Echipamentul va conține următoarele accesorii (conectori, cabluri, adaptoare):	- Sursă și cablu de alimentare la curent electric compatibile cu priză schuko; - Minim 4 x Cabluri SATA/SAS; - 1 x adaptor pentru interfata M.2 SATA; -1 x adaptor pentru interfața M.2 NVME -1 x adaptor mSATA la SATA; - 1 x adaptor IDE; - Manual de utilizare în format electronic
2.2.8	Dimensiuni maxime ale dispozitivului	30 cm x 10 cm x 20 cm
	Funcționalități:	
2.2.9	Detectează zone ascunse de pe dispozitivul de stocare sursă, precum: HPA (Host Protected Area), DCO (Device Configuration Overlay);	
2.2.10	Capacitatea de a continua operația de clonare sau citire în cazul unor dispozitive de stocare cu sectoare defecte.	

2.2.11	Conține o funcție dedicată pentru ștergerea datelor de pe dispozitivele de stocare atașate (funcție Wipe).
2.2.12	Permite clonarea unei surse către mai multe destinații.
2.2.13	Permite utilizatorului setarea unui set de operațiuni care să fie executate secvențial (copiere, hash, ștergere);
2.2.14	Permite clonarea simultană a minim două medii de stocare sursă către minim 4 medii de stocare destinație
2.2.15	Permite clonarea unei locații din rețea, precum și folosirea unei locații din rețea ca și destinație pentru operațiunea de clonare. (Folosind porturile 10 Gigabit Ethernet);
2.2.16	Permite formatarea mediilor de stocare în sistemele de fișiere NTFS, exFAT, FAT32, EXT4;
2.2.17	Verifică dacă un mediu de stocare este gol sau a fost șters;
2.2.18	Sunt create fișiere de jurnalizare pentru operațiunilor efectuate. Acestea pot fi vizualizate pe echipament sau exportate;
2.2.19	Asigură restaurarea unei imagini de tip DD, E01, EX01, DMG pe un hard disk;
2.2.20	Deține funcția de previzualizare (browsing) pentru conținutul sistemului de fisiere al dispozitivului de stocare atașat.
2.2.21	Deține funcție pentru criptarea unui dispozitiv de stocare atașat.
2.2.22	Asigură detecția dispozitivelor de stocare criptate cu tehnologia BitLocker.
2.2.23	Permite clonarea sub formă de imagine logică, selectând anumite fișiere sau folosind funcția de căutare.
2.2.24	Dispozitivul dispune de un ecran tactil incorporat prin care se accesează interfața grafică cu toate operațiunile disponibile.

2.3 Soluție clonat terminale mobile

Descriere:

Obiectul achiziției îl reprezintă o soluţie software completă pentru investigaţii informatice pentru terminale mobile.

Caracteristici tehnice minimale:

2.3.1	Soluția asigură extragerea/ achiziţia de date informatice din telefoanele mobile (inclusiv telefoane produse de companii chinezești), cât şi din mediile de stocare de tip memory card;
2.3.2	Soluția conţine cabluri de date şi adaptoare specifice conectării la dispozitivele mobile;
2.3.3	Soluția asigură extragerea automată a informaţiilor despre echipament (model/ producător/ IMEI);
2.3.4	Soluția efectuează extracţii la nivel logic;
2.3.5	Soluția asigură fotografierea terminalului mobil cu o cameră video pentru adnotarea raportului cu elemente de identificare fizică ale terminalului;
2.3.6	Soluția asigură extracţia fişierelor din telefoanele mobile cu cel puţin următoarele sisteme de operare: Ios, Android, Windows mobile, Blackberry;

2.3.7	Soluția asigură extracţia fişierelor din telefoane mobile cu cel puţin următoarele chipset-uri: Mediatek, Qualcomm, Spreadtrum, Exynos şi Infineon;
2.3.8	Soluția asigură extracţia fizică de date (clona integrală a memoriei fizice) şi decodare a dispozitivelor mobile;
2.3.9	Soluția asigură extracţia sistemului de fişiere;
2.3.10	Soluția asigură funcția de deblocare parole/ ecran prin metode de bypass;
2.3.11	Soluția asigură copierea cartelelor SIM/ microsim/ nanosim;
2.3.12	Soluția realizează atât decodarea datelor extrase, cât şi analiza acestora prin categorisirea lor;
2.3.13	Soluția asigură sortarea şi filtrarea fişierelor în funcţie de categorie;
2.3.14	Soluția decodează şi analizează agenda telefonică, liste SMS/MMS, istoric apeluri, calendar aplicaţii instalate, istoric locaţii bazat pe GPS;
2.3.15	Soluția asigură extragerea datelor şterse;
2.3.16	Soluția realizează automat legături şi evidenţiază relaţii între datele obţinute din diferite extracţii de pe telefoanele mobile;
2.3.17	Soluția generează rapoarte personalizate şi detaliate, prin exportarea datelor extrase cel puţin în fişiere format PDF şi DOC/DOCX/Excel;
2.3.18	Soluția va include: software de extragere a datelor din telefonul mobil; software de analiză a datelor extrase; software de analiză integrată a datelor provenite din surse multiple; set cabluri de conectare şi adaptoare pentru dispozitivele mobile (cu update pentru cele mai noi dispozitive); adaptor SIM/ MicroSIM/ NanoSIM; cititor de carduri cu protecţie WRITE-Block;
2.3.19	Soluția va avea sistem de operare Microsoft Windows 10.
2.3.20	Soluția va avea următoarele caracteristici tehnice: Procesor minim dual core cu frecvența de minim 1.9 GHz; Ecran LCD capacitiv de înaltă rezoluție minim 1024x600 pixeli; Cititor de cartelă multi SIM (SIM, Micro SIM, Nano SIM); Cititor de card SD, SDHC, SDXC, MMC; Memorie internă tip DDR3 minim 4 GB RAM; Unitate de stocare internă tip SSD SATA2 cu capacitate de minim 128 GB.
2.3.21	Soluția permite accesarea prin comandă tactilă a funcțiilor de oprire/pornire echipament și recuperare conținut a dispozitivelor mobile.
2.3.22	Soluția va avea dimensiunile: maxim 300 (L) x 300 (l) x 80 (î) milimetri.

2.4 Soluție de tip server

Caracteristici tehnice minimale:

2.4.1	Produsul va fi rackabil, în rack standard de 19” și va avea înălțimea de 2U.
2.4.2	Produsul va include toate accesoriile necesare montării în rack și realizării unei cablări ergonomice a conexiunilor electrice și de date.
2.4.3	**Procesor:** Minim Intel Xeon Gold 6248 (2.5GHz, 27.5MB Cache, 20 cores, DDR4-2933MHz, TDP 150W), High Performance heatsink, sau echivalent. Produsul va fi echipat cu minim 2 procesoare.
2.4.4	**Memorie RAM:** Produsul va suporta minim 24 module DIMM și o capacitate totală de memorie RAM de minim 3 TB. Produsul va fi echipat cu minim 512 GB DDR4-2933, Registered DIMMs, distribuiți în module de capacități egale.
2.4.5	**Unități de stocare:** Produsul va fi echipat cu un număr suficient de module (cage) pentru a suporta instalarea a minim 12 disk-uri SFF, hot plug, interfață SAS, în partea frontală. Produsul va fi echipat cu un controller dedicat de stocare ce permite configurarea de disk-uri SAS 12G în sistem RAID (RAID 0, 1, 1+0, 5, 5+0, 6, 6+0). Produsul va fi echipat cu minim 2 disk-uri SSD, format SFF 2.5” standard, interfață SAS 12G, capacitate minim 400GB, mixed-usage.
2.4.6	**Securitate:** Produsul va veni echipat cu modul TPM minim versiunea 2.0. Produsul va suporta UEFI Secure Boot și Secure Start.
2.4.7	**Interfaţă video:** Rezoluție max 1920x1200@60Hz-32 bpp, memorie video 16MB, integrată pe placa de bază.
2.4.8	**Panou monitorizare stare:** Panou frontal cu led-uri pentru monitorizarea stării serverului: sursă alimentare, stare generală server.

2.4.9	**Interfeţe reţea:** Produsul va fi echipat cu placă de rețea (on-board sau distinctă) care oferă minim 2 conexiuni RJ45 ethernet la viteza de 10Gb/s fiecare. Produsul va fi echipat cu placă de rețea (on-board sau distinctă) care oferă minim 2 conexiuni FO tip LC ethernet la viteza de 10Gb/s fiecare. Produsul va include interfețele de conectare (GBIC), în cazul în care acestea nu fac parte implicit din modulul FC. plăcile de rețea vor fi compatibile cu aplicația de network-teaming oferită de sistemul de operare Windows Server 2019. Produsul va oferi o interfață de rețea RJ45 distinctă pentru management.
2.4.10	**Fibre Channel:** Produsul va fi echipat cu minim un modul distinct care să ofere minim 2 porturi FC cu conectori LC, la viteza de minim 16Gb, compatibilitate Windows 2012R2/2016/2019 Server, Linux, multi-path suport, posibilitatea utilizării de conexiuni tip F_Port şi FL_Port; Produsul va include interfețele de conectare (GBIC), în cazul în care acestea nu fac parte implicit din modulul FC.
2.4.11	**Interfețe adiționale:** Minim 2xUSB 3.0 liber pe panoul din spate; Minim 1xUSB 3.0 liber pe panoul frontal; Minim 1 port video pe panoul frontal.
2.4.12	**Management:** Produsul va permite monitorizarea şi managementul stării echipamentului prin interfaţă web, prin portul dedicat de management, ce va permite monitorizarea stării de funcţionare a disk-urilor, procesoarelor, ventilatoarelor etc., consolă virtuală, media virtual, pornire/oprire/reboot; Produsul va veni cu licență perpetuă pentru funcționalitățile avansate ale interfeței de management.
2.4.13	**Sursă de alimentare:** Produsul va fi echipat cu minim 2 surse de alimentare redundante, hot plug; Putere minimă 800W per sursă; Eficienţă min. 90%; Tensiune de alimentare 100 – 240 $V_{c.a}$; Frecvenţă curent de alimentare 50 – 60 Hz.
2.4.14	**Ventilatoare:** Produsul va include minim 6 ventilatoare cu viteză variabilă, în funcție de temperatura sistemului.

2.5 Soluție de tip sistem de stocare

Caracteristici tehnice minimale:

2.5.1	Unitatea/unitățile de control, precum și modulele de expansiune cu discuri vor avea dimensiuni standard ce permit montarea în rack și vor include toate elementele necesare montării în rack standard de 19”
2.5.2	Sistemul va conține cel puțin două unități de control (storage processors /

	controller nodes / service processors)
2.5.3	Fiecare unitate de control va fi echipată cu procesor de minim 1.8GHz, minim 6-core
2.5.4	Fiecare modul hardware al sistemului va fi echipat cu minim două surse de alimentare, în configurație redundantă
2.5.5	Administrarea sistemului se poate face de la distanță, prin interfață web
2.5.6	Alimentarea va fi cu curent alternativ, între 100-240V, 50-60Hz
2.5.7	Sistemul va fi livrat într-o configurație care să includă cel puțin diskuri SSD și SAS 10K, conform capacităților precizate în prezentul document
2.5.8	Sistemul va asigura configurarea de Fast/Flash Cache de minim 800 GB pe dispozitive de stocare tip SSD, separat de cele folosite pentru stocare propriu zisă.
2.5.9	Sistemul va permite o capacitate maximă de stocare (raw) de minim 2.4PB, în configurație complet echipată
2.5.10	Sistemul va permite adăugarea ulterioară de shelf-uri cu medii de stocare suplimentare și va include shelf-urile necesare pentru a suporta capacitatea de stocare solicitată. Sistemul va veni echipat cu următoarele capacități de stocare: - minim 8 TB capacitate raw pe discuri de tip SSD (fără diskurile de Fast Cache) - minim 18 TB capacitate raw pe discuri de tip SAS 10K - minim 108 TB capacitate totală pe discuri rotaționale (SAS și NL-SAS. Include capacitatea obligatorie pe discuri SAS)
2.5.11	Sistemul va include licențe perpetue pentru folosirea întregii capacități ofertate și a facilităților solicitate
2.5.12	Sistemul va permite nativ configurarea de volume virtuale Vmware (vVOL). Dacă este necesar, va fi inclusă licența aferentă.
2.5.13	Sistemul va permite configurarea de LUN-uri de tip Thin sau Thick. Dacă este necesar, va fi inclusă licența aferentă.
2.5.14	Sistemul va permite configurații RAID 1/0, 5, 6. Dacă este necesar, va fi inclusă licența aferentă.
2.5.15	Sistemul va permite deduplicare. Dacă este necesar, va fi inclusă licența aferentă.
2.5.16	Sistemul va suporta nativ tehnologiile de conectare iSCSI și Fibre Channel. Dacă este necesar, va fi inclusă licența aferentă.
2.5.17	Sistemul va veni echipat cu minim 4 porturi Fibre Channel per controller, viteză minimă 16GBps
2.5.18	Numărul maxim de porturi Fibre Channel 16GBps suportate de sistem în configurație maximală nu va fi mai mic de 16
2.5.19	Numărul maxim de inițiatori suportați de sistem nu va fi mai mic de 2048
2.5.20	Sistemul va veni echipat cu minim 4 porturi RJ45 10 Gbps per controller
2.5.21	Sistemul va permite criptarea datelor stocate. Dacă este necesar, va fi inclusă licența aferentă.
2.5.22	Sistemul va permite realizarea de snapshot-uri. Dacă este necesar, va fi inclusă licența aferentă.
2.5.23	Sistemul va permite replicarea datelor stocate. Dacă este necesar, va fi inclusă licența aferentă.

2.5.24	În cazul defectării unui mediu de stocare persistent (HDD, SSD, M2, card SD etc.), acesta va fi înlocuit în baza garanției fără returnarea la producător a mediului defect

2.6 Soluție de tip mediu virtualizat

Descriere:

Ofertantul va furniza o aplicație sau suită de aplicații ce permit rularea de mașini virtuale pe infrastructură fizică, cu o interfață unică de configurare.

Caracteristici tehnice minimale:

2.6.1	Permite crearea, importarea, rularea și administrarea de mașini virtuale
2.6.2	Soluția este instalată direct pe platforma hardware a unuia dintre sistemele informatice de tip *server* şi îndeplineşte rolul de *hypervisor tip1 (nativ)* pentru administrarea maşinilor virtuale.
2.6.3	Platforma permite configurarea maşinilor virtuale cu cel puţin următoarele sisteme de operare: Microsoft Windows: 7, 7 SP1, 8, 8.1, 10, Server 2012, Server 2012 R2, Server 2016, Server 2019; CentOS: 7; Red Hat Enterprise Linux: 7; SUSE Linux Enterprise: 12; Ubuntu;
2.6.4	Oferă o interfață unică de administrare a întregii infrastructuri virtualizate – mașini virtuale, noduri fizice, rețeaua virtuală, stocarea externă, librării software
2.6.5	Administrarea centralizată va permite efectuarea operațiunilor asupra sistemului prin intermediul unei interfețe web
2.6.6	Administrarea centralizată a sistemului va permite definirea de roluri de administrare, pentru a restricționa selectiv nivelul de acces al unor grupuri de utilizatori la funcționalitățile platformei de virtualizare
2.6.7	Soluţia trebuie să permită integrare cu Active Directory, în sensul autentificării utilizatorilor din domeniu la nivelul consolei de management a soluţiei de virtualizare
2.6.8	Soluția oferă posibilitatea de a crea și utiliza șabloane (templates) pentru implementarea rapidă de noi mașini virtuale ce include şi posibilitatea de personalizare.
2.6.9	Soluția trebuie să ofere un set de instrumente software care asigură integrarea acesteia în arhitectura de rețea (Virtual Switch)
2.6.10	Soluția permite controlul QoS pentru accesul maşinilor virtuale la resursele hardware ale sistemelor de stocare
2.6.11	Permite migrarea live a mașinilor virtuale, fără întreruperea funcționării serviciilor acestora și fără pierdere de date. Migrarea live permite mutarea uneia sau mai multor mașini virtuale de pe un server fizic pe altul (inclusiv între servere cu specificaţii hardware diferite), prin balansarea automată a resurselor
2.6.12	Asigură o funcționare în regim de high-availability integrat pentru anumite mașini virtuale, care presupune inclusiv disponibilitatea continuă a aplicațiilor şi relocarea acestora pe un alt server fizic fără pierderea datelor, în cazul defectării mașinilor fizice gazdă

2.6.13	Asigură disponibilitatea continuă a aplicațiilor şi mutarea automată a maşinilor virtuale pe alte servere fizice în condițiile desfășurării de operațiuni de mentenanță asupra serverului fizic care găzduiește mașina virtuală
2.6.14	Permite integrarea redundantă (SAN multipath) cu soluții de stocare externe, prin tehnologii de rețea Ethernet (iSCSI) și Fibre Channel
2.6.15	Soluția permite configurarea și accesarea simultană a unui spațiu de stocare extern de către toate nodurile fizice pe care este instalată soluția de virtualizare (Shared Storage)
2.6.16	Soluția oferă posibilitatea de replicare a maşinilor virtuale către un centru de date secundar pentru crearea unui proces de tip disaster recovery.
2.6.17	Soluția de virtualizare dispune de instrumente virtuale de securitate integrate.
2.6.18	Permite optimizarea alocării spaţiului pe disk-uri (thin disk provisioning).
2.6.19	Soluţia are implementat un mecanism care să permită administrarea ordinii de pornire a maşinilor virtuale prin impunerea unor timpi de întârziere într-un mod centralizat, prin intermediul platformei de management a platformei de virtualizare
2.6.20	Soluția propusă permite alocarea dinamică a resurselor hardware disponibile (spre exemplu CPU sau memorie RAM) prin subpartiţionarea resurselor hardware şi asocierea acestora unor grupuri de maşini virtuale
2.6.21	Permite balansarea manuală sau dinamică, pe baza unor politici prestabilite, a resurselor de procesare existente în platforma virtuală.
2.6.22	Permite crearea și administrarea de infrastructuri virtuale de rețea în cadrul sistemului
2.6.23	Asigură posibilitatea de creare și configurare de rețele virtuale (VLAN și PVLAN) prin integrarea directă cu echipamente active de rețea.
2.6.24	Asigură prioritizarea accesului la resursele de rețea prin monitorizarea permanentă a traficului de reţea şi gestionarea încărcării (network offload).
2.6.25	Asigură posibilitatea de administrare a resurselor de rețea ca resurse multiple, separate, și de organizare a acestora sub formă de clustere (NIC teaming) pentru balansarea încărcării la nivelul reţelei.
2.6.26	Soluția permite controlul QoS pentru conexiunile de rețea ale mașinilor virtuale.
2.6.27	Soluția ofertată asigură realizarea backup-ului datelor şi informaţiilor ce includ şi configurările maşinilor virtuale.
2.6.28	Soluția oferă interfețe API pentru automatizarea și integrarea funcționalităților cu terțe aplicații.
2.6.29	Oferă posibilitatea de actualizare a hypervisor-ului prin procesul de update și/sau patching, în vederea optimizării soluției și eliminării vulnerabilităților de securitate.
2.6.30	Conține licențierea necesară pentru integrarea inițială a 8 noduri fizice bi-procesor
2.6.31	Permite realizarea de snapshot-uri live ale mașinilor virtuale.
2.6.32	Permite gestionarea snapshot-urilor mașinilor virtuale și restaurarea acestora la orice versiune anterioară înregistrată.
2.6.33	Asigură alertarea proactivă cu privire la depășirea pragurilor de funcționare normală a parametrilor componentelor de procesare (memoria RAM, capacitatea CPU etc.).

2.6.34	Permite extinderea ulterioară a numărului de noduri ce alcătuiesc clusterul prin achiziționarea de licențe suplimentare, până la minim 64 noduri fizice
2.6.35	Permite rularea a minim 5000 mașini virtuale la nivelul întregului cluster
2.6.36	Permite minim 256 de nuclee de procesare logice pentru fiecare nod
2.6.37	Permite minim 6TB de memorie RAM pentru fiecare nod
2.6.38	Permite rularea a minim 512 de mașini virtuale pe fiecare nod
2.6.39	Permite alocarea a minim 64 de nuclee de procesare per mașină virtuală
2.6.40	Permite alocarea a minim 1TB de memorie RAM per mașină virtuală

2.7 Suport fizic pentru servere de tip Rack

Descriere:

Ofertantul va furniza un cabinet metalic de tip rack pentru echipamente IT, cu lățimea standard de 19”.

Caracteristici tehnice minimale:

2.7.1	Produsul va avea o capacitate de 42U de lățime standard de 19”
2.7.2	Produsul va veni echipat cu șinele verticale pe care se montează echipamentele și pereți metalici detașabili pe ambele laturi
2.7.3	Produsul va avea uși metalice perforate cu densitate între 30-80%, atât în față cât și în spate, sau care permit un flux de aer de minim 5000cm2
2.7.4	Lățime exterioară între 700 – 800 mm
2.7.5	Înălțime exterioară maxim 2000 mm (fără roți sau suporți)
2.7.6	Adâncime exterioară între 900 - 1200 mm
2.7.7	Greutate suportată: minim 800kg
2.7.8	Ușile frontale și posterioare vor avea o deschidere de minim 90 grade
2.7.9	Ușile frontale și posterioare vor fi detașabile
2.7.10	Produsul va avea lăcașe pentru introducerea cablurilor atât în partea de sus cât și jos
2.7.11	Produsul va avea roți pe partea posterioară pentru a facilita manevrarea
2.7.12	Culoare exterioară: negru
2.7.13	Produsul va avea lăcașe laterale pentru organizarea cablurilor, distribuite vertical pe toată înălțimea

2.8 Stații de lucru pentru management

Caracteristici tehnice minimale:

	Caracteristică	**Cerință**
2.8.1	Procesor	Intel Core i7-8700, AMD Ryzen 3600 sau echivalent Frecvență: minim 3.2 GHz Număr core-uri minim: 6 Număr thread-uri minim: 12 Cache minim: 12 MB
2.8.2	Placă de bază	Soclu: compatibil cu procesorul Chipset: Intel B360/AMD B450 sau echivalent LAN: Inclus pe placa de baza, suporta 10/100/1000 Mbps

		Dual Bios sau echivalent SATA: minim 4 porturi
2.8.3	Placa video	Chipset: AMD Radeon RX 560 sau echivalent Memorie: minim 4 Gb GDDR5 Interfață: PCIeX 16 Frecvență nucleu: minim 1200 MHz Interfață memorie: minim 128 bit Viteză memorie (Memory speed): minim 7 Gbps Cooler: activ Display Port: Da HDMI: Da Sa suporte vizualizarea simultană pe minim doua monitoare
2.8.4	Memorie	DDR4: minim 32GB, Dual Channel Kit Frecvență: minim 2400 Mhz; Radiator: Da
2.8.5	Hard Disk	Capacitate minim 2 TB 7200 rpm SATA III Buffer: 256 MB
2.8.6	SSD	Capacitate minim 500 GB Suport NVMe: Da Interfata: M.2
2.8.7	Unitate optica	CD/DVD-RW
2.8.8	Placă de retea suplimentară	Interfață PCI-E, 1 x RJ-45 10/100/1000.
2.8.9	Sursa	Minim 600 W PFC activ; Eficiență : minim 85%; Protecții, minim: SCP, OCP, OVP
2.8.10	Standard I/O Ports, minim	1 x USB 3.1 2 x USB 3.x 2 x USB 2.0 1 x USB Type-C 1 x RJ-45 10/100/1000 1 x ieșire audio 1 x intrare audio 1 x DVI 1 x HDMI
2.8.11	Tastatura	Interfață: USB Taste numerice: Da Format tastatură: US English sau echivalent
2.8.12	Mouse	Interfață: USB Tehnologie: laser Rotita scroll: Da
2.8.13	Căști	Cablu: minim 1.2m Conectivitate: 3.5mm jack Tip: over-head

		Microfon: nu/detașabil Active noise cancelling
2.8.14	Monitor	Bucăți: 2 Tip: LED Diagonală: min 23.6 inch Wide; Rezoluție: 1920x1080; Posibilitate montare VESA: 100 x 100 mm Interfețe video minim: HDMI, DisplayPort; Cabluri: HDMI, DisplayPort, Alimentare
2.8.15	Suport VESA pentru 2 monitoare	Tip: reglabil Compatibilitate: 100 x 100 mm Înălțime reglabilă Rotire: 360 grade; se poate învârti liber până la 90 grade Accesorii montare incluse
2.8.16	Sistem de operare	Va fi instalat și licențiat sistemul de operare Microsoft Windows 10 Professional, 64 bit.
2.8.17	Accesorii	Set cabluri de alimentare
2.8.18	Performanţă energetică	Produsele trebuie să respecte cele mai recente standarde ENERGY STAR în materie de performanţă energetică. Cerinţa va fi considerată îndeplinită prin prezentarea unei etichete ecologice relevante de tip I sau altor mijloace doveditoare adecvate (ex: dosar tehnic al producătorului sau un raport de încercare din partea unui organism recunoscut care să demonstreze respectarea cerinţelor).
2.8.19	Folosirea substanţelor periculoase	În cazul în care produsul ofertat conţine substanţe înscrise pe lista REACH a substanţelor cu o concentraţie mai mare de 0,1% (procent de masă) în întregul produs şi/sau subansamblurile produsului, se va prezenta o declaraţie care să indice substanţele specifice prezente.
2.8.20	Gestiunea scoaterii din uz: reciclarea părţilor componente şi marcarea carcaselor, a suporturilor şi a ramelor din plastic	Se vor prezenta documente sau declarații din care să reiasă greutatea, compoziţia polimetrică, precum şi marcajele ISO 11469 şi ISO 1043 ale părţilor din plastic cu greutatea mai mare de 100 grame şi suprafaţa mai mare de 50 cm^2.

2.9 Soluție de tip sursă de alimentare continuă (UPS)

Descriere:

Ofertantul va furniza o soluție de acces neîntreruptibil cu alimentare electrică de tip Smart UPS.

Caracteristici tehnice minimale:

2.9.1	Produsul va avea o tensiune nominală de intrare de 230V AC, frecvență 50/60Hz și o capacitate de minim 3000VA.
2.9.2	Produsul va permite nativ montarea în rack standard de 19” și va conține toate elementele necesare montării în rack.
2.9.3	Produsul va avea înălțime maximă 3U.
2.9.4	Produsul va permite monitorizarea prin rețea ethernet prin protocoale HTTP, HTTPS, IPv4, SNMP, TCP/IP.
2.9.5	Produsul va avea minim 8 ieșiri de tensiune nominală 230V.
2.9.6	Produsul va avea un randament la încărcare de minim 92%.
2.9.7	Produsul va oferi protecție in-line (line-interactive) în cazul întreruperii alimentării cu energie electrică sau a devierii de la standard a parametrilor tensiunii de intrare.
2.9.8	Sursa va permite configurarea tensiune de ieșire la 220, 230 sau 240V
2.9.9	Produsul va avea panou de control cu afișaj pentru următorii parametri: prezentă tensiune reţea; gradul de încărcare al bateriei; mod de lucru pe baterie; alertă pentru schimbarea acumulatorilor; alertă suprasarcină; - procent al sarcinii faţă de sarcina maximă.
2.9.10	Produsul va avea alarmă sonoră pentru: •alarmă în mod de lucru pe baterie; •alarmă distinctă pentru acumulatori descărcaţi.
2.9.11	Produsul va include cabluri de alimentare: - 1 cablu alimentare reţea; - 8 cabluri IEC 320 C13 min. 10A.

3. Livrabile

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

Documentația de administrare și operare

Ofertantul va livra versiunea electronică a manualului de administrare care va cuprinde instalarea, administrarea zilnică, instalarea up-grade-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.

Documentațiile vor fi în limba română, cu excepția documentațiilor tehnice ale bunurilor, furnizate de către producător, care pot fi în limba engleză, necesare pentru implementarea, funcționarea, operarea și întreținerea soluției Platformă Analiză Malware.

4. Implementare

4.1 Instalare și/sau integrare în cadrul infrastructurilor

Soluția Platformă Analiză Malwarese va implementa cu amplasare, instalare, punere în funcțiune, configurare și testare, în locațiile comunicate la încheierea contractului şi va include cel puțin următoarele servicii:

- montarea în rack,
- conectarea la rețeaua informatică,
- instalarea de firmware și drivere,
- configurarea conexiunilor de alimentare cu energie electrică,
- securizarea sistemului de operare și a serviciilor active pentru a asigura protecția împotriva atacurilor informatice,
- realizarea tuturor configurărilor la nivelul sistemului de operare,
- configurarea pachetelor software,
- configurarea conexiunilor de reţea,
- realizarea altor configurări necesare pentru integrarea echipamentului livrat în reţeaua de destinaţie,
- instalarea și configurarea echipamentelor în mod redundant, acolo unde este cazul, pentru asigurarea înaltei disponibilităţi,
- asigurare sprijin beneficiarului pentru realizarea de copii de siguranță ale configurațiilor finale implementate pe soluțiile de securitate.

4.2 Garanţie și suport

Garanție echipamente hardware

Furnizorul trebuie să asigure funcționarea produselor hardware de la data instalării și până la finalizarea implementării proiectului pentru o durată de minim 3 ani, începând cu data de 23.08.2022.

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 situaţia în care un echipament este înlocuit, acesta va beneficia de o perioadă de garanţie 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 instalării și până la finalizarea implementării proiectului pentru o durată de minim 5 ani, începând cu data de 23.08.2022.

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 şi 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 gratuit la actualizarea semnăturilor prin intermediul conexiunilor la site-ul producătorului - online;
- acces on-line permanent la baza de date a producătorului soluției în scopul menţinerii tuturor funcţionalităţilor solicitate pentru asigurarea securităţii sistemelor informatice privind prevenirea, detecţia şi eliminarea ameninţărilor şi/sau vulnerabilităţilor specifice acestora, inclusiv pentru informaţiile de tip „threat intelligence”.